Citrix Secure Private Access™ - On premises

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

What's new 2

Known issues 2

Secure Private Access installer 5

Upgrade the database using scripts 10

Sizing guidelines 10

Set up Secure Private Access 13

Configure NetScaler Gateway 20

Configure contextual tags 26

Configure StoreFront 31

Configure applications 33

Configure access policies for the applications 36

End user flow 39

Secure Private Access integration with Web Studio integration 41

Deploy Secure Private Access as a cluster 42

Manage settings after installation 44

Dashboard overview 46

Troubleshooting some common errors 47

Retain troubleshooting logs 54

Logs and telemetry cleanup 55

Uninstall Secure Private Access 56

Secure Private Access 2311 compatibility with legacy versions 57

Third-party notifications 59

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's new

August 18, 2025

December 2023

Citrix Secure Private Access™ for on-premises –General Availability

Citrix Secure Private Access for on-premises is now generally available as part of the Citrix Virtual Apps and Desktops 2311 release. Citrix Secure Private Access on-premises solution enhances an organization's overall security and compliance posture with the ability to easily deliver Zero Trust Network Access to browser-based apps (internal web apps and SaaS apps) using StoreFront as a unified access portal to web and SaaS apps, along with virtual apps and desktops as an integrated part of Citrix Workspace. The solution is compatible with existing releases of NetScaler and StoreFront without any change to the versions. For details, see Secure Private Access for on-premises.

Integrated Secure Private Access installer with Citrix Virtual Apps and Desktops™

The Secure Private Access installer is integrated with the Desktop Delivery Controller (DDC) and can now be installed using the command line and the GUI. For details, see Install core components.

Known issues

September 13, 2025

The Citrix Secure Private Access™ for on-premises solution has the following known issues that are planned to be addressed in the future releases.

Domain Controller configurations

- The one-way or two-way trust with trust type as "Forest"between domains across different AD forests isn't supported.

  For example, if a.com and b.com domains are in two different AD forests, and SPA is installed on a machine where the domain is joined to a.com / b.com, then other domain users cannot access SPA published apps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If the machine's domain where Secure Private Access for on-premises is installed is different than the domain of the administrator logged in to Secure Private Access, then you must do the following:
  - Add a different domain service account as identify in the IIS Application pool for both the Secure Private Access Admin and Runtime service.
- The alternate UPN suffix is not supported by Secure Private Access for Intranet (StoreFront) login and Internet/Extranet (gateway) app enumeration.
- Distributed groups are not supported in Secure Private Access. Therefore, policies cannot search for distributed groups to add user and group conditions.
- Secure Private Access does not capture the domain details in the admin console or service. Hence, it relies completely on the domain that the user provided. Therefore, if the corresponding domain is not accessible or if the domain name is not a valid name, then that domain is not supported.

NetScaler® Gateway

The SSL virtual server with SSL profile configuration isn't supported in the following scenario.

- The customer is using NetScaler Gateway 13.1–48.47 and later or 14.1–4.42 and later.
- The `ns_vpn_enable_spa_onprem` toggle is enabled.

Workaround:

Bind the SSL parameters configured in the SSL profile directly to the SSL virtual server or disable the `ns_vpn_enable_spa_onprem` toggle.

For details on the toggle, see Support for smart access tags.

RfWeb / Workspace for web

RfWeb / Workspace for web isn't supported. Though the apps are enumerated, the app launch might fail.

Application icons

Only the ICO icon format is supported. The PNG, JPEG and other formats aren't supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Admin management

Administrator's RBAC role changes are reflected only after the current session is invalidated (by sign out or token expiry).

Upgrades

Upgrade of 2308 to 2311 and later is not supported. You must uninstall 2308 and reinstall the required version (2311 and later).

StoreFront™

- In **Stores > Configure Unified Experience**, the default receiver for Website must be configured to /Citrix/<`StoreName`>Web. In earlier versions of StoreFront, the default receiver for Website is set to a blank value and that does not work for Secure Private Access. Also, the earlier version of the Receiver UI is displayed on the client.
- If you are using the StoreFront versions 2308 or earlier, the **Stores > Manage Delivery Controllers** page displays the Secure Private Access plug-in type as **XenMobile®**. This doesn't impact the functionality.

Logging

- Support bundle generation for the cluster isn't supported.
- The logs folders for admin and runtime services must not be deleted. Secure Private Access can't recreate if these folders are deleted.

Admin account requirements to install Secure Private Access

- To install Secure Private Access, you must be logged in with a local machine administrator account.
- To set up Secure Private Access, you must sign into the Secure Private Access admin console with a domain user which is also a local machine administrator for the machine where Secure Private Access is installed.
- After the setup is complete, that user becomes the first Secure Private Access administrator and can then add other administrators.
- To manage Secure Private Access after the setup, you must sign into the Secure Private Access admin console with a Secure Private Access administrator account.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Security restrictions

Security restrictions associated with an app fail to work if a related domain that is initially published is replaced with a different domain.

For example, you create an app with a related domain as `edition.test.com` and enforce print restrictions and watermark on the application. The security restrictions are enforced when the application URL is accessed. However, if you edit the same application and replace the related domain `edition.test.com` with `*.1800flowers.com`, then the security restrictions are not enforced when the new application URL is accessed.

Admin console

The **Edit App** page does not auto close after the **Edit App** page (****Secure Private Access > Applications > Edit Application)** of a published application does not close after a related domain entry is modified.

For example, if the related domain you entered while creating an app was `www.example.com`. After the app is published, you replace the related domain `www.example.com` with `abc.com`, and click **Save**. The **Edit App** page does not close, though the app is updated successfully.

Installer display in Uninstall or change a program page

When you upgrade Secure Private Access from 2308 to 2311 by using the ISO file, the **Uninstall or change a program** page (**Control Panel > Programs > Programs and Features**) displays two entries for the Secure Private Access installer instead of replacing the initial entry.

- **Citrix virtual apps and desktops™ 7 2311**
- **Citrix Virtual Apps and Desktops 7 2308 - Secure private access**

You can uninstall the preview build installer by selecting **Citrix virtual apps and desktops 7 2308 - Secure private access**.

> **Note:**
>
> This issue is not observed when the Secure Private Access 2308 standalone installer is upgraded using the 2311 standalone installer.

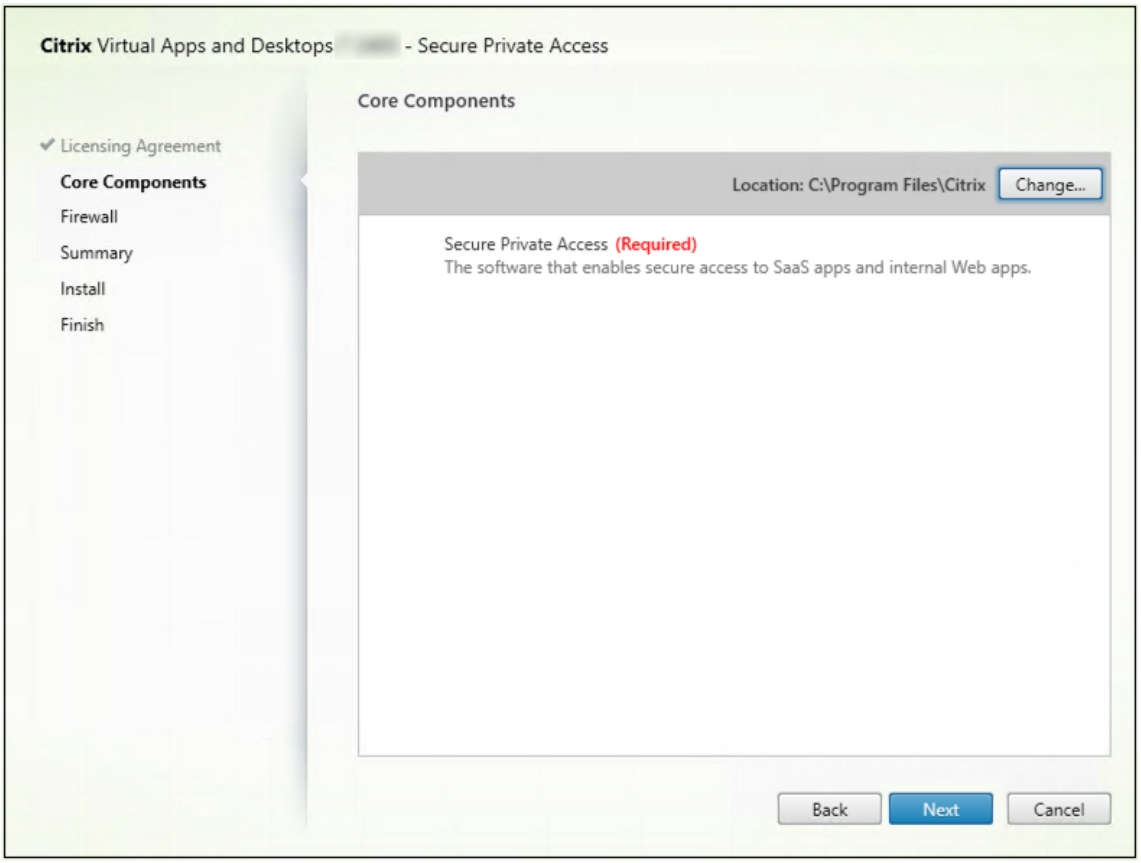
Secure Private Access installer

August 18, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

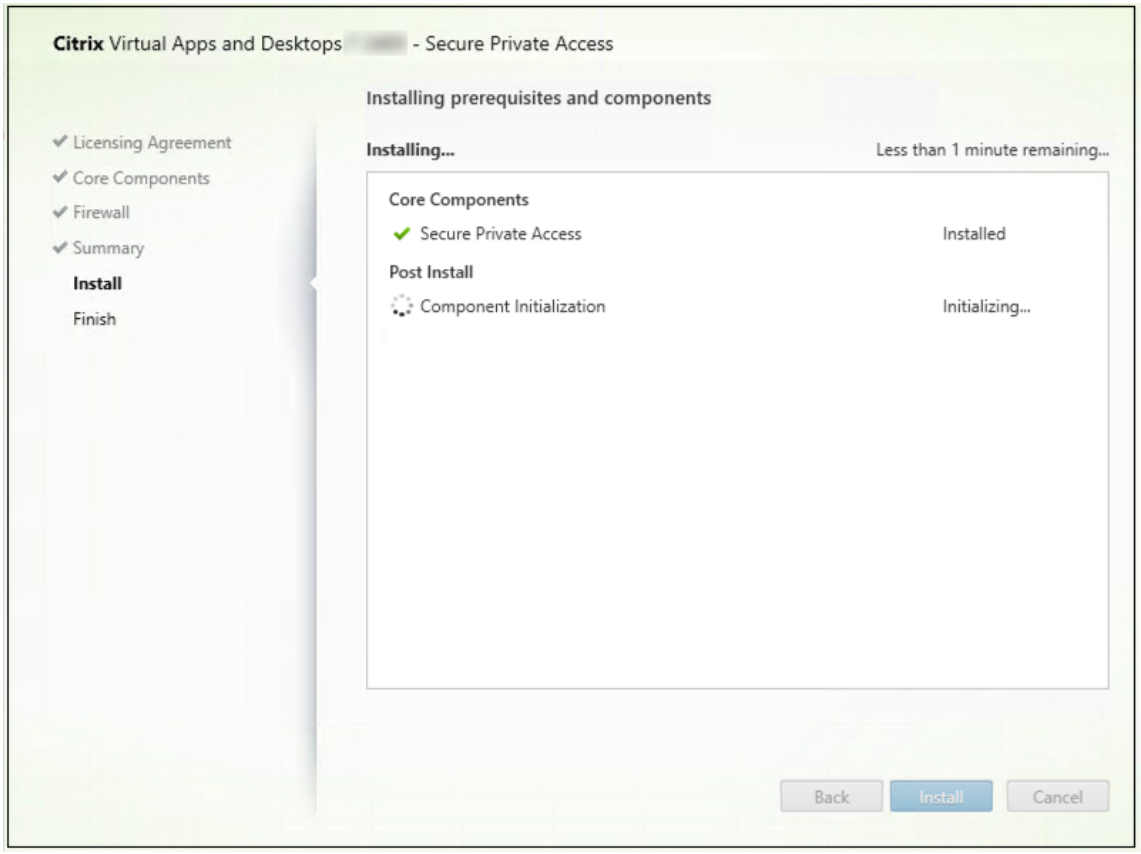
1. Download the Citrix Secure Private Access installer from https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/.
2. Run the .exe as an administrator on a domain joined machine.

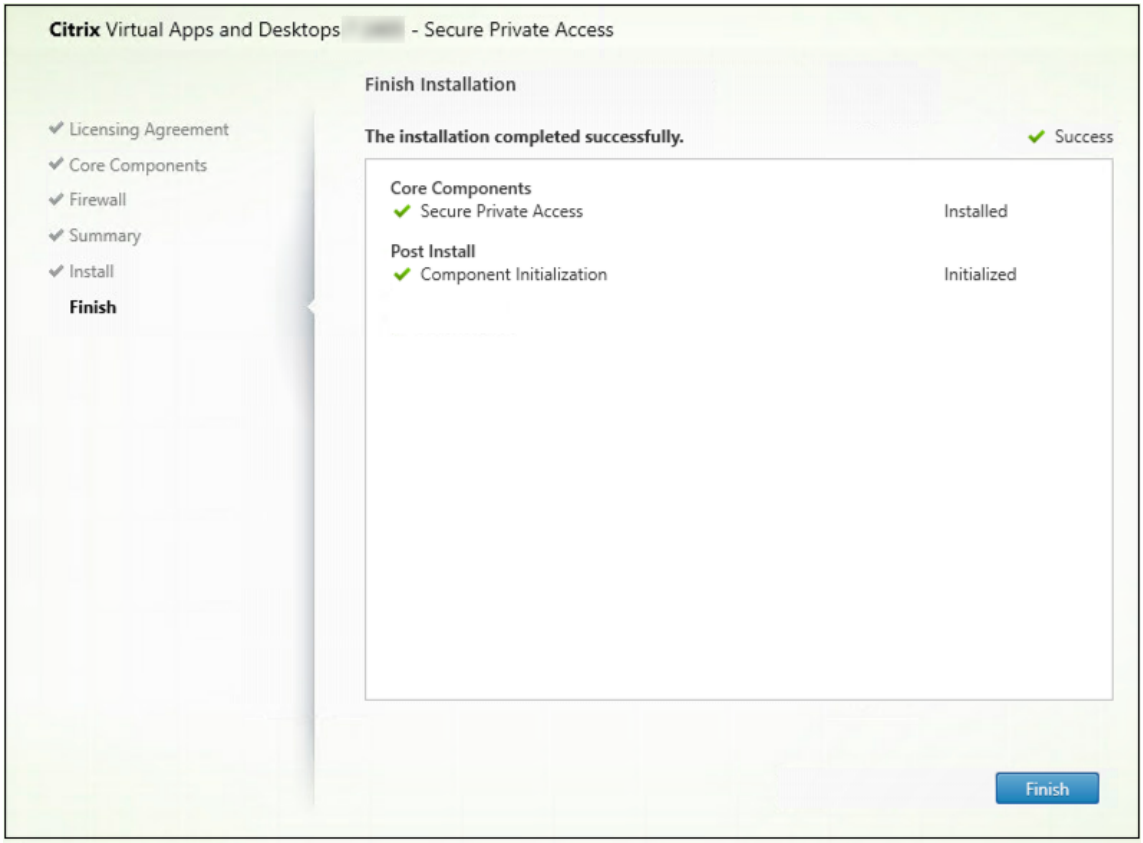
   > **Note:**
   >
   > For POC purposes, it is recommended that you install Secure Private Access on the same machine on which StoreFront™ is installed.



3. Follow the on-screen instructions to complete the installation.

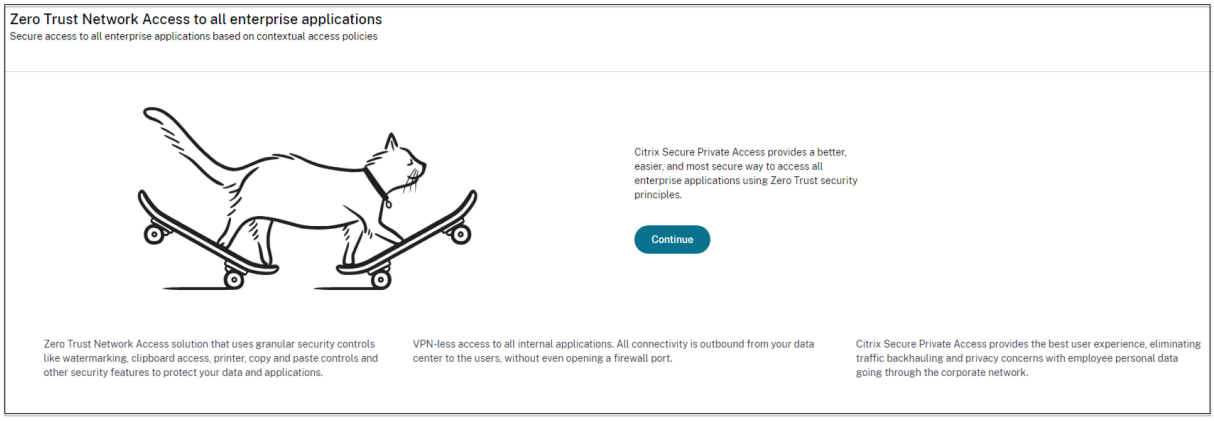
© 1997–2026 Citrix Systems, Inc. All rights reserved.



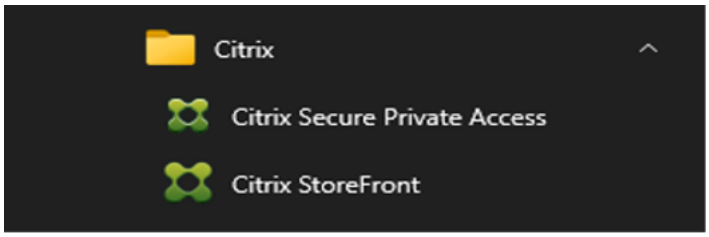


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Once the installation is complete, the first-time setup admin console opens automatically in the default browser window. You can click **Continue** to set up Secure Private Access.



You can also see the Secure Private Access shortcut on the desktop Start menu (**Citrix > Citrix Secure Private Access™)**.



For more information, see the following topics:

- Install core components
- Install using the command line

SSO to admin console

It is recommended that you configure Kerberos authentication for the browser that you use for the Secure Private Access admin console. This is because Secure Private Access uses Integrated Windows Authentication (IWA) for its admin authentication.

If Kerberos authentication isn't set, you're prompted by the browser to enter your credentials when accessing the Secure Private Access admin console.

- If you enter your credentials, you enable Integrated Windows Authentication (IWA) sign on.
- If you do not enter your credentials, you're presented with the Secure Private Access sign-on page.

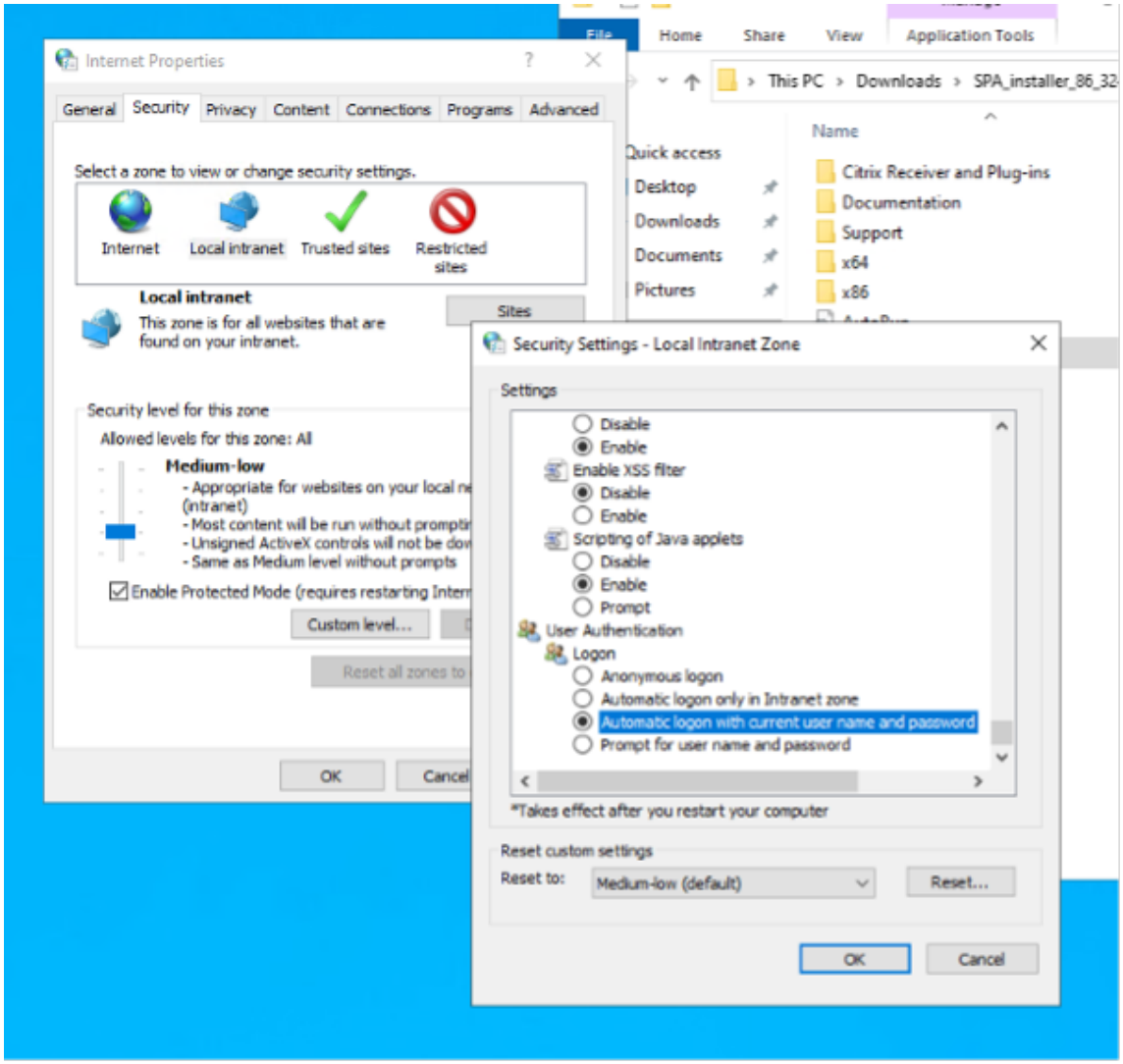
You must sign into the admin console to continue with the Secure Private Access setup. You can set up Secure Private Access with any user who belongs to the same domain as the installation machine, if the user has local administrator privileges on the installation machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For Google Chrome and Microsoft Edge browsers, perform the following steps to enable Kerberos.

1. Open **Internet Options**.
2. Select the **Security** tab and click **Local Intranet Zone**.
3. Click **Sites** and add the Secure Private Access URL.

   You can also use a wildcard if planning to install Secure Private Access on multiple machines. For example, `"https://*.fabrikam.local"`.
4. Click **Custom Level** and in **User Authentication > Logon**, select **Automatic logon with current user name and password**.



> **Note:**
>
> - If using Chrome Incognito sessions, create a DWORD registry key Computer\HKEY_LOCAL_MACHINE\SOFTWA and set to value 1.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You must restart all Chrome windows (including non-Incognito windows) before Kerberos gets enabled for the Incognito mode.
- For other browsers, check the specific browser's documentation on Kerberos authentication.

Next steps

- Set up Secure Private Access
- Configure NetScaler Gateway
- Configure applications
- Configure access policies for the applications

Upgrade the database using scripts

August 18, 2025

You can use the admin config tool to download the database upgrade scripts for the Secure Private Access plug-in.

1. Open the PowerShell or the command prompt window with admin privileges.
2. Change the directory to the Admin\AdminConfigTool folder under the Secure Private Access installation folder (for example, cd "C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool").
3. Run the following command:

   ```
   .\AdminConfigTool.exe /DOWNLOAD_UPGRADE_DB_SCRIPTS <output folder>
   ```

Sizing guidelines

August 18, 2025

Database storage requirements

Most of the database storage is consumed by the logs. The storage space consumption by the application and policy configuration is negligible when compared to the logs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The following table displays the server storage requirement based on parameters such as user sessions, logs, app enumeration per user per day.

Users sessions	App enumeration per user per day	App access per user per day	Total app access per day	Storage consumed per day	Log retention period in days	Total storage usage during log retention period (7 days)
1000	20	100	100000	2.5 GB	7	17.5 GB
1000	10	50	50000	1.27 GB	7	9 GB

Note:

- The metrics are derived based on the assumption that the logs event cleanup is disabled and the log retention period is set to 7 days.
- By default, the logs are retained for 90 days or up to 100 K log events are retained depending on the configured settings. These settings are available in the Secure Private Access Runtime service appsettings.json file and can be modified as required. For details, Settings to retain event logs.

Deployment guidelines

The following table displays the database sizing requirement based on parameters such as concurrent app access user sessions, app enumeration per minute, and CPUs used by Secure Private Access.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Concurrent app access user sessions	App enumeration per min	Secure Private Access memory in GB	Secure Private Access CPUs	Storage in GB	Notes
< 20 (PoC purposes)	2	4 GB	2	40 GB*	For PoC purposes SPA can be deployed on the same machine as StoreFront™ without any change in existing VMs specs.
20	5	8 GB	4	60 GB	-
160**	18	16 GB	4***	60 GB	2 or more SPA nodes can be deployed for better performance

Note:

- * The storage is mainly consumed by CDF logs. By default, Secure Private Access keeps 600 rollover log files with each file of size 10 MB. So if both Secure Private Access admin and runtime services are running in the same machine, the maximum storage utilization by the logs is 12 GB. Also, SQL express can be installed on the local VM for PoC purposes.
- ** For this load profile and higher, it's recommended to deploy Secure Private Access on a dedicated server instead of co-hosting with StoreFront, unless the NetScaler Gateway version is lesser 13.0 or lesser than 13.1-48.47.
- *** It is recommended that you use at least 2 Secure Private Access nodes cluster for such load as there some known performance issues. These issues are planned to be addressed in the upcoming releases.

Other components configuration

Component	vCPUs	Memory

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SQL Server	4	16 GB
Storefront	4	8 GB
Active Directory	8	16 GB

Set up Secure Private Access

August 18, 2025

You can set up Secure Private Access by creating a new site or by joining an existing site. In both scenarios, you can use the web admin console to set up the Secure Private Access environment.

- Set up Secure Private Access by creating a new site
- Set up Secure Private Access by joining an existing site

Prerequisites

- You must sign into the Secure Private Access admin console with a domain user which is also a local machine administrator for the machine where Secure Private Access is installed.
- The SQL database server must be installed before creating a site.

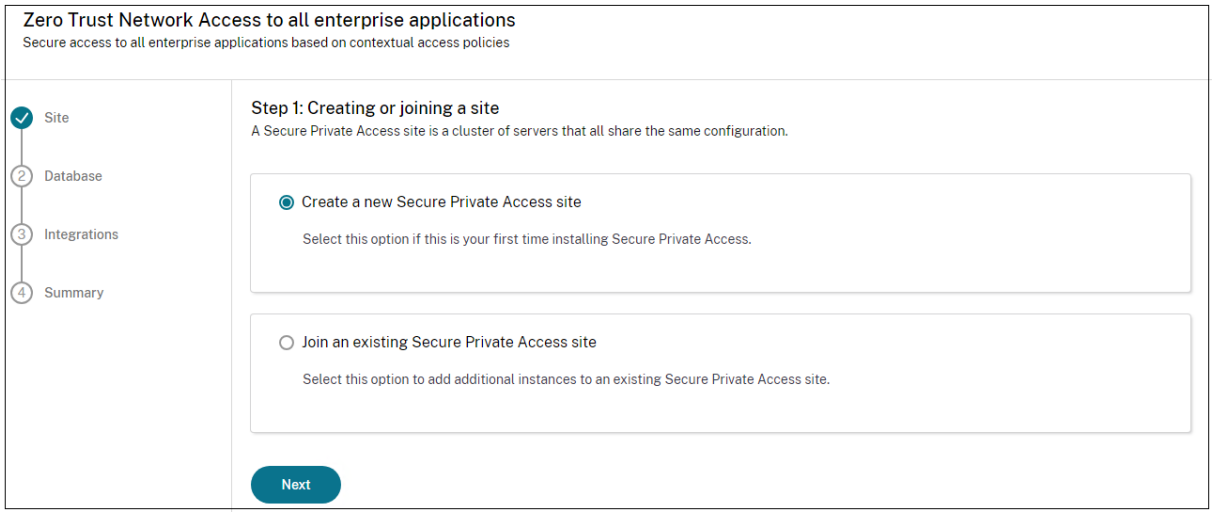
Set up Secure Private Access by creating a new site

Step 1: Set up a Secure Private Access site

A site is the name of your Secure Private Access deployment. You can either create a site or join an existing site.

1. Launch the Secure private access web admin console.
2. On the **Creating or Joining a Site** page, **Create a new Secure Private Access site** is selected, by default.
3. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



When you choose to create a site, you must automatically or manually configure a database for the new site as the database corresponding to the site name might not be available in the setup.

Step 2: Configure databases

You must create a database for the new Secure Private Access site. This can be done manually or automatically.

1. In **SQL Server Host**, enter the server host name. For example, `sql1.fabrikam.local\citrix`.

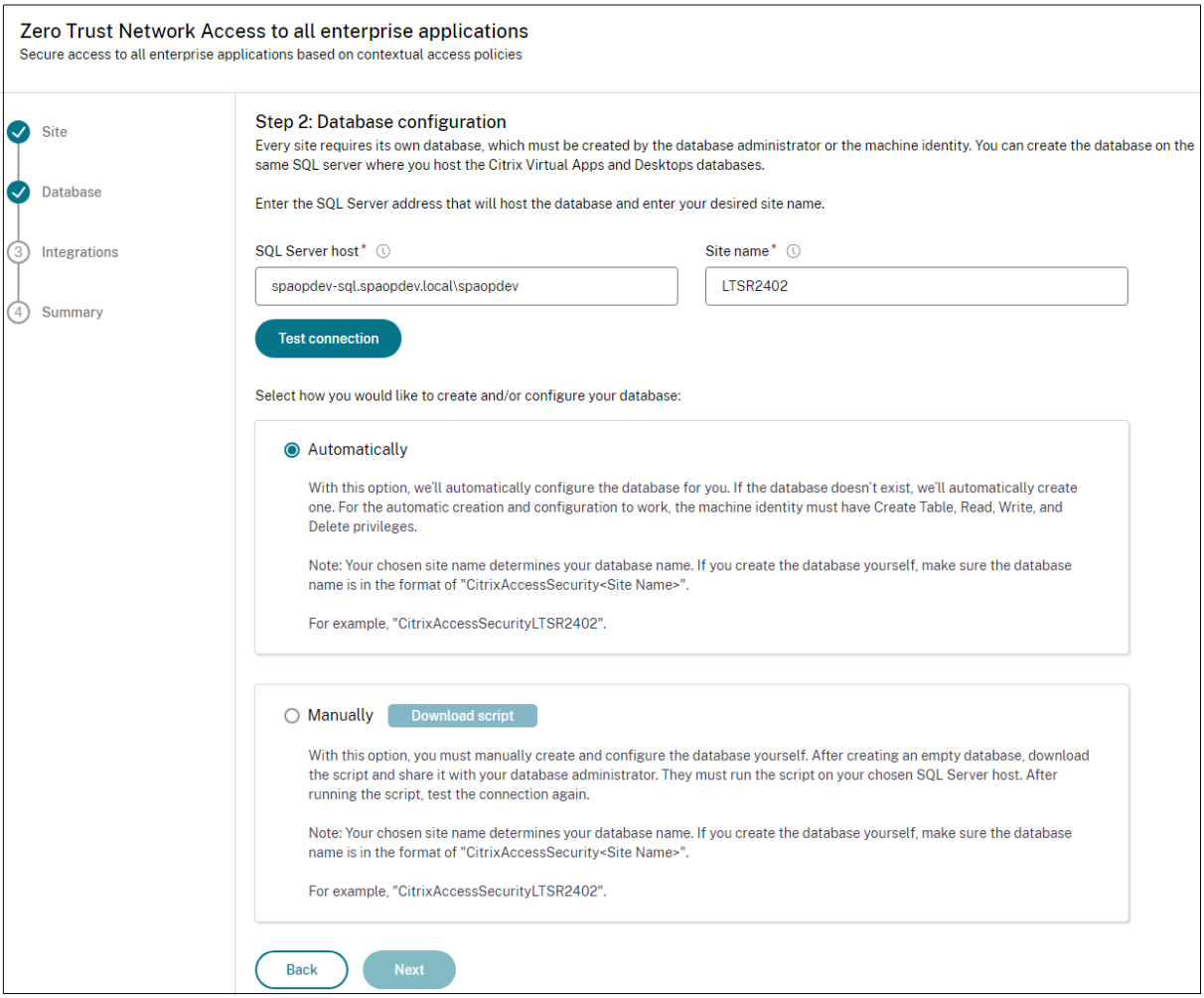
   You can specify a database address in one of the following forms:

   - ServerName
   - ServerName\InstanceName
   - ServerName,PortNumber

   For more information, see Databases.

2. In **Site**, type a name for the Secure Private Access site.
3. Click **Test Connectivity** to check that the SQL server instance is valid and also to confirm that the specified database exists for the site.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Note:**

- If an SQL server is not available for the site, the connectivity check fails.
- If an SQL server is available but the database does not exist, the connectivity check passes. However, a warning message is displayed.
- Secure Private Access uses Windows authentication using machine Identity to authenticate to an SQL server.

Automatic configuration:

- You can use the **Automatic Configuration** option only if the machine identity has the required database privileges.
- If a database does not exist at the specified address, a database is automatically created.
- When you create a database, ensure that it is empty but has the required database privileges. For details about the privileges, see Permissions required to set up databases.

Manual configuration:

You can use the **Manual Configuration** option to set up the databases.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In manual configuration, you must first download the scripts and then run the scripts on the database server that you have specified in the **SQL Server Host** field.

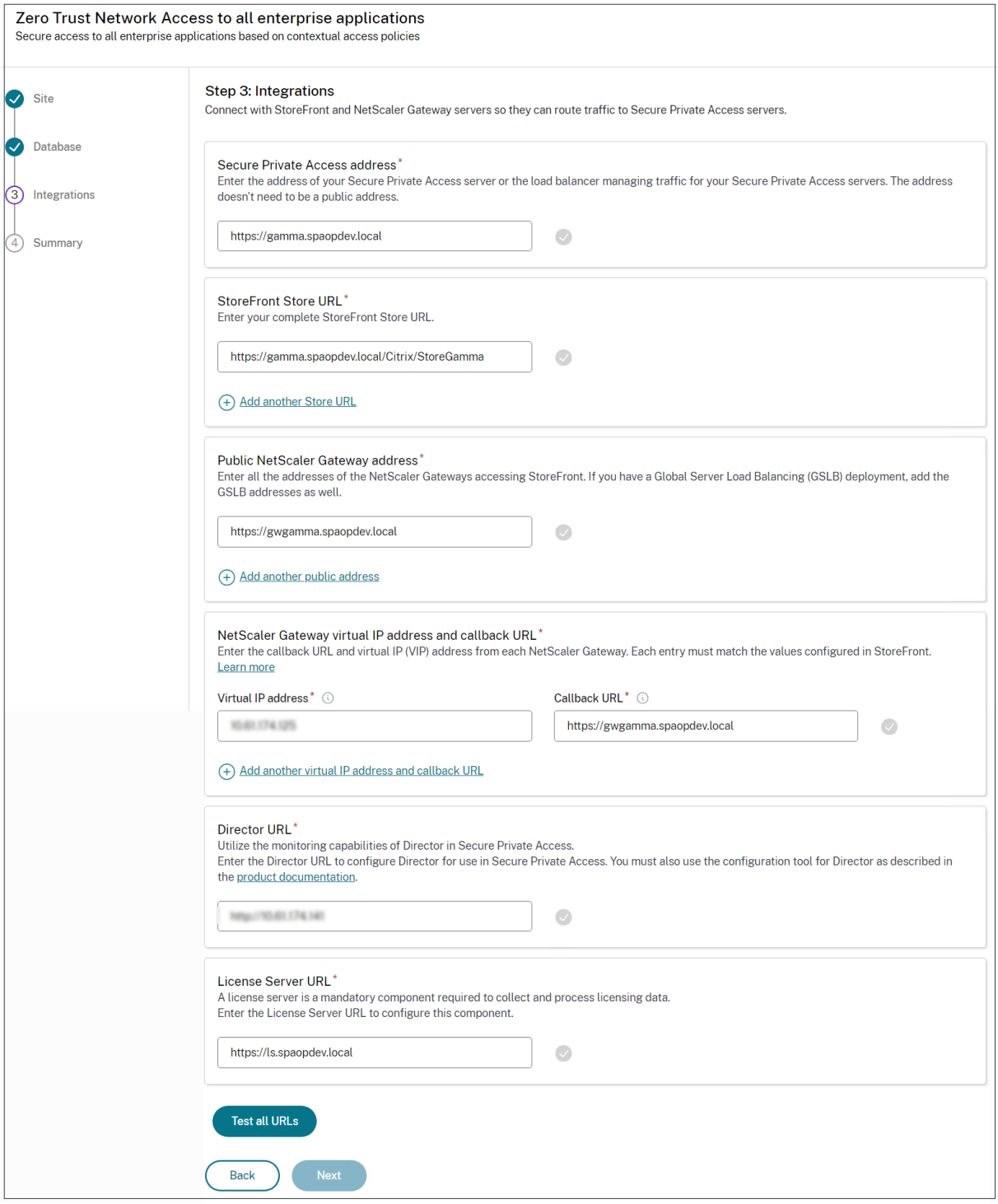
> **Note:**
>
> The database creation might fail if the machine does not have the READ, WRITE, UPDATE permissions to create tables within the database on the SQL server. You must enable appropriate permissions on the machine. For details, see Permissions required to set up databases.

Step 3: Integrate StoreFront and NetScaler® Gateway servers

You must specify StoreFront and NetScaler Gateway server details to connect Secure Private Access with StoreFront and NetScaler Gateway servers. This connection must be established to enable StoreFront and NetScaler Gateway to route traffic to Secure Private Access.

1. Enter the following details.
    - **Secure Private Access server address**. For example, `https://secureaccess.domain.com`.
    - **StoreFront Store URL**. For example, `https://storefront.domain.com/Citrix/StoreMain`.
    - **Public Gateway Address** –URL of the NetScaler Gateway. For example, `https://gateway.domain.com`.
    - **Gateway Callback Address** –This URL must be the same as the one configured in StoreFront. For example, `https://gateway.domain.com`.
    - **Gateway VIP** –This virtual IP address must be the same as the one configured in StoreFront for callbacks.
2. Click **Validate all URLs**.
3. Click **Next** and then click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

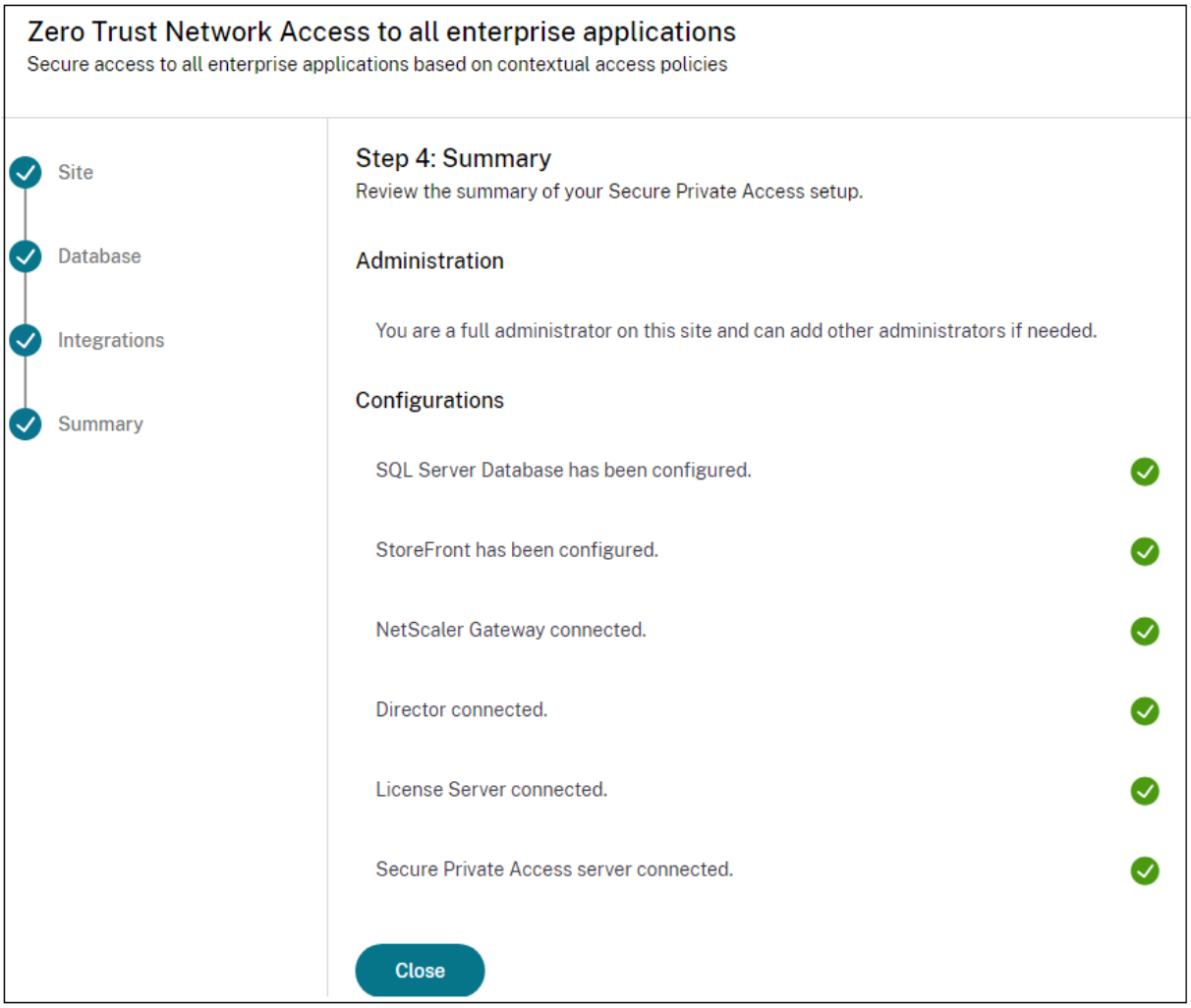


Step 4: Configuration summary

After the configuration is complete, validation is done to ensure that the servers that are configured are reachable. Also, a check is done to ensure that the Secure Private Access server is reachable.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If the configuration summary page displays any errors, see Troubleshooting errors for details. If this does not solve the issue, contact Citrix Support.



Note:

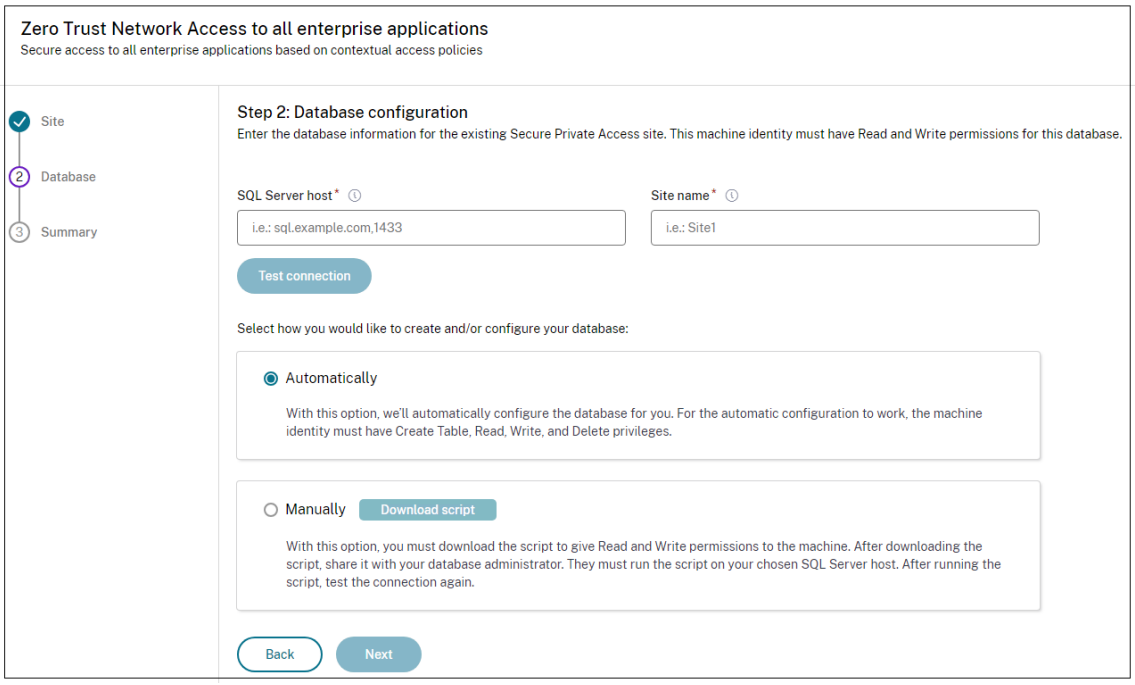
- After you have set up the environment, you can modify the settings from Settings > Integrations in the web admin console.
- The administrator that installs Secure Private Access the first time is granted full permission. This administrator can then add other administrators to the setup. You can view the list of administrators from **Settings > Administrators**.
- You can also add administrator groups so that access is enabled for all the administrators in that group.

For details, see Manage settings after installation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Set up Secure Private Access by joining an existing site

1. On the **Creating or Joining a Site** page, select **Join an existing site**, and then click **Next**.



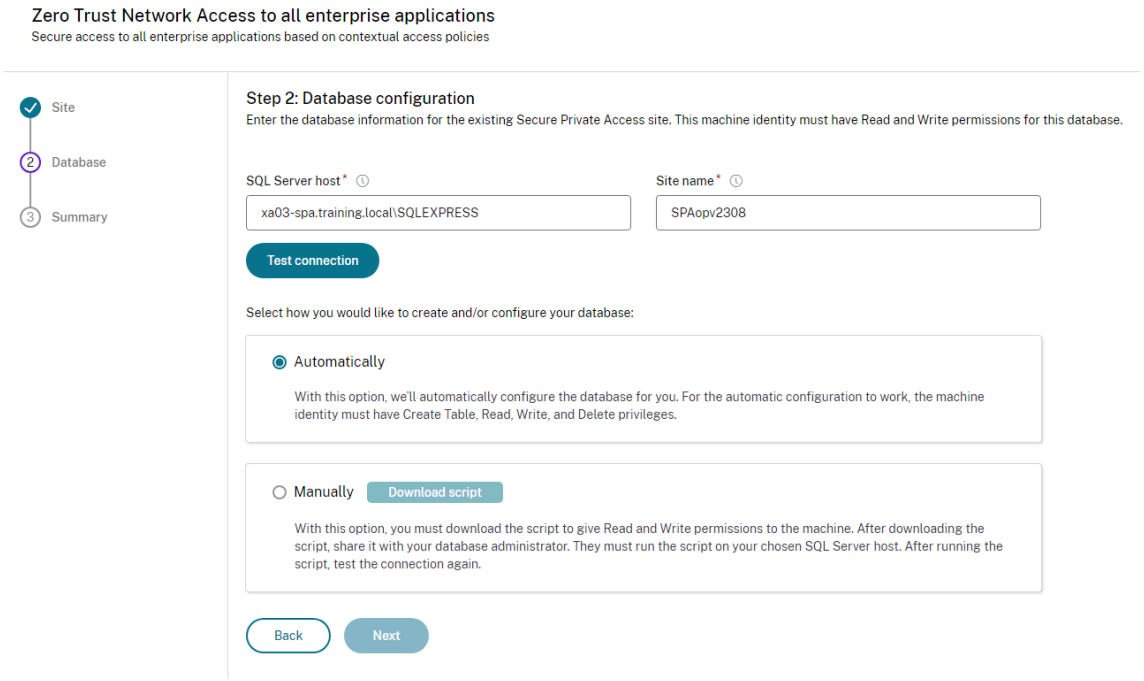
2. In **SQL Server Host**, enter the server host name. Ensure that a database corresponding to the site name that you enter is already present in the SQL server that you have selected. You can specify a database address in one of the following forms:

   - ServerName
   - ServerName\InstanceName
   - ServerName,PortNumber

   For more information, see Databases.

3. In **Site**, type a name for the Secure Private Access site.
4. Click **Test Connectivity** to check that the SQL server instance is valid and also to confirm that the specified site exists in the database.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If there is no corresponding database for the site, the connectivity check fails.

5. Click **Save**.

The configuration validation check happens to ensure that the SQL database server is configured and to check that the Secure Private Access server is reachable.

Next Steps

- Configure NetScaler Gateway
- Configure applications
- Configure access policies for the applications

Configure NetScaler Gateway

August 18, 2025

> **Important:**
>
> We recommend that you create NetScaler snapshots or save the NetScaler configuration before applying these changes.

1. Download the script from https://www.citrix.com/downloads/citrix-secure-private-access/Shell-Script/Shell-Script-for-Gateway-Configuration.html.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To create a new NetScaler Gateway, use *ns_gateway_secure_access.sh*.
To update an existing NetScaler Gateway, use *ns_gateway_secure_access_update.sh*.

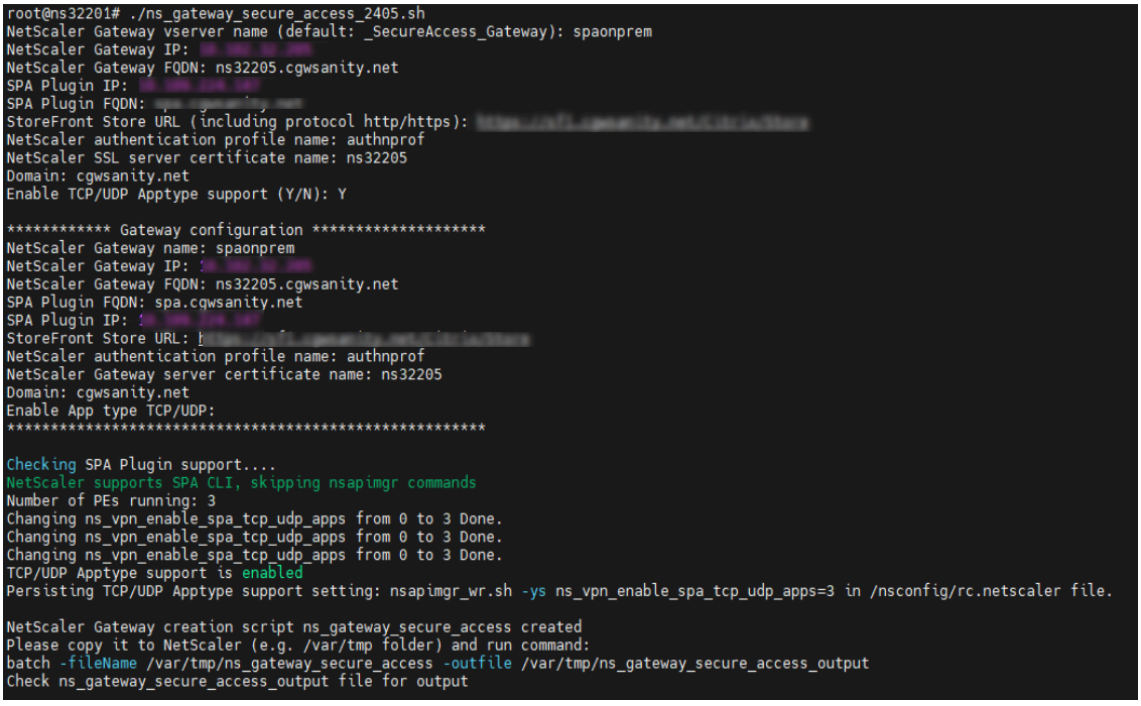
2. Upload these scripts to the NetScaler machine. You can use the WinSCP app or the SCP command. For example, *`scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp`*.

   > **Note:**
   >
   > - It's recommended to use NetScaler /var/tmp folder to store temp data.
   > - Make sure that the file is saved with LF line endings. FreeBSD does not support CRLF.
   > - If you see the error `-bash: /var/tmp/ns_gateway_secure_access.sh : /bin/sh^M: bad interpreter: No such file or directory`, it means that the line endings are incorrect. You can convert the script by using any rich text editor, such as Notepad++.

3. SSH to NetScaler and switch to shell (type 'shell'on NetScaler CLI).
4. Make the uploaded script executable. Use the chmod command to do so.

   ```
   chmod +x /var/tmp/ns_gateway_secure_access.sh
   ```

5. Run the uploaded script on the NetScaler shell.

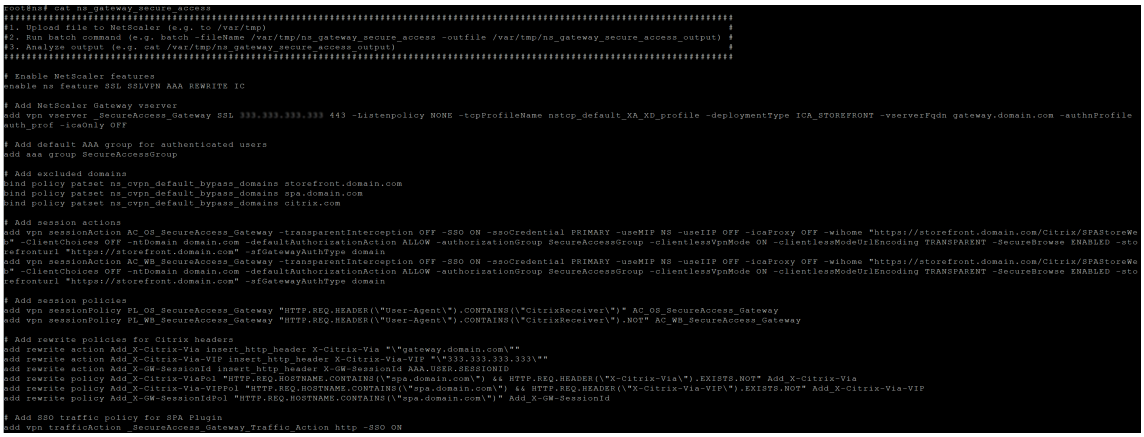


6. Input the required parameters. For the list of parameters, see Prerequisites.

   For authentication profile and SSL certificate you have to provide names on NetScaler.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

A new file with multiple NetScaler commands (the default is var/tmp/ns_gateway_secure_access) is generated.



7. Switch to the NetScaler CLI and run the resultant NetScaler commands from the new file with the batch command. For example,
   `batch -fileName /var/tmp/ns_gateway_secure_access -outfile /var/tmp/ns_gateway_secure_access_output`

   NetScaler runs the commands from the file one by one. If a command fails, it continues with the next command.

   A command can fail if a resource exists or one of the parameters entered in step 6 is incorrect.
8. Ensure that all commands are successfully completed.

> **Note:**
>
> If there's an error, NetScaler still runs the remaining commands and partially creates/updates/binds resources. Therefore, if you see an unexpected error because of one of the parameters being incorrect, it's recommended to redo the configuration from the start.

Configure Secure Private Access on a NetScaler Gateway with existing configuration

You can also use the scripts on an existing NetScaler Gateway to support Secure Private Access. However, the script does not update the following:

- Existing NetScaler Gateway virtual server
- Existing session actions and session policies bound to NetScaler Gateway

Ensure that you review each command before execution and create backups of the gateway configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Settings on NetScaler Gateway virtual server

When you add or update the existing NetScaler Gateway virtual server, ensure that the following parameters are set to the defined values.

tcpProfileName: nstcp_default_XA_XD_profile
deploymentType: ICA_STOREFRONT
icaOnly: OFF

Examples:

To add a virtual server:

```
`add vpn vserver _SecureAccess_Gateway SSL 333.333.333.333 443 -
   Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile -
   deploymentType ICA_STOREFRONT -vserverFqdn gateway.mydomain.com -
   authnProfile auth_prof_name -icaOnly OFF`
```

To update a virtual server:

```
`set vpn vserver  _SecureAccess_Gateway -icaOnly OFF`
```

For details on the virtual server parameters, see vpn-sessionAction.

NetScaler Gateway session actions

Session action is bound to a gateway virtual server with session policies. When you create a session action, ensure that the following parameters are set to the defined values.

- `transparentInterception`: OFF
- `SSO`: ON
- `ssoCredential`: PRIMARY
- `useMIP`: NS
- `useIIP`: OFF
- `icaProxy`: OFF
- `wihome`: `"https://storefront.mydomain.com/Citrix/MyStoreWeb"` - replace with real store URL
- `ClientChoices`: OFF
- `ntDomain`: mydomain.com - used for SSO
- `defaultAuthorizationAction`: ALLOW
- `authorizationGroup`: SecureAccessGroup (Make sure that this group is created, it's used to bind Secure Private Access specific authorization policies)
- `clientlessVpnMode`: ON
- `clientlessModeUrlEncoding`: TRANSPARENT
- `SecureBrowse`: ENABLED

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `Storefronturl`: `"https://storefront.mydomain.com"`
- `sfGatewayAuthType`: domain

Examples:

To add a session action:

```
add vpn sessionAction AC_OS_SecureAccess_Gateway -transparentInterception
 OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy
 OFF -wihome "https://storefront.mydomain.com/Citrix/MyStoreWeb"-
ClientChoices OFF -ntDomain mydomain.com -defaultAuthorizationAction
 ALLOW -authorizationGroup SecureAccessGroup -clientlessVpnMode
ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -
storefronturl "https://storefront.mydomain.com"-sfGatewayAuthType
domain
```

To update a session action:

```
set vpn sessionAction AC_OS_SecureAccess_Gateway -transparentInterception
 OFF -SSO ON
```

For details on session action parameters, see https://developer-docs.netscaler.com/en-us/adc-command-reference-int/13-1/vpn/vpn-sessionaction.

Compatibility with the ICA® apps

NetScaler Gateway created or updated to support the Secure Private Access plug-in can also be used to enumerate and launch ICA apps. In this case, you must configure Secure Ticket Authority (STA) and bind it to the NetScaler Gateway.
Note: STA server is usually a part of Citrix Virtual Apps and Desktops™ DDC deployment.

For details, see the following topics:

- Configuring the Secure Ticket Authority on NetScaler Gateway
- FAQ: Citrix Secure Gateway/ NetScaler Gateway Secure Ticket Authority

Support for smart access tags

In the following versions, NetScaler Gateway sends the tags automatically. You do not have to use the gateway callback address to retrieve the smart access tags.

- 13.1.48.47 and later
- 14.1–4.42 and later

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Smart access tags are added as a header in the Secure Private Access plug-in request.

Use the toggle `ns_vpn_enable_spa_onprem` or `ns_vpn_disable_spa_onprem` to enable/disable this feature on these NetScaler versions.

- You can toggle with command (FreeBSD shell):

  ```
  nsapimgr_wr.sh -ys call=ns_vpn_enable_spa_onprem
  ```

- Enable SecureBrowse client mode for HTTP callout config by running the following command (FreeBSD shell).

  ```
  nsapimgr_wr.sh -ys call=toggle_vpn_enable_securebrowse_client_mode
  ```

- To disable, run the same command again.
- To verify whether the toggle is on or off run the `nsconmsg` command.
- To configure smart access tags on NetScaler Gateway, see Configuring Custom Tags (SmartAccess Tags) on NetScaler Gateway.

Known limitations

- Existing NetScaler Gateway can be updated with script but there can be an infinite number of possible NetScaler configurations that can't be covered by a single script.
- Do not use ICA Proxy on NetScaler Gateway. This feature is disabled when NetScaler Gateway is configured.
- If you use NetScaler deployed in the cloud, you must make some changes in the network. For example, allow communications between NetScaler and other components on certain ports.
- If you enable SSO on NetScaler Gateway, make sure that NetScaler communicates to StoreFront™ using a private IP address. You might have to add a new StoreFront DNS record to NetScaler with a StoreFront private IP address.

Upload public gateway certificate

If the public gateway is not reachable from the Secure Private Access machine, then you must upload a public gateway certificate to the Secure Private Access database.

Perform the following steps to upload a public gateway certificate:

1. Open PowerShell or the command prompt window with the admin privileges.
2. Change the directory to the Admin\AdminConfigTool folder under the Secure Private Access installation folder (for example, cd "C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool")

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Run the following command:

```
\AdminConfigTool.exe /UPLOAD_PUBLIC_GATEWAY_CERTIFICATE <PublicGatewayUrl
> <PublicGatewayCertificatePath>
```

Configure contextual tags

August 18, 2025

The Secure Private Access plug-in provides contextual access (smart access) to Web or SaaS applications based on the user session context such as device platform and OS, installed software, geolocation.

Administrators can add conditions with contextual tags to the access policy. The contextual tag on the Secure Private Access plug-in is the name of a NetScaler® Gateway policy (session, preauthentication, EPA) that is applied to the sessions of the authenticated users.

The Secure Private Access plug-in can receive smart access tags as a header (new logic) or by making callbacks to Gateway. For details, see Smart access tags.

> **Note:**
>
> The Secure Private Access plug-in supports only classic gateway preauthentication policies that can be configured on NetScaler Gateway.

Configure custom tags using the GUI

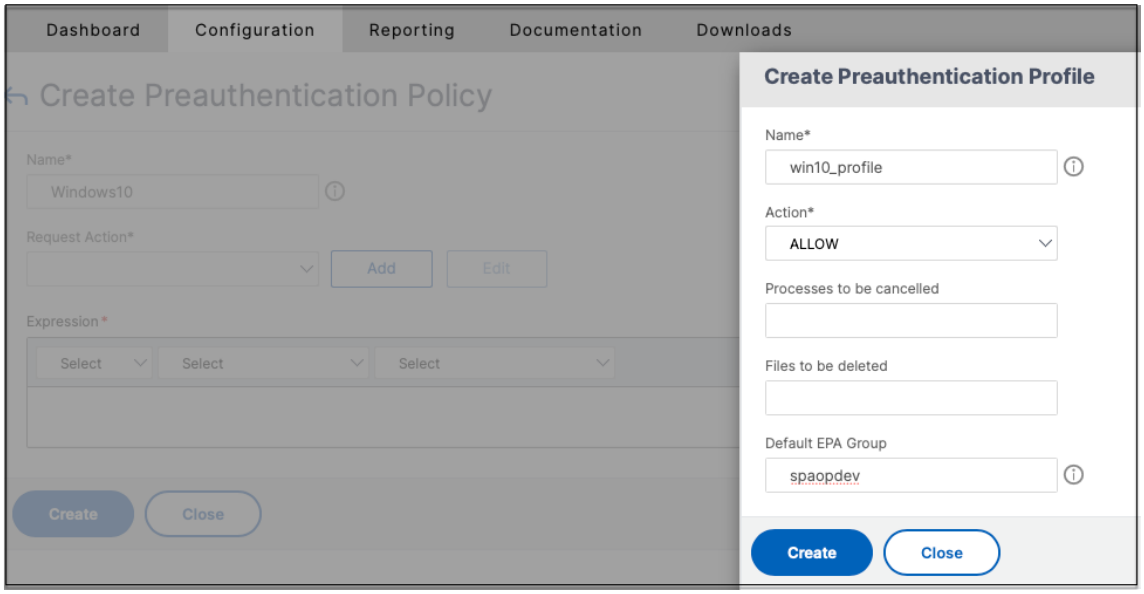
The following high-level steps are involved in configuring contextual tags.

1. Configure a classic gateway preauthentication policy
2. Bind the classic preauthentication policy to the gateway virtual server

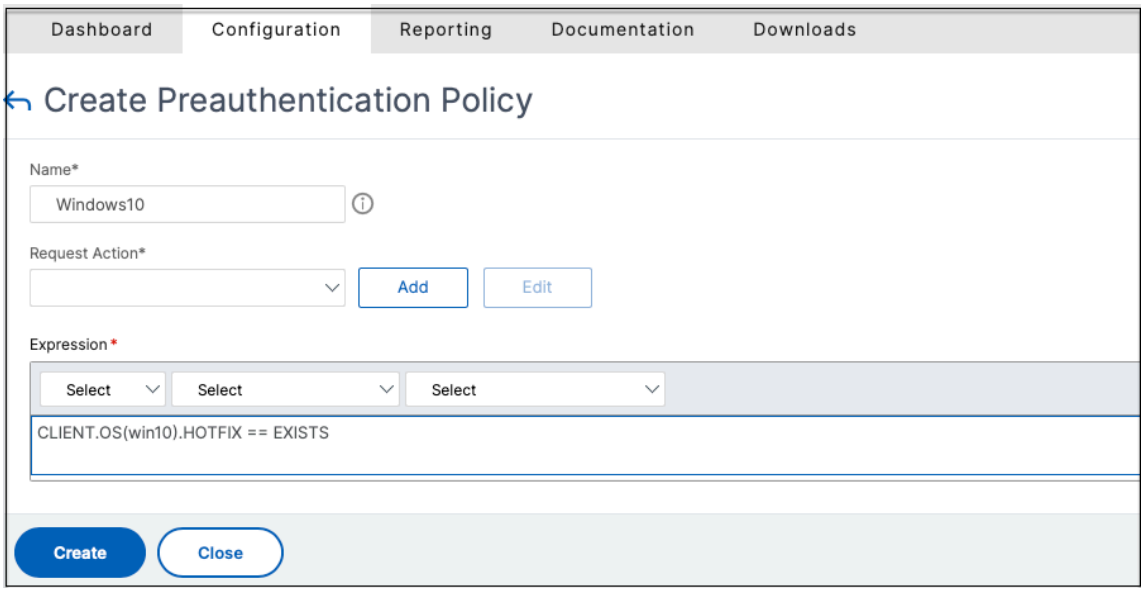
Configure a classic gateway preauthentication policy

1. Navigate to **NetScaler Gateway > Policies > Preauthentication** and then click **Add**.
2. Select an existing policy or add a name for the policy. This policy name is used as the custom tag value.
3. In **Request Action**, click **Add** to create an action. You can reuse this action for multiple policies, for example, use one action to allow access, another to deny access.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

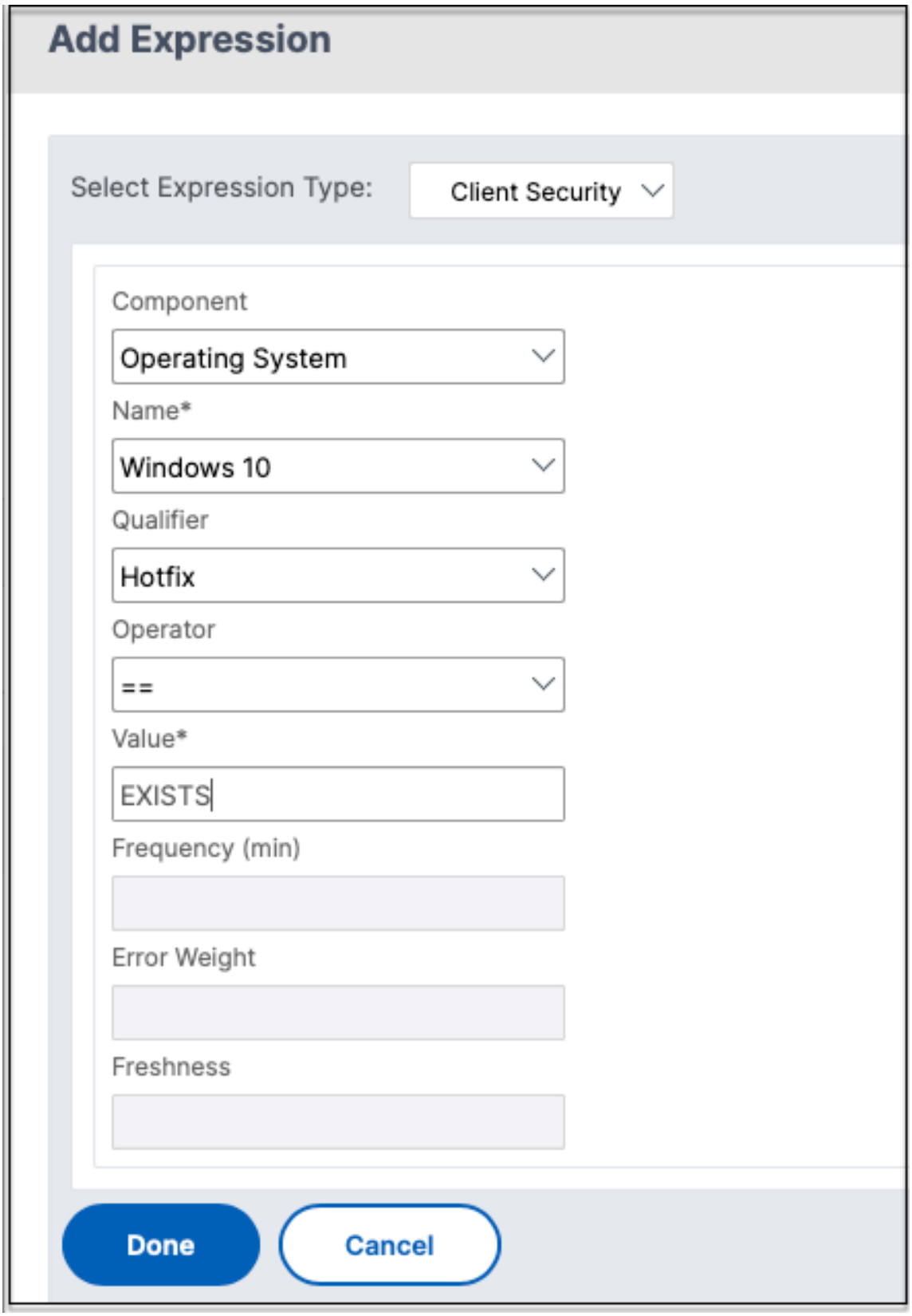


4. Fill in the details in the required fields and click **Create**.
5. In **Expression**, enter the expression manually or use the Expression editor to construct an expression for the policy.



The following figure displays a sample expression constructed for checking the Windows 10 OS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

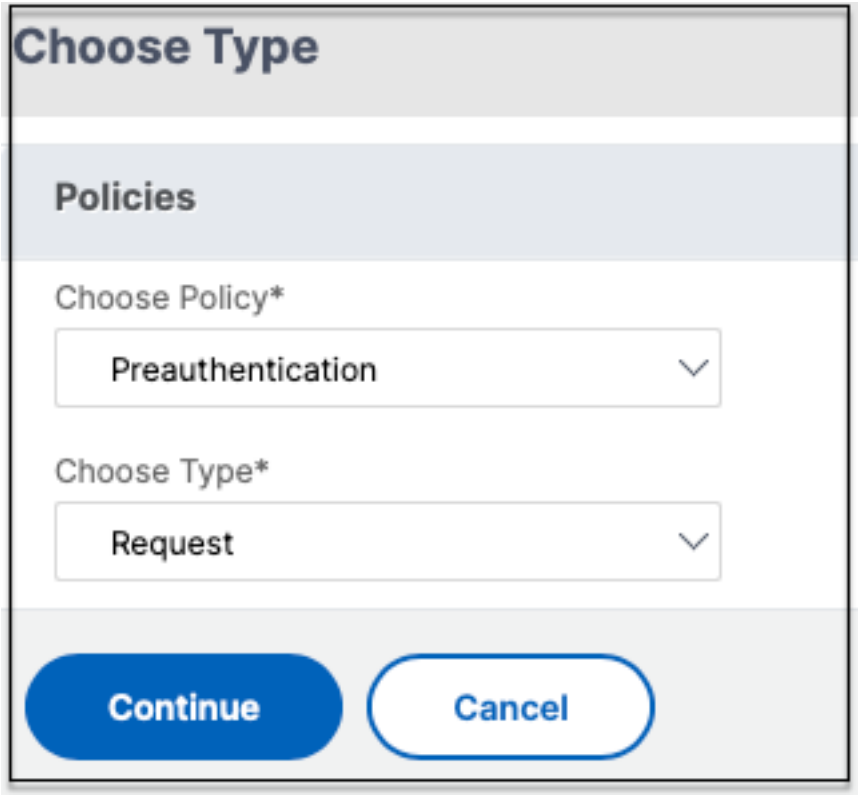


6. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

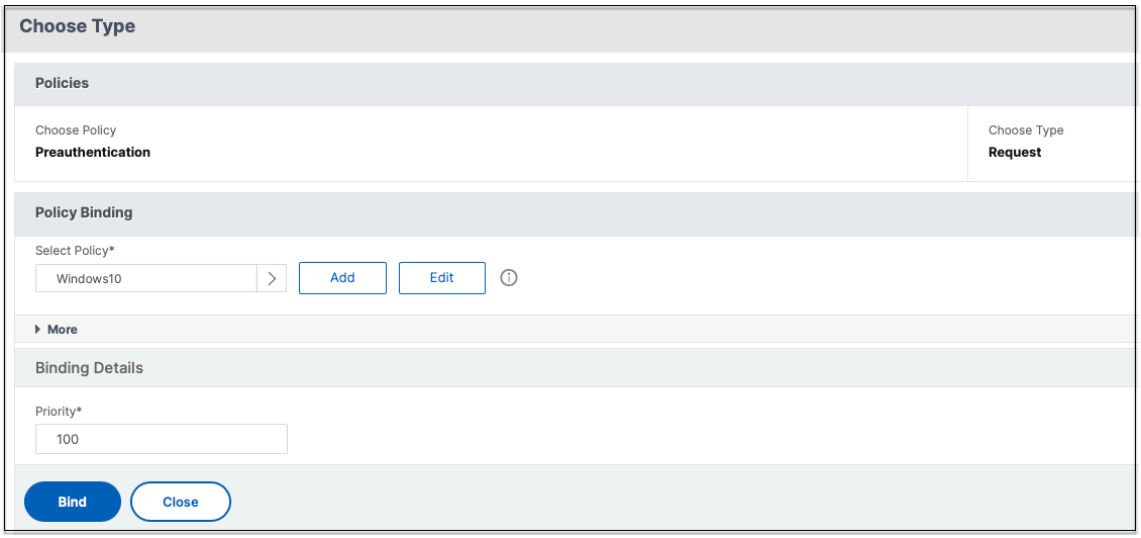
Bind the custom tag to NetScaler Gateway

1. Navigate to **NetScaler Gateway > Virtual Servers**.
2. Select the virtual server for which the preauthentication policy is to be bound and then click **Edit**.
3. In the **Policies** section, click **+** to bind the policy.
4. In **Choose Policy**, select the preauthentication policy and select **Request** in **Choose Type**.



5. Select the policy name and the priority for the policy evaluation.
6. Click **Bind**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Configure custom tags using the CLI

Run the following commands on the NetScaler CLI to create and bind a preauthentication policy:

Example:

- `add aaa preauthenticationaction win10_prof ALLOW`
- `add aaa preauthenticationpolicy Windows10 "CLIENT.OS(win10)EXISTS "win10_prof`
- `bind vpn vserver _SecureAccess_Gateway -policy Windows10 -priority 100`

Adding new contextual tag

1. Open the Secure Private Access admin console and click **Access Policies**.
2. Create a new policy or select an existing policy.
3. In the **If the following condition met** section, click **Add condition** and select **Contextual Tags**, **Matches all of**, and then enter the contextual tag name (for example, `Windows10`).

References

- Configure access policies for the applications.
- Support for smart access tags.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure StoreFront

August 18, 2025

If Secure Private Access is co-hosted with StoreFront, then the Secure Private Access configuration on StoreFront is done automatically by the first time setup wizard.

However, if Secure Private Access is not co-hosted with StoreFront, then certain configuration changes have to be done manually.

Perform the following steps to configure StoreFront manually.

1. Download the script from the Secure Private Access admin console (**Settings > Integrations**).
2. Click **Download Script** corresponding to the StoreFront entry for which the configuration changes have to be done.

   The downloaded zip file contains a configuration script, a README file, and a configuration cleanup script. The cleanup script can be used in case integration between StoreFront and Secure Private Access is to be removed.
3. Run the script as an admin on a PowerShell 64-bit instance by using the command `./ConfigureStorefront.ps1`.

   - No other parameters are required.
   - The PowerShell script execution policy must be set to Unrestricted or Bypass to run the StoreFront script.
   - The script also propagates the configuration to other StoreFront servers if StoreFront is configured as a cluster.

Once StoreFront is configured with the Secure Private Access settings, the Secure Private Access plug-in configuration can be seen in the StoreFront admin UI (**Manage Delivery Controllers** screen).

The StoreFront script automatically configures the aggregation group setting for Secure Private Access if the same is configured for the Citrix Virtual Apps and Desktops™ delivery controller. By default, the script configures Secure Private Access for everyone (**User Mapping and Multi-Site Aggregation Configuration > Configured**).

> **Important:**
>
> - It is recommended to use the StoreFront script downloaded from the Secure Private Access admin UI to configure StoreFront for Secure Private Access only. Do not configure Secure Private Access from the StoreFront admin UI as the UI does not cover all the required configuration on StoreFront. The script must be run to complete all the necessary configurations.
> - One Secure Private Access site can be configured on multiple StoreFront deployments (ei-

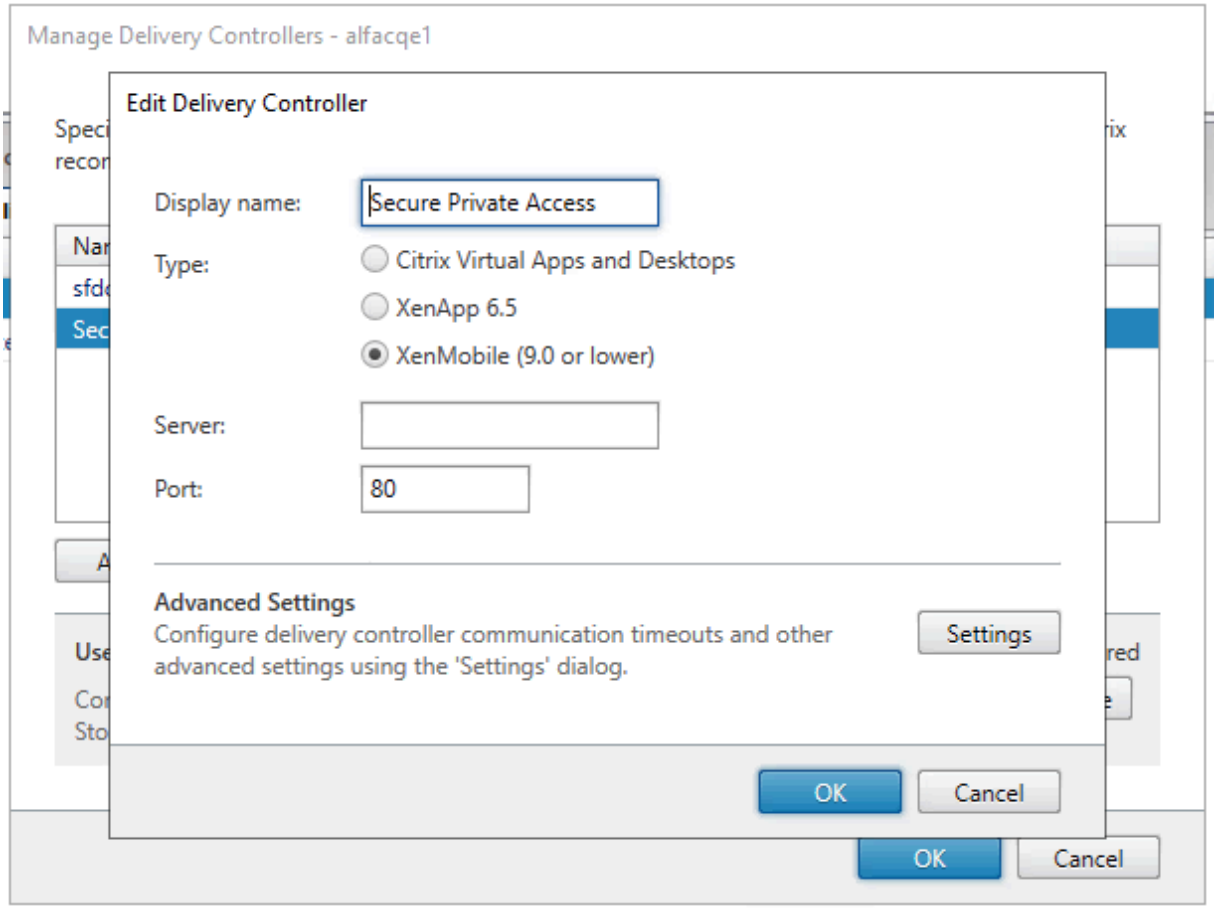
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> ther on another store on the same StoreFront or a different StoreFront deployment) as well. StoreFront can be added from the **Settings > Integrations** page.
>
> - The StoreFront auto configuration doesn't work from **Settings > Integration** page even if Secure Private Access is co-hosted with StoreFront. Autoconfiguration is done only during the first-time setup. If a new store configuration is added from the **Settings** page, the StoreFront script must be downloaded and run on the corresponding StoreFront machine.

When using StoreFront version 2308 or earlier

If you are using StoreFront version 2308 or earlier, the StoreFront admin UI has the following known issues:

- The Secure Private Access plug-in type is shown as XenMobile.
- The Secure Private Access server URL is not displayed.
- The Secure Private Access port is always shown as 80.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

When using StoreFront version 2311 or later

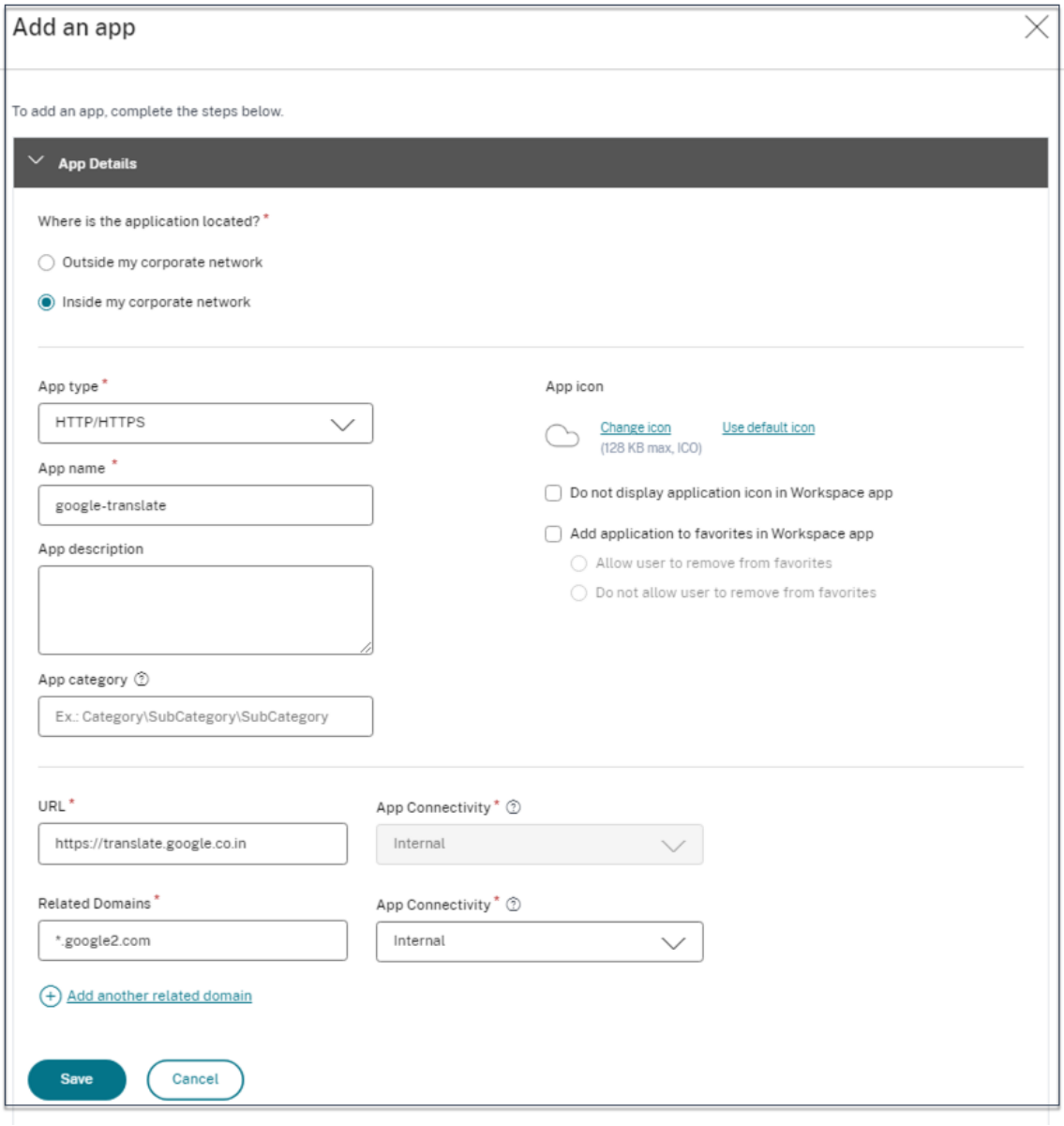
In StoreFront version 2311 and later, the Citrix Workspace™ for Web client doesn't enumerate the Secure Private Access apps. This is because Secure Private Access doesn't support the Secure Private Access app launch in the Workspace for Web platform.

Configure applications

August 18, 2025

1. Select the location where the app resides.
    - **Outside my corporate network** for external applications.
    - **Inside my corporate network** for internal applications.
2. Enter the following details in the App Details section and click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **App name** –Name of the application.
- **App description** - A brief description of the app. This description is displayed to your users in the workspace. You can also enter keywords for the applications in the format `KEYWORDS: <keyword_name>`. You can use the keywords to filter the applications. For details, see Filter resources by included keywords.
- **App category** - Add the category and the subcategory name (if applicable) under which the app that you are publishing must appear in the Citrix Workspace™ UI. You can add a new category for each app or use existing categories from the Citrix Workspace UI. Once you specify a category for a web or a SaaS app, the app shows up in the Workspace UI under the specific category.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The category/subcategory are admin configurable and administrators can add a new category for every app.
- The category/subcategory names must be separated by a backslash. For example, Business And Productivity\Engineering. Also, this field is case sensitive. Administrators must ensure that they define the correct category. If there is a mismatch between the name in the Citrix Workspace UI and the category name entered in the App category field, the category gets listed as a new category.

  For example, if you enter the Business and Productivity category incorrectly as Business And productivity in the App category field, then a new category named Business and productivity gets listed in the Citrix Workspace UI in addition to the Business And Productivity category.

- **App icon** –Click **Change icon** to change the app icon. The icon file size must be 128x128 pixels and only the Ico format is supported. If you do not change the icon, the default icon is displayed.
- **Do not display application to users** - Select this option if you do not want to display the app to the users.
- **URL** –URL of the application.
- **Related Domains** –The related domain is auto-populated based on the application URL. Administrators can add more related internal or external domains.
  Add application to favorites automatically –Click this option to add this app as a favorite app in Citrix Workspace app.
- **Allow user to remove from favorites** –Click this option to allow app subscribers to remove the app from the favorites apps list in Citrix Workspace app.
  When you select this option, a yellow star icon appears at the top left-hand corner of the app in Citrix Workspace app.
- **Do not allow user to remove from favorites** –Click this option to prevent subscribers from removing the app from the favorites apps list in Citrix Workspace app.

When you select this option, a star icon with a padlock appears at the top left-hand corner of the app in Citrix Workspace app.

If you remove the apps marked as favorites from the Secure Private Access console, then these apps must be removed manually from the favorites list in Citrix Workspace. The apps are not automatically deleted from StoreFront™ if the apps are removed from the Secure Private Access console.
App Connectivity: Select Internal for Web apps and External for SaaS apps.

3. Click **Save**, and then click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can view all the application domains that are configured in **Settings > Application Domain**. For more details, see Manage settings after installation.

Next Steps

Configure access policies for the applications

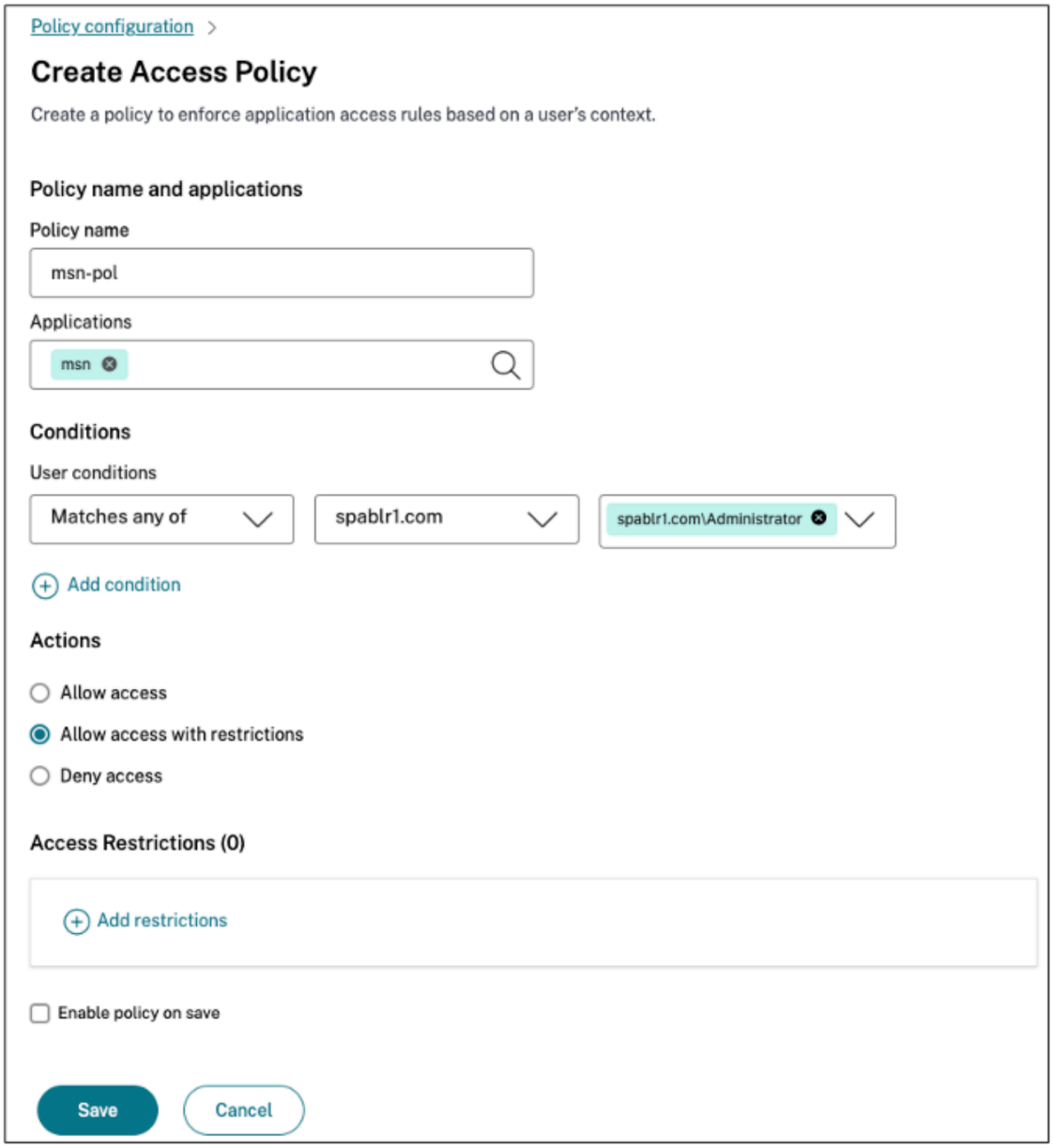
Configure access policies for the applications

August 18, 2025

Access policies allow you to enable or disable access to the apps based on the user or user groups. In addition, you can enable restricted access to the apps by adding the security restrictions.

1. Click **Create Policy**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. In **Applications**, select the apps for which you want to enforce the access policies.
3. In **Users/User groups** –Select the conditions and users or user groups based on which app access must be allowed or denied.

    - **Matches any of**: Only the users or groups that match any of the names listed in the field are allowed access.
    - **Does not match any**: All users or groups except those listed in the field are allowed access.

4. Click **Add condition** to add another condition based on contextual tags. These tags are derived from the NetScaler® Gateway.
5. Select **Conditional Tags** and then select the conditions based on which app access must be

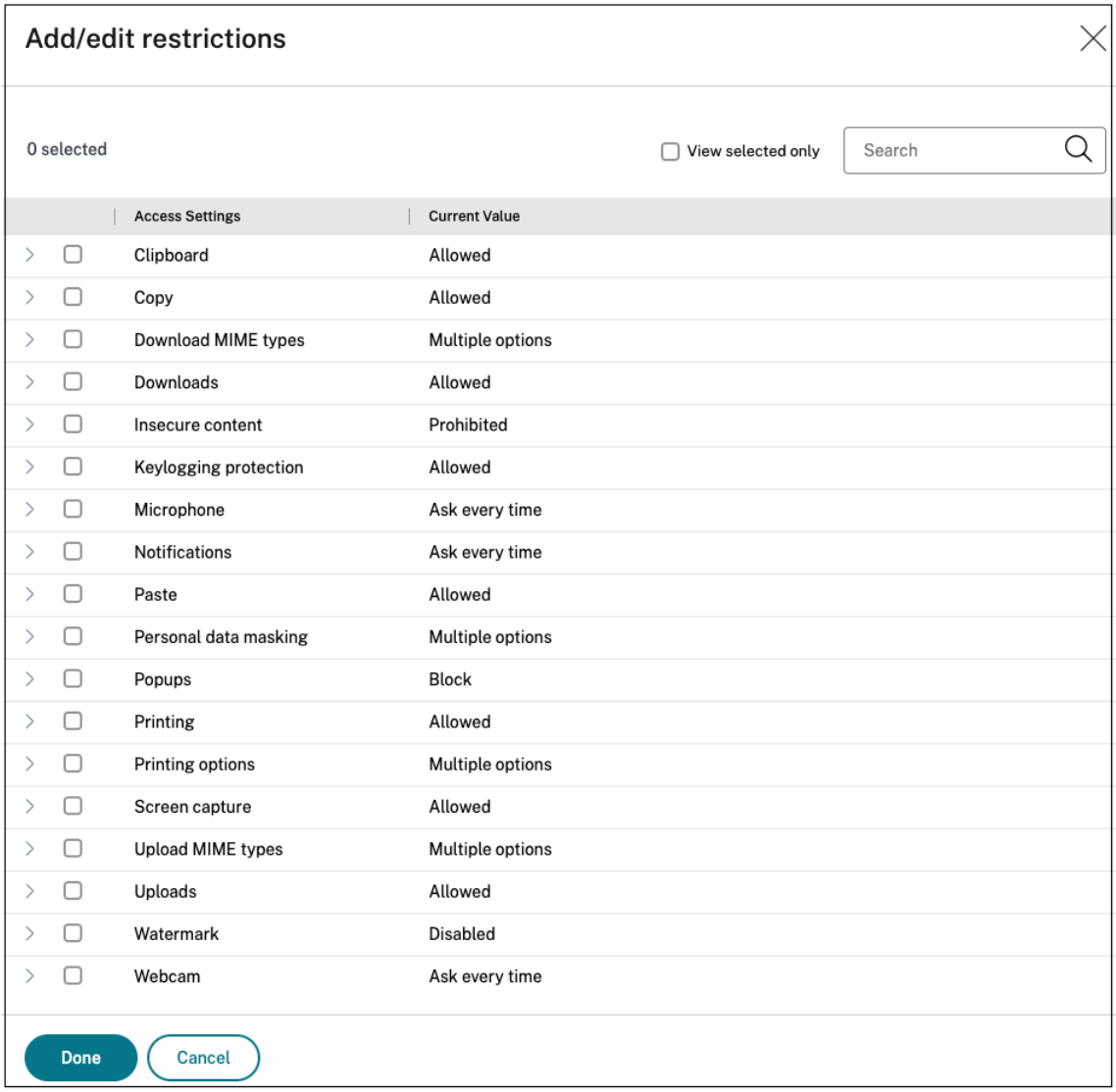
© 1997–2026 Citrix Systems, Inc. All rights reserved.

allowed or denied.

6. In **Then do the following**, select one of the following actions that must be enforced on the app based on the condition evaluation.

   - **Allow access**
   - **Allow access with restriction**
   - **Deny access**

   When you select **Allow access with restrictions**, you can select the following restrictions.



   - **Restrict clipboard access**: Disables cut/copy/paste operations between the app and the system clipboard.
   - **Restrict printing**: Disables the ability to print from within the Citrix Enterprise Browser.
   - **Restrict downloads**: Disables the user's ability to download from within the app.
   - **Restrict uploads**: Disables the user's ability to upload within the app.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Display watermark**: Displays a watermark on the user's screen displaying the user name and IP address of the user's machine.
- **Restrict key logging**: Protects against key loggers. When a user tries to log on to the app using the user name and password, all the keys are encrypted on the key loggers. Also, all activities that the user performs on the app are protected against key logging.
  For example, if app protection policies are enabled for Office 365 and the user edit an Office 365 word document, all key strokes are encrypted on key loggers.
- **Restrict screen capture**: Disables the ability to capture the screens using any of the screen capture programs or apps. If a user tries to capture the screen, a blank screen is captured.

> **Note:**
>
> Key logging and screen capture restrictions are applicable only to Citrix Workspace™ desktop clients.

7. In **Policy name**, enter a name for the policy.
8. Select **Enable policy on save**. If you do not select this option, the policy is only created and not enforced on the applications. Alternatively, you can also enable the policy from the Access Policies page by using the toggle switch.

Access policy priority

After an access policy is created, a priority number is assigned to the access policy, by default. You can view the priority on the Access Policies home page.

A priority with a lower value has the highest preference and is evaluated first. If this policy does not match the conditions defined, the next policy with the lower priority number is evaluated and so on.

You can change the priority order by moving the policies up or down by using the up-down icon in the **Priority** column.

Next steps

Validate your configuration from the client machines (Windows and macOS).

Example

End user flow

August 18, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

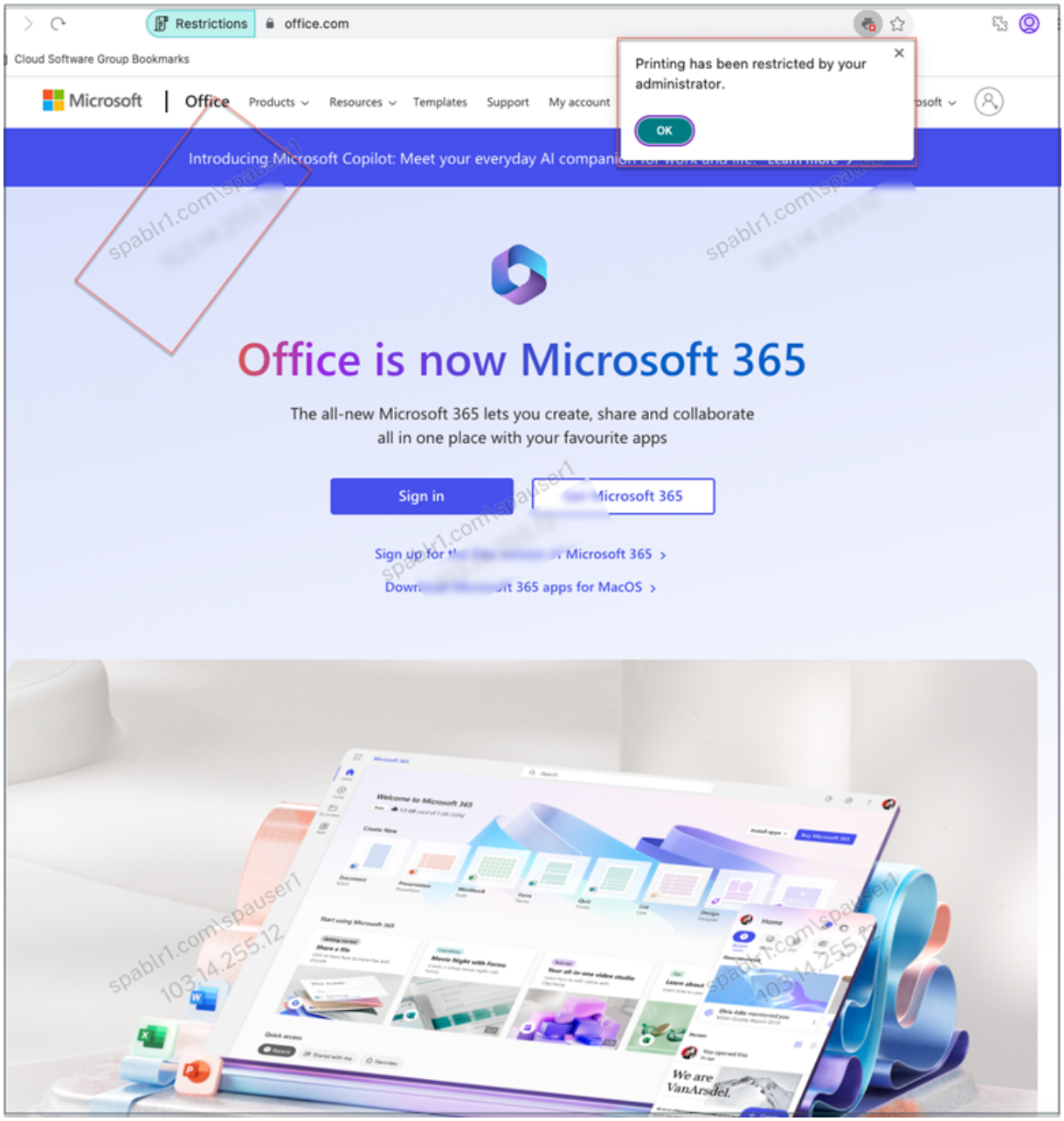
Assume that an admin has configured the Office365 app with the watermark and print restriction for the end user. Now, when the end user accesses the Office365 app, the watermark and print restrictions must be applied on the app.

The end user must perform the following steps to access the Office365 app:

1. Access the StoreFront™ store from the Citrix Workspace™ app.
2. Log on to the store.
3. Click the **Apps** tab, and then click the **Office365** application.

   The end user must now notice that the Office365 application is launched and contains the watermark. Also, if the end user tries to print some data from the Office365 application, the print restriction message must be displayed to the user.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Note:

Administrators must provide users with the account information that they need to access virtual desktops and applications. For details, see Adding store URL to Citrix Workspace app.

Secure Private Access integration with Web Studio integration

August 18, 2025

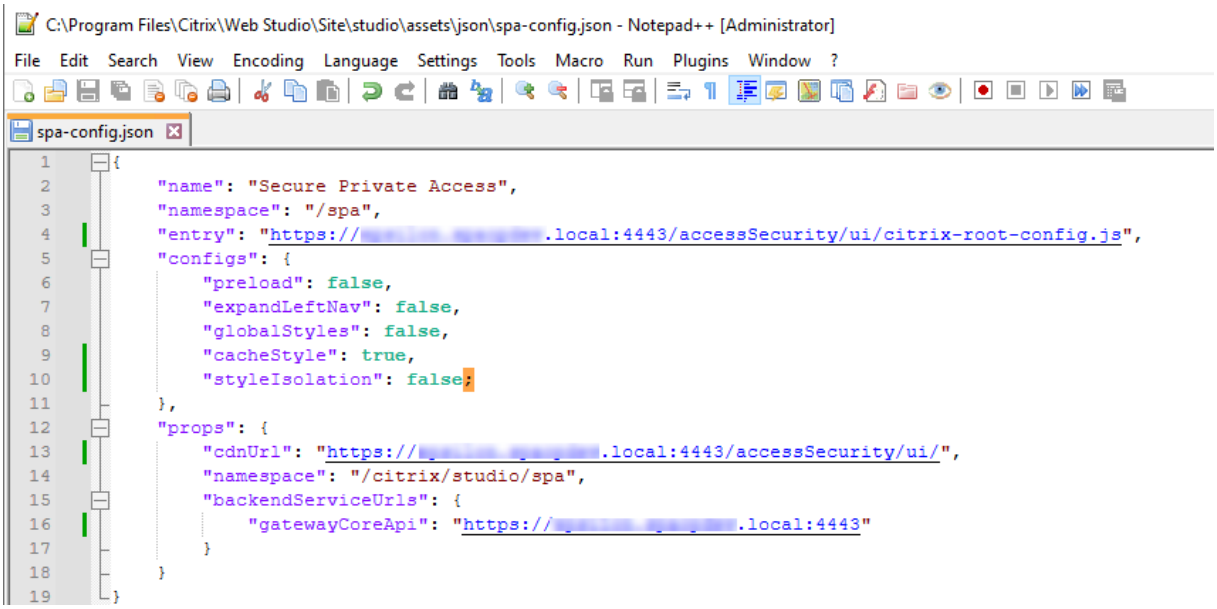
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Secure Private Access™ is also integrated into the Web Studio console to enable users seamlessly access the service through Web Studio.

You must install Web Studio version 2308 or later.

Perform the following steps to enable Web Studio integration:

1. Install Citrix Web Studio by using the Citrix Virtual Apps and Desktops™ installer or integrated DDC installer.
2. Follow the onscreen instructions and complete the installation. When prompted for a controller address, enter the DDC FQDN as the controller address.
3. After successful installation, navigate to the folder C:\Program Files\Citrix\Web Studio\Site\assets\json and modify the content of the spa-config.json file.
   If a non-default location was used for the Web Studio installation, replace the default installation location in C:\Program Files\Citrix with the correct location.



1. Replace “SpaServer”with the FQDN of your Secure Private Access plug-in.
2. Log in to Web Studio.
3. On the left navigation menu, click **Secure Private Access** to access the Secure Private Access admin console from Web Studio.

Deploy Secure Private Access as a cluster

August 18, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The Secure Private Access on-premises solution can be deployed as a cluster to provide high availability, high throughput, and scalability. It is recommended to deploy standalone Secure Private Access nodes for large deployments (for example, more than 5000 users).

If you are using NetScaler Gateway versions 13.0 or 13.1 build 48.47 or earlier, it is recommended that you co-host Secure Private Access with StoreFront.

Create Secure Private Access nodes

- Create a new Secure Private Access site. For details, see Setup a Secure Private Access site.
- Add the required number of cluster nodes to the Secure Private Access site. For details, see Setup Secure Private Access by joining an existing site.
- In each Secure Private Access node, configure the same server certificates. The certificate subject common name or subject alternative name must match the load balancer FQDN.

Load balancer configuration

There are no specific load balancing configuration requirements for the Secure Private Access cluster setup. If you are using NetScaler® as the load balancer, note the following:

- Secure Private Access services (both admin and runtime) are stateless, and so persistency is not required.
- Secure Private Access services are recommended to run as HTTPS but this is not a mandatory requirement. Secure Private Access services can be deployed as HTTP as well.
- SSL offload or SSL bridge is supported, so any load balancer configuration can be used. When using SSL bridge, ensure to configure the same server certificates in each Secure Private Access node. Also, the certificate subject common name or subject alternative name (SAN) must match the load balancer FQDN. Also, SAN must be configured in the Load Balancer service.
- Load balancers (for example NetScaler) have default built-in monitors (probes) for back-end servers. If you must configure a custom HTTP based monitor (probe) for Secure Private Access on-premises servers, the following endpoint can be used:

  `/secureAccess/health`

  Expected response:

```
Http status code: 200 OK

Payload:

{
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
"status":"OK","details":{
"duration":"00:00:00.0084206","status":"OK" }
 }
```

For details about configuring a NetScaler load balancer, see Setup basic load balancing.

Manage settings after installation

August 18, 2025

After you have installed Secure Private Access, you can modify the settings from the Settings page.

To modify the settings, you must sign into the Secure Private Access admin console with a Secure Private Access administrator account.

Manage routing of application domains

You can view a list of application domains added in your Secure Private Access setup. The application domains table lists all the related domains and how the app traffic is routed (externally or internally).

1. Click **Settings > Application Domain**.
2. You can click the edit icon and change the routing type, if required.

Manage administrators for Secure Private Access

You can view the list of administrators and also add administrators from the **Settings > Administrators** page. The administrator who installs the Secure Private Access the first time is granted full permission. This admin can then add other administrators to the setup.

You can also add admin groups so that access is enabled for all the admins in that group.

1. In the **Administrators** page, click **Add**.
2. In **Domain**, select the domain to which this administrator must be added.
3. In **Users or user group**, select the user or a group to which this user belongs.
4. In **Admin Type**, select the permission type that must be assigned to this user.

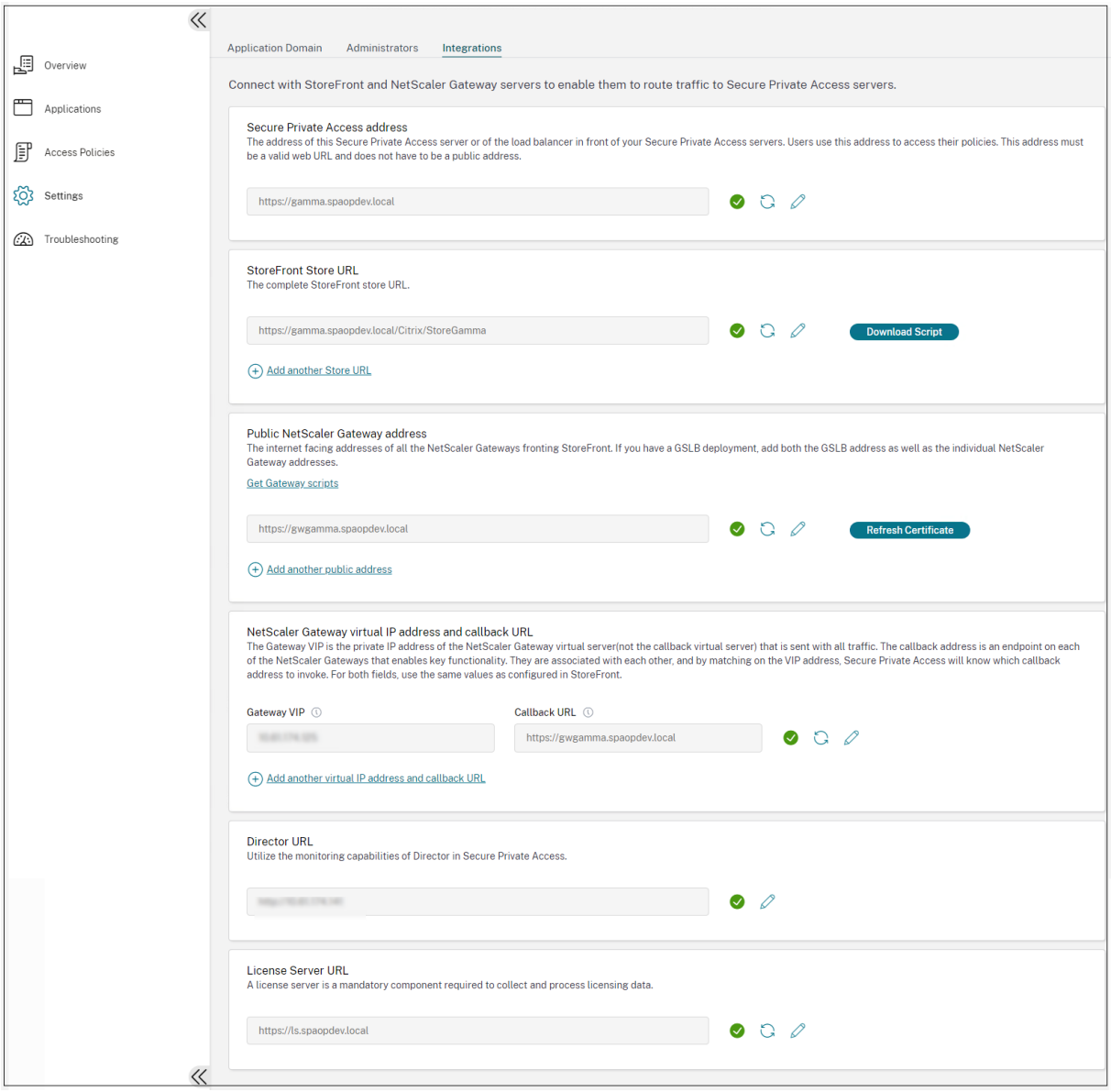
Update StoreFront™ or the NetScaler Gateway server details after the setup

After you have set up Secure Private Access, you can modify or update the StoreFront and NetScaler® Gateway entries from the **Integrations** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Click **Settings > Integrations**.
2. Click the edit icon in line with the setting that you want to modify and update the entry.
3. Click the refresh icon to ensure that the settings are valid.

> **Note:**
>
> If Secure Private Access is installed on a machine different that StoreFront, then download the StoreFront script and run it on the StoreFront.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

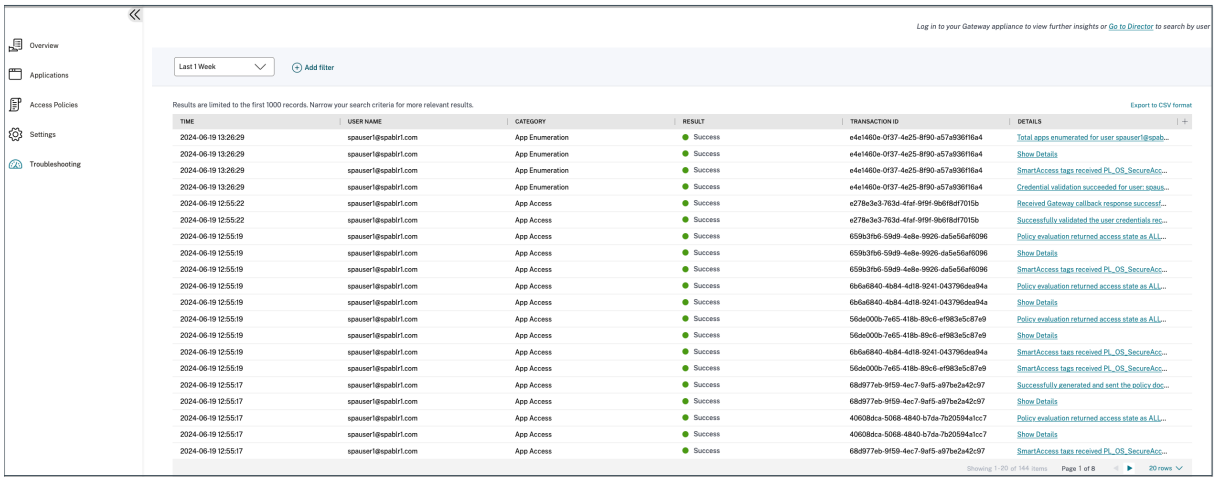
Dashboard overview

August 18, 2025

The Secure Private Access troubleshooting logs dashboard displays the logs related to application launch, app enumeration, and their statuses.

You can view the logs for the pre-set time or for a custom timeline. You can add columns to the chart by clicking the + sign depending on what information you want to see in the dashboard. You can export the user logs into CSV format.

You can use the filters (CATEGORY and RESULT) to refine your search results.



You can also refine your search based on the following parameters along with the operators in the search field.

- User-Name
- Category
- Event-Type
- Result
- Transaction-ID
- Details

The following are the search operators that you can use to refine your search in the User logs and Top access policies by enforcement charts.

- =: To search for the logs/policies that exactly match the search criteria.
- !=: To search for the logs/policies that do not contain the specified criteria.
- ~: To search for the logs/policies that match the search criteria partially.
- !~: To search for the logs/policies that do not contain some of the specified criteria.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

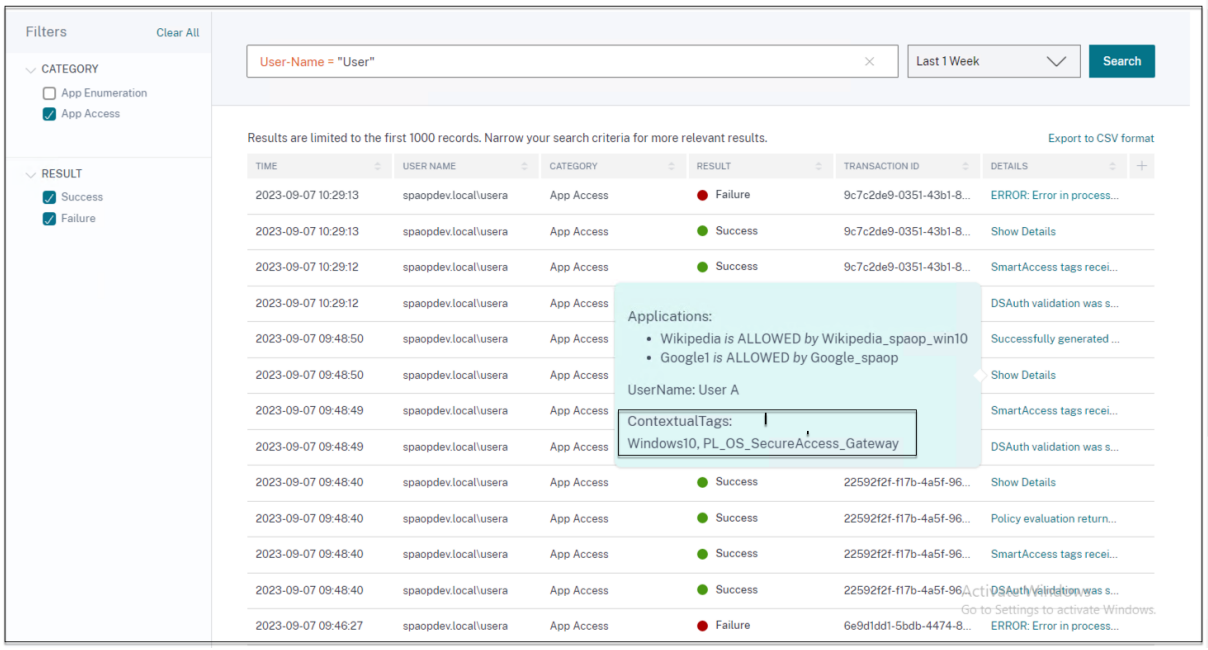
For example, you can search for an event type “DSAuth”by using the string **Event-Type = DSAuth** in the search field.

Similarly, to search for users that partially contain the term “operator”, use the string **User-Name ~ operator**. This search lists all the user names that contain the term “operator”. For example, “local operator”, “admin operator”

You can search for all logs related to a single event by using the transaction ID. The transaction ID correlates all Secure Private Access logs for an access request. One app access request can have multiple logs generated, starting from authentication, then app enumeration and then app access itself. All these events generate their own logs. Transaction ID is used to correlate all of these logs. You can filter the troubleshooting logs using the transaction ID to find all logs related to a particular app access request.

View contextual tags from logs

The **Show Details** link in the **Details** column displays the list of applications associated with the specific access policy and also the contextual tags associated with the policy.



Troubleshooting some common errors

August 18, 2025

This topic list some of the errors that you might come across while setting up Secure Private Access.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Certificate errors

Database creation errors

StoreFront failures

Public gateway/callback gateway failures

Secure Private Access Server not reachable

Certificate errors

Error message: Unable to get the certificates automatically from one or more Gateway servers.

This error message appears when you try to add a public NetScaler® Gateway address and there is an issue fetching the certificate. This issue can occur when setting up Secure Private Access or updating settings after the setup is complete.

Workaround: Update the gateway certificate the same way in which you would for Citrix Virtual Apps and Desktops.

Database creation errors

- **Error message**: Failed to create database

  Resolution: For Automatic case - The machine must have READ, WRITE, UPDATE permissions to create tables within the database on the SQL server.

- **Error message**: Failed to create database: A database already exists.

  This error message might appear in any of the following scenarios.

  - If the **Automatic configuration** option is selected while configuring the databases.
  - If the admin is creating a database, it must be an empty database. This error message can appear if the database is a non-empty database.

    Resolution: You must create an empty database.
  - You uninstall Secure Private Access and retry the setup with the same site name. In this case, the database from the previous installation would not have been deleted.

    Resolution: You must manually delete the database.
  - You choose to set up the database manually (by selecting Manual Configuration in the Configuring Databases page) by using the script, and then change to the Automatic Configuration option but use the same site name. In this case, a database with the same name is already created while running the script.

    Resolution: You must rename the site and then run the script again.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The machine does not have the READ, WRITE, UPDATE permissions to create tables within the database on the SQL server.

  Resolution: Enable appropriate permissions on the machine. For details, see Permissions required to set up databases.

- **Error message**: Failed to create database: Connection failed

  Resolution:

  - Check database network connectivity from your machine. Ensure that the SQL server port is open on the firewall.
  - If using a remote SQL server, check if the SQL server has login created with the Secure Private Access machine identity, Domain\hostname$.
  - If using a remote SQL server, confirm that the machine identity has the correct role assigned, system administrator role.
  - If using a Local SQL server (not from the installer), check if the NT AUTHORITY\SYSTEM user must have a login created.

StoreFront™ failures

- **Error message**: Failed to create StoreFront entry for: `<Store URL>`

  Update the StoreFront entries from the **Settings** tab if it is not visible. After you have set up Secure Private Access using the wizard, you can edit StoreFront entries from the **Settings** tab. Note down the StoreFront Store URL for which this error occurred.

  Resolution:

  1. Click **Settings** and then click the **Integrations** tab.
  2. In **StoreFront Store URL**, add the StoreFront entry if it is not visible.

- **Error message**: Failed to configure StoreFront entry for: `<Store URL>`

  Resolution:

  1. There might be a PowerShell execution policy restriction in place. Run the PowerShell script command `Get-ExecutionPolicy` for details.
  2. If it is restricted, you must bypass this and run a StoreFront configuration script manually.
  3. Click **Settings** and then click the **Integrations** tab.
  4. In **StoreFront Store URL**, identify the StoreFront URL entry for which the error occurred.
  5. Click the **Download Script** button next to this Store URL and run this PowerShell script with admin privileges on the machine on which the corresponding StoreFront installation is present. This script must be run on all the StoreFront machines.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> If you are retrying the installation after uninstalling, ensure that you don't have an entry with the name "Secure Private Access"in the StoreFront configuration (**StoreFront > store> Delivery Controller™ -> Secure Private Access**). If Secure Private Access is present, delete this entry. Manually download and run the script from the Settings > Integrations page.

- **Error message**: StoreFront configuration is not local for: <`Store URL`>

  After you have set up Secure Private Access using the wizard, you can edit gateway entries from the Settings tab. Note down the StoreFront Store URL for which this error occurred.

  Resolution:

  This issue occurs if StoreFront is not installed on the same machine as Secure Private Access. You must manually run the StoreFront configuration on the machine where you have installed StoreFront.

  1. Click **Settings** and then click the **Integrations** tab.
  2. In **StoreFront Store URL**, identify the StoreFront URL entry for which the error occurred.
  3. Click the Download Script button next to this Store URL and run this PowerShell script with admin privileges on the machine on which the corresponding StoreFront installation is present. This script must be run on all the StoreFront machines.

  > **Note:**
  >
  > To run the StoreFront PowerShell script, open the Windows x64 compatible PowerShell window with admin privileges and then run ConfigureStorefront.ps1. StoreFront script is not compatible with Windows PowerShell (x86).

- **Error message**: "Get-STFStoreService : Exception of type 'Citrix.DeliveryServices.Framework.Feature.Except was thrown."while running StoreFront script using PowerShell.

  This error occurs when the StoreFront script is run on a x86-compatible PowerShell window.

  Resolution:

  To run the StoreFront PowerShell script, open the Windows x64 compatible PowerShell window with admin privileges and then run `ConfigureStorefront.ps1`.

Public gateway/callback gateway failures

Error message: Failed to create Gateway entry for: <`Gateway URL`> OR Failed to create Callback Gateway entry for: <`Callback Gateway URL`>

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Resolution:

Note the Public Gateway or Callback Gateway URL for which the failure occurred. After you have set up Secure Private Access using the wizard, you can edit gateway entries from the **Settings** tab.

1. Click **Settings** and then click the **Integrations** tab.
2. Update the public gateway address or the callback gateway address and the virtual IP address for which the failure occurred.

Secure Private Access Server not reachable

Error message: Failed to update IIS pool. Failed to restart IIS pool

Resolution:

Go to Application pools in Internet Information Services (IIS) and check that the following application pools have started and are running:

- Secure Private Access Runtime Pool
- Secure Private Access Admin Pool

Also check that the default IIS site `"Default Web Site"` is up and running.

Database connectivity check failures

Error Message: Connectivity check failed

Database connectivity check can fail due the multiple reasons:

- The database server is not reachable from the Secure Private Access plug-in host machine due to a firewall.

  Resolution: Check if the database port (default port 1433) is open on the firewall.

- The Secure Private Access plug-in host machine does not have the permission to connect to the database.

  Resolution: See SQL database permissions for Secure Private Access.

Gateway connectivity check failed. Unable to fetch public certificate

Error Message: Post installation configuration fails with the error "Gateway connectivity check failed. Unable to fetch a public certificate…."

Resolution:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Upload the gateway public certificate to the Secure Private Access database manually using the config tool.
- Open the PowerShell or the command prompt window with admin privileges.
- Change the directory to the Admin\AdminConfigTool folder under the Secure Private Access installation folder (for example, cd "C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool")
- Run the following command:

```
.\AdminConfigTool.exe /UPLOAD_PUBLIC_GATEWAY_CERTIFICATE <PublicGatewayUrl
> <PublicGatewayCertificatePath>
```

Application enumeration failure

Application enumeration breaks if the StoreFront URL or the NetScaler Gateway URL contains a trailing slash (/).

Resolution:

Delete the trailing slash in the StoreFront store URL or the NetScaler Gateway URL. For details, see Update StoreFront or the NetScaler Gateway server details after the setup.

Miscellaneous

Create Secure Private Access diagnostics support bundle

Perform the following steps to create a Secure Private Access diagnostics support bundle:

- Open the PowerShell or the command prompt window with admin privileges.
- Change the directory to the Admin\AdminConfigTool folder under the Secure Private Access installation folder (for example, cd "C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool").
- Run the following command:

```
.\AdminConfigTool.exe /SUPPORTBUNDLE <output folder>
```

SQL database permissions for Secure Private Access

For automatic database creation, the Secure Private Access plug-in host machine must have the permissions to connect to the database and create the database schema.

Remote database:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Perform the following steps to set up the permissions for a remote database.

1. Create an empty database with the name syntax `CitrixAccessSecurity<Site Name>`. Here `<Site Name>` is the Secure Private Access site name. (for example. CitrixAccessSecuritySPA).

   ```
   CREATE DATABASE CitrixAccessSecurity<SiteName>
   ```

2. Create an SQL server login for the machine identity for the Secure Private Access virtual machine. For example, if your Secure Private Access broker machine name is HOST1 and the machine domain is DOMAIN1, then the machine identity is "DOMAIN1\HOST1$". If the login is already created, then you can ignore this step.

   ```
   USE CitrixAccessSecurity<SiteName>

   CREATE LOGIN [DOMAIN1\HOST1$] FROM WINDOWS
   ```

   Domain name can be found using the following query:

   ```
   SELECT DEFAULT_DOMAIN()[DomainName]
   ```

3. Assign the db_owner role to the machine identity.

   ```
   USE CitrixAccessSecurity<SiteName>

   EXEC sys.sp_addrolemember [db_owner], 'DOMAIN1\HOST1$'

   ALTER USER [DOMAIN1\HOST1$] WITH DEFAULT_SCHEMA = dbo;
   ```

Local database:

Perform the following steps to set up the permissions for a local database.

1. Create an empty database with the name syntax `CitrixAccessSecurity<Site Name>`. Here `<Site Name>` is the Secure Private Access site name. (for example, CitrixAccessSecuritySPA).

   ```
   CREATE DATABASE CitrixAccessSecurity<SiteName>
   ```

2. Create an SQL server login for the `NT AUTHORITY\SYSTEM` user. If the login is already created then you can ignore this step.

   ```
   USE CitrixAccessSecurity<SiteName>

   CREATE LOGIN [NT AUTHORITY\SYSTEM] FROM WINDOWS
   ```

3. Assign the db_owner role to the "NT AUTHORITY\SYSTEM"user.

   ```
   USE CitrixAccessSecurity<SiteName>

   EXEC sys.sp_addrolemember [db_owner], 'NT AUTHORITY\SYSTEM'

   ALTER USER [NT AUTHORITY\SYSTEM] WITH DEFAULT_SCHEMA = dbo;
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When you manually create the database, the downloaded database script adds the permissions to the machine identity.

Retain troubleshooting logs

August 18, 2025

The logs in the **Troubleshooting Logs** page are stored in the Secure Private Access database for 90 days. If the total log count becomes too large, for example over 100,000, you can delete the oldest logs earlier than 90 days. The clean-up job, by default, runs every 12 hours. The job also runs whenever the runtime service restarts.

Customizing the troubleshooting logs retention settings

The cleanup of the logs is configurable through the appsettings.json file in the Runtime service's installation folder. You can set the cleanup based on the age of the logs and the number of logs that can be stored in the database. Modify the following entries in the appsettings.json file, as required:

Sample appsettings.json file:

```
"TroubleshootingLogs": {

  "CleanupPeriodInHours": 12,
  "CleanupDataOlderThanDays": 90,
  "CleanupOldestDataIfEntriesCountAbove": 100000
 }
```

To disable cleanup, configure the following settings as required:

- To retain logs for 7 days only, set `CleanupDataOlderThanDays` to 7.
- To disable the days-based cleanup, set `CleanupDataOlderThanDays` to 0.
- To disable the count-based cleanup, set `CleanupOldestDataIfEntriesCountAbove` to 0.
- If both of these settings are set to 0, or if `CleanupPeriodInHours` is set to 0, the logs are retained forever.
    - Setting both `CleanupDataOlderThanDays` or `CleanupOldestDataIfEntriesCountAbove` to 0 or setting `CleanupPeriodInHours` to 0 is not recommended as it might cause 100% disk usage issue.
    - The logs cleanup frequency can also be changed by modifying the `CleanupPeriodInHours` entry.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> If Secure Private Access is deployed as a cluster, then these settings must be modified in each cluster node. If there is a mismatch in the node settings, the instance that is cleaned up most frequently takes precedence.

Logs and telemetry cleanup

August 18, 2025

Telemetry data cleanup

Telemetry data is stored in the Secure Private Access database for 3 months. The checks to identify telemetry data that is due for cleanup are done every 30 seconds.

> **Note:**
>
> The Runtime service must be running for triggering the telemetry data cleanup.

CDF logs cleanup

CDF logs are stored on the Secure Private Access installation machine, inside the installation folders for the Admin and the Runtime service. The CDF logs are placed in .csv files with a 10MB size limit applied to each file.
The Admin service can retain up to 90 CDF log files at once, after which it deletes the oldest files to clear space for the new CDF log files to be created.
The Runtime service works in the same way as the Admin service but can retain a larger number of files at once, up to 600.

Custom cleanup of CDF logs

The CDF logs cleanup is configurable through the appsettings.json files in the installation folders of the Admin and Runtime services. To change the file size and count limit for the files, update the following entries in the appsettings.json file:

```
"CdfFile": {

      "fileSizeLimitBytes": 10485760, // 10 MB
      "retainedFileCountLimit": 600
     }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> If multiple instances of Secure Private Access are set up for the site, update the appsettings.json files for CDF cleanup on each Secure Private Access installation machine.

Uninstall Secure Private Access

August 18, 2025

You can uninstall Secure Private Access from **Control Panel > Programs > Programs and Features**.

1. Select **Citrix Virtual Apps and Desktops™ 7 2308 –Secure Private Access**.
2. Click **Uninstall**.
3. Follow the on-screen instructions and complete the uninstallation.

> **Note:**
>
> If the Secure Private Access post installation setup is completed, then before uninstalling Secure Private Access, download the StoreFrontScripts.zip file from the admin console to remove the Secure Private Access plug-in from the StoreFront store configuration.

To download StoreFrontScripts zip file, follow these steps:

1. Log in to the Secure Private Access admin console.
2. Click **Settings** and then click the **Integrations** tab.
3. Click **Download Script** in the StoreFront Store URL section.

Remove the Secure Private Access plug-in from the StoreFront store configuration

After you uninstall Secure Private Access, you must remove the Secure Private Access plug-in from the StoreFront store configuration.

1. Log in to the StoreFront machine.
2. Download the StoreFrontScripts.zip file.
3. Unzip StoreFrontScripts.zip to a folder.
4. Open a PowerShell window with the admin privileges.
5. Run the following command:

```
cd <unzipped folder>
.\RemoveStorefrontConfiguration.ps1
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Private Access 2311 compatibility with legacy versions

September 13, 2025

Secure Private Access 2311 is incompatible with the legacy versions. NetScaler Gateway must be configured using the new script as described earlier in Configure NetScaler Gateway. No configuration is required in the Citrix Virtual Apps and Desktops delivery controller for Secure Private Access legacy versions.

The best way to migrate from legacy versions to 2311 is to clean up the following:

- Citrix Virtual Apps and Desktops Delivery controller from Web/SaaS apps
- Update Citrix StoreFront™ to default configuration or create a new store on StoreFront
- NetScaler® Gateway

Citrix Virtual Apps and Desktops™ Delivery Controller cleanup

The Secure Private Access applications created on Citrix Virtual Apps and Desktops Delivery Controller can be removed manually or using the PowerShell script.

Manual:

1. Open Citrix Studio or Citrix WebStudio.
2. Click **Applications**.
3. Select the app, right click, and then select **Delete**.

Using a script:

1. Fetch the current Secure Private Access apps by running the following command:

   ```
   Get-BrokerApplication -Description "KEYWORDS:SPAENABLED"
   ```

   For details, see Remove-BrokerApplication.

2. After verifying the apps, run the following command to remove them:

   ```
   Get-BrokerApplication -Description "KEYWORDS:SPAENABLED"| Remove-BrokerApplication
   ```

Citrix StoreFront cleanup

You can either create a new StoreFront store or clean up the existing store.

- Create a new StoreFront store: You must create a new StoreFront store for Secure Private Access 2311 as the existing StoreFront stores created for legacy versions aren't compatible with 2311. This is the recommended option to avoid configuration related issues.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Clean up existing StoreFront store: The existing store on StoreFront can be cleaned manually or using the script. However, the best option for migrating Secure Private Access on-premises to 2311 is to create a new Store on StoreFront.

Manual:

1. Find and remove policy.json (e.g C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBrowser\policy.json).
2. Find and remove folders SecureBrowser (for example C:\inetpub\wwwroot\Citrix\Store\Resources\SecureBr and Resources (for example C:\inetpub\wwwroot\Citrix\Store\Resources).
3. Remove the "route"node from web.config (you can find it in C:\inetpub\wwwroot\Citrix\Store) with the name "webSecurePolicy"routing to the URL "Resources\SecureBrowser\policy.json".
4. Restart the **Default Web Site on Internet Information Service (IIS) Manager** console to apply changes.

Using a script:

1. Download the script from https://www.citrix.com/downloads/citrix-secure-private-access/.
2. Upload the script to a StoreFront machine.
3. Run the script as administrator on PowerShell.
4. Enter the Store name.

   The Script removes the C:\inetpub\wwwroot\Citrix\Store\Resources folder, subfolder and files, and updates the web.config file.
5. Restart the **Default Web Site on Internet Information Service (IIS) Manager** console to apply changes.

NetScaler Gateway cleanup

NetScaler Gateway virtual server

The NetScaler Gateway virtual server created for legacy versions can be reused for Secure Private Access 2311.

- To update an existing NetScaler Gateway, see Update an existing NetScaler Gateway.
- To configure a new NetScaler Gateway, see Configure NetScaler Gateway.

Session policies and actions

Session policies and actions created for legacy versions can be reused by Secure Private Access 2311.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To update an existing NetScaler Gateway session policies/actions, see NetScaler Gateway session actions.
- To configure a new NetScaler Gateway, see Configure NetScaler Gateway

The script also creates fully configured session policies/actions.

Authorization policies

Authorization policies created on NetScaler Gateway for legacy versions can interfere with Secure Private Access 2311 policies and break the flow.

You can do the following to clean up the authorization policies.

- Manually unbind the authorization policies from authentication and authorization groups that are used as default groups on NetScaler Gateway. In this case, the policies can be reused.
- Remove the authorization policies.

Third-party notifications

August 18, 2025

Citrix Secure Private Access for on-premises

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.