Citrix Secure Private Access™ - On premises

Contents

Technical overview

September 6, 2025

Citrix Secure Private Access on-premises is a customer-managed Zero Trust Network Access (ZTNA) solution that provides secure access to internal web/SaaS and TCP/UDP applications with the following along with a seamless end-user experience:

- VPN less access for SaaS and internal web apps
- Least privilege principle
- Single sign-on (SSO)
- Multifactor authentication
- Device posture assessment
- Application-level security controls
- App protection features

The solution uses the StoreFront on-premises and Citrix Workspace app to enable a seamless and secure access experience to access internal web/SaaS and TCP/UDP apps within Citrix Enterprise Browser. This solution also uses NetScaler Gateway to enforce authentication and authorization controls.

Citrix Secure Private Access on-premises solution enhances an organization's overall security and compliance posture with the ability to easily deliver zero-trust access to browser-based apps (internal web/SaaS apps) and client-server apps (TCP/UDP apps) using the StoreFront on-premises portal as a unified access portal to internal web/SaaS, TCP/UDP apps, along with virtual apps and desktops as an integrated part of Citrix Workspace.

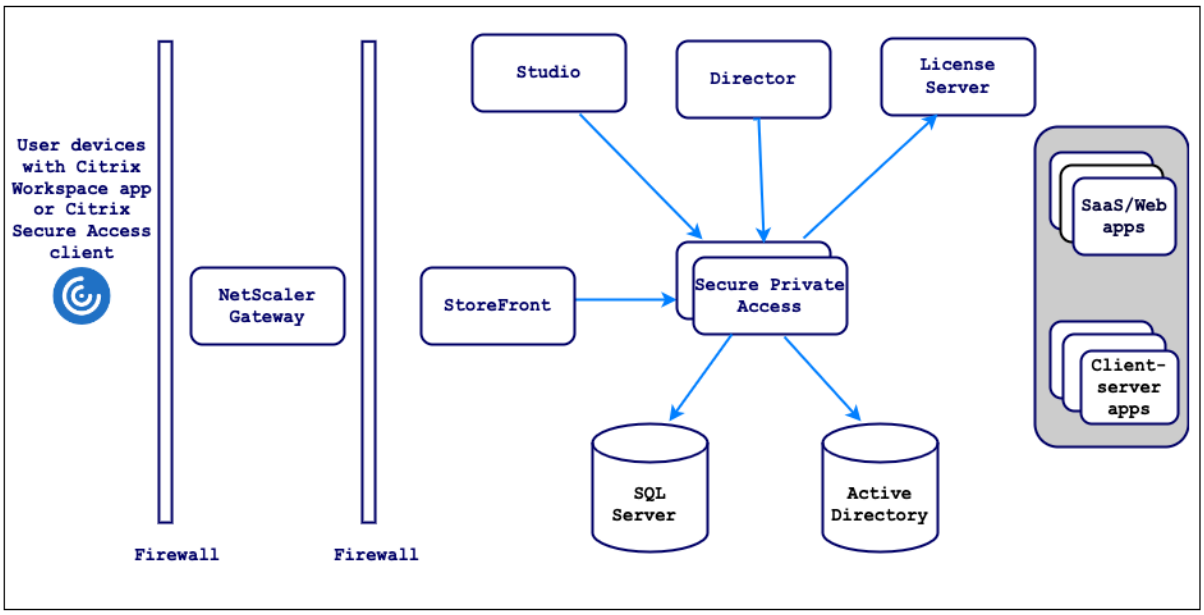
Citrix Secure Private Access™ combines the elements of NetScaler Gateway and StoreFront to deliver an integrated experience for end users and administrators.

Functionality	Service/Component providing the functionality
Consistent UI to access apps	StoreFront on-premises/Citrix Workspace app
SSO to SaaS and Web apps	NetScaler® Gateway
Multifactor Authentication (MFA) and device posture (aka End-Point Analysis)	NetScaler Gateway
Security controls and App protection controls for web and SaaS apps	Citrix Enterprise Browser™
Authorization policies	Secure Private Access
Access enforcement	NetScaler Gateway and Citrix Secure Access™ clients

Functionality	Service/Component providing the functionality
Configuration and Management	Secure Private Access
Visibility, Monitoring, and Troubleshooting	Secure Private Access, NetScaler Console (formerly ADM), and Citrix Director

Components

This illustration shows the components of a typical Secure Private Access deployment.



For information about each component, see Key components.

Release notes

September 6, 2025

Fixed issues

August 18, 2025

The following issue is addressed in release 2507.

Domain Controller configuration

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.

[SPAOP-2031]

Known issues

September 6, 2025

The following issues exist in release 2507.

> **Note:**
>
> Some issues are assigned a tracking ID for internal reference only and these do not have any impact on the customer.

Director UI

When multiple applications are launched within a session, only the initially launched application is displayed in the Director UI. Subsequent application launches are not shown in the monitoring interface.

[SPAOP-8483]

Policy Modeling tool

User names are not populated in the **Access Policies > Policy Modeling** tool for administrators with the Read Only Administrator role.

Workaround: To display user names for these administrators, ensure that the **General** service is also enabled for the Read Only Administrator role.

Domain Controller configurations

- 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 an identity in the IIS Application pool for both the Secure Private Access admin and runtime service.

[SPAOP-1558]

- Distribution groups are not supported in Secure Private Access. Therefore, policies cannot search for distribution 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 and hence the apps are not enumerated. For details, see When using StoreFront version 2311 or later.

  [SPAOP-2487]

Application launch

- Application launch fails if LDAP UPN and sAMAccountName are different.

  [SPAOP-1412]

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. For information on StoreFront configuration, see StoreFront.
- 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.

Upgrade

- After the database upgrade, the module/section tabs in the UI do not appear for some time (approximately an hour).

  Workaround: Manually restart the IIS service if you want the tabs in the UI to be visible immediately after the database upgrade.

  [SPAOP-5331]

- When attempting to upgrade versions 2402 or later to 2507 by replacing the MSI, the Secure Private Access tile in the Citrix Virtual Apps and Desktops™ installer shows **Upgrade available**. However, clicking the Secure Private Access tile to proceed with the upgrade results in Secure Private Access being uninstalled instead of being upgraded. The **Core Components** page displays the message "**Secure Private Access will be removed**.

  [SPAOP-5495]

- You cannot upgrade the Secure Private Access plug-in from earlier versions to 2507 if the plug-in was installed using the Delivery Controller.

  [SPAOP-4505]

User interface

- The **Application launch count** counter in the **Secure Private Access > Overview** page is not incremented for TCP/UDP apps.

  [SPAOP-4201]

System requirements

September 6, 2025

Ensure that your product meets the minimal version requirements.

Product	Minimum version
Citrix Workspace™ app	Windows –2403 and later macOS –2402 and later
StoreFront™	LTSR 2203 or CR 2212 and later
NetScaler	13.1, 14.1, and later. It is recommended to use the latest builds of the NetScaler Gateway version 13.1 or 14.1 for optimized performance. For TCP/UDP apps - 14.1–25.56 and later
NetScaler FIPS	13.1-37.219 and later FIPS builds
Citrix Secure Access client	Windows - 24.6.1.17 and later macOS - 24.06.2 and later Linux - 24.10.1 and later
Director	2402 or later
Operating system for Secure Private Access plug-in server	Windows Server 2019 and later

Communication ports: Ensure that you have opened the required ports for the Secure Private Access plug-in. For details, see Communication ports.

Databases: The following is the list of supported Microsoft SQL server versions for the site configuration, configuration logging, and monitoring databases:

- SQL Server 2022, Express, Standard, and Enterprise Editions.

- SQL Server 2019, Express, Standard, and Enterprise Editions.
- SQL Server 2017, Express, Standard, and Enterprise Editions.

For new installations: By default, SQL Server Express 2017 with Cumulative Update 16 is installed when installing the Controller, if an existing supported SQL Server installation is not detected.

For upgrades, any existing SQL Server Express version is not upgraded.

The following database high availability solutions are supported (except for SQL Server Express, which supports only standalone mode):

- SQL Server Always On Failover Cluster Instances
- SQL Server AlwaysOn Availability Groups (including Basic Availability Groups)
- SQL Server Database Mirroring

Windows authentication is required for connections between the Controller and the SQL Server site database.

For more information about the databases, see Databases.

> **Note:**
>
> - The Secure Private Access for on-premises is not supported on Citrix Workspace app for iOS and Android.
> - The Citrix Secure Access client for Linux, iOS, and Android does not support Secure Private Access on-premisesTCP/UDP apps.

Prerequisites

For creating or updating an existing NetScaler® Gateway, ensure that you have the following details:

- A Windows server machine with IIS running, configured with a SSL/TLS certificate, on which the Secure Private Access plug-in will be installed.
- StoreFront store URLs to enter during the setup.
- Store on StoreFront must have been configured and the Store service URL must be available. The format of the Store service URL is `https://store.domain.com/Citrix/StoreSecureAccess`.
- NetScaler Gateway IP address, FQDN, and NetScaler Gateway Callback URL.
- IP address and FQDN of the Secure Private Access plug-in host machine (or a load balancer if the Secure Private Access plug-in is deployed as a cluster).
- Authentication profile name configured on NetScaler.
- SSL server certificate configured on NetScaler.
- Domain name.

- Certificate configurations are complete. Admins must ensure that the certificate configurations are complete. The Secure Private Access installer configures a self-signed certificate if no certificate is found in the machine. However, this might not always work.

> **Note:**
>
> The Runtime service (secureAccess application in the IIS default website) requires anonymous authentication to be enabled as it does not support Windows authentication. These settings are set by the Secure Private Access installer by default and must not be changed manually.

Admin account requirements

The following administrator accounts are required while setting up Secure Private Access.

- Install Secure Private Access: You must be logged in with a local machine administrator account.
- 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.
- Manage Secure Private Access: You must sign into the Secure Private Access admin console with a Secure Private Access administrator account.

Communication ports

The following table lists the communication ports that are used by the Secure Private Access plug-in.

Source	Destination	Type	Port	Details
Admin Workstation	Secure Private Access plug-in	HTTPS	4443	Secure Private Access plug-in - Admin console
Secure Private Access plug-in	NTP Service	TCP, UDP	123	Time synchronization
	DNS Service	TCP, UDP	53	DNS lookup
	Active Directory	TCP, UDP	88	Kerberos

Source	Destination	Type	Port	Details
	Director	HTTP, HTTPS	80, 443	Communication to Director for performance management and enhanced troubleshooting
	License server	TCP	8083	Communication to license server for collecting and processing licensing data
		TCP	389	LDAP over Plaintext (LDAP)
		TCP	636	LDAP over SSL (LDAPS)
	Microsoft SQL Server	TCP	1433	Secure Private Access plug-in - Database communication
	StoreFront	HTTPS	443	Authentication validation
	NetScaler Gateway	HTTPS	443	NetScaler Gateway Callback
StoreFront	NTP Service	TCP, UDP	123	Time synchronization
	DNS Service	TCP, UDP	53	DNS lookup
	Active Directory	TCP, UDP	88	Kerberos
		TCP	389	LDAP over Plaintext (LDAP)
		TCP	636	LDAP over SSL (LDAPS)
		TCP, UDP	464	Native Windows authentication protocol to allow users to change expired passwords

Source	Destination	Type	Port	Details
	Secure Private Access plug-in	HTTPS	443	Authentication and application enumeration
	NetScaler Gateway	HTTPS	443	NetScaler Gateway Callback
NetScaler Gateway	Secure Private Access plug-in	HTTPS	443	Application authorization validation
	StoreFront	HTTPS	443	Authentication and Application enumeration
	Web applications	HTTP, HTTPS	80, 443	NetScaler Gateway communication to configured Secure Private Access applications *(Ports can differ based on the application requirements)*
User Device	NetScaler Gateway	HTTPS	443	Communication between end-user device and NetScaler Gateway

References

- Authentication profiles.
- How Authentication Policies Work.
- Bind an SSL Certificate to a Virtual Server (SSL) on NetScaler.

Sizing guidelines

September 6, 2025

Secure Private Access on-premises databases

The Secure Private Access on-premises database contains information about the applications, policies, and related artwork. It also contains information related to troubleshooting and telemetry.

Due to their dynamic nature, the records for telemetry and troubleshooting undergo frequent changes and are kept for a short period. Therefore, a Secure Private Access on-premises database must be configured considering the need for frequent updates.

During internal scalability testing, the following configuration of Secure Private Access on-premises database was able to handle a 10000-user load.

Component	Specification
Processor	8 vCPU
Memory	16 GB
Network	10 GBPs networking
Host storage	Size: 127 GB IOPS: 500 Maximum throughput: 100
Operating system	Windows Server 2022
SQL Server	SQL Server 2022 CU12
Daily database space used for 10000 users	5 GB

> **Note:**
>
> - The metrics are derived based on the assumption that the log 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, see Settings to retain event logs.

Decision server sizing

The scalability of Secure Private Access on-premises server depends on the database used. The database stores telemetry and troubleshooting information. The database's scale depends on memory, disk speed, and the number of CPUs used to process the load.

During the internal scalability testing, it was confirmed that the following configuration of 3 Secure Private Access on-premises nodes was able to handle a 10000-user load.

Component	Specification
Processor	4 vCPU
Memory	8 GB
Network	10 GBPs
Host storage	Premium SSD LRS Size: 127 GB IOPS: 500 Maximum throughput: 100
Operating system	Windows Server 2022

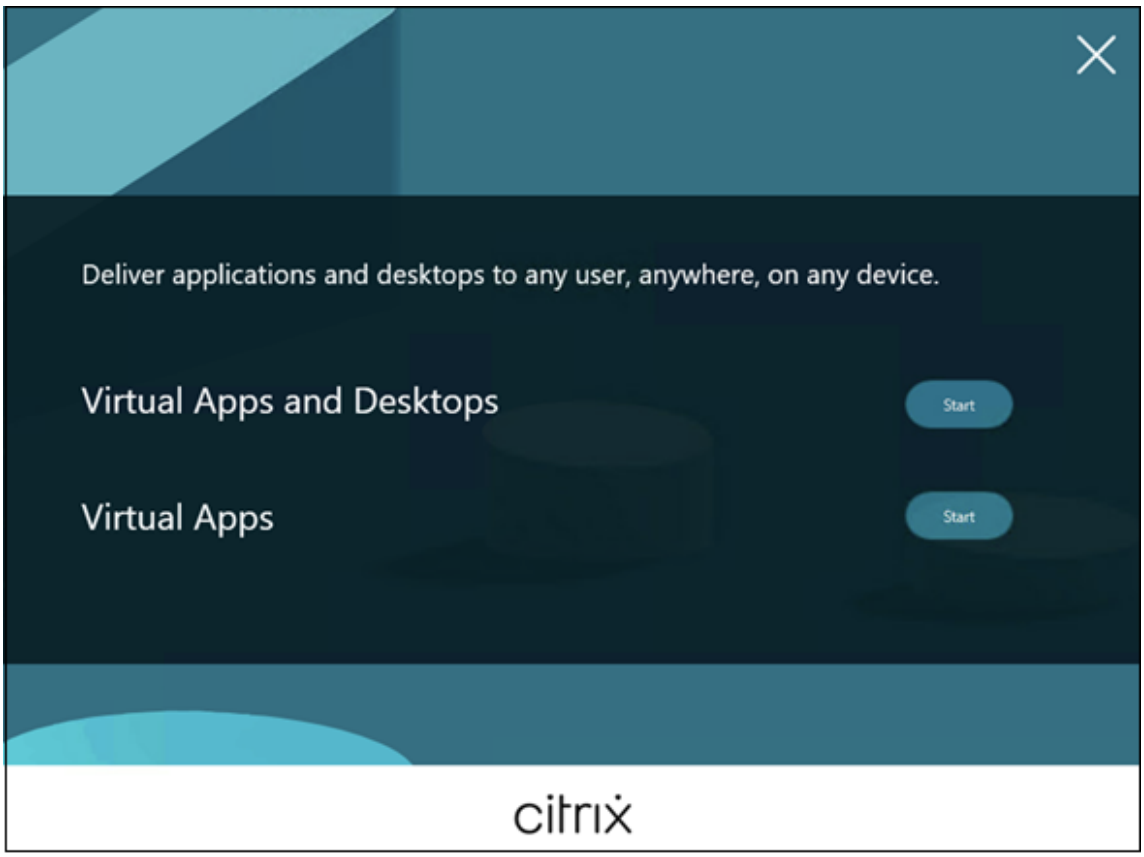
Install Secure Private Access

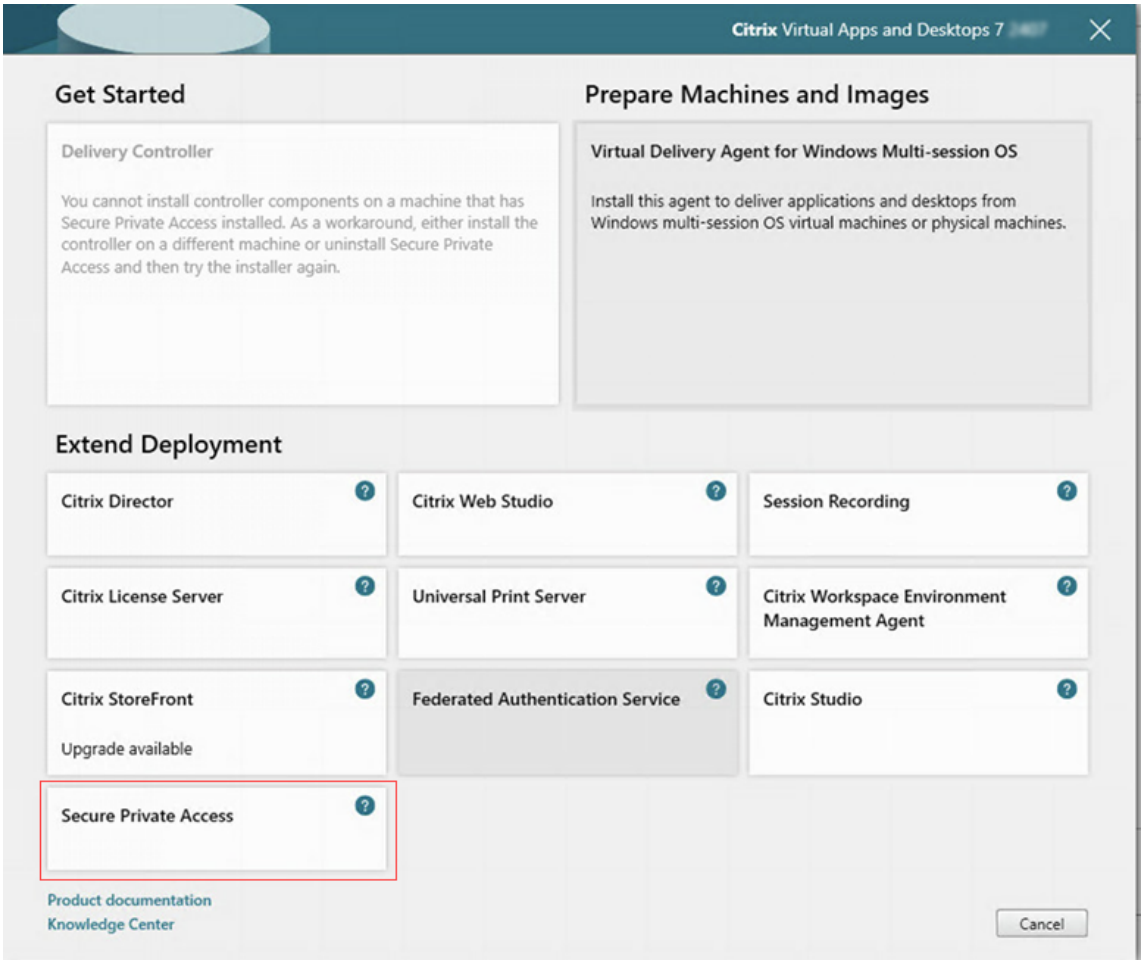
September 6, 2025

The Secure Private Access installer is part of the integrated Citrix Virtual Apps and Desktops™ installer.

Perform the following steps to install Secure Private Access:

1. Download the Citrix Virtual Apps and Desktops product software from https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/ and launch the wizard.
2. Click **Start** next to **Virtual Apps or Virtual Apps and Desktops**.
3. Choose **Secure Private Access** and follow the on-screen instructions to complete the installation.

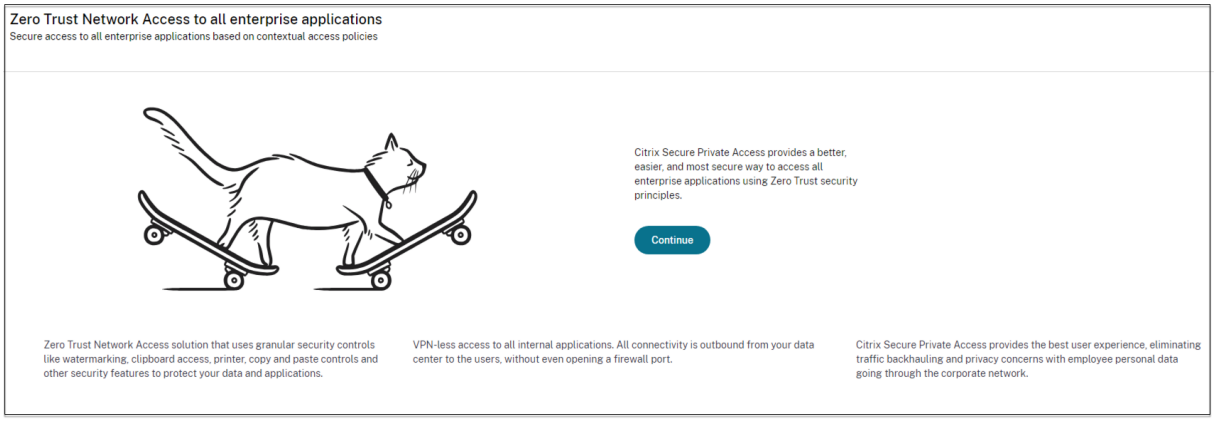




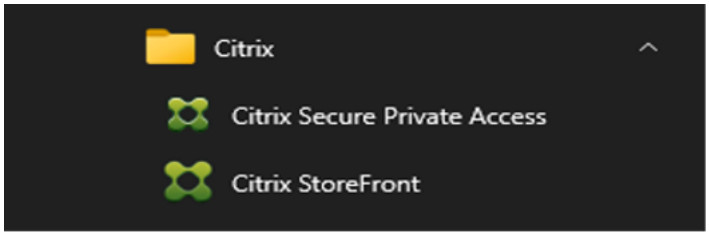
For detailed instructions, see the following topics:

- Install core components.
- Install using the command line.

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™)**.



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.

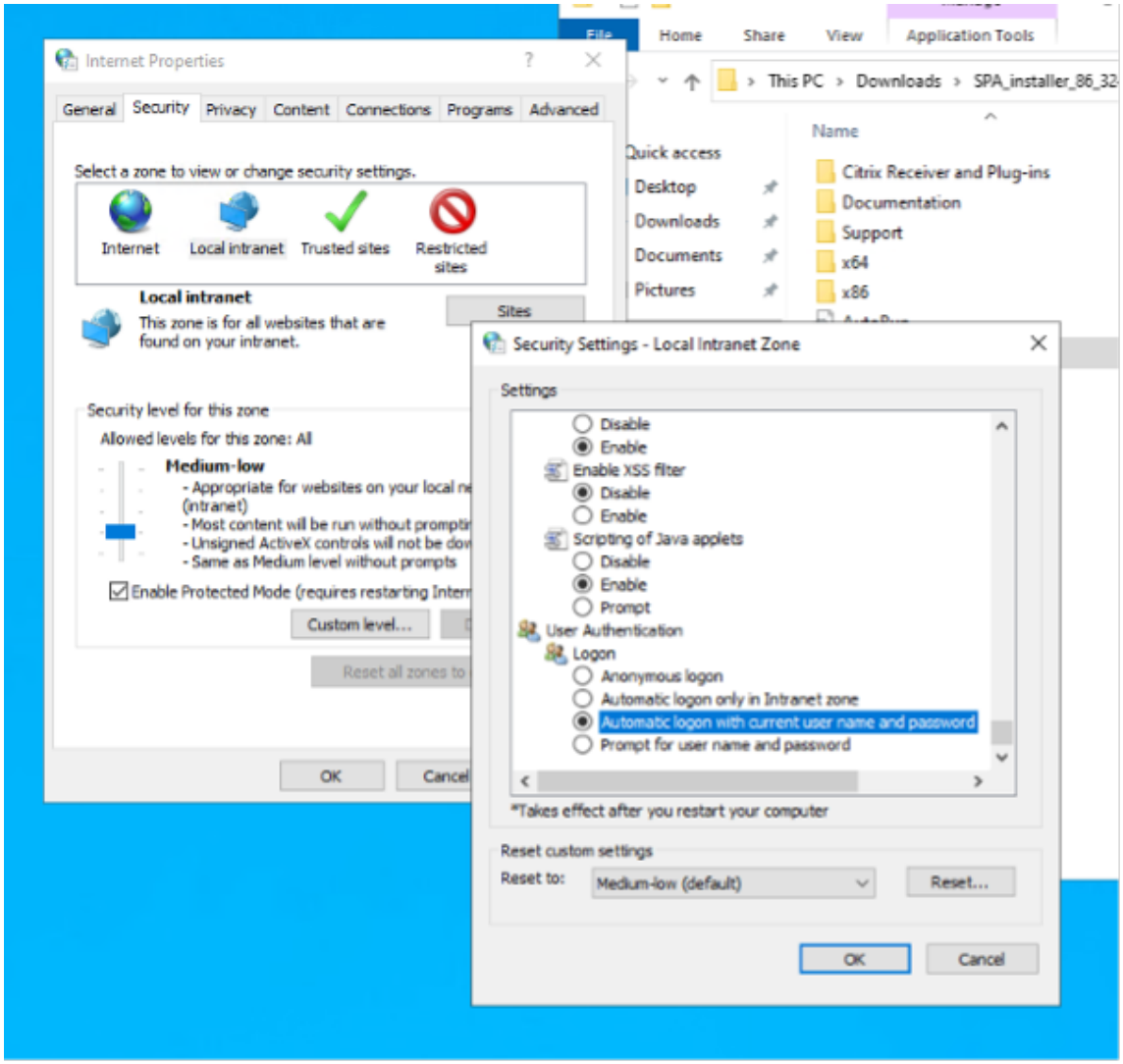
- If you enter your credentials, you enable Integrated Windows Authentication (IWA) sign on.
- If you do not enter your credentials, you're presented with the Secure Private Access sign-on page.

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.

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**.
5. 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.
- 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

Components

September 6, 2025

The following are the key components in a typical Secure Private Access for on-premises deployment.

- **StoreFront:** - StoreFront authenticates users and manages stores of desktops and applications that users access. It can host your enterprise application store, which gives users self-service access to the desktops and applications that you make available to them. It also tracks users' application subscriptions, shortcut names, and other data. This helps ensure that users have a consistent experience across multiple devices. For details about the integration of StoreFront with Secure Private Access, see StoreFront.
- **NetScaler Gateway:** - NetScaler Gateway provides a single secure point of access through the corporate firewall. For details about the integration of NetScaler Gateway with Secure Private Access, see NetScaler Gateway.
- **Director:** (Optional) Director enables you for effective performance monitoring and troubleshooting. To integrate Director with Secure Private Access, you must enter the IP address of the FQDN of the Director server that must be registered with Secure Private Access. For details about the integration of Director with Secure Private Access, see Secure Private Access integration with Director.
- **License Server:** License server collects and processes licensing data. For details about the integration of license server with Secure Private Access, see License Server integration with Secure Private Access.
- **Web Studio:** (Optional) Citrix Secure Private Access is integrated into the Web Studio console to enable users seamlessly access the service through Web Studio. For details about the Secure Private Access integration with Web Studio, see Secure Private Access integration with Web Studio.

For information about the minimum versions requirements of these products, see System requirements.

> **Note:**
>
> Director and License Server are integrated with Secure Private Access starting from release 2402.

StoreFront

September 6, 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**).

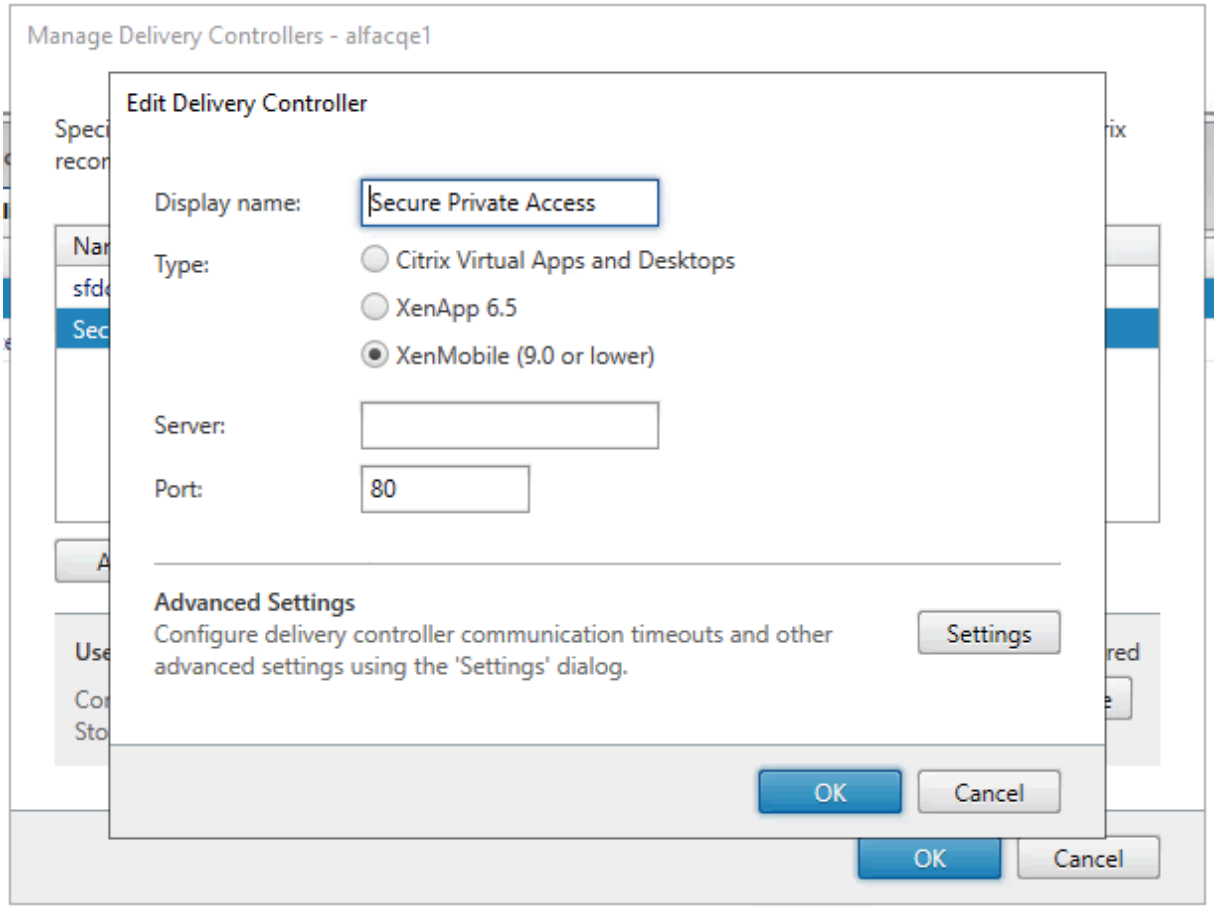
> **Important:**
>
> - It is recommended to use the StoreFront script downloaded from the Secure Private Access admin UI to configure StoreFront for Secure Private Access only. Do not configure Secure Private Access from the StoreFront admin UI as the UI does not cover all the required configuration 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 (either 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 dur-

> ing 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.



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.

NetScaler Gateway

September 6, 2025

NetScaler Gateway configuration is supported for both Web/SaaS and TCP/UDP applications. You can create a NetScaler Gateway or update an existing NetScaler Gateway configuration for Secure Private Access. It is recommended that you create NetScaler snapshots or save the NetScaler configuration before applying these changes.

For details on NetScaler Gateway configurations for Web/SaaS and TCP/UDP applications, see the following topics:

- NetScaler Gateway configuration for Web/SaaS applications
- NetScaler Gateway configuration for TCP/UDP applications

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™ 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

> **Note:**
>
> - The information provided in this section is applicable only if your NetScaler Gateway version is before 14.1-25.56.
> - If your NetScaler Gateway version is 14.1–25.56 and later, then you can enable the Secure Private Access plug-in on NetScaler Gateway by using the CLI or GUI. For details, see Enable Secure Private Access plug-in on NetScaler Gateway.

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

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

Configure Secure Private Access toggles

The following table lists the toggles that must be used to support smart access tags for on-premises deployments:

Toggle name	Description
nsapimgr_wr.sh -ys call=ns_vpn_enable_spa_onprem	Enable Secure Private Access for on-premises deployments
`nsapimgr_wr.sh -ys call= ns_vpn_disable_spa_onprem`	Disable Secure Private Access for on-premises deployments
`nsapimgr_wr.sh -ys ns_vpn_enable_spa_tcp_udp_apps=3`	Enable TCP/UDP apps
`nsapimgr_wr.sh -ys ns_vpn_enable_spa_tcp_udp_apps=0`	Disable TCP/UDP apps
`nsapimgr_wr.sh -ys call= toggle_vpn_enable_securebrowse_client_mode`	Enable SecureBrowse client mode for HTTP callout config
`nsapimgr -ys call= toggle_vpn_redirect_to_access_restricted_page_on_deny`	Enable redirection to the “Access restricted” page if access is denied
`nsapimgr -ys call= toggle_vpn_use_cdn_for_access_restricted_page`	Use the “Access restricted”page hosted on CDN.

Note:

- To disable the toggles that do not have separate disable commands, run the same command again. This is applicable only for commands that have “toggle”in the command.
- To verify whether the toggle is on or off run the `nsconmsg` command.
- To configure smart access tags on NetScaler Gateway, see Configure contextual tags.

Persist Secure Private Access plug-in settings on NetScaler

To persist the Secure Private Access plug-in settings on NetScaler, do the following:

1. Create or update the file /nsconfig/rc.netscaler.
2. Add the following commands to the file.

```
nsapimgr -ys call=ns_vpn_enable_spa_onprem
nsapimgr -ys call=toggle_vpn_enable_securebrowse_client_mode
nsapimgr -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny

nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page
```

3. Save the file.

The Secure Private Access plug-in settings are automatically applied when NetScaler is restarted.

Enable Secure Private Access plug-in on NetScaler Gateway

Starting from NetScaler Gateway 14.1–25.56 and later, you can enable the Secure Private Access plug-in on NetScaler Gateway by using the NetScaler Gateway CLI or the GUI. This configuration replaces the `nsapimgr_wr.sh -ys call=ns_vpn_enable_spa_onprem` knob used in versions before 2407.

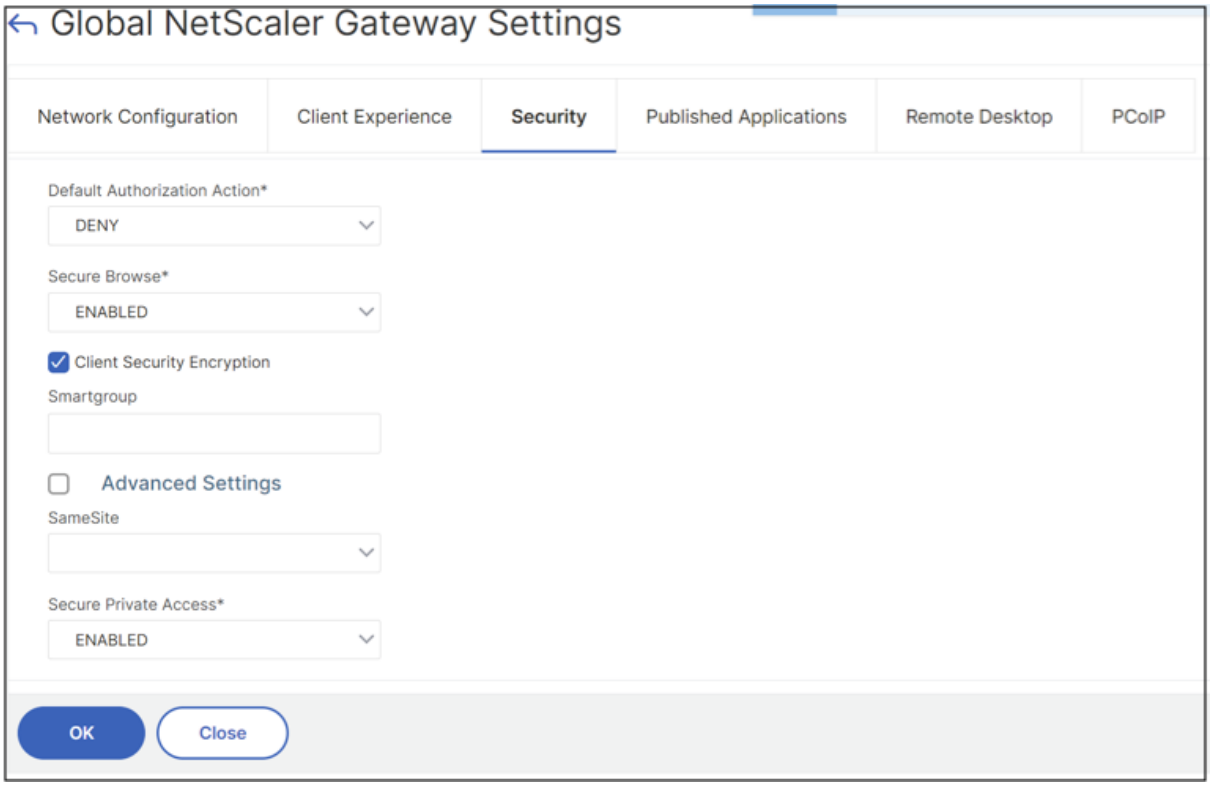
CLI:

At the command prompt, type the following command:

```
set vpn parameter -securePrivateAccess ENABLED
```

GUI:

1. Navigate to **NetScaler Gateway > Global Settings > Change Global NetScaler Gateway Settings**.
2. Click the **Security** tab.
3. In **Secure Private Access**, select **ENABLED.**



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")
3. Run the following command:

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

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.

- 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. For details on the ports, see Communication 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.

NetScaler Gateway configuration for Web/SaaS applications

September 6, 2025

To create NetScaler Gateway for Web/SaaS applications, perform the following steps:

1. Download the latest script *`ns_gateway_secure_access.sh`*. from https://www.citrix.com/downloads/citrix-secure-private-access/Shell-Script/.
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`*.

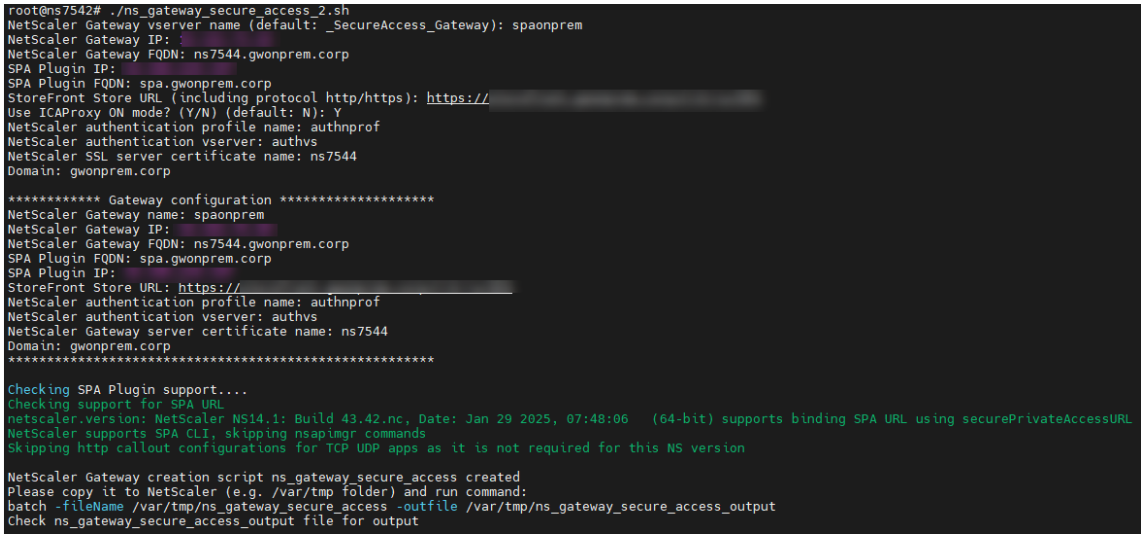
   For example, *`scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp`*

   > **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 the authentication profile and SSL certificate you have to provide names of existing resources on NetScaler.

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

   > **Note:**
   >
   > During script execution, NetScaler and Secure Private Access plug-in compatibility is checked. If NetScaler supports the Secure Private Access plug-in, the script enables NetScaler features to support smart access tags sending improvements and redirection to a new Deny Page when access to a resource is restricted. For details about smart tags, see Support for smart access tags.
   >
   > The Secure Private Access plug-in features persisted in the /nsconfig/rc.netscaler file allow to keep them enabled after NetScaler is restarted.

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.

Update existing NetScaler Gateway configuration for Web and SaaS apps

You can use the `ns_gateway_secure_access_update.sh`script on an existing NetScaler Gateway to update the configuration for Web and SaaS apps. However, if you want to update the existing configuration (NetScaler Gateway version 14.1–4.42 and later) manually, use the Example commands to update an existing NetScaler Gateway configuration. Also, you must update the NetScaler Gateway virtual server and session action settings.

> **Note:**
>
> Starting from NetScaler Gateway 14.1–25.56 and later, you can enable the Secure Private Access plug-in on NetScaler Gateway by using the NetScaler Gateway CLI or the GUI. For details, see Enable Secure Private Access plug-in on NetScaler Gateway.

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.

NetScaler Gateway virtual server settings

When you add or update the existing NetScaler Gateway virtual server, ensure that the following parameters are set to the defined values. For sample commands, see Example commands to update an existing NetScaler Gateway configuration.

Add a virtual server:

- tcpProfileName: nstcp_default_XA_XD_profile
- deploymentType: ICA_STOREFRONT (available only with the `add vpn vserver` command)
- icaOnly: OFF

Update a virtual server:

- tcpProfileName: nstcp_default_XA_XD_profile
- icaOnly: OFF

NetScaler Gateway session actions settings

Session action is bound to a gateway virtual server with session policies. When you create or update a session action, ensure that the following parameters are set to the defined values. For sample commands, see Example commands to update an existing NetScaler Gateway configuration.

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

> **Note:**
>
> Starting from NetScaler Gateway release 14.1 build 43.x and later, ICA Proxy mode is supported for Web/SaaS apps.

Example commands when ICA® Proxy is disabled

- Add/update a virtual server.

```
add vpn vserver SecureAccess_Gateway SSL 999.999.999.999 443 -
Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile -
deploymentType ICA_STOREFRONT -vserverFqdn gateway.mydomain.com -
authnProfile auth_prof_name -icaOnly OFF -dtls OFF
```

- Add a session action.

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

- Add a session policy.

```
add vpn sessionPolicy PL_OSspahybrid "HTTP.REQ.HEADER(\"User-Agent\")
.CONTAINS(\"CitrixReceiver\")"AC_OSspahybrid
```

- Bind the session policy to the VPN virtual server.

```
bind vpn vserver SecureAccess_Gateway -policy PL_OSspahybrid -
priority 100 -gotoPriorityExpression NEXT -type REQUEST
```

- Bind the Secure Private Access provider to the VPN virtual server.

```
bind vpn vserver spahybrid -securePrivateAccessUrl "https://spa.
example.corp"
```

For details on session action parameters, vpn-sessionAction.

Example commands when ICA Proxy is enabled

- Add/update a virtual server.


```
add vpn vserver SecureAccessGroup SSL 999.999.999.999 443 -
Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile
-deploymentType ICA_STOREFRONT -vserverFqdn gateway.mydomain.com
-authnProfile auth_prof_name -icaOnly OFF -dtls OFF
```

- Add a session action

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

- Add authorization policies

```
add authorization policy ALLOW_STOREFRONT "(HTTP.REQ.HOSTNAME
.SET_TEXT_MODE(IGNORECASE).STARTSWITH(\"gateway.example..corp
\")|| HTTP.REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE).STARTSWITH
(\"storefront.example.corp\"))&& (HTTP.REQ.URL.SET_TEXT_MODE(
IGNORECASE).STARTSWITH(\"/Citrix\")|| HTTP.REQ.URL.SET_TEXT_MODE(
IGNORECASE).STARTSWITH(\"/AGServices\"))"ALLOW

add authorization policy SECUREACCESS_AUTHORIZATION "(CLIENT.
SSLVPN.MODE.EQ(\"SECURE_BROWSE\")|| HTTP.REQ.HEADER(\"X-Citrix
-AccessSecurity\").EXISTS || HTTP.REQ.HEADER(\"X-Citrix-Secure-
Browser\").EXISTS)&& sys.HTTP_CALLOUT(SecureAccess_httpCallout)"
ALLOW

add authorization policy SECUREACCESS_AUTHORIZATION_ICAPROXY "
CLIENT.SSLVPN.MODE.EQ(\"ICAPROXY\")&& HTTP.REQ.HOSTNAME.SET_TEXT_MODE
(IGNORECASE).STARTSWITH(\"gateway.example.corp\").NOT && HTTP.
REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE).STARTSWITH(\"storefront.
example.corp\").NOT && sys.HTTP_CALLOUT(SecureAccess_httpCallout)
"ALLOW
```

- Bind the secure access authorization policy to the VPN virtual server

```
bind aaa group SecureAccessGroup -policy ALLOW_STOREFRONT -
priority 100 -gotoPriorityExpression END

bind aaa group SecureAccessGroup -policy SECUREACCESS_AUTHORIZATION
 -priority 1000 -gotoPriorityExpression END
```



```
bind aaa group SecureAccessGroup -policy SECUREACCESS_AUTHORIZATION_ICAPRO
 -priority 1100 -gotoPriorityExpression END
```

- Bind the Secure Private Access provider to the VPN virtual server.

```
bind vpn vserver spahybrid -securePrivateAccessUrl "https://spa.
example.corp"
```

Additional information

For additional information on NetScaler Gateway for Secure Private Access, see the following topics:

- Compatibility with the ICA apps
- Support for smart access tags
- Persist Secure Private Access plug-in settings on NetScaler
- Enable Secure Private Access plug-in on NetScaler Gateway
- Upload public gateway certificate
- Known limitations

NetScaler Gateway configuration for TCP/UDP applications

September 6, 2025

You can use the procedure outlined in NetScaler Gateway configuration for Web/SaaS applications to configure TCP/UDP applications.

Update existing NetScaler Gateway configuration for TCP/UDP apps

If you are updating the configuration from earlier versions to 2407, it is recommended that you update the configuration manually. For details, see Example commands to update an existing NetScaler Gateway configuration. Also, you must update the NetScaler Gateway virtual server and session action settings.

NetScaler Gateway virtual server settings

When you add or update the existing NetScaler Gateway virtual server, ensure that the following parameters are set to the defined values. For sample commands, see Example commands to update an existing NetScaler Gateway configuration. Also, you must update the NetScaler Gateway virtual server and session action settings.

Add a virtual server:

- tcpProfileName: nstcp_default_XA_XD_profile
- deploymentType: ICA_STOREFRONT (available only with the `add vpn vserver` command)
- icaOnly: OFF

Update a virtual server:

- tcpProfileName: nstcp_default_XA_XD_profile
- icaOnly: OFF

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

NetScaler Gateway session policy settings

Session action is bound to a gateway virtual server with session policies. When you create or update a session action, ensure that the following parameters are set to the defined values. For sample commands, see Example commands to update an existing NetScaler Gateway configuration. Also, you must update the NetScaler Gateway virtual server and session action settings.

- `transparentInterception`: ON
- `SSO`: ON
- `ssoCredential`: PRIMARY
- `useMIP`: NS
- `useIIP`: OFF
- `icaProxy`: OFF
- `ClientChoices`: ON
- `ntDomain`: mydomain.com - used for SSO (optional)
- `defaultAuthorizationAction`: ALLOW
- `authorizationGroup`: SecureAccessGroup
- `clientlessVpnMode`: OFF
- `clientlessModeUrlEncoding`: TRANSPARENT
- `SecureBrowse`: ENABLED

Example commands to update an existing NetScaler Gateway configuration

> **Note:**
>
> If you are manually updating the existing configuration, then in addition to the following commands, you must update the /nsconfig/rc.netscaler file with the command `nsapimgr_wr.sh -ys ns_vpn_enable_spa_tcp_udp_apps=3`.

- Add a VPN session action to support Citrix Secure Access-based connections.

```
add vpn sessionAction AC_AG_PLGspaonprem -splitDns BOTH -splitTunnel
 ON -transparentInterception ON -defaultAuthorizationAction ALLOW
 -authorizationGroup SecureAccessGroup -SSO ON -ssoCredential
PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF -ClientChoices ON -
ntDomain example.corp -clientlessVpnMode OFF -clientlessModeUrlEncoding
 TRANSPARENT -SecureBrowse ENABLED
```

- Add a VPN session policy to support Citrix Secure Access-based connections.

```
add vpn sessionPolicy PL_AG_PLUGINspaonprem "HTTP.REQ.HEADER
(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT && (HTTP.REQ
.HEADER(\"User-Agent\").CONTAINS(\"plugin\")|| HTTP.REQ.HEADER(\"
User-Agent\").CONTAINS(\"CitrixSecureAccess\"))"AC_AG_PLGspaonprem
```

- Bind the session policy to the VPN virtual server to support Citrix Secure Access-based connections.

```
bind vpn vserver spaonprem -policy PL_AG_PLUGINspaonprem -priority
 105 -gotoPriorityExpression NEXT -type REQUEST
```

- Add an HTTP callout policy to support authorization validation for TCP/UDP based connections.

> **Note:**
>
> This step is required only if your NetScaler Gateway version is lower than 14.1-29.x.

```
add policy httpCallout SecureAccess_httpCallout_TCP -IPAddress
192.0.2.24 -port 443 -returnType BOOL -httpMethod POST -hostExpr
 "\"spa.example.corp\""-urlStemExpr "\"/secureAccess/authorize\"
"-headers Content-Type("application/json")X-Citrix-SecureAccess-
Cache("dstip="+HTTP.REQ.HEADER("CSIP").VALUE(0)+"&sessid="+aaa.
user.sessionid)-bodyExpr q/"{ "+"\"userName\":\""+aaa.USER.NAME
.REGEX_REPLACE(re#\\\#,"\\\\\",ALL)+"\","+"\"domain\":\""+aaa.
USER.DOMAIN+"\","+"\"customTags\":\""+http.REQ.HEADER("X-Citrix
-AccessSecurity").VALUE(0)+"\","+"\"gatewayAddress\":\"ns224158
.example.corp\","+"\"userAgent\":\"CitrixSecureAccess\","+"\"
applicationDomain\":\""+http.REQ.HEADER("CSHOST").VALUE(0)+"\",
"+"\"smartAccessTags\":\""+aaa.user.attribute("smartaccess_tags
")+"\",\"applicationType\":\"ztna\",\"applicationDetails\":{
\"destinationIp\":\""+HTTP.REQ.HEADER("CSIP").VALUE(0)+"\",\"
destinationPort\":\""+HTTP.REQ.HEADER("PORT").VALUE(0)+"\",\"
```



```
protocol\":\"TCP\" } } "/ -scheme https -resultExpr "http.RES.
HEADER(\"X-Citrix-SecureAccess-Decision\").contains(\"ALLOW\")"
```

where

- **192.0.2.24** is the Secure Private Access plug-in IP address
- **spa.example.corp** is the FQDN of the Secure Private Access plug-in
- **ns224158.example.corp** is the FQDN of the gateway VPN virtual server

- Add an authorization policy to support TCP/UDP based connections.

```
add authorization policy SECUREACCESS_AUTHORIZATION_TCP "HTTP.REQ
.URL.EQ(\"/cs\")&& HTTP.REQ.HEADER(\"PRTCL\").EQ(\"TCP\")&& sys.
HTTP_CALLOUT(SecureAccess_httpCallout_TCP)"ALLOW
```

- Bind the authorization policy to the authentication and authorization group to support TCP/UDP based applications.

```
bind aaa group SecureAccessGroup -policy SECUREACCESS_AUTHORIZATION_TCP
 -priority 1010 -gotoPriorityExpression END
```

- Bind the Secure Private Access plug-in to the VPN virtual server.

```
bind vpn vserver spaonprem -appController "https://spa.example.
corp"
```

Additional information

For additional information on the NetScaler Gateway for Secure Private Access, see the following topics:

- Compatibility with the ICA apps
- Support for smart access tags
- Persist Secure Private Access plug-in settings on NetScaler
- Enable Secure Private Access plug-in on NetScaler Gateway
- Upload public gateway certificate
- Known limitations

Contextual tags

September 6, 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:**
>
> - Starting from NetScaler Gateway 14.1-25.x and later, nFactor EPA policies are supported.
> - If your NetScaler Gateway version is lower than 14.1-25.x, then only classic gateway preauthentication policies can be configured on NetScaler Gateway.

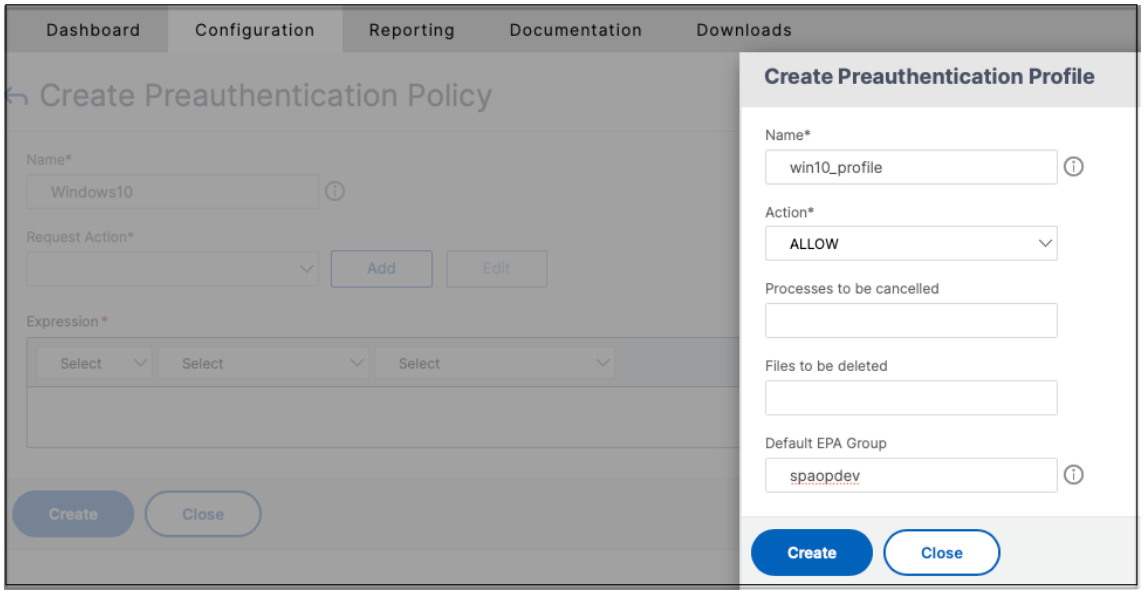
Configure custom tags using the GUI

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

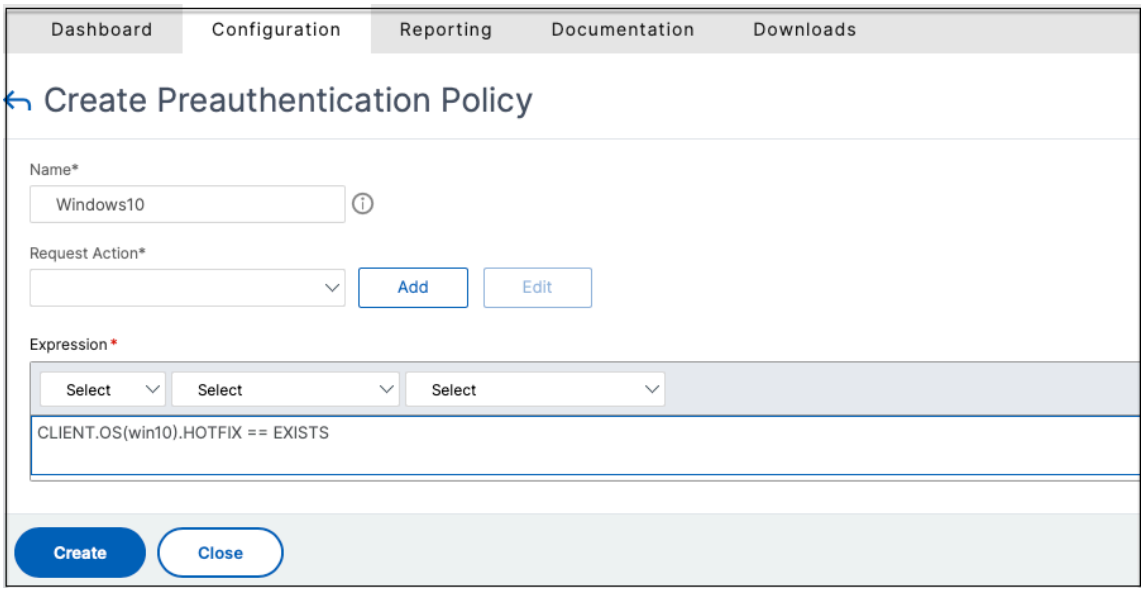
1. Configure a classic gateway preauthentication policy
2. Bind the classic preauthentication policy to the gateway virtual server

Configure a classic gateway preauthentication policy

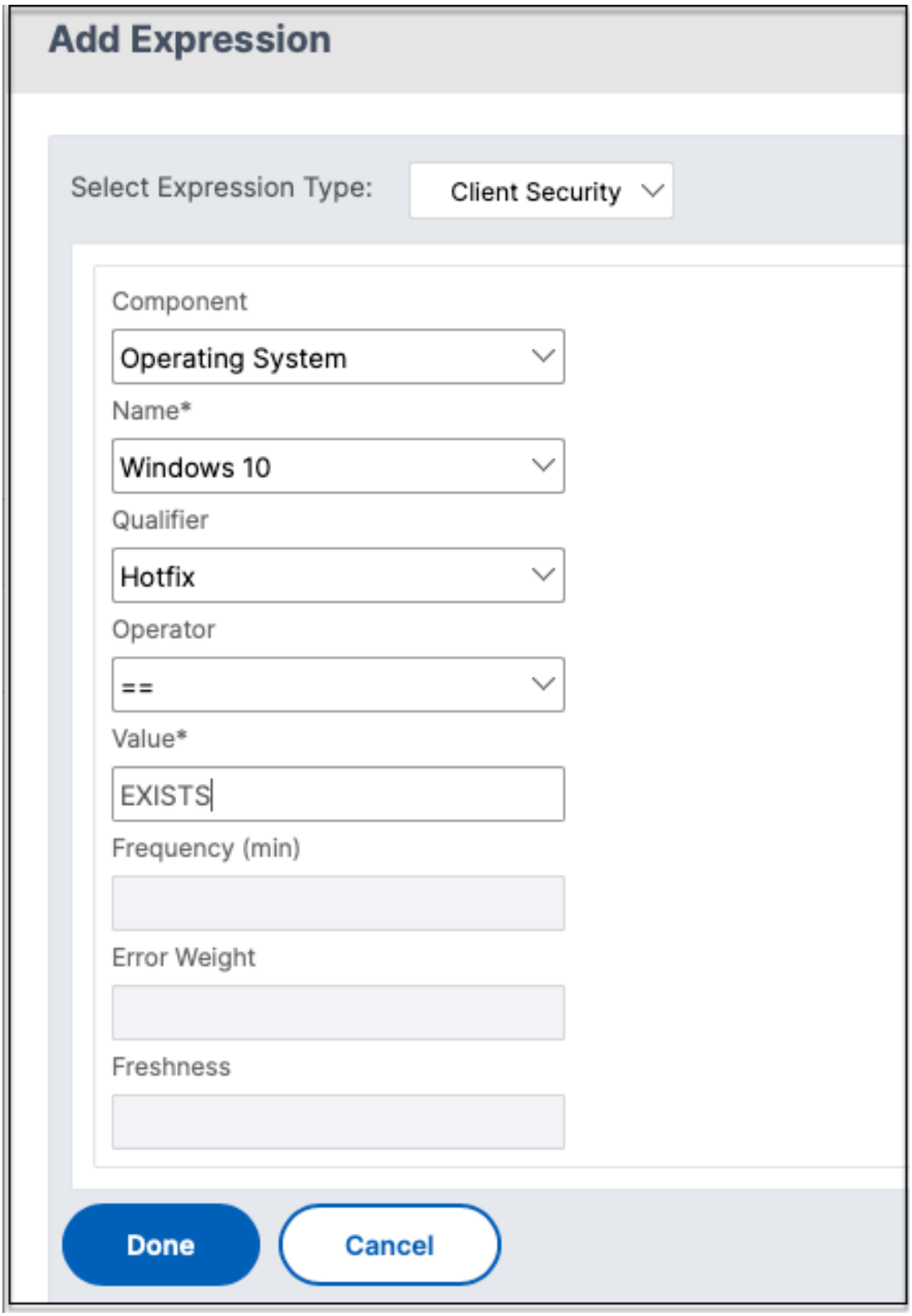
1. Navigate to **NetScaler Gateway > Policies > Preauthentication** and then click **Add**.
2. Select an existing policy or add a name for the policy. This policy name is used as the custom tag value.
3. In **Request Action**, click **Add** to create an action. You can reuse this action for multiple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



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.



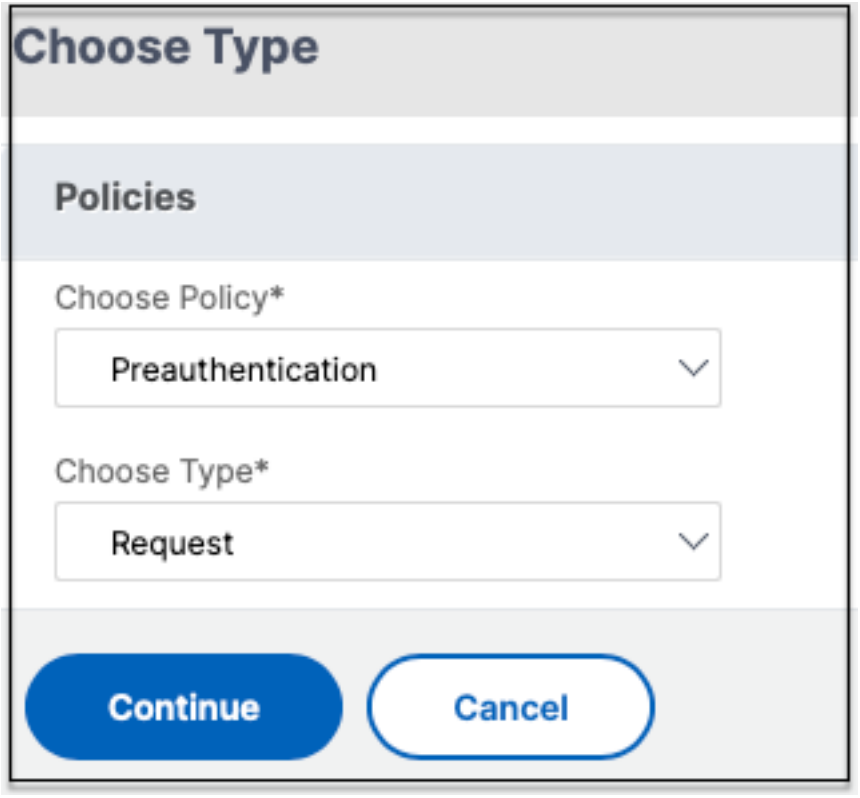
The following figure displays a sample expression constructed for checking the Windows 10 OS.



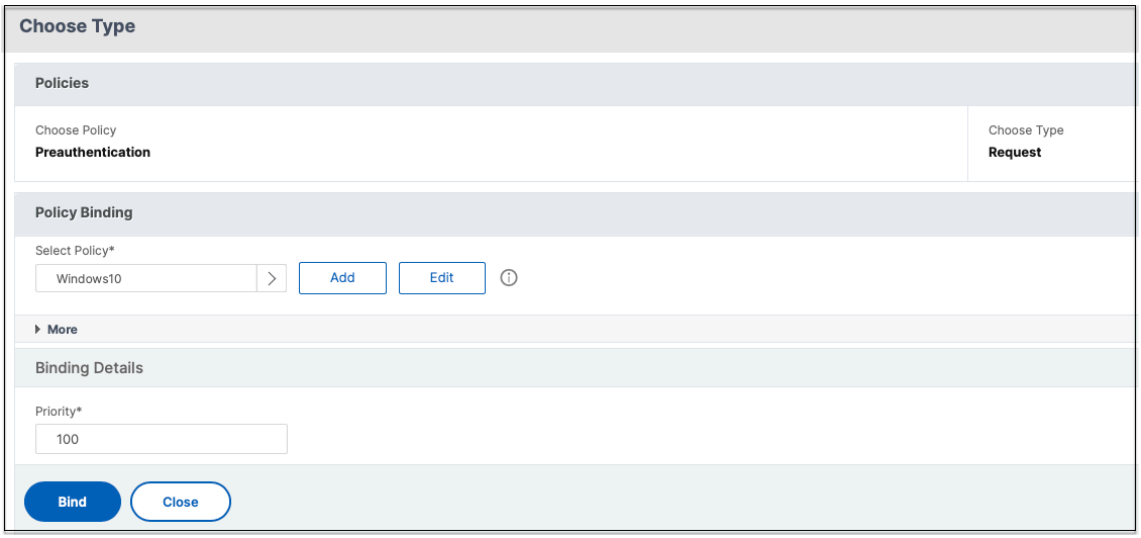
6. Click **Create**.

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**.



Configure custom tags using the CLI

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

- `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`

Run the following sample command on the NetScaler CLI to configure nFactor EPA policy:

- `add authentication epaAction epaallowact -csecexpr "sys.client_expr (\"proc_0_notepad.exe\")"-defaultEPAGroup allow_app -quarantineGroup deny_app`
- `add authentication Policy epaallow -rule true -action epaallowact`

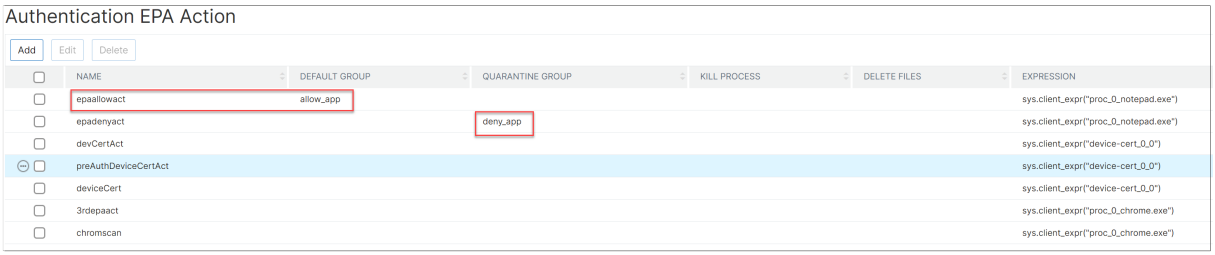
Adding a new contextual tag

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

Note on EPA tags sent to Secure Private Access plug-in

The EPA action name configured in nFactor EPA policy and the associated group name as smart access tags to the Secure Private Access plug-in. However, the tags that are sent are dependent on the outcome of the EPA action evaluation.

- If all EPA actions in an nFactor EPA policy results in action **DENY** and a quarantine group is configured in the last action, the quarantine group name is sent as the smart access.
- If an EPA action in an nFactor EPA policy results in action **ALLOW**, the EPA policy names associated with the action and the default group name (if configured) are sent as the smart access tags.



In this example, when the action is denied, *deny_app* is sent as the smart access tag to the Secure Private Access plug-in. When the action is allowed, *epaallowact* and *allow_app*, are sent as the smart access tags to the Secure Private Access plug-in.

References

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

License server

September 6, 2025

A license server for the Secure Private Access plug-in is a mandatory component required to collect and process licensing data. A license server can be registered with Secure Private Access during the initial setup or it can also be configured or updated after the setup is complete. For details about registering a license server with Secure Private Access, see Integrate StoreFront and NetScaler Gateway servers.

You must specify the license server URL to connect Secure Private Access with the license server. The Secure Private Access plug-in automatically registers itself on the license server.

> **Note:**
>
> - You must install at least one Citrix Virtual Apps and Desktops™ broker license on the license server to register the Secure Private Access plug-in on the license server.
> - License server for the Secure Private Access plug-in is supported from version 11.17.2 build 45000 and later. If you already have a license server, you must upgrade the license server to version 11.17.2 build 45000 version or later.

Configuration tool parameters

The following configuration tool parameters are available for the license server:

- Hashing - `.\AdminConfigTool.exe LICENSE_SERVER_ENABLE_HASHING <true|false>`
- Downloading PII data - `.\AdminConfigTool.exe DOWNLOAD_PII_DATA <filename>`

For more information about the licensing server, see Licensing Server.

Citrix Secure Access client

September 6, 2025

You can now access all private apps including TCP/UDP and HTTPS/HTTP apps either using a native browser or a native client application via the Citrix Secure Access client running on your machine.

With the additional support of TCP/UDP applications within Citrix Secure Private Access, you can now eliminate the dependency on a traditional VPN solution to provide access to all private apps for remote users. For more information, see the Citrix Secure Access document.

Director (Optional)

September 6, 2025

Director integration with Secure Private Access enables effective performance monitoring and troubleshooting. To integrate Director with Secure Private Access, you must enter the IP address of the FQDN of the Director server that must be registered with Secure Private Access. For details, see Integrate servers.

Registering Director with Secure Private Access is a mandatory configuration for the Secure Private Access for on-premises version 2402 customers. If you do not have Director configured, you must install the latest version of Director, LTSR 2402 or later. If you already have Director configured, you must upgrade it to the latest version, LTSR 2402 or later. The Secure Private Access setup cannot be completed without registering a Director. The validation also fails in the following cases.

- Director is not registered with Secure Private Access.
- The Director IP address or the FQDN that you have entered does not exist.

For details about registering Director with Secure Private Access, see Integrate StoreFront and NetScaler Gateway servers and Manage settings after installation.

> **Note:**
>
> - Starting from Secure Private Access 2407 or later, the TCP/UDP sessions are also displayed in addition to the Web/SaaS apps in the Director dashboard.
> - Observability is not supported for Always On machine tunnel sessions. Therefore monitoring and visibility into the activities and performance of these sessions are unavailable.
> - Director registration or logon does not support Integrated Windows Authentication (IWA). If the admin has logged into the Secure Private Access console using IWA, then the admin is prompted to enter the credentials for Director registration.
> - If the admin has done a manual sign-on to the Secure Private Access console, then those details are leveraged for authenticating to the Director server. If that does not succeed, then the admin is prompted to enter the credentials.
> - If the admin has to add a different Director after the setup is complete, register the new Director from the **Manage Settings** page. While updating the Director details after the setup, admins must enter the credentials to make the changes. Single sign-on is not supported for editing the Director URL IPv6, SSLv3.

Configure Director with Secure Private Access using the Director config tool

Configuring Director with Secure Private Access by using the Config tool is a mandatory step for the integration to be complete. For details, see Secure Private Access integration with Director.

View Secure Private Access user sessions in Director

You can view the View Secure Private Access user sessions in Director. For details, see View a Secure Private Access session by user.

Web Studio (Optional)

September 6, 2025

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

To enable this integration, you must install Web Studio version 2308 or later.

For details, see Integration of Secure Private Access with Web Studio.

> **Important:**
>
> For the Secure Private Access 2507 integration into Web Studio, you must manually add the `baseAppServiceUrl` in the Web Studio template file. For example, `"baseAppServiceUrl": "https://<URL>:4443"`. The base app URL is required because all Secure Private Access logs are sent to the base app.

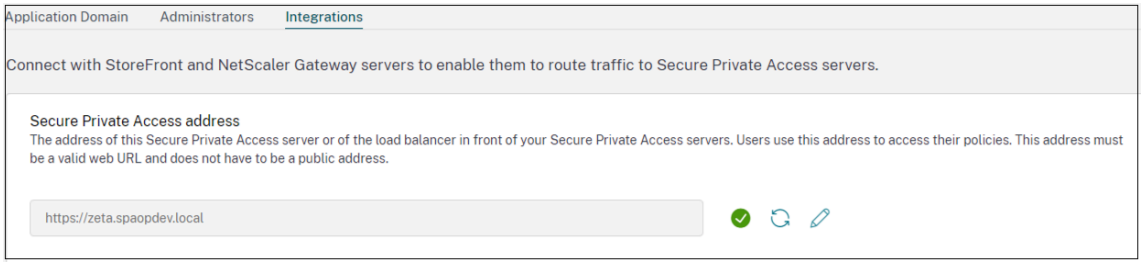
Deploy Secure Private Access as a cluster (Optional)

September 6, 2025

The Secure Private Access on-premises solution can be deployed as a cluster for high availability, high throughput, and scalability. For large deployments (for example, over 5000 users), multiple separate Secure Private Access nodes can be deployed to distribute the workload and enhance scalability.

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.
- While configuring the first node in Secure Private Access, use the load balancer names. To add the subsequent nodes, specify the database address in the Integrations tab and manually run the database script. For details on upgrading the database using scripts, see Upgrade the database using scripts.



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:

- The FQDNs used to access StoreFront are included in the DNS field as subject alternative name (SAN). If you are using a load balancer, then include both the individual server's FQDN and the load balancer FQDN. This is applicable for SSL certificates. For Secure Private Access, configuring a load balancer is sufficient. For details, see Load balancing with NetScaler.
  Before configuring Secure Private Access, the StoreFront Store must be configured. If using a load balancer, configure the base URL with the load balancer name and use HTTPS for secure communication. For details, see Securing StoreFront with HTTPS.
- 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.
- The correct SSL certificate is bound to the IIS server and NetScaler.
- Secure ciphers are used.
- Secure Private Access services (both admin and runtime) are stateless, and so persistency is not required.
- 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:
```



```
4
5   {
6   "status":"OK","details":{
7   "duration":"00:00:00.0084206","status":"OK" }
8    }
```

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

Create monitor for Secure Private Access

Use the following CLI command to create a monitor for Secure Private Access.

```
add lb monitor SPAHealth HTTP -respCode 200 -httpRequest "GET /
secureAccess/health"-secure YES
```

After creating a monitor, bind the certificate to the monitor.

For details about creating monitors using the NetScaler UI, see Create monitors.

Configure Secure Private Access plug-in

September 6, 2025

After you install the Citrix Secure Access plug-in, you can set up the Secure Private Access environment and then configure applications and access policies for applications. Secure Private Access supports Web/SaaS and TCP/UDP apps. 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 (HTTP/HTTPS and TCP/UDP) by enabling the appropriate security restrictions.

- Configure HTTP/HTTPS applications
- Configure TCP/UDP apps
- Configure TCP/UDP - server to client apps
- Configure access policies for the applications
- Access restriction options

Set up Secure Private Access

September 6, 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

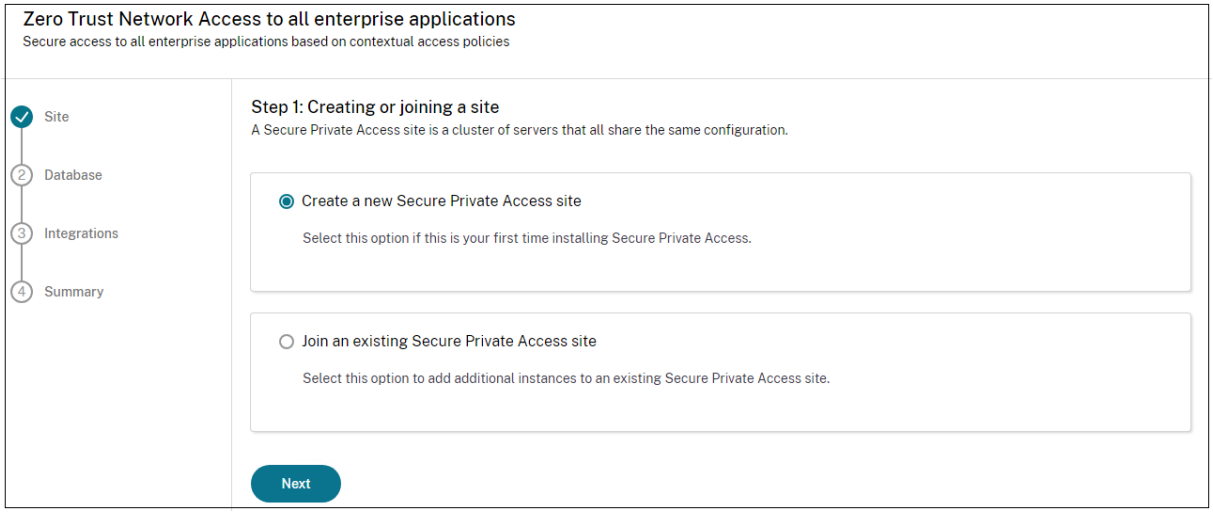
- You must sign into the Secure Private Access admin console with a domain user, which is also a local machine administrator for the machine where Secure Private Access is installed.
- The SQL database server must be installed before creating a site.
- If you have multi-domain environments, ensure to establish domain trust between the Active Directory domains located in different forests. For details, see Multi-domain environments.

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**.



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:

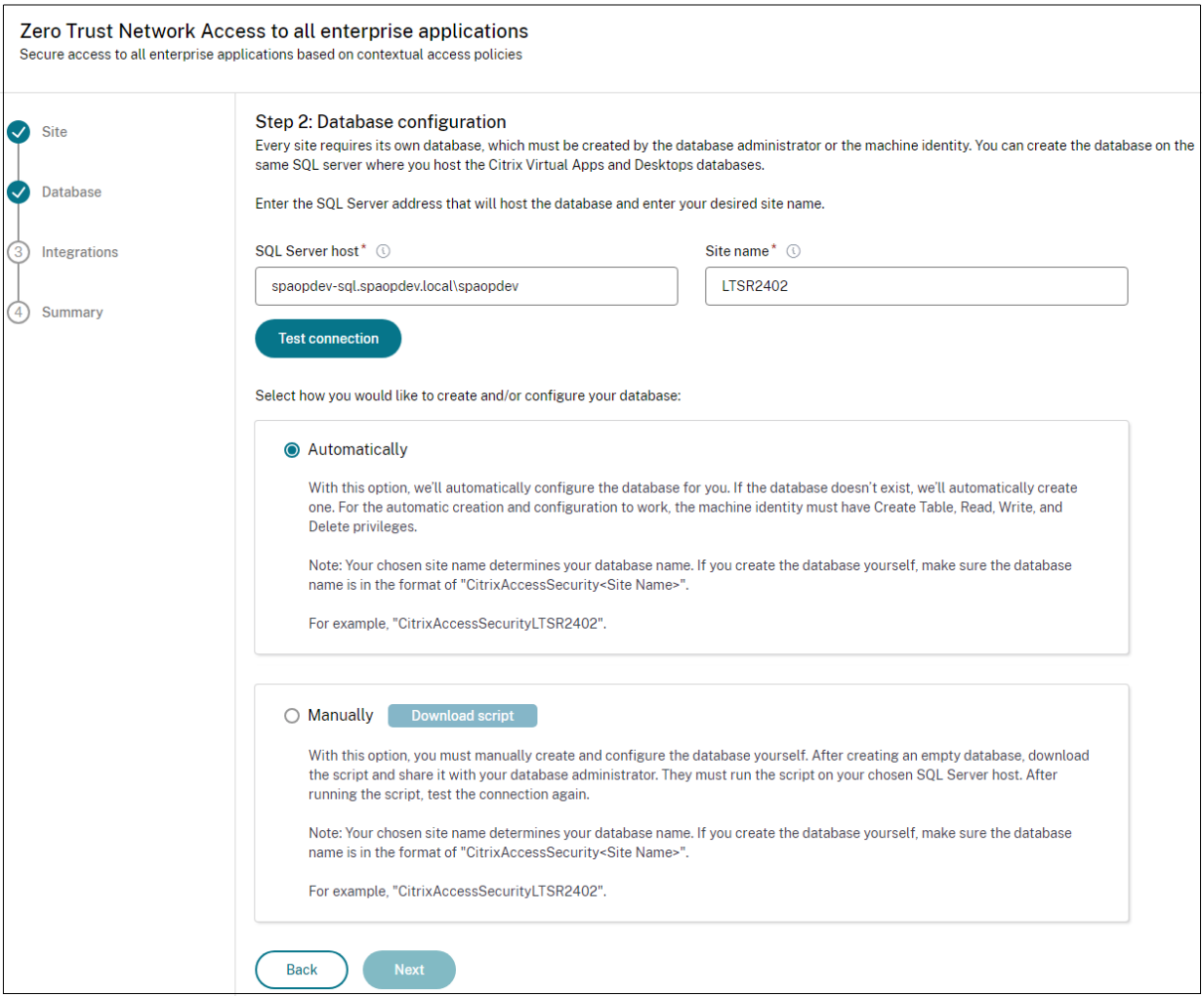
   - ServerName
   - ServerName\InstanceName
   - ServerName,PortNumber

   For more information, see Databases.

2. In **Site**, type a name for the Secure Private Access site.

   > **Note:**
   >
   > The site name that you enter is suffixed to the database name. The database name format is `CitrixAccessSecurity<sitename>` and cannot be modified. If you must customize the database name, contact Citrix Support.

3. Click **Test connection** to check that the SQL server instance is valid and also to confirm that the specified database exists for the site.



> **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.

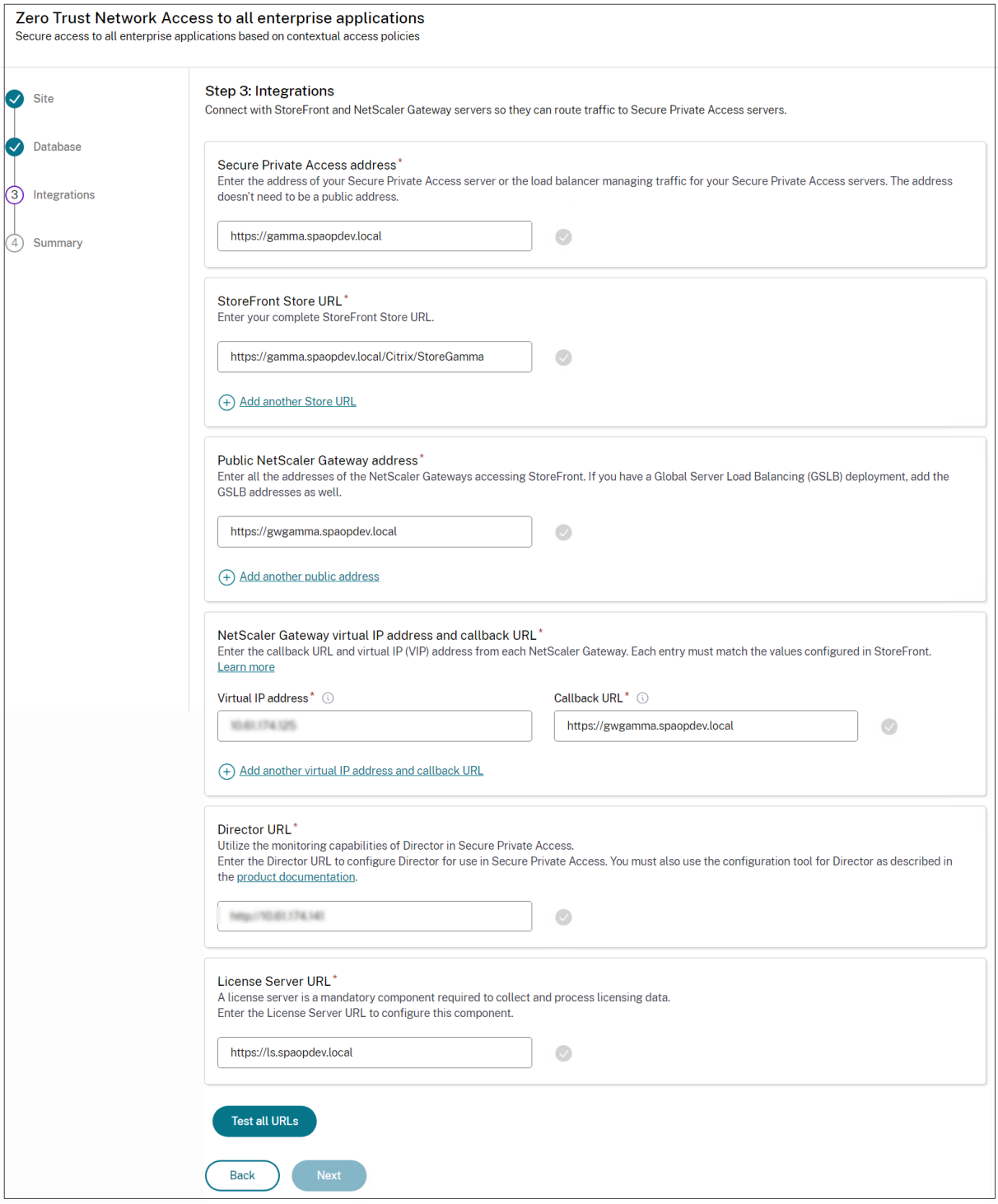
In manual configuration, you must first download the scripts and then run the scripts on the database server that you have specified in the **SQL Server Host** field.

> **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 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. You must also specify the Director server and license server details.

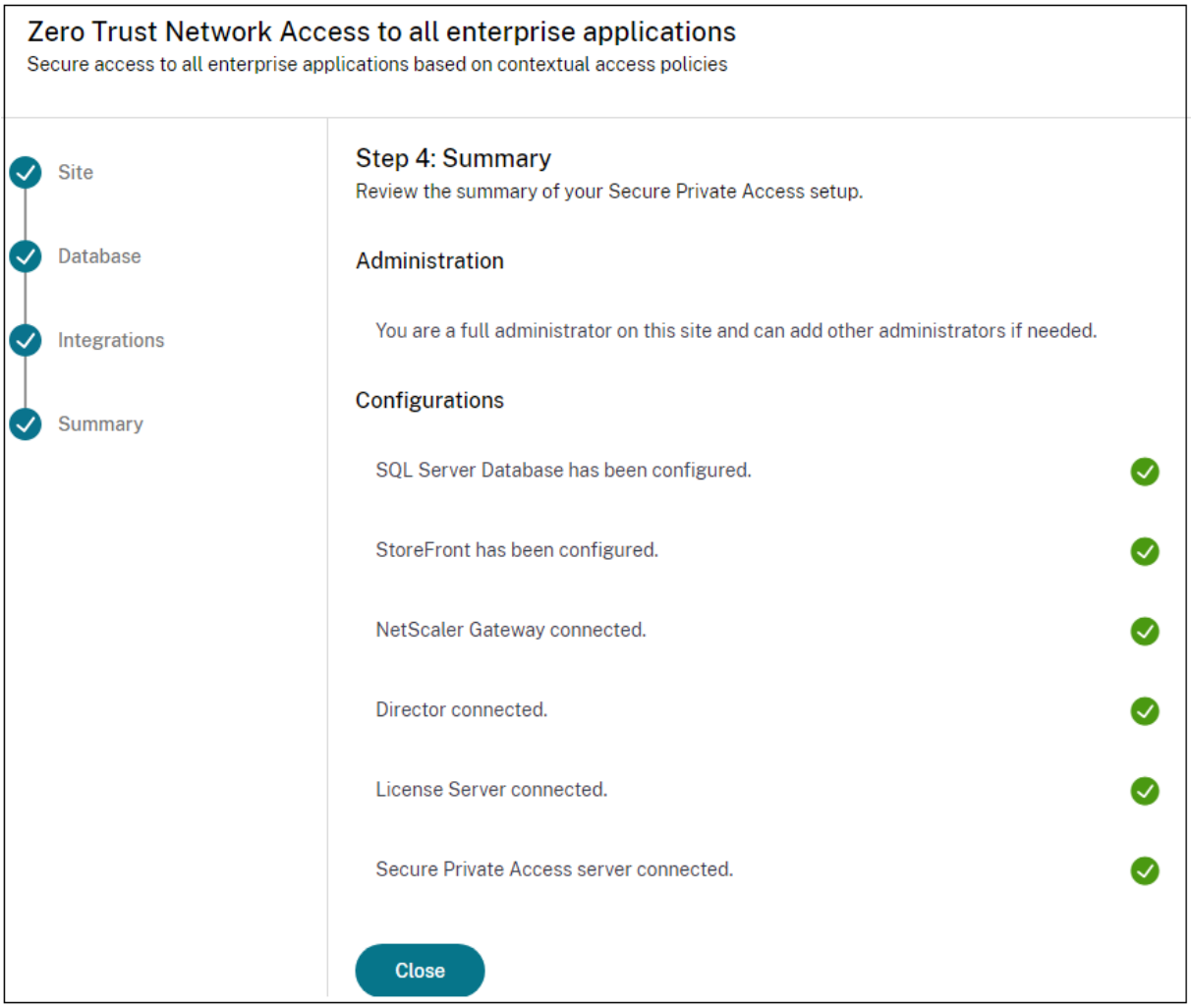
1. Enter the following details.
    - **Secure Private Access server address**. For example, `https://secureaccess.domain.com`.
    - **StoreFront Store URL**. For example, `https://storefront.domain.com/Citrix/StoreMain`.
    - **Public NetScaler Gateway Address** –URL of the NetScaler Gateway. For example, `https://gateway.domain.com`.
    - **Virtual IP address** –This virtual IP address must be the same as the one configured in StoreFront for callbacks.
    - **Callback URL** –This URL must be the same as the one configured in StoreFront. For example, `https://gateway.domain.com`.
    - **Director URL:** - (Optional) The Director server IP address or FQDN to connect Secure Private Access with Citrix Director.
    - **License server URL:** - The License server IP address to collect and process licensing data.
2. Click **Validate all URLs**
3. Click **Next** and then click **Save**.



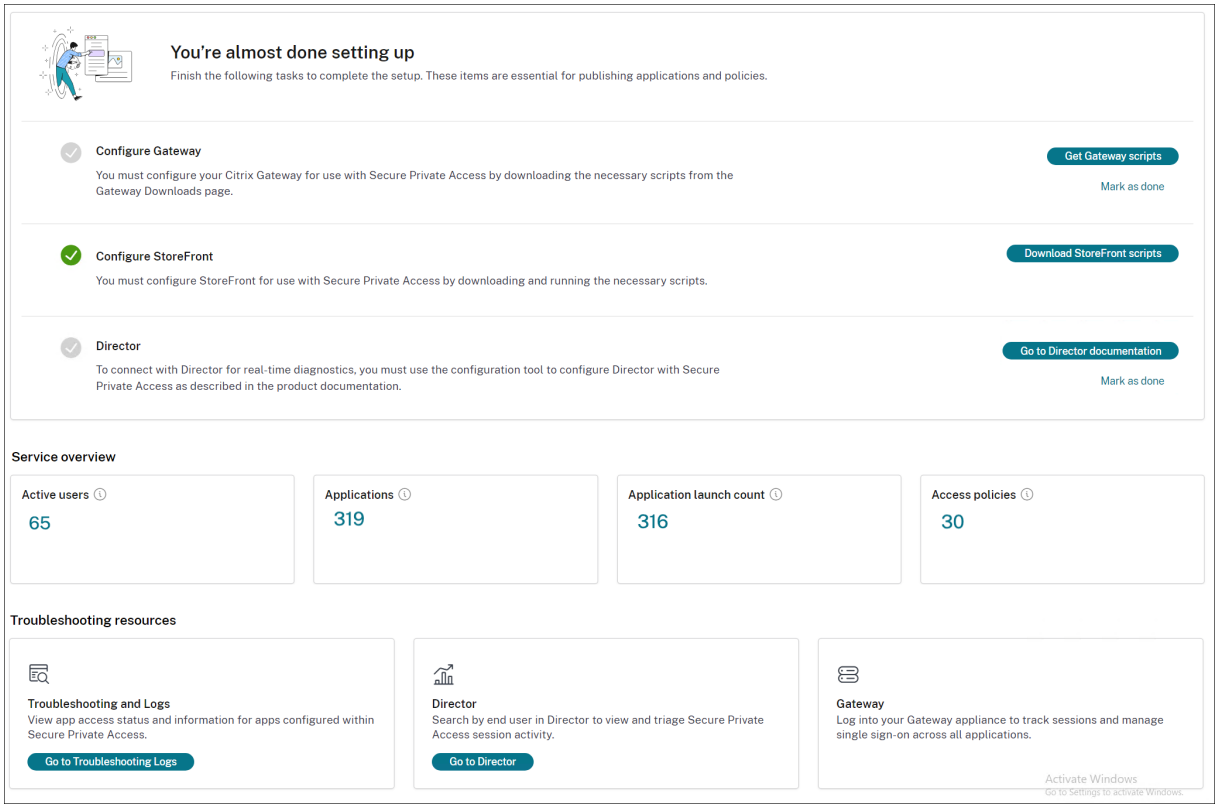
Step 4: Configuration summary

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.

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



After the setup is complete, the following page displayed once you click **Close** on the **Summary** page.



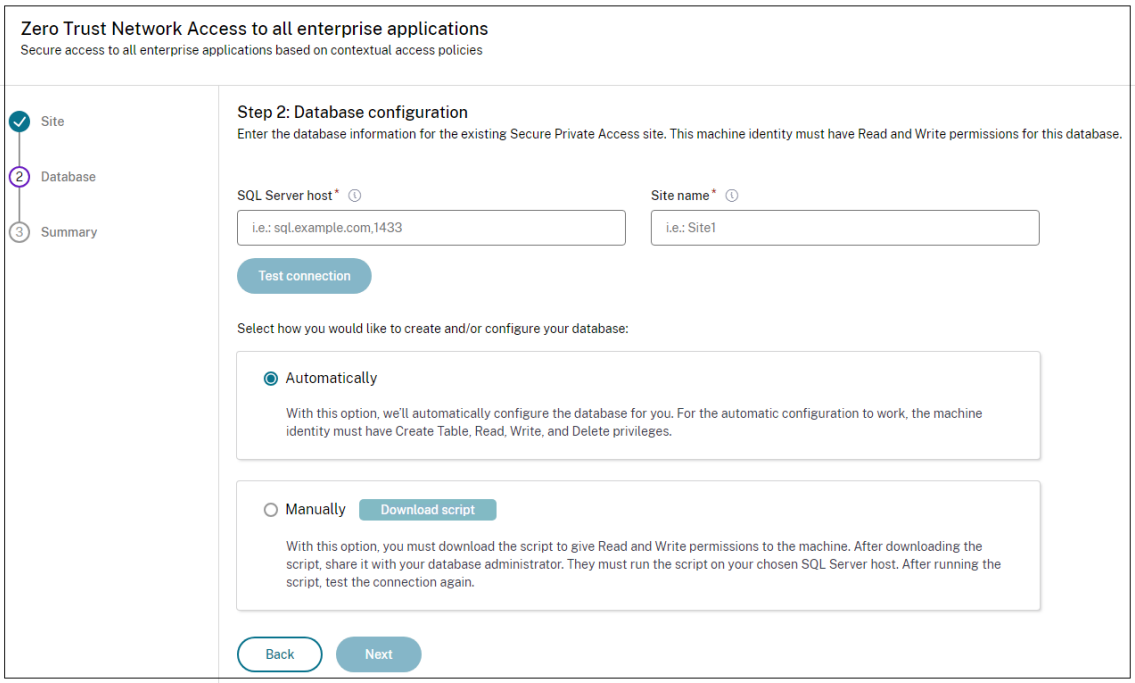
Note:

- 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.

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**.

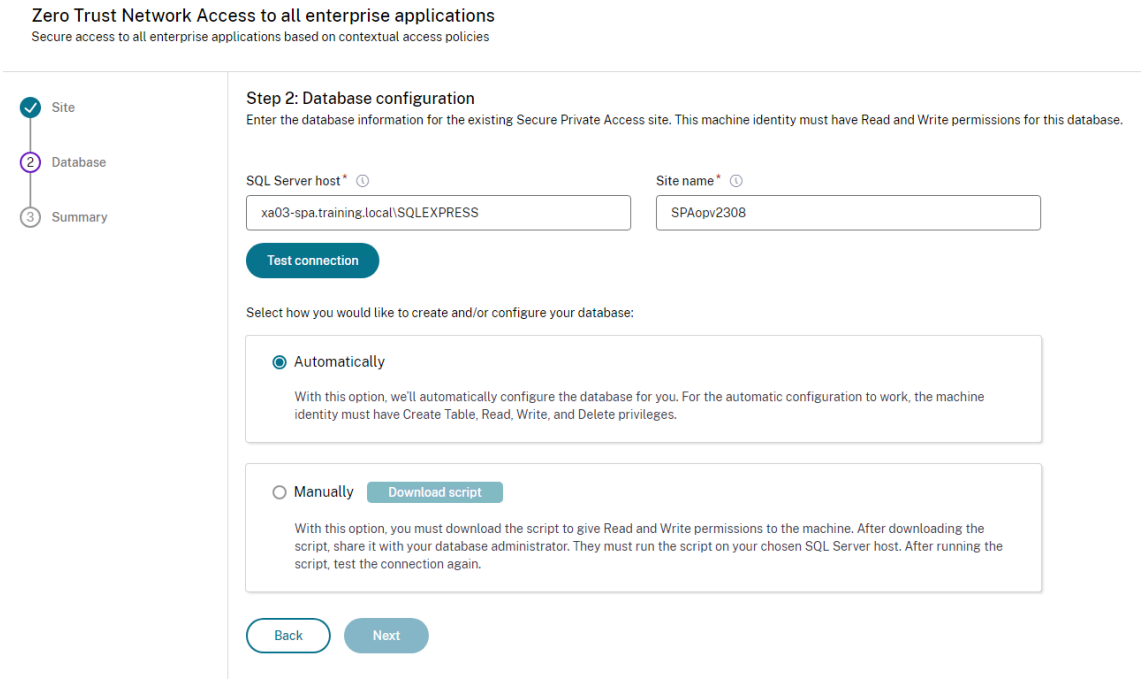


2. In **SQL Server Host**, enter the server host name. Ensure that a database corresponding to the site name that you enter is already present in the SQL server that you have selected. You can specify a database address in one of the following forms:

   - 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 connection** to check that the SQL server instance is valid and also to confirm that the specified site exists in the database.



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

5. Click **Save**.

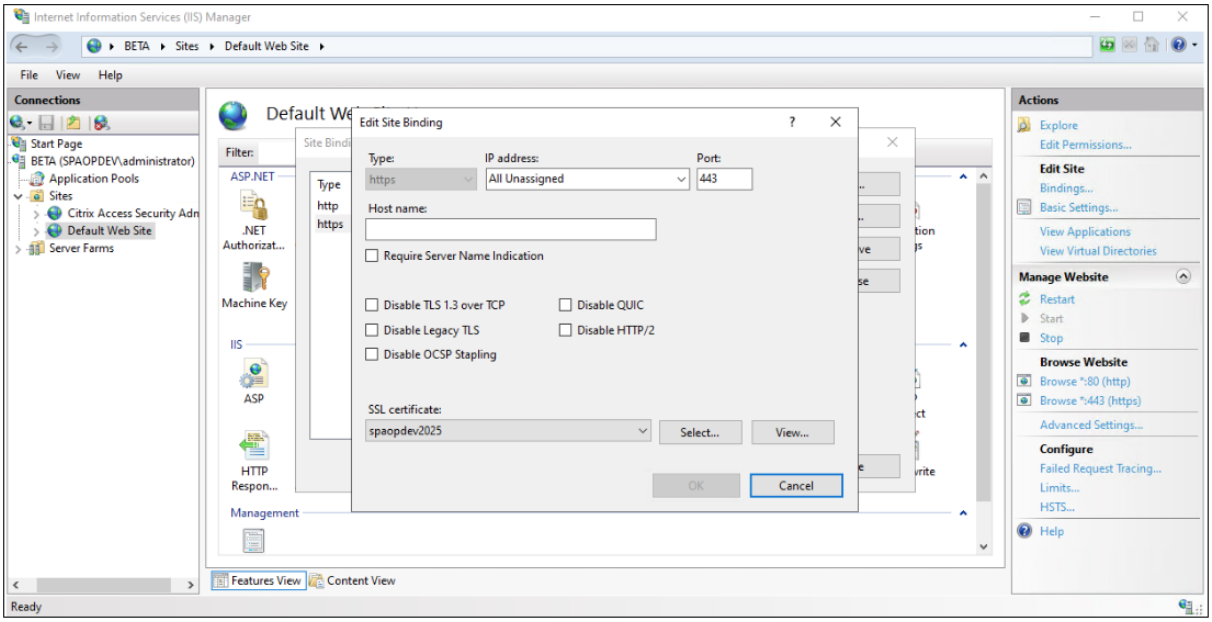
The configuration validation check happens to ensure that the SQL database server is configured and to check that the Secure Private Access server is reachable.

Disable the HTTP2 setting

Secure Private Access for on-premises operates within the Internet Information Services (IIS) environment. Consequently, any potential common vulnerability affecting HTTP/2 within IIS is directly addressed and patched by Microsoft. In the interim, customers can mitigate this vulnerability by manually modifying the HTTP/2 setting directly within IIS ensuring that Secure Private Access for on-premises solution remains protected even before an official patch is released.

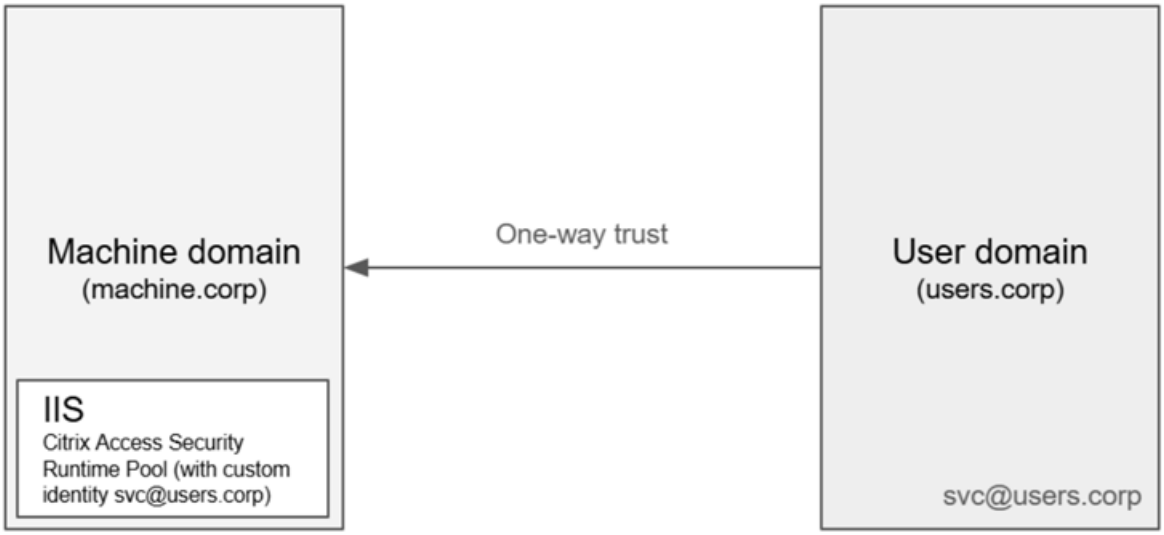
Perform the following steps to disable HTTP2 per site.

1. Open the Internet Information Services (IIS) manager.
2. In the navigation pane, expand **Sites** and select **Default Web Site**.
3. In the **Actions** pane, click **Bindings** and modify the HTTPS binding by selecting the **Disable HTTP/2** checkbox.
4. Save and restart the IIS manager.



Multi-domain environments

Secure Private Access on-premises deployment supports multi-domain environments where the machine server and user account servers reside in different Active Directory domains. This cross-domain deployment capability offers flexibility in managing infrastructure and user identities. However, for this environment to be successful, at least a one-way trust relationship must be established between the Active Directory domains located in different forests.



To establish domain trust for Secure Private Access on-premises deployment in multi-domain environments, the following prerequisites must be met:

- The service account from the machine domain (example, Domain B) used for initial configuration must be provisioned in the user account domain (example, Domain A).

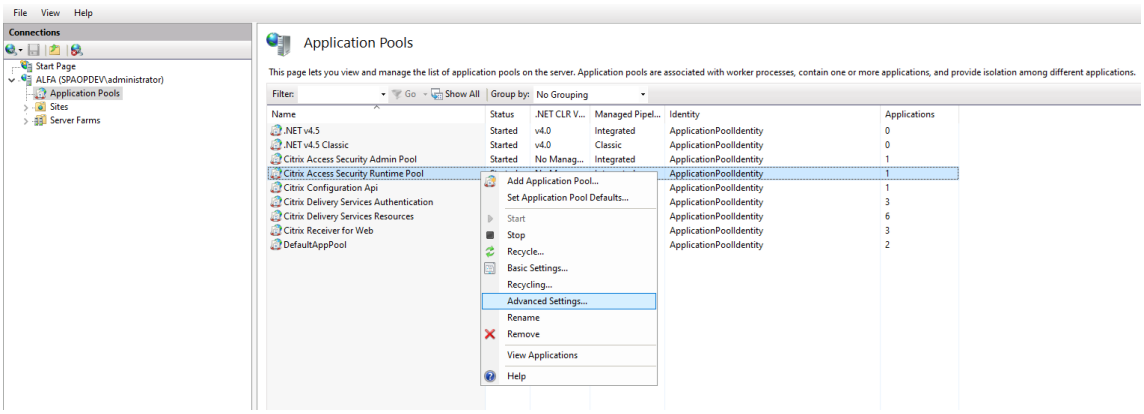
  > **Note:**
  >
  > The service account must be added in the IIS for the Citrix Access Security Runtime Service Pool. The service account does not require admin privileges. For details, see Steps to configure the service account.

- If the installation server (in Domain A, referred to as "server domain a") is also in Domain A, the service account must be created as a database user with 'db owner'permissions within the relevant database instance.

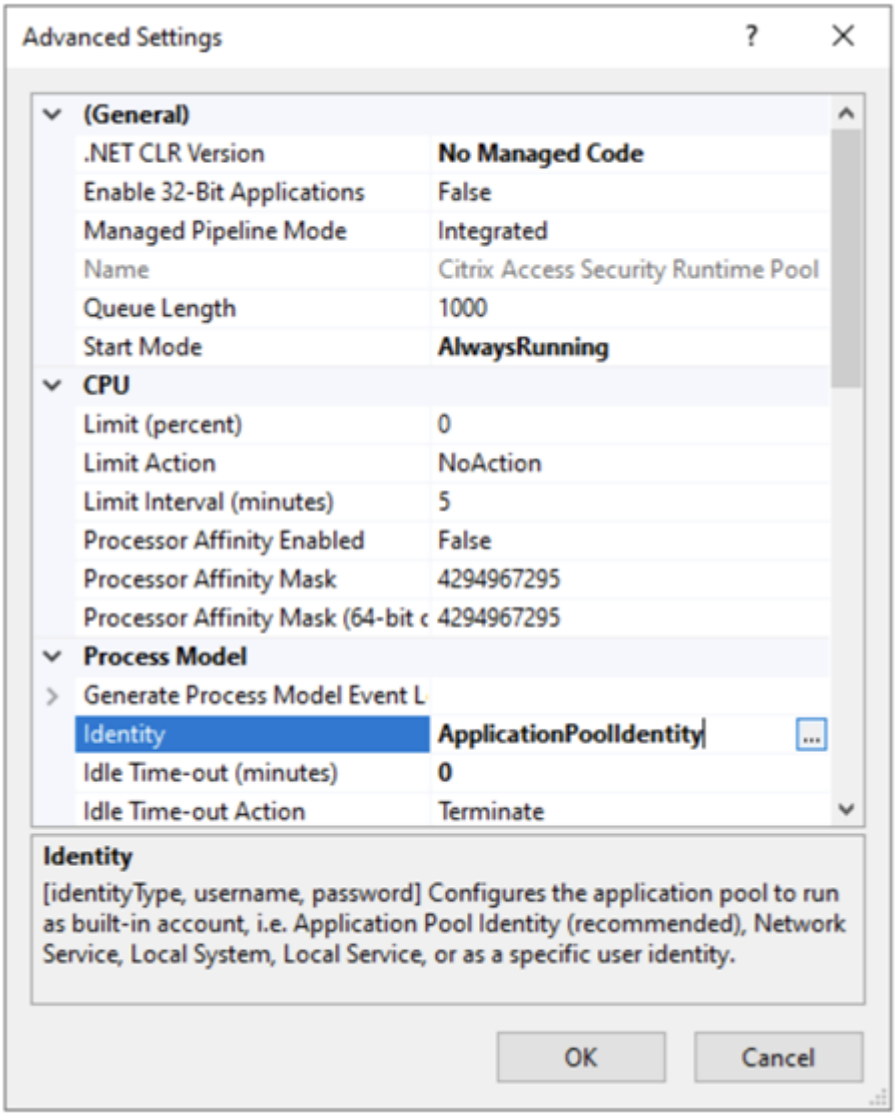
Configure the service account

Perform the following steps to configure the service account:

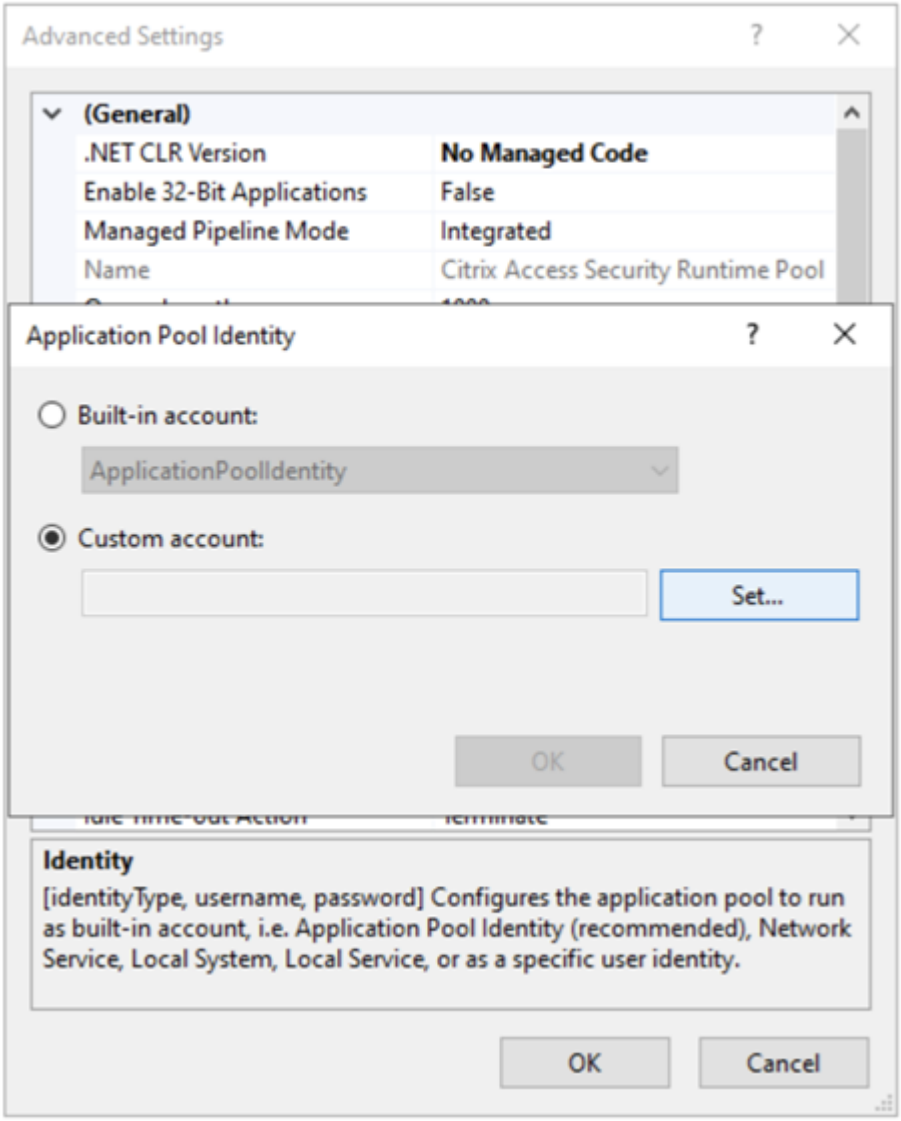
1. Launch the Internet Information Services (IIS) manager.
2. Under the site server, select **Application Pools > Citrix Access Security Runtime Pool > Advanced Settings**.



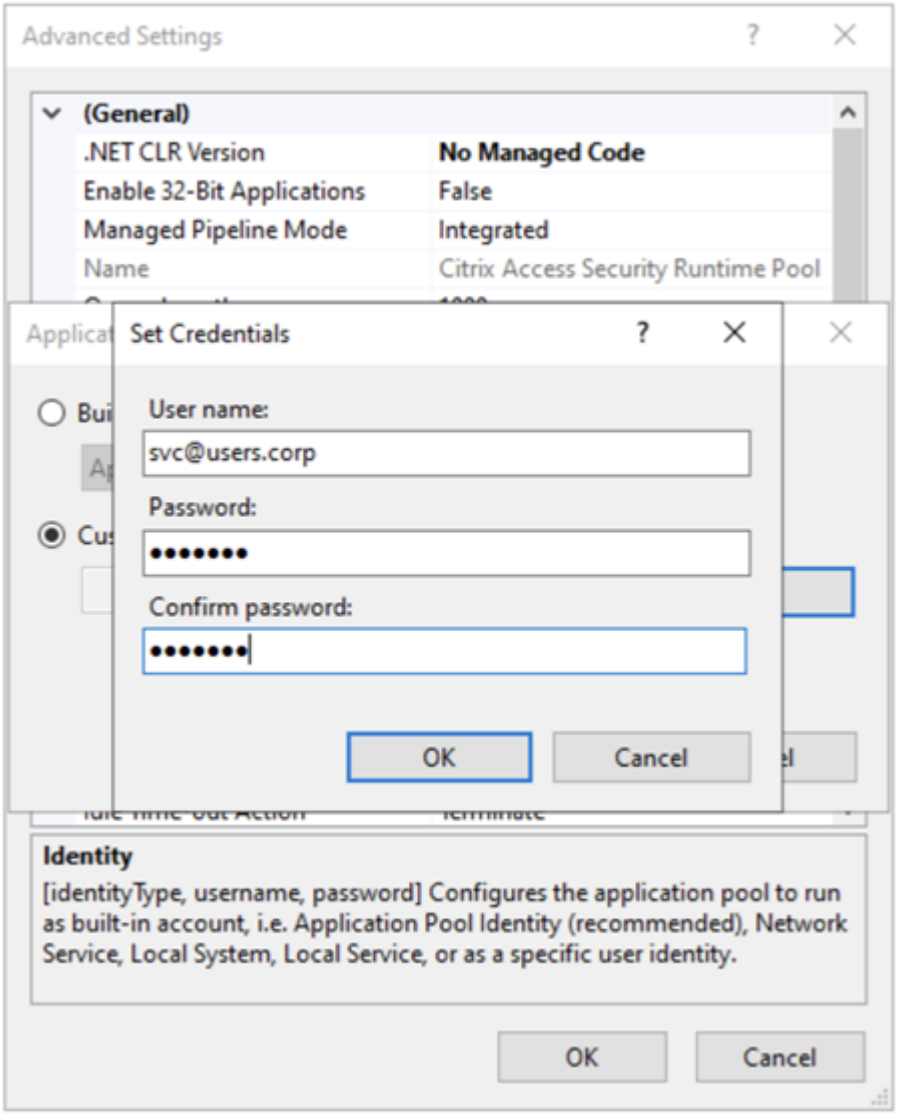
3. Click the edit icon in **Identity > ApplicationPoolIdentity**.



4. In **Custom account:** click **Set**.



5. Set credentials for the user.
6. Click **OK**.



Next steps

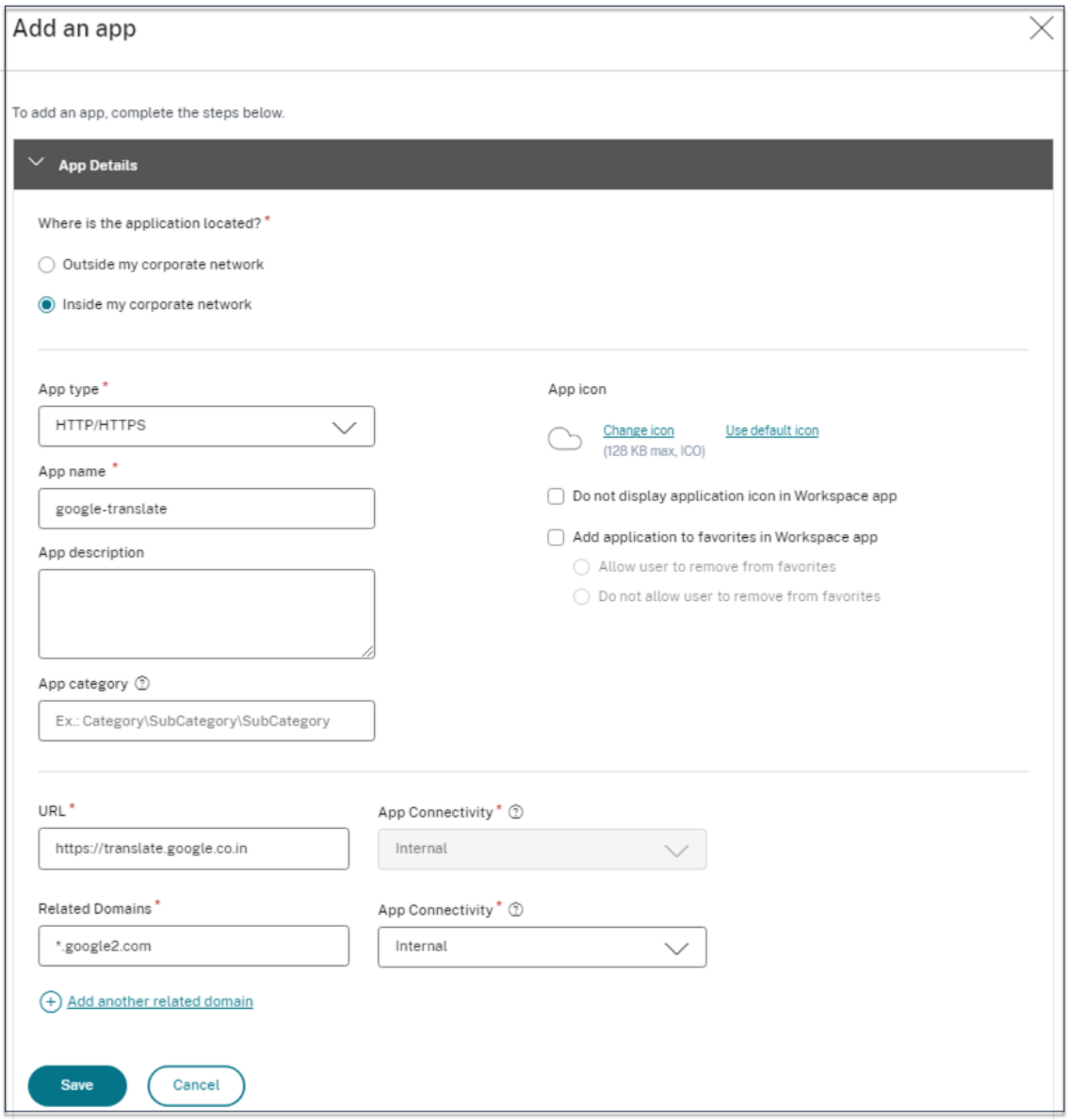
- Configure NetScaler Gateway
- Configure applications
- Configure access policies for the applications

Configure Web/SaaS applications

September 6, 2025

After you have set up Secure Private Access, you can configure apps and access policies from the admin console.

1. In the admin console, click **Applications**.
2. Click **Add an app**.
3. Select the location where the app resides.
   - **Outside my corporate network** for external applications.
   - **Inside my corporate network** for internal applications.
4. Enter the following details in the App Details section and click **Next**.



   - **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.
  - 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.

> **Note:**
>
> - Ensure that an app's related domain does not overlap with another app's related domain. If this occurs, remove the related domain from all apps and create a new app with this domain and then set access accordingly in the access policy. You can also consider if you want to display this app in StoreFront™ or hide it. You can hide the app in StoreFront using the option **Do not display application to users** while publishing the app.

> – Similarly, a published app's URL must not be added as another app's related domain.
> – For more details, see Best practices for Web and SaaS application configurations.

- **Add application to favorites automatically** –Click this option to add the app as a favorite app 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.
  - **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.

  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.

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

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 TCP/UDP apps

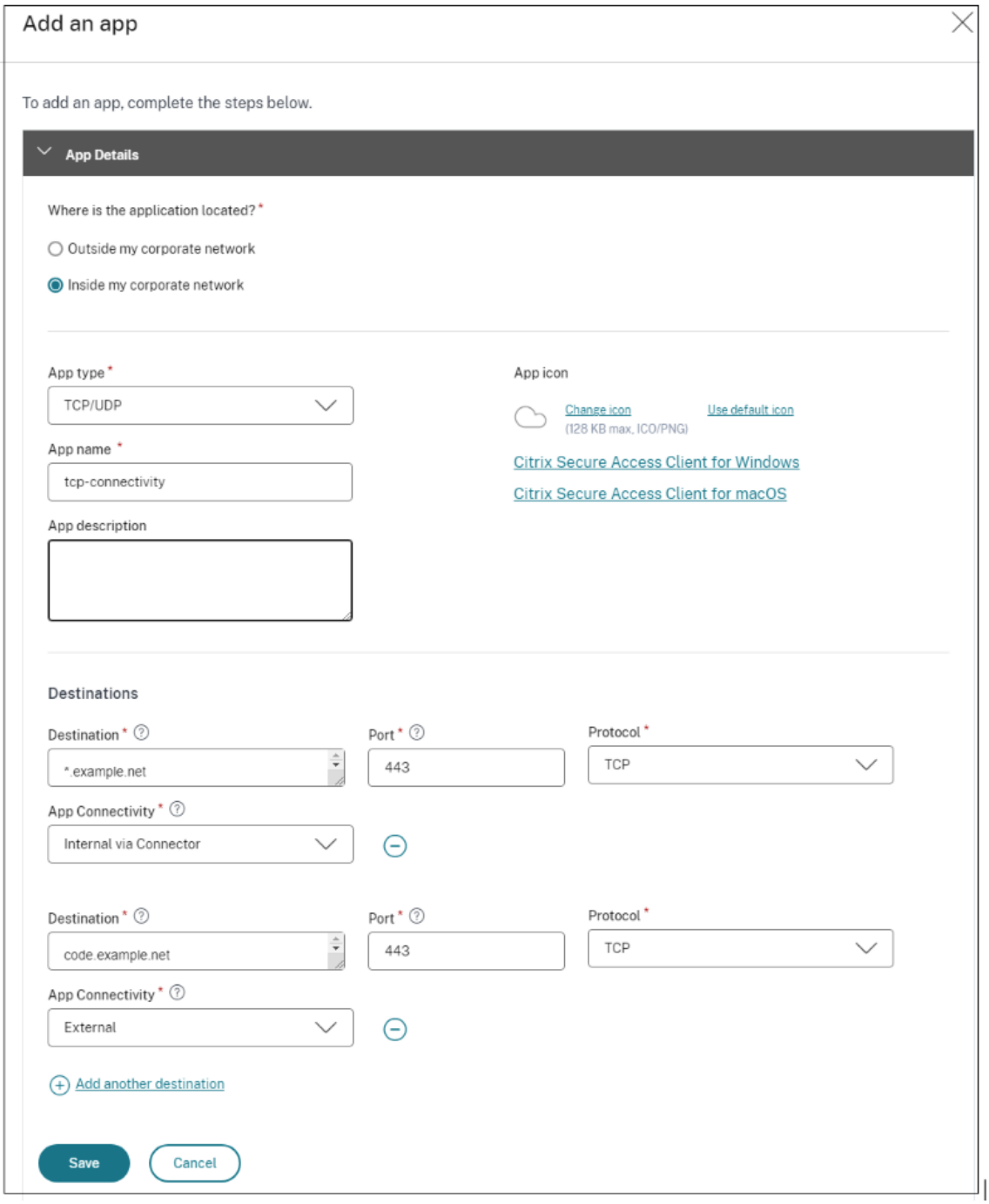
September 6, 2025

Prerequisites:

- Secure Private Access setup is complete.
- Client versions meet the following requirements:
  - Windows - 24.6.1.17 and later
  - macOS - 24.06.2 and later

Perform the following steps to configure TCP/UDP apps from the admin console:

1. In the admin console, click **Applications** and then click **Add an app**.
2. Select the location **Inside my corporate network**.



3. Enter the following details:
   - **App type** –Select **TCP/UDP** for initiating connections with the back-end servers residing in the data center.

> **Note:**
>
> The TCP/UDP option appears grayed out if the SPAOP-3315-EnableZTNAApplications feature flag is disabled. You must manually update the database to enable this feature flag.

- **App name**–Name of the application.
- **App description** –Description of the app you are adding. This field is optional.
- **Destinations** –IP Addresses or FQDNs of the back-end machines residing in the data center. One or more destinations can be specified as follows.
  - **IP address v4**
  - **IP address Range** –Example: 10.68.90.10-10.68.90.99
  - **CIDR** –Example: 10.106.90.0/24
  - **FQDN of the machines or Domain name** –Single or wildcard domain. Example: ex.destination.domain.com, *.domain.com

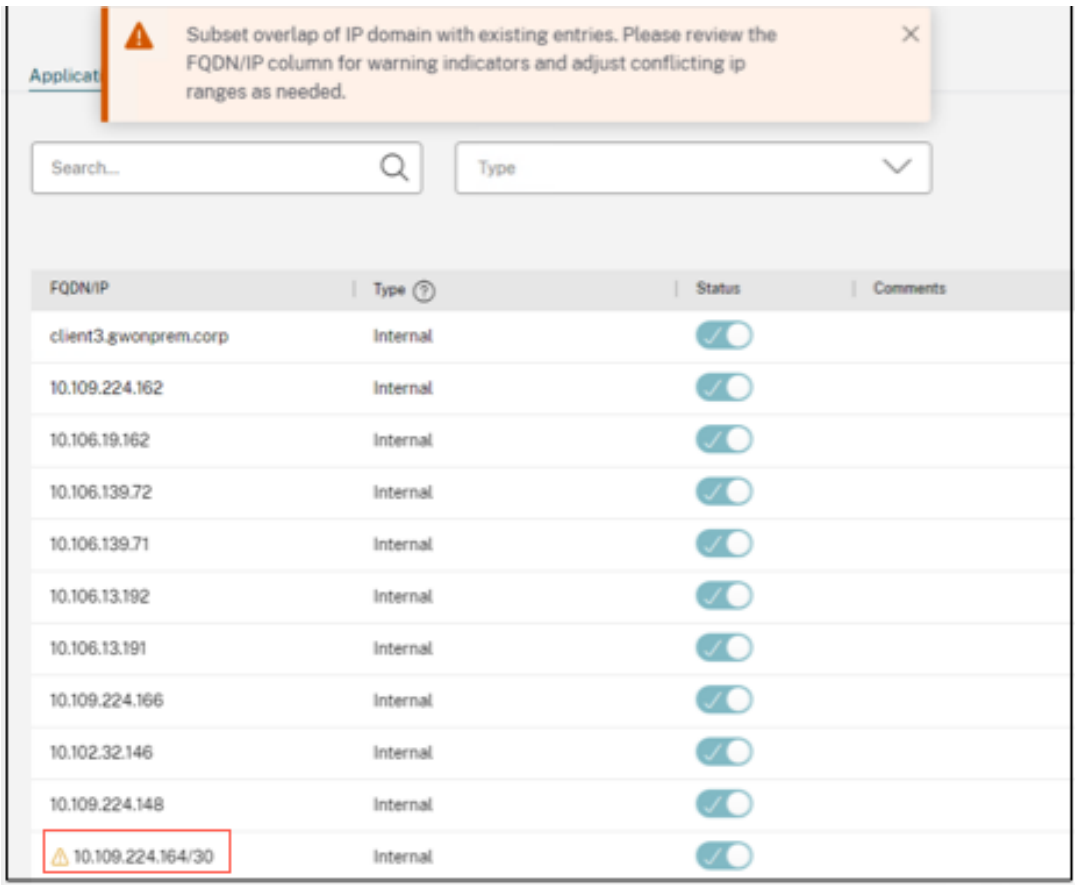
    > **Note:**
    >
    > * End users can access the apps using FQDN even if the admin has configured the apps using the IP address. This is possible because the Citrix Secure Access™ client can resolve an FQDN to the real IP address.

The following table provides examples of various destinations and how to access the apps with these destinations:

Destination input	How to access the app
10.10.10.1-10.10.10.100	The end user is expected to access the app only through IP addresses in this range.
10.10.10.0/24	The end user is expected to access the app only through IP addresses configured in the IP CIDR.
10.10.10.101	The end user is expected to access the app only through 10.10.10.101

Destination input	How to access the app
`*.info.citrix.com`	The end user is expected to access subdomains of `info.citrix.com` and also `info.citrix.com` (the parent domain). For example, `info.citrix.com`, `sub1.info.citrix.com`, `level1.sub1.info.citrix.com` **Note:** The wildcard must always be the starting character of the domain and only one *. is allowed.
info.citrix.com	The end user is expected to access `info.citrix.com` only and no subdomains. For example, `sub1.info.citrix.com` is not accessible.

The destination IP address must be unique across resource locations. If a conflicting configuration exists, a warning symbol is displayed against the specific IP address in the Application Domain table (**Settings > Application Domain**).



- **Port** –The destination port on which the app is running. Admins can configure multiple ports or port ranges per destination.

  The following table provides examples of ports that can be configured for a destination.

Port input	Description
*	By default, the port field is set to " * " (any port). The port numbers from 1 to 65535 are supported for the destination.
1300–2400	The port numbers from 1300 to 2400 are supported for the destination.
38389	Only the port number 38389 is supported for the destination.
22,345,5678	The ports 22, 345, 5678 are supported for the destination.
1300–2400, 42000-43000,22,443	The port number range from 1300 to 2400, 42000–43000, and ports 22 and 443 are supported for the destination.

> **Note:**
>
> Wildcard port (*) cannot co-exist with port numbers or ranges.

- **Protocol** –TCP/UDP
- **App Connectivity:** Define how your applications traffic must be routed.

  Internal: DNS resolution is done via a remote DNS server.

  By default, all the traffic to the domain marked as Internal is intercepted and tunneled through NetScaler Gateway. For example, if the connectivity for .example.net is set as Internal, all of its related domains/subdomains (for example; code.example.net, test.example.net, 123.example.net) are intercepted and tunneled through NetScaler Gateway.

  External: DNS resolution is done via a local DNS server.

  When a related domain/subdomain is marked as External, traffic to that domain is not intercepted and tunneled through NetScaler Gateway. For example, if connectivity to code.example.net is set as External, then traffic to this domain is routed directly through the internet while traffic to subdomains (for example text.example.net and 123.example.net) is tunneled through NetScaler Gateway.

4. Click **Add** to add additional destinations or servers accordingly.

5. Click **Save**. The app is added to the **App Configuration** page. You can edit or delete an app from the **Applications** page after you have configured the application. To do so, click the ellipsis button in line with the app and select the actions accordingly.

    - **Edit Application**
    - **Delete**

Configure access policies for TCP/UDP apps

To enable access to the apps for the users, admins are required to create access policies. For details, see Configure access policies.

References

Citrix Secure Access client.

Configure TCP/UDP - server to client apps

September 6, 2025

Starting from 2408, Secure Private Access supports a new app type (**TCP/UDP - server to client**). This app type can be used for supporting features such as the following:

- Software distribution using Microsoft Endpoint Configuration Manager or similar solutions
- Remote policy updates on managed devices using GPO Push
- Remote assistance to troubleshoot and debug user workstations.

Prerequisites:

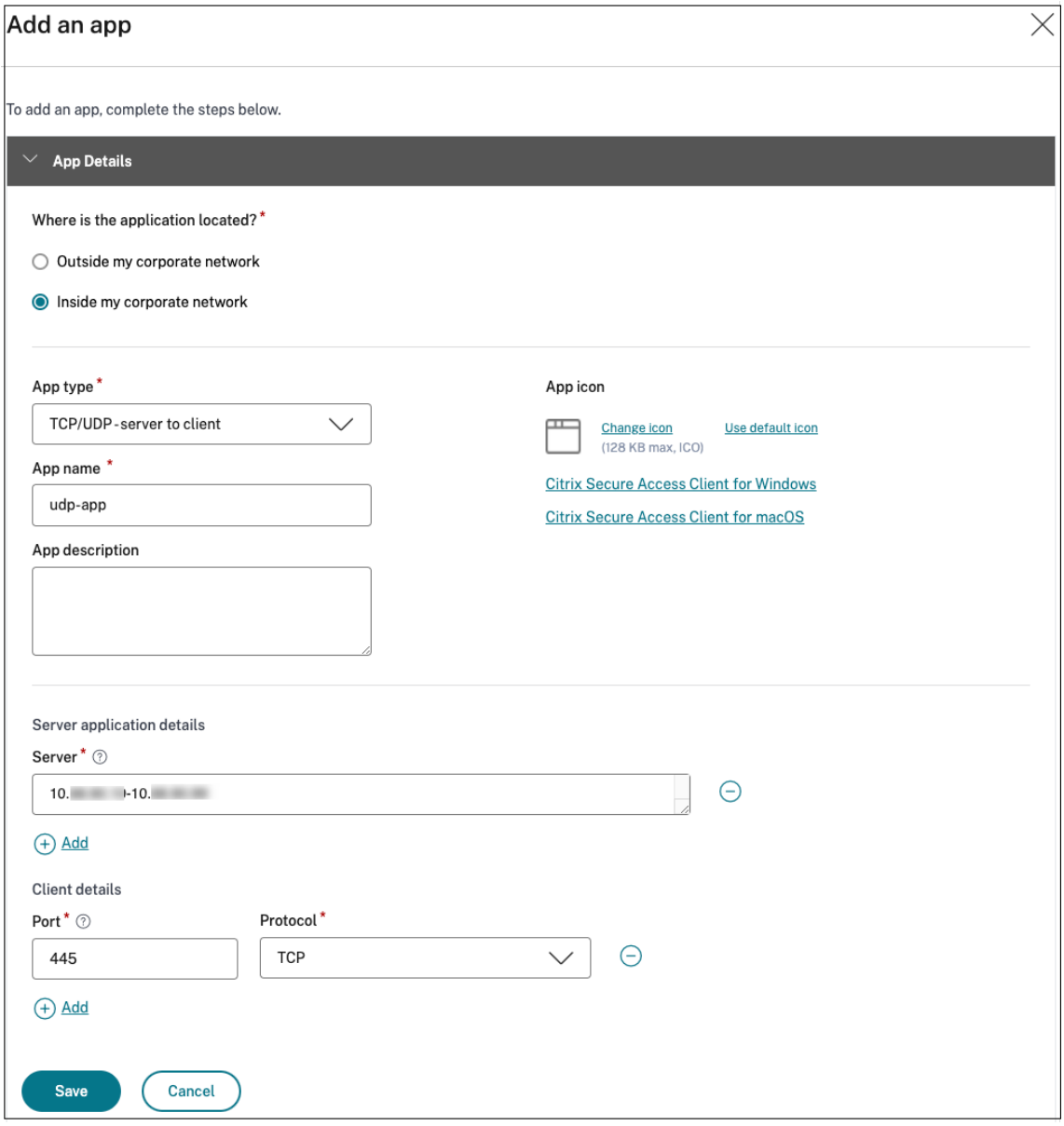
- Secure Private Access setup is complete.
- Client versions meet the following requirements:
    - Windows - 24.6.1.18 and later
    - macOS - 24.06.2 and later
- The intranet IP address is configured on NetScaler® Gateway and is bound to the respective VPN virtual server. Use the following sample commands for reference:

```
set vpn sessionAction AC_AG_PLGspaonprem -useMIP NS -useIIP
NOSPILLOVER

bind vpn vserver spaonprem -intranetIP <IP address>
```


Perform the following steps to configure TCP/UDP apps from the admin console:

1. In the admin console, click **Applications** and then click **Add an app**.
2. Select the location **Inside my corporate network**.



3. Enter the following details:

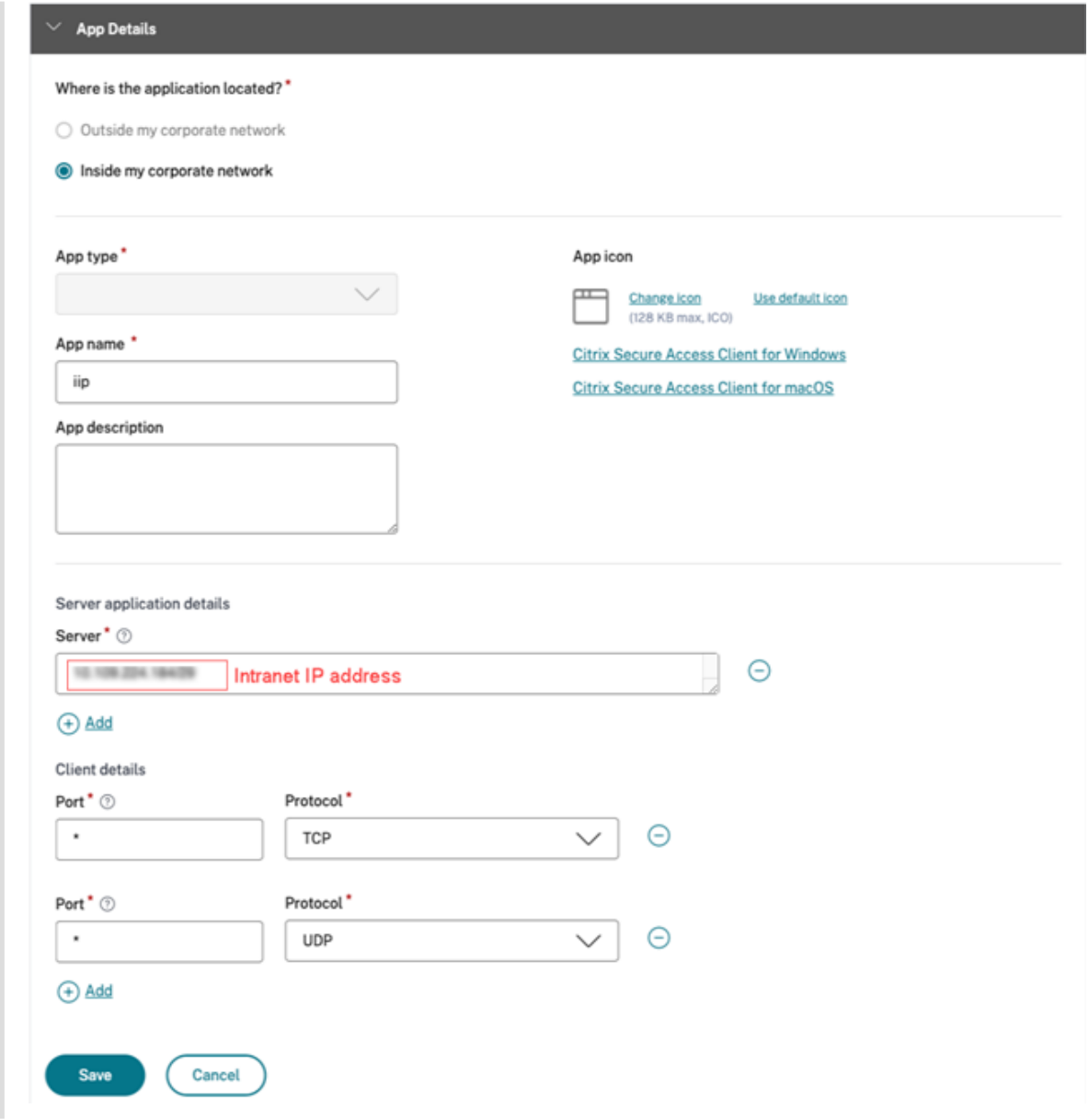
   - **App type** –Select **TCP/UDP - server to client**.
   - **App name**–Name of the application.
   - **App description** –Description of the app you are adding. This field is optional.
   - **Server** - Details of the application servers that are authorized to establish connection with the client. You can enter the IP address, IP address range, or the CIDR.
   - **Port** –The client port number.

- **Protocol** –TCP/UDP.

4. Click **Add** to add additional servers.
5. Click **Save**. The app is added to the **App Configuration** page. You can edit or delete an app from the **Applications** page after you have configured the application. To do so, click the ellipsis button in line with the app and select the actions accordingly.

   - **Edit Application**
   - **Delete**

> **Important:**
>
> After you add an app for server-client communication, to enable server-client and client-client communication, intranet IP address ranges configured on NetScaler Gateway must be added as a TCP/UDP app.



Configure access policies for TCP/UDP server-client apps

To enable access to the apps for the users, admins are required to create access policies. For details, see Configure access policies.

References

Citrix Secure Access client.

Configure access policies for the applications

September 6, 2025

Access policies allow you to enable or disable access to the apps based on the user/user groups or machine/machine groups. In addition, you can enable restricted access to the apps (HTTP/HTTPS and TCP/UDP) by adding the security restrictions.

1. In the admin console, click **Access Policies**.
2. Click **Create Policy**.
3. In the **Create Access Policy** page, select one of the following:

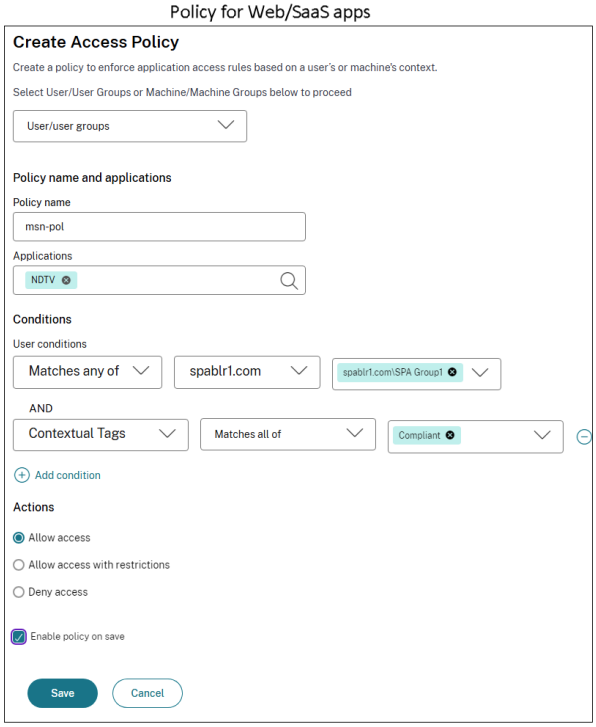
   - **Users/User groups**
   - **Machines/Machine groups**

   Application access rules are enforced based on a user's or machine's context, based on the selection in the access policy.

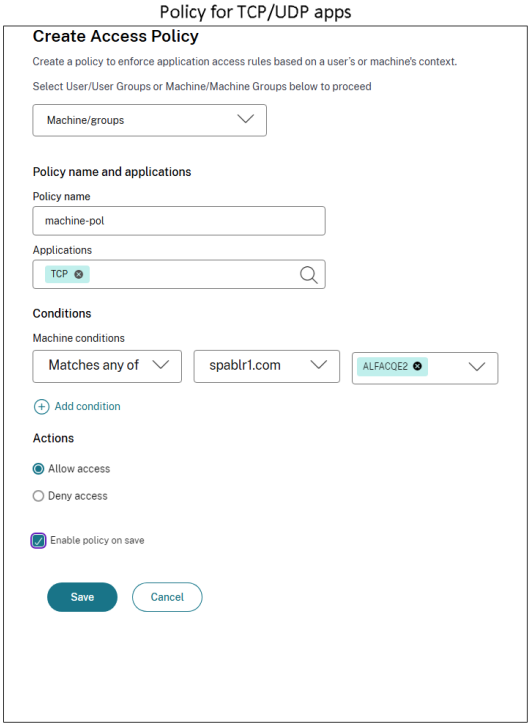
   You can select **Machine/Machine groups** to enable Always On connectivity. For Always On connectivity, you must have the device certificates enrolled. For details see Device certificate enrollment configuration.

   For more information on the machine tunnel, see Always On VPN before Windows Logon.

Policy for Web/SaaS apps



Policy for TCP/UDP apps



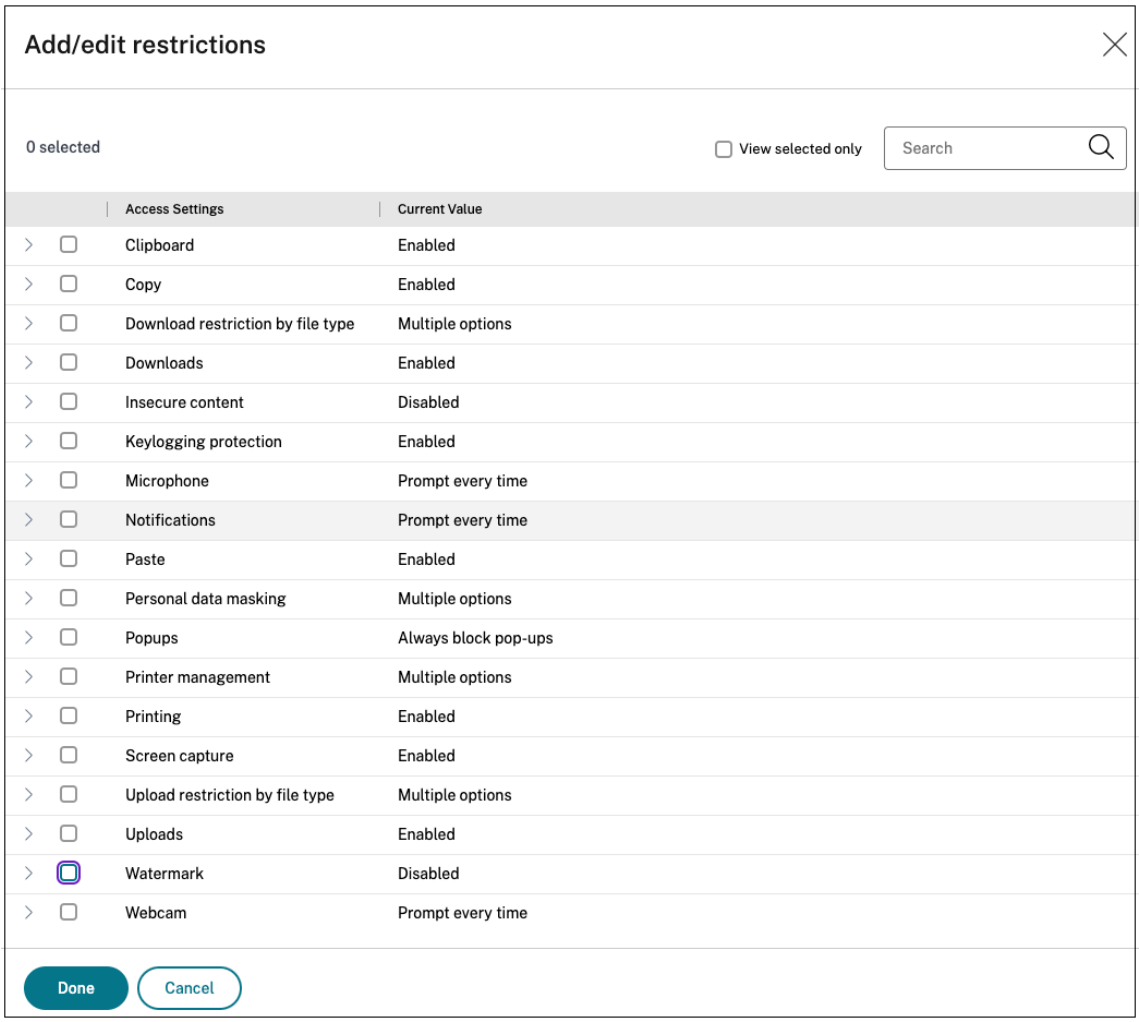
4. a) In **Policy name**, enter a name for the policy.
5. In **Applications**, select the apps for which you want to enforce the access policies.
6. In **Users conditions** –Select the conditions and users or user groups based on which app access must be allowed or denied.

   - **Matches any of**: Only the users/user groups or machines/machine 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.

7. Click **Add condition** to add another condition based on contextual tags. These tags are derived from the NetScaler® Gateway.
8. In **Actions**, 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**

   > **Note:**
   >
   > - The action **Allow access with restriction** is not applicable for the TCP/UDP apps.
   > - When you select **Allow access with restrictions**, you must click **Add restrictions** to select the restrictions. For more information on each restriction, see Available access restrictions.



9. Select the restrictions and then click **Done**.
10. 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.

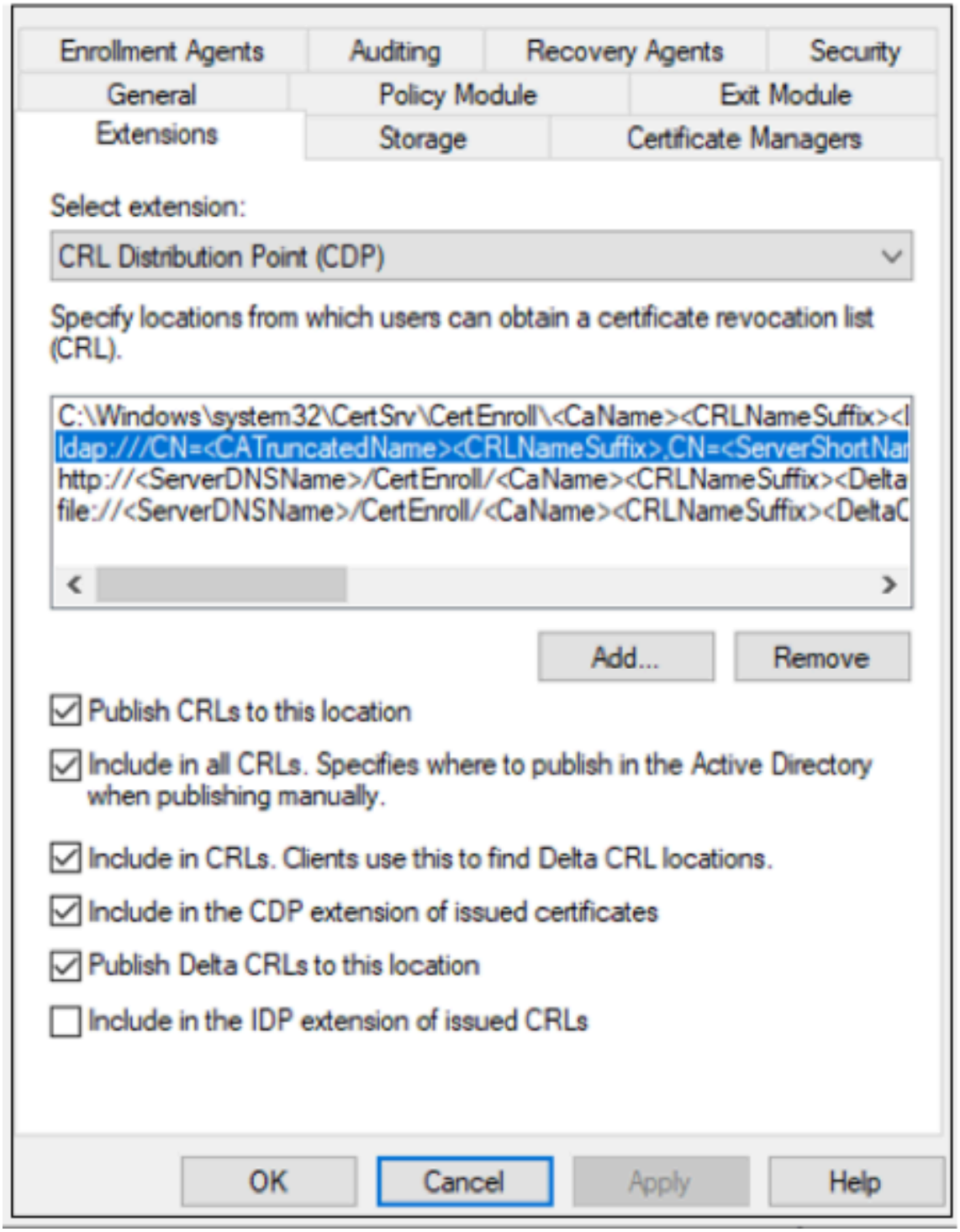
You can change the priority order by moving the policies up or down by using the up-down icon in the **Priority** column.

Device certificate enrollment configuration

Device certificates must be enrolled for Always On configurations to ensure that devices can consistently and securely connect to the network.

The following steps are involved in device certificate enrollment:

1. The Active Directory Enterprise Certificate Authority issues a Device Certificate for machine authentication.
2. The certificate authority must have the LDAP URL published for the CRL distribution point (CDP) extension.

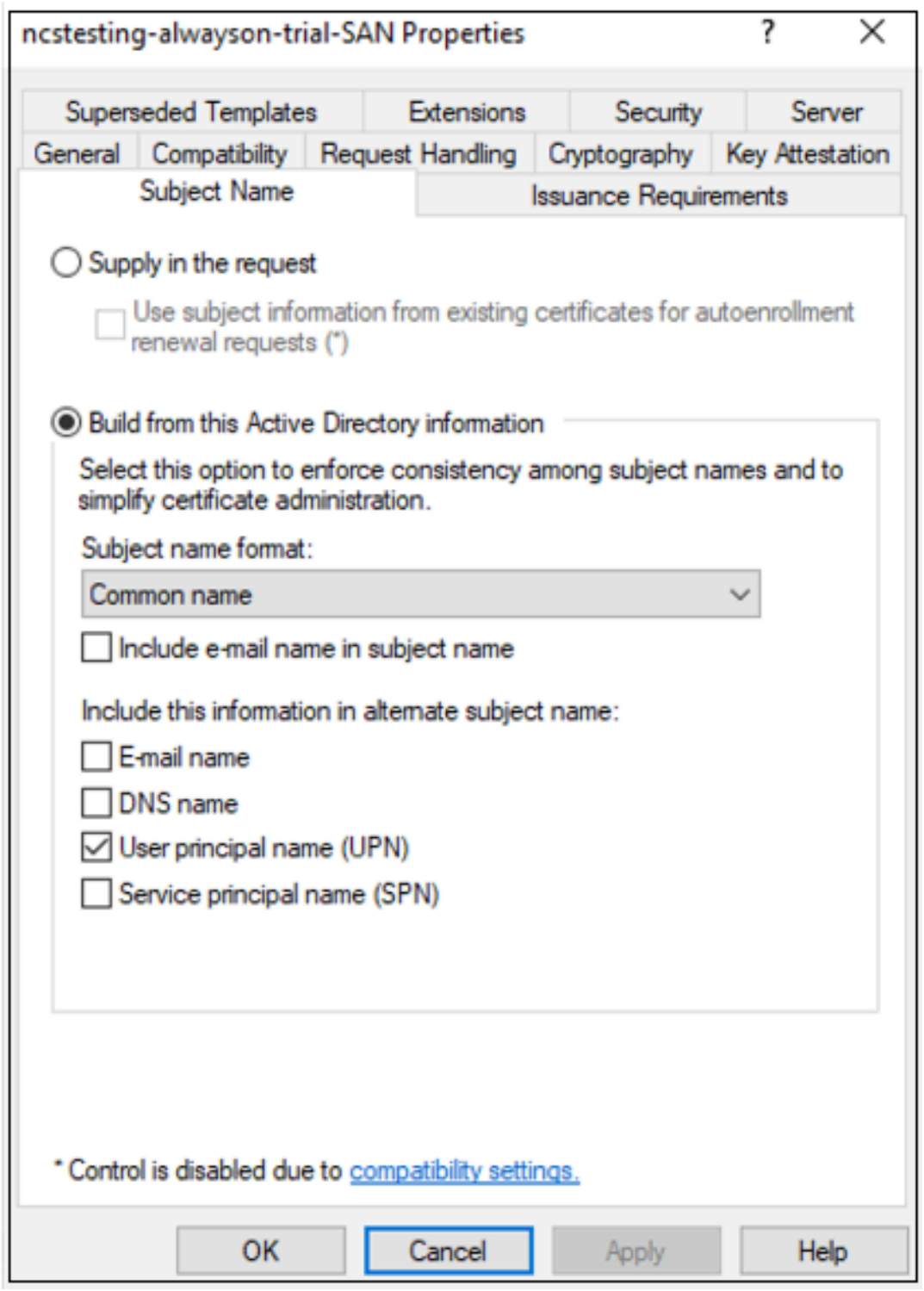


3. A certificate template in this certificate authority must be created to enroll the device certificate with the following details.

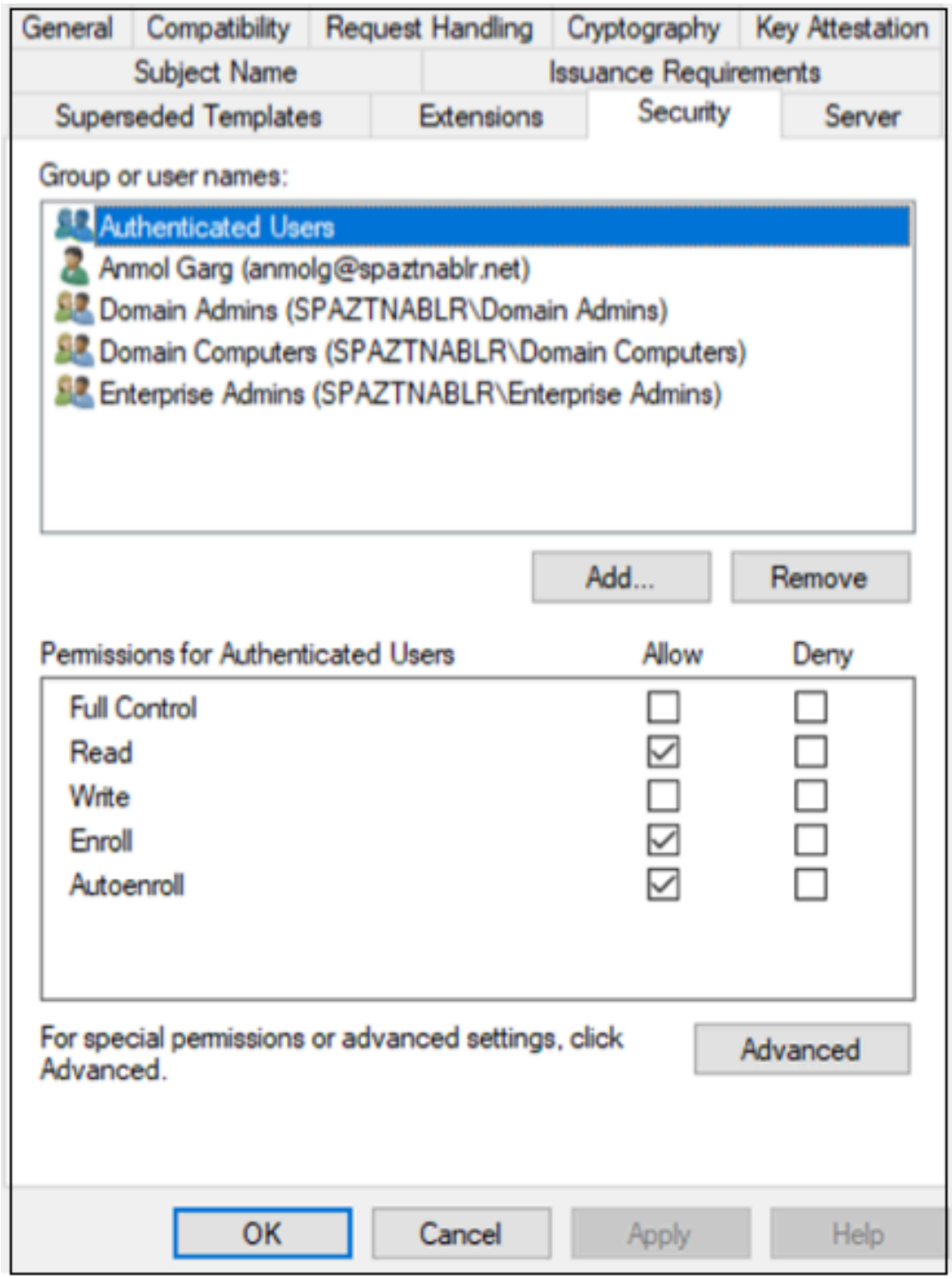
    a) Open the certification template snap-in and duplicate either the **Computer** or **Workstation Authentication** (preferred) template.

b) Provide a new name for the certificate.

c) Switch to the **Subject Name** tab, change the **Subject name format** setting to **Common name**, and check **User Principal Name (UPN)** to be included in the alternate subject name.



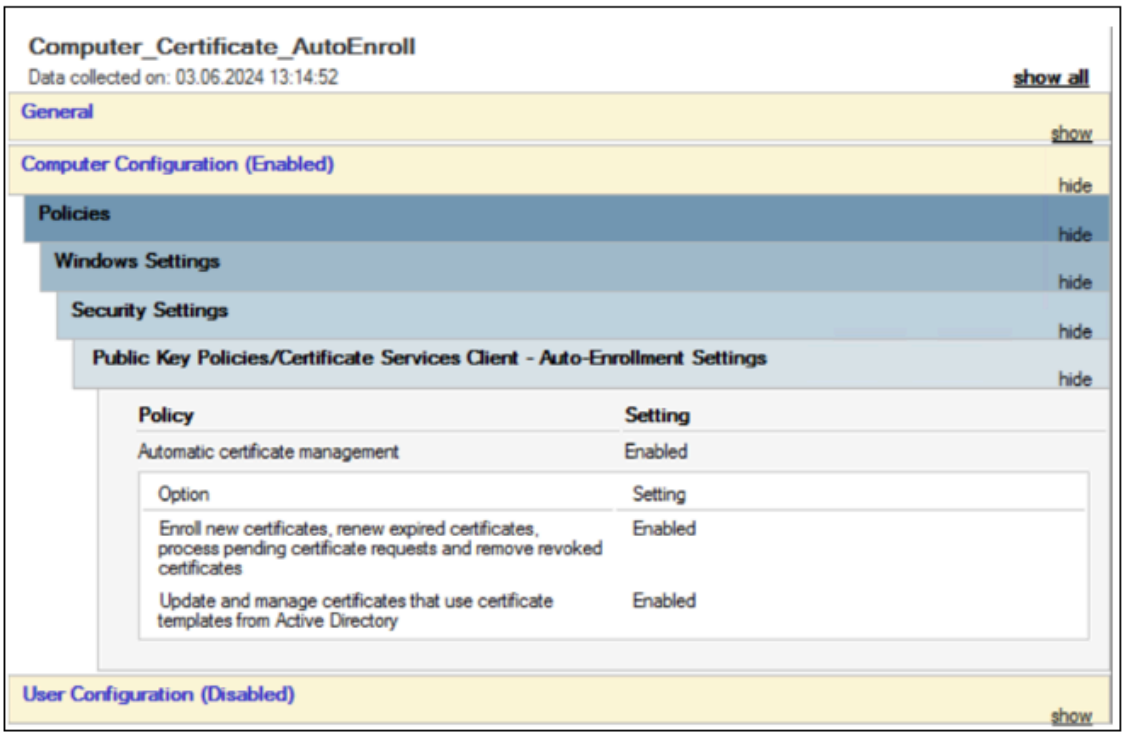
d) Switch to the **Security** tab and add a security group (containing only computer accounts) to which you want to autoenroll the new certificate template. Select the added group and select **Allow** for **Autoenroll**.



Note:

> In the preceding image, **Authenticated Users** (all computer objects) are permitted to enroll/autoenroll the new certificate template.

e) (Optional) Create a group policy object (GPO) that allows for auto certificate enrollment and bind it to an organization unit (OU) or at the domain level.



Next steps

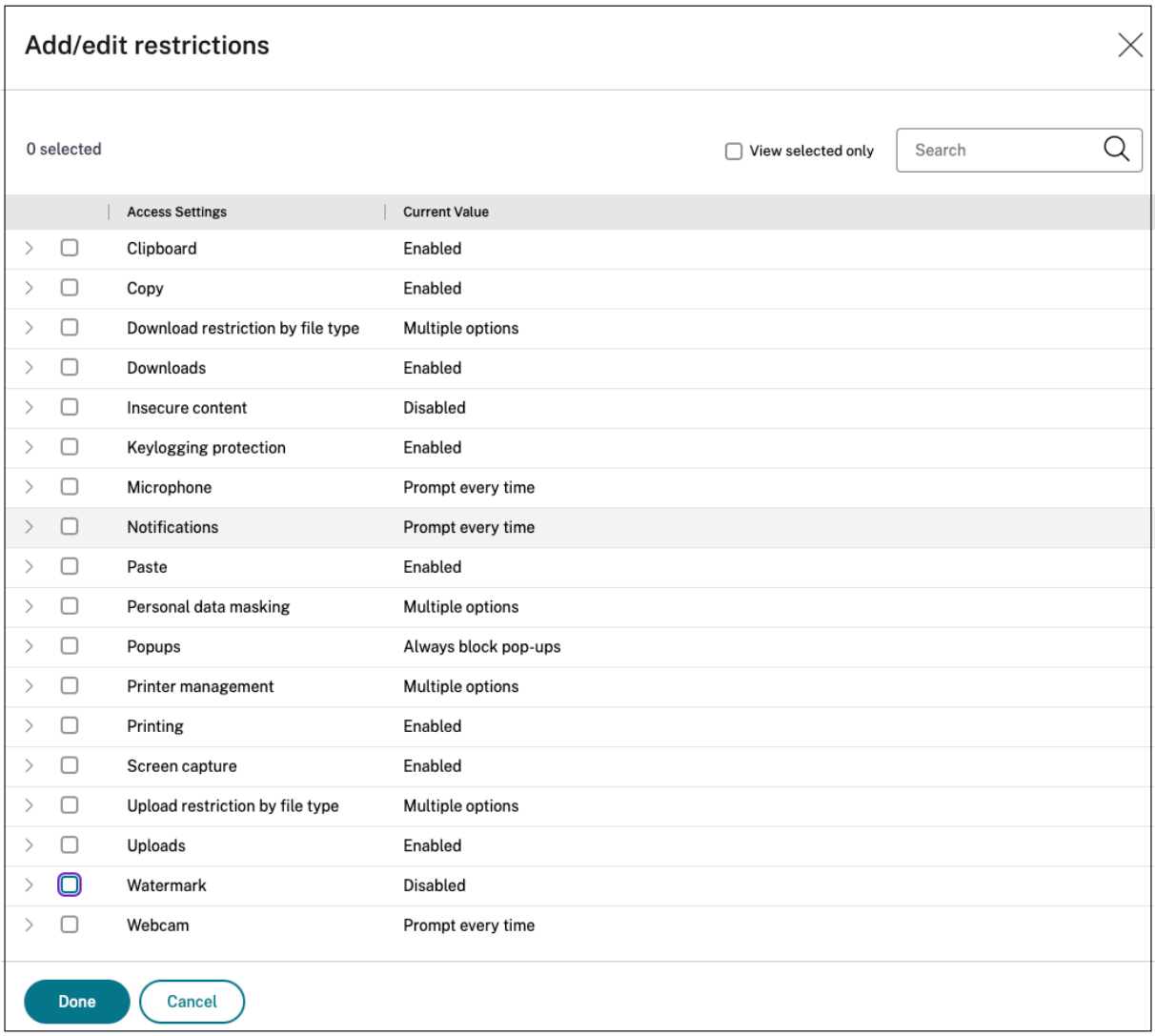
- Validate your configuration from the client machines (Windows and macOS).
- For the TCP/UDP apps, validate your configuration from the client machines (Windows and macOS) by logging into the Citrix Secure Access client.

Sample configuration validation

Access restriction options

September 6, 2025

When you select the action **Allow access with restrictions**, you can select the security restrictions as per the requirement. These security restrictions are predefined in the system. Admins cannot modify or add other combinations.



Clipboard

Enable/disable cut/copy/paste operations on a SaaS or internal web app with this access policy when accessed via Citrix Enterprise Browser. Default value: Enabled.

Copy

Enable/disable copying of data from a SaaS or internal web app with this access policy when accessed via the Citrix Enterprise browser. Default value: Enabled.

> **Note:**
>
> - If both **Clipboard** and **Copy** restrictions are enabled in a policy, the **Clipboard** restriction

takes precedence over the **Copy** restriction.
- End users must use Citrix Enterprise Browser™ version 126 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.
- For granular control of copy operations within the apps, admins can use the **Security groups** restriction. For details, see Clipboard restriction for security groups.

Downloads

Enable/disable the user's ability to download from within the SaaS or internal web app with this policy when accessed via Citrix Enterprise Browser. Default value: Enabled.

Note:

- If you have disabled the **Download** restriction for the end user, the end users can request download access from within the app when accessed via Citrix Enterprise Browser. For details, see Download access by request.
- If both **Downloads** and **Download restriction by file type** restrictions are enabled in a policy, the **Downloads** restriction takes precedence over the **Download restriction by file type**.

Download restriction by file type

Enable/disable the user's ability to download specific MIME (file) type from within the SaaS or internal web app with this policy when accessed via Citrix Enterprise Browser.

Note:

- The **Download restriction by file type** restriction is available in addition to the **Download** restriction.
- If both **Downloads** and **Download restriction by file type** restrictions are enabled in a policy, the **Downloads** restriction takes precedence over the **Download restriction by file type** restriction.
- End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.

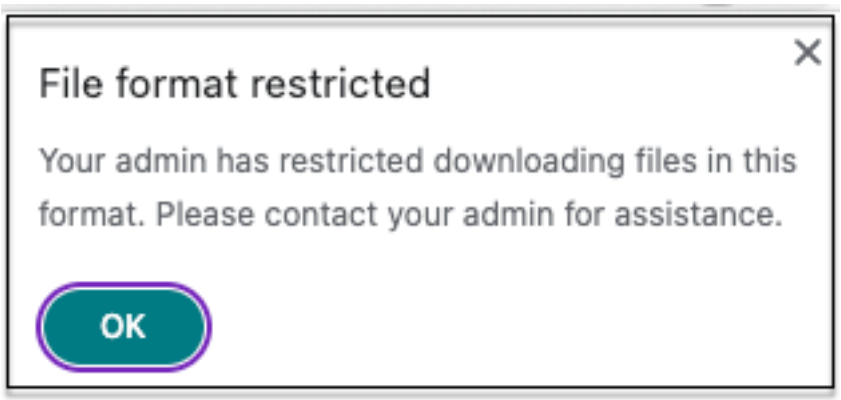
To enable downloading of MIME types, perform the following steps:

1. Create or edit an access policy. For details on creating an access policy, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Download restriction by file type** and then click **Edit**.

4. In the **Download restriction by file type settings** page, select one of the following:
   - **Allow all downloads with exceptions** –Select the types that must be blocked and allow all other types.
   - **Block all downloads with exceptions** –Select only the types that can be uploaded and block all other types.
5. If the file type does not exist in the list, then do the following:
   a) Click **Add custom MIME types**.
   b) In **Add MIME types**, enter the MIME type in the format `category/subcategory<extension>`. For example, `image/png`.
   c) Click **Done**.

   The MIME type now appears in the list of exceptions.

When an end user tries to download a restricted file type, Citrix Enterprise Browser displays the following warning message:



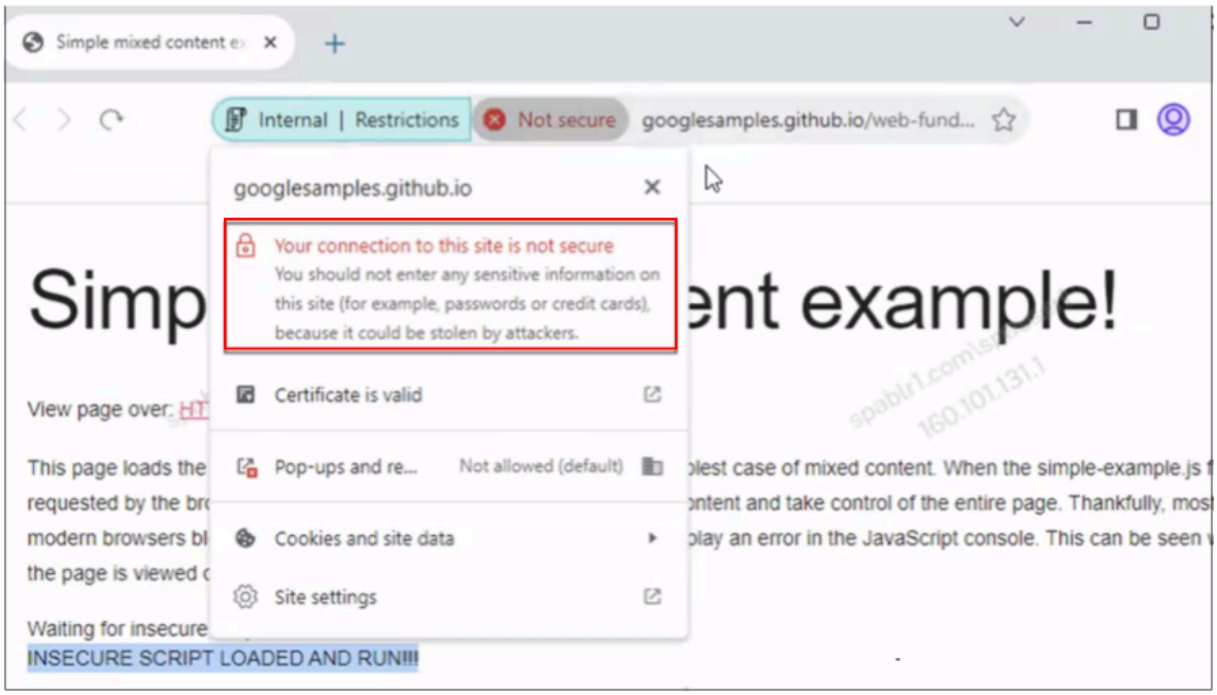
Insecure content

Enable/disable end users from accessing insecure content within the SaaS or internal web app configured with this policy when accessed via Citrix Enterprise Browser. Insecure content is any file linked to from a webpage using an HTTP link rather than an HTTPS link. Default value: Disabled.

To enable viewing insecure content, perform the following steps:

1. Create or edit an access policy. For details on creating an access policy, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Insecure content**.
4. Click **Save**, and then click **Done**.

The following figure displays a sample notification when you access an insecure content.



Keylogging protection

Enable/disable keyloggers from capturing keystrokes from the SaaS or internal web app with this access policy when accessed via Citrix Enterprise Browser. Default value: Enabled.

Microphone

Prompt/do not prompt users every time to access the microphone within the SaaS or internal web app configured with this policy when accessed via Citrix Enterprise Browser. Default value: Prompt every time.

End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which the **Microphone** restriction is enabled.

To allow microphone every time without being prompted, perform the following steps:

1. Create or edit an access policy. For details, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Microphone** and then click **Edit**.
4. In the **Microphone settings** page, click **Always allow access**.
5. Click **Save**, and then click **Done**.

> **Note:**
>
> - If the **Microphone** restriction is enabled in the Secure Private Access policy, then Citrix Enterprise Browser displays the settings **Allow**.
> - If the option **Prompt every time** in the Secure Private Access policy, then the setting applied on Citrix Enterprise Browser varies depending on whether the Global App Configuration service (GACS) is used to manage Citrix Enterprise Browser.
>
> - If GACS is used, then the GACS setting is applied on Citrix Enterprise Browser.
> - If GACS is not used, then Citrix Enterprise Browser displays the setting **Ask**.
>
> - Currently, Secure Private Access does not support blocking of the microphone. If you must block a microphone, you must do it through GACS.

For more information on GACS, see Manage Citrix Enterprise Browser through Global App Configuration service.

Notifications

Allow/prompt users every time to view the notifications within the SaaS or internal web app configured with this policy when accessed via Citrix Enterprise Browser. Default value: Prompt every time.

End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which this restriction is enabled.

To block the display of notifications without prompting, perform the following steps.

1. Create or edit an access policy. For details, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Notifications** and then click **Edit**.
4. In the **Notification settings** page, click **Always block notifications**.
5. Click **Save**, and then click **Done**.

Paste

Enable/disable pasting of copied data into the SaaS or internal web app with this access policy when accessed via Citrix Enterprise Browser. Default value: Enabled.

> **Note:**
>
> - If both **Clipboard** and **Paste** restrictions are enabled in a policy, the **Clipboard** restriction

takes precedence over the **Paste** restriction.
- End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.
- For granular control of paste operations within the apps, admins can use the **Security groups** restriction. For details, see Clipboard restriction for security groups.

Personal data masking

Enable/disable redacting or masking personally identifiable information (PII) on the SaaS or internal web app with this policy when accessed via Citrix Enterprise Browser.

> **Note:**
>
> End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.

To redact or mask personally identifiable information, perform the following steps:

1. Create or edit an access policy. For details, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Personal data masking** and then click **Edit**.
4. Select the information type that you want to obscure or mask and then click **Add**.

   If the information type does not appear in the pre-defined list, then you can add a custom information type. For details, see Add custom information type.
5. Select the masking type.

   - **Full masking** –Completely cover the sensitive information to make it unreadable.
   - **Partial masking** –Partially cover the sensitive information. Only the relevant sections are covered leaving the rest intact.

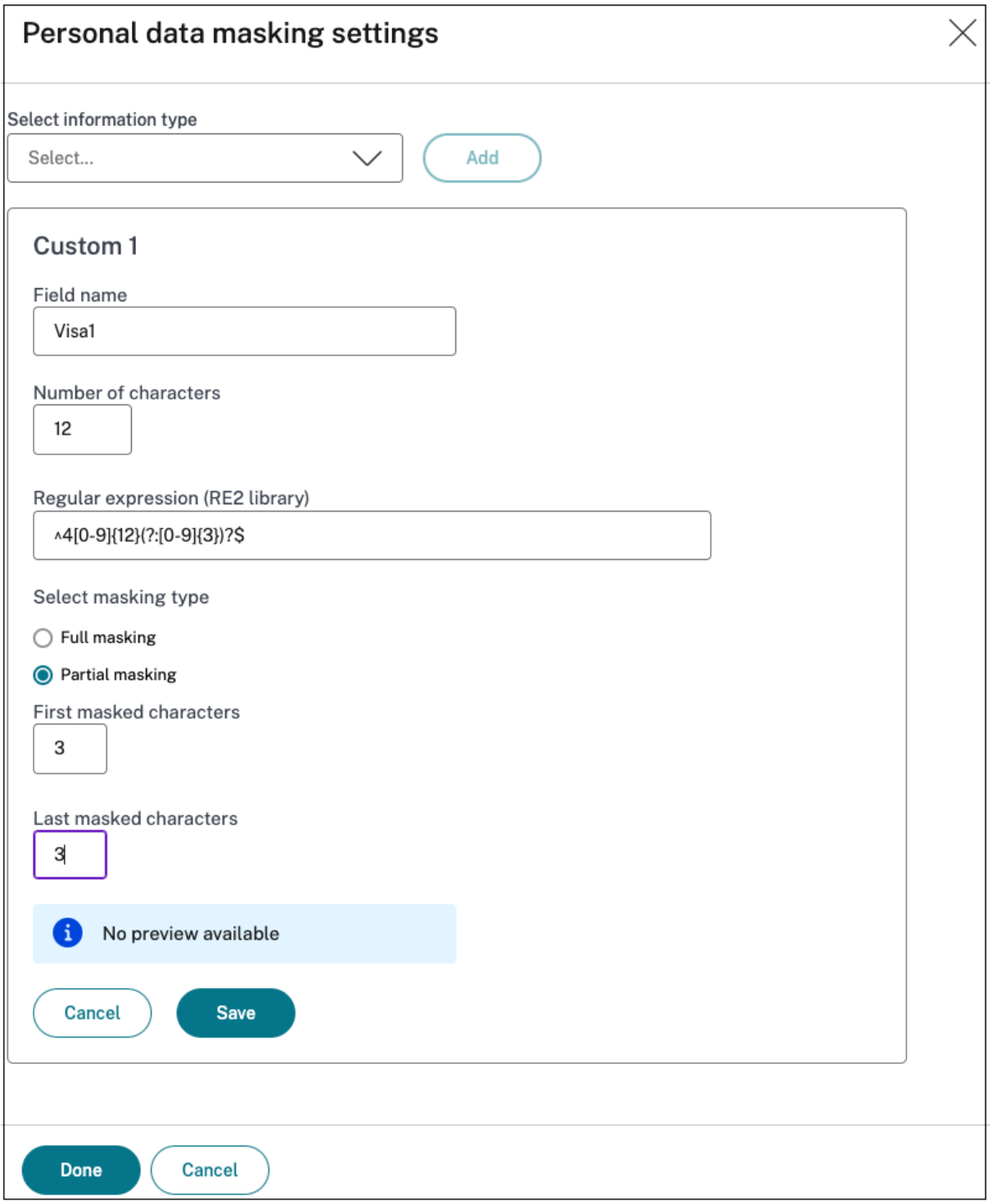
     When you select **Partial marking**, you must select characters starting from the beginning or the end of the document. You must enter the numbers in the **First masked characters** and **Last masked characters** fields.

     The **Preview** field displays the masking format. This preview is not available for custom policies.
6. Click **Save** and then click **Done**.

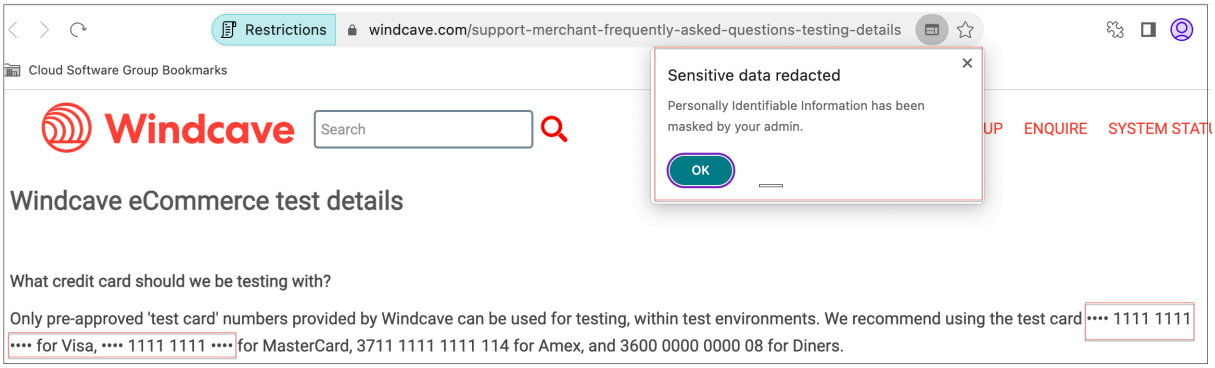
Add custom information type

You can add a custom information type by adding the information type's regular expression.

1. In **Select Information type**, select **Custom**, and then click **Add**.
2. In **Field name**, enter the name for the information type that you want to mask.
3. In **Number of characters**, enter the number of characters of the information type.
4. In **Regular Expression (RE2 library)**, enter the expression for the custom information type. For example, `^4[0-9]{ 12 } (?:[0-9]{ 3 } )?$`.
5. Select a masking type, if you want to mask the complete information or the first or last few characters.
6. Click **Save**, and then click **Done**.



The following figure displays a sample app in which the PII is masked. The figure also displays the notification related to masking of the PII.



Popups

Enable/disable the display of popups within the SaaS or internal web app configured with this policy when accessed via Citrix Enterprise Browser. By default popups are disabled within webpages. Default value: Always block pop-ups.

End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which this restriction is enabled.

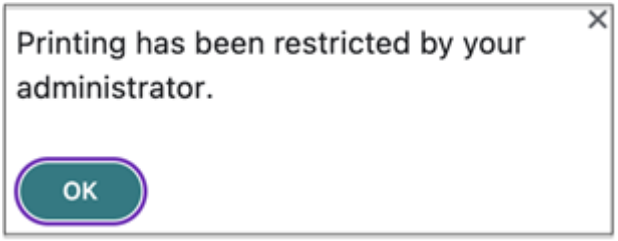
To enable display of popups, perform the following steps:

1. Create or edit an access policy. For details, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Popups** and then click **Edit**.
4. In the **Popups settings** page, click **Always allow pop-ups**.
5. Click **Save**, and then click **Done**.

Printing

Enable/disable printing data from the configured SaaS or Internal web apps with this policy when accessed via Citrix Enterprise Browser. Default value: Enabled.

The following message appears when an end user tries to print content from the application for which the printing restriction is enabled.



> **Note:**
>
> - If you have disabled the printing option for the end user, the end users can request printing access from within the app when accessed via Citrix Enterprise Browser. For details, see Print access by request.
> - If both **Printing** and **Printer management** restrictions are enabled in a policy, the **Printing** restriction takes precedence over the **Printer management** restriction.

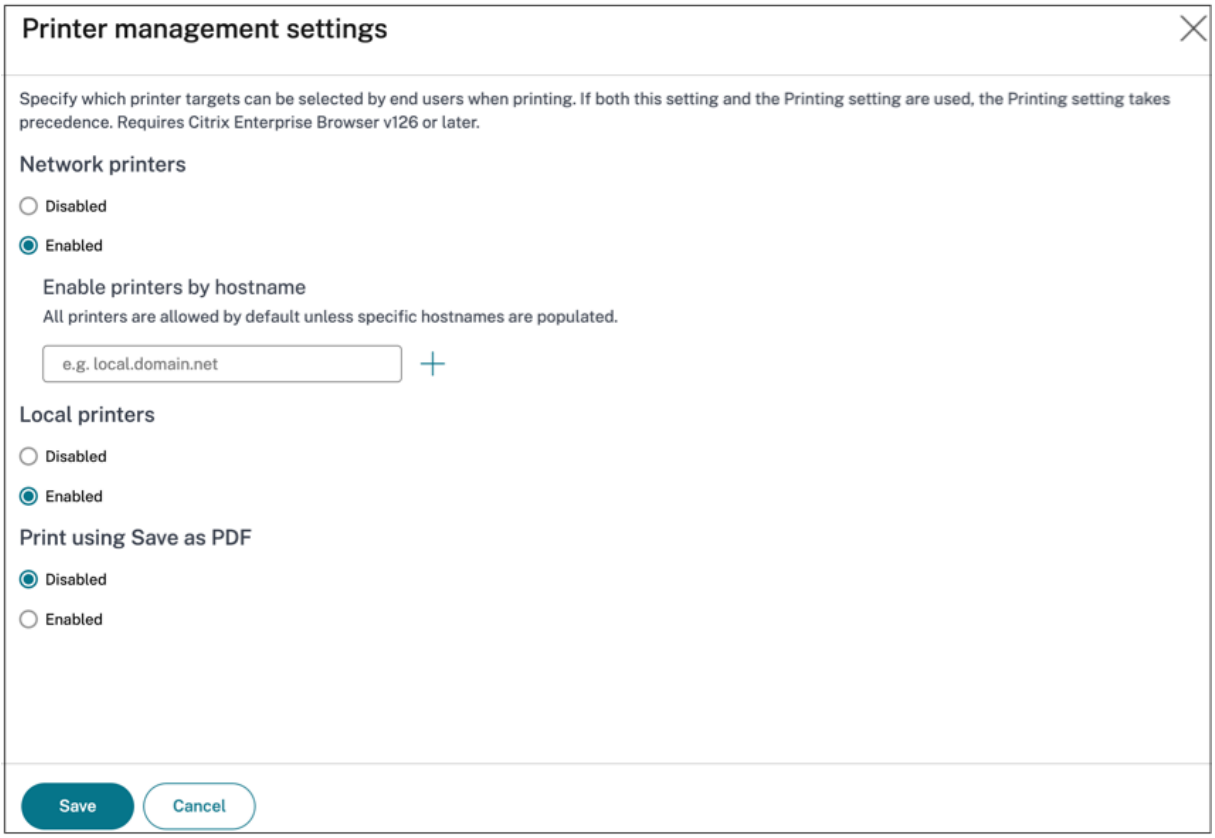
Printer management

Enable/disable printing data by using the admin-configured printers from the configured SaaS or internal web apps with this policy when accessed via Citrix Enterprise Browser.

> **Note:**
>
> - The **Printer management** restriction is available in addition to the **Printing** restriction where printing is either enabled or disabled.
>
> If both **Printing** and **Printer management** restrictions are enabled in an access policy, the **Printing** restriction takes precedence over the **Printer management** restriction.
> - End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.

To enable/disable printing restrictions, perform the following steps:

1. Create or edit an access policy. For details on creating an access policy, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Printer management** and then click **Edit**.



1. Select the exceptions as per your requirement.

   - **Network printers** - A network printer is a printer that can be connected to a network and used by multiple users.

     - **Disabled:** Printing from any printers in the network is disabled.
     - **Enabled:** Printing from all network printers is enabled. If printer host names are specified, then all other network printers apart from the ones specified are blocked.

     Note: Network printers are identified by their host names.

   - **Local printers** - A local printer is a device directly connected to an individual computer through a wired connection. This connection is typically facilitated through USB, parallel ports, or other direct interfaces.

     - **Disabled:** Printing from all local printers is disabled.
     - **Enabled:** Printing from all local printers is enabled.

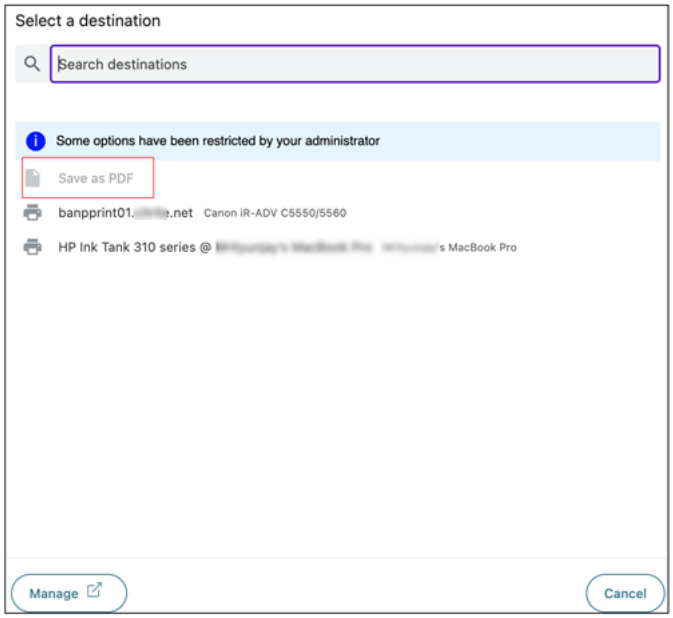
   - **Print using Save as PDF**

     - **Disabled**: Saving the content from the application in a PDF format is disabled.
     - **Enabled:** Saving the content from the application in a PDF format is enabled.

2. Click **Save**.

If a network printer is disabled, then the specific printer name appears grayed out when you try to select the printer in the **Destination** field.

Also, if **Print using Save as PDF** is disabled, then when you click the **See more** link in the **Destination** field, the **Save as PDF** option appears grayed out.



Screen capture

Enable/disable the ability to capture the screens from the SaaS or internal web app with this policy when accessed via Citrix Enterprise Browser using any of the screen capture programs or apps. If a user tries to capture the screen, a blank screen is captured. Default value: Enabled.

Upload restriction by file type

Enable/disable the user's ability to download specific MIME (file) type from the SaaS or internal web app with this policy when accessed via Citrix Enterprise Browser.

> **Note:**
>
> - The **Upload restriction by file type** restriction is available in addition to the **Upload** restriction.
> - If both **Upload** and **Upload restriction by file type** restrictions are enabled in a policy, the **Uploads** restriction takes precedence over the **Upload restriction by file type** restriction.
> - End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.

To enable/disable uploading of MIME types, perform the following steps:

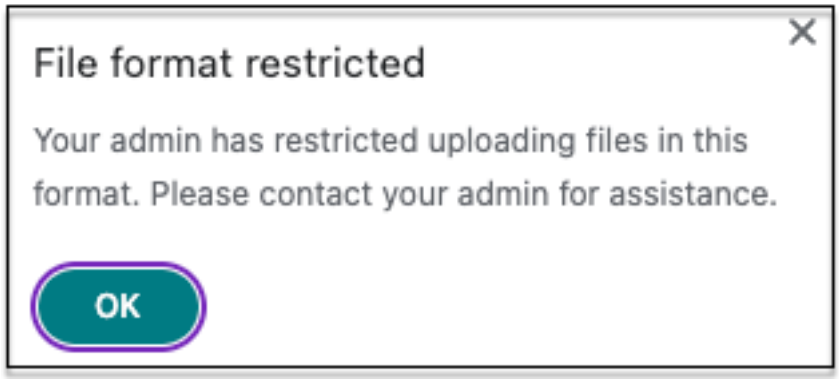
1. Create or edit an access policy. For details, see Create access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Upload restriction by file type** and then click **Edit**.
4. In the **Upload restriction by file type settings** page, select one of the following:

   Allow all uploads with exceptions –Upload all files except the selected types.
   Block all uploads with exceptions –Blocks all file types from uploading except the selected types.
5. If the file type does not exist in the list, then do the following:

   a) Click **Add custom MIME types**.
   b) In **Add MIME types**, enter the MIME type in the format `category/subcategory<extension>`. For example, `image/png`.
   c) Click **Done**.

   The MIME type now appears in the list of exceptions.

When an end user tries to upload a restricted file type, Citrix Enterprise Browser displays a warning message.



Uploads

Enable/disable the user's ability to upload within the SaaS or internal web app configured with this policy when accessed via Citrix Enterprise Browser. Default value: Enabled.

> **Note:**
>
> If both **Uploads** and **Upload restriction by file type** restrictions are enabled in a policy, the **Uploads** restriction takes precedence over the **Upload restriction by file type** restriction.

Watermark

Enable/disable the watermark on the user's screen displaying the user name and IP address of the user's machine. Default value: Disabled.

Webcam

Prompt/do not prompt users every time to access the webcam within the SaaS or internal web app configured with this policy when accessed via Citrix Enterprise Browser. Default value: Prompt every time.

End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which the **Webcam** restriction is enabled.

To allow webcam every time without being prompted, perform the following steps:

1. Create or edit an access policy. For details, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Webcam** and then click **Edit**.
4. In the **Webcam settings** page, click **Always allow access**.
5. Click **Save**, and then click **Done**.

> **Note:**
>
> - If the Webcam restriction is enabled in the Secure Private Access policy, then Citrix Enterprise Browser displays the settings **Allow**.
> - If the option **Prompt every time** in Secure Private Access policy, then the setting applied on Citrix Enterprise Browser varies depending on whether the Global App Configuration service (GACS) is used to manage Citrix Enterprise Browser.
>
> - If GACS is used, then the GACS setting is applied on Citrix Enterprise Browser.
> - If GACS is not used, then Citrix Enterprise Browser displays the setting **Ask**.
>
> - Currently, Secure Private Access does not support blocking of the webcam. If you must block webcam, you must do it through GACS.

For more information on GACS, see Manage Citrix Enterprise Browser through Global App Configuration service.

Clipboard restriction for security groups

You can enable clipboard access for a designated group of apps by using the **Security groups** restriction **(Applications > Security groups)**. Security groups are assigned a set of apps within which the

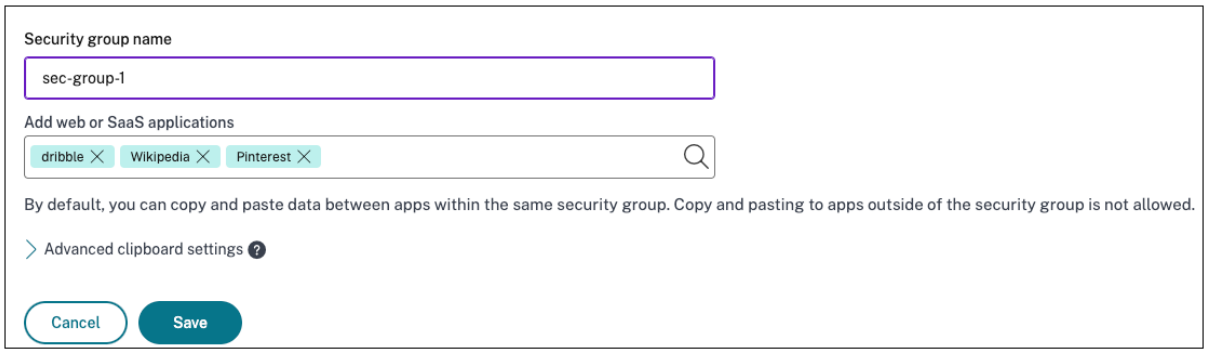
copy and paste operations can be performed. To enable clipboard access within the apps in a security group, you must just have an access policy configured with the action **allow** or **allow with restrictions** without selecting any access setting.

- When the **Security groups** restriction is enabled, you cannot copy / paste data between applications in different security groups. For example if the app "ProdDocs"belongs to security group "SG1"and the app "Edocs"belong to security group "SG2", you cannot copy / paste content from "Edocs"to "ProdDocs"even if **Copy** / **Paste** restriction is enabled for both groups.
- For apps not part of a security group, you can have an access policy created with action **allow with restrictions** and selecting the restrictions (**Copy**, **Paste**, or **Clipboard**). In this case, the app is not part of a security group and hence the **Copy** / **Paste** restriction can be applied on that app.

> **Note:**
>
> You can also restrict clipboard access for apps accessed via Citrix Enterprise Browser through the Global App Configuration service (GACS). If you are using GACS to manage Citrix Enterprise Browser, then use the **Enable Sandboxed Clipboard** option to manage the clipboard access. When you restrict clipboard access through GACS, it applies to all apps accessed via Citrix Enterprise Browser. For more information on GACS, see Manage Citrix Enterprise Browser through Global App Configuration service.

To create a security group, perform the following steps:

1. In the Secure Private Access console, click **Applications** and then click **Security groups**.
2. Click **Add a new security group**.

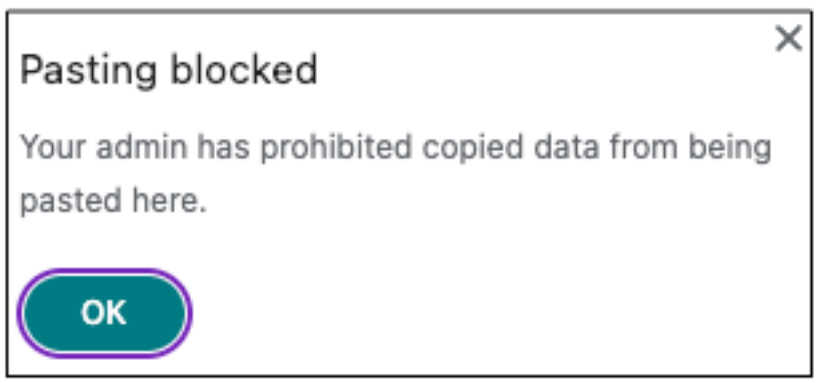


1. Enter a name for the security group.
2. In **Add web or SaaS applications**, choose the applications that you want to group to enable the copy and paste control. For example, Wikipedia, Pinterest and Dribble.
3. Click **Save**.

For details on Advanced clipboard settings, see Enable copy / paste controls for native applications and unpublished apps.

When end users launch these applications (Wikipedia, Pinterest and Dribble) from Citrix Workspace, they must be able to share data (copy / paste) from one application to the other applications within the security group. The copy / paste occurs irrespective of other security restrictions that are already enabled for the applications.

However, end users cannot copy and paste content from their local applications on their machines or unpublished applications to these designated applications and conversely. The following notification appears when the content is copied from the designated application into another application:



> **Note:**
>
> You can enable copy / paste content from local applications on user machines or unpublished applications controls by using the options in the **Advanced clipboard settings** section. For details, see Enable copy / paste controls for native applications and unpublished apps.

Enable granular level copy / paste

You can enable granular level clipboard access within the applications in a designated group. You can do so by creating access policies for the applications and enabling the **Copy** / **Paste** restriction as per your requirement.

> **Note:**
>
> Ensure that the specific access policy that you have created for granular level clipboard access has a higher priority than the policy that you have created for the security groups.

Example:

Consider that you have created a security group with three applications namely, Wikipedia, Pinterest, and Dribble.

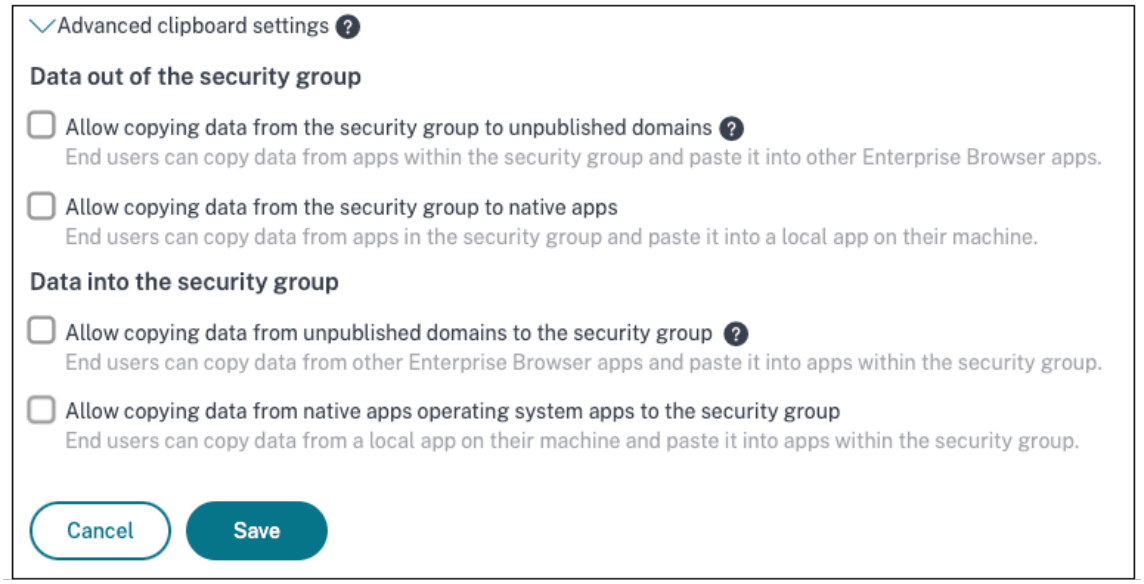
Now, you want to restrict the pasting of content from Wikipedia or Dribble into Pinterest. To do so, perform the following steps:

1. Create or edit an access policy assigned for the application `Pinterest`. For details on creating an access policy, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Select **Paste**.

Although Pinterest is part of a security group which also contains Wikipedia and Dribble, users cannot copy content from Wikipedia or Dribble to Pinterest because of the access policy associated with Pinterest in which the **Paste** restriction is enabled.

Enable copy / paste controls for native applications and unpublished apps

1. Create a security group. For details, see Clipboard security groups for Copy and Paste restrictions.
2. Expand **Advanced clipboard settings**.



3. Select the following options as per your requirement:

   - **Allow copying of data from the security group to unpublished domains** –Enable copying of data from applications in the security groups to the apps that are not published in Secure Private Access.
   - **Allow copying of data from the security group to native apps** - Enable copying of data from the applications in the security groups to the local applications on your machines.

- **Allow copying of data from the unpublished domains to the security group** –Enable copying of data from the apps not published through Secure Private Access to the applications in the security groups.
- **Allow copying of data from native apps operating system the security group** - Enable copying of data from local applications on the machines to the applications.

Known issues

- The routing table in (**Settings > Application Domain**) retains the domains of a deleted application. Hence, these applications are also considered as published applications in Secure Private Access. If these domains are accessed directly from Citrix Enterprise Browser, copy / paste is disabled from these applications irrespective of the options that you have selected in **Advanced clipboard settings**.

  For example, assume the following scenario:

  - You have deleted an application named Jira2 (`https://test.citrite.net`) that was part of a security group.
  - You have enabled the option **Allow copying of data from the security group to unpublished domains**.

  In this scenario, if the user tries to copy data from this application into another application in the same security group, the pasting control is disabled. A notification regarding the same is displayed to the user.

- For a SaaS app, the app access can be denied if the application is configured with an access policy with action **Deny access.** The end users can still access the app because the app traffic is not tunneled through Secure Private Access. Also, if the application is part of the security group, the security group settings are not honored and hence you cannot copy / paste content from the application.

Discover domains or IP addresses accessed by end users

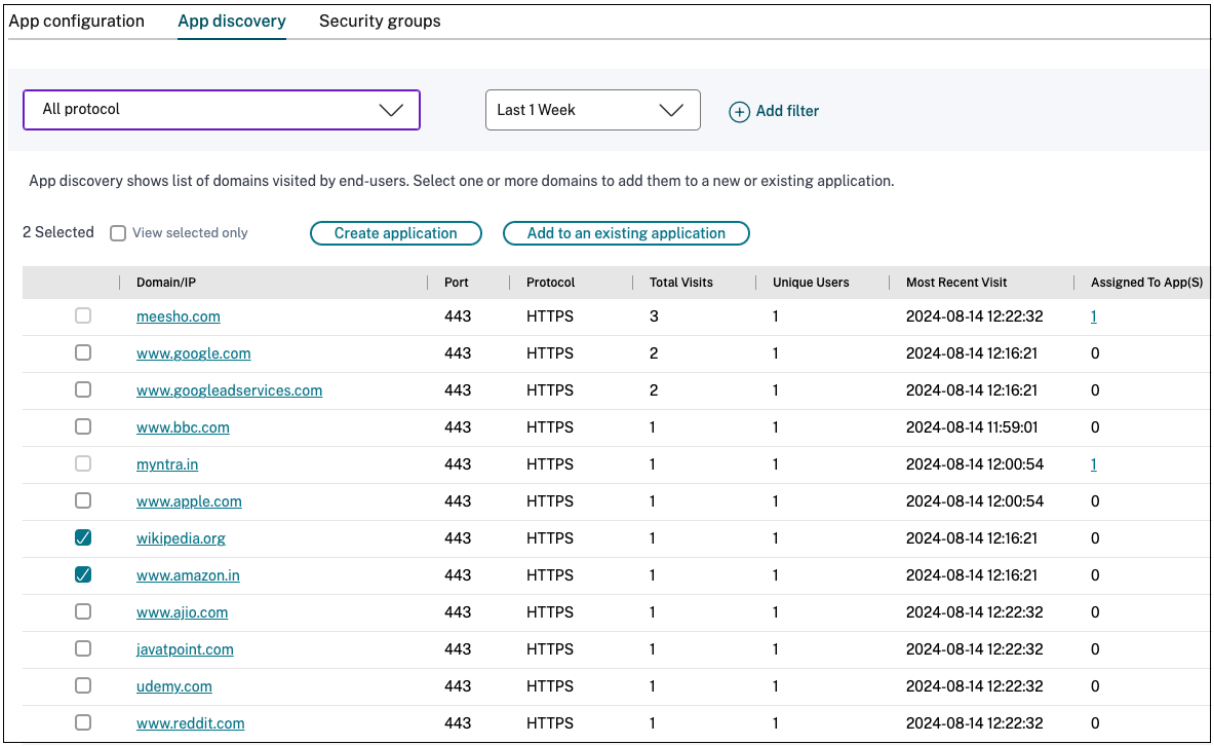
September 6, 2025

The Application Discovery feature helps an admin get visibility into the external and internal applications (HTTP/HTTPS and TCP/UDP apps) that are being accessed in an organization. This feature discovers and lists all the domains/IPs addresses, published or unpublished. Thus, admins can see what domains/IP addresses are getting accessed, by whom, and decide if they want to publish them as applications, providing access to those users.

The Application Discovery feature provides the following capabilities to the admins:

- Provides visibility into both internal or external domains/IPs addresses accessed by the end users.
- Provides a comprehensive visibility into all types of applications accessed (HTTP, HTTPS, TCP, and UDP). Access Citrix Enterprise Browser™ and Citrix Secure Access agent are supported.
- Displays both published or unpublished domains/IP addresses accessed by the end users.

The following figure displays a sample **App discovery** page. The **App discovery** page allows filtering of domains based on the protocol (HTTP/HTTPS, TCP/UDP) and Domain/IP address and port numbers. It also displays the unpublished (not assigned to any app) domains accessed by the end users.

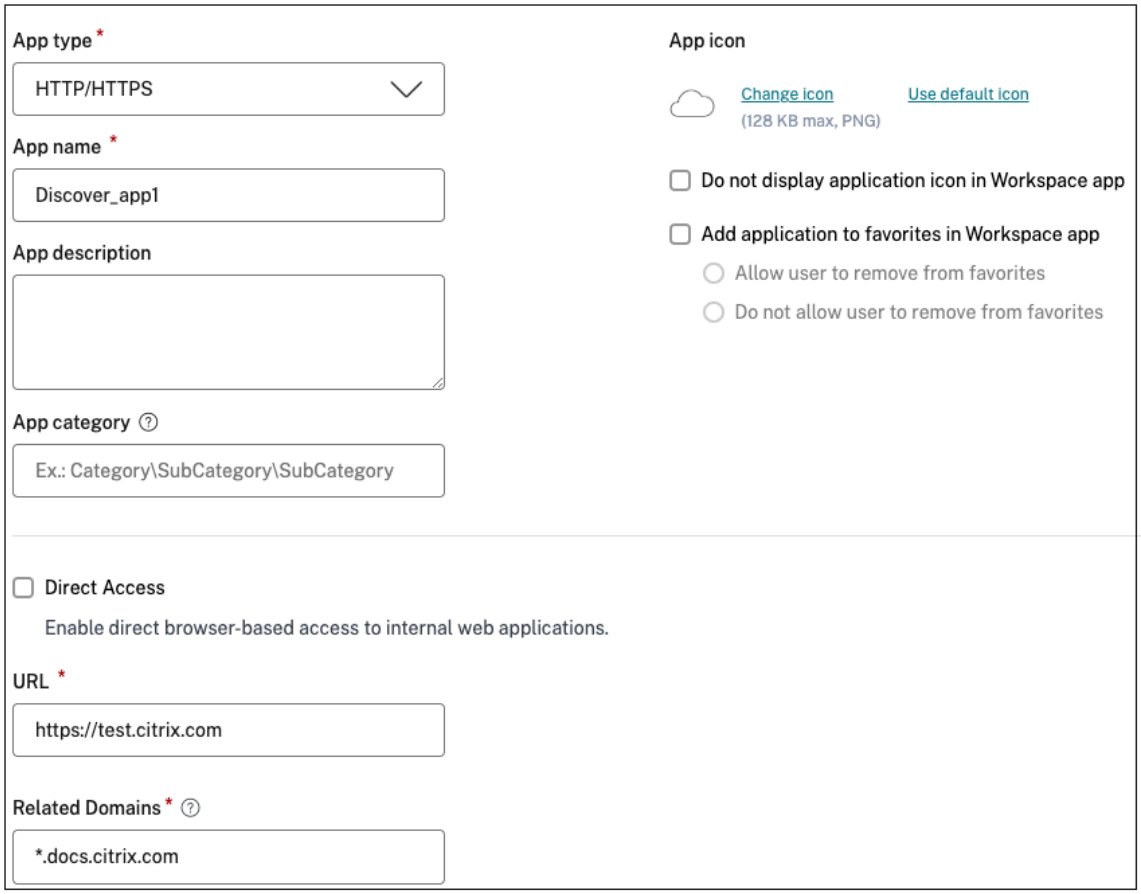


Application Discovery for internal domains in a new environment

The Application Discovery feature can be used if you are setting up a new Secure Private Access environment and want visibility into the applications that are to be configured. This feature discovers and lists all domains/IPs addresses that are accessed by your end users so you can configure them as applications. Use the following steps to enable the Application Discovery feature when you are setting up your Secure Private Access environment:

- To discover internal web applications, configure an application within Secure Private Access and specify the wildcard related domain that belongs to the domain/subdomain of the applications that you want to discover.

For example, if you want to discover all applications with the domain citrix.com, create an application with a related wildcard domain as `*.citrix.com`. To allow completion of application configuration, add any test URL as the main web app URL section.

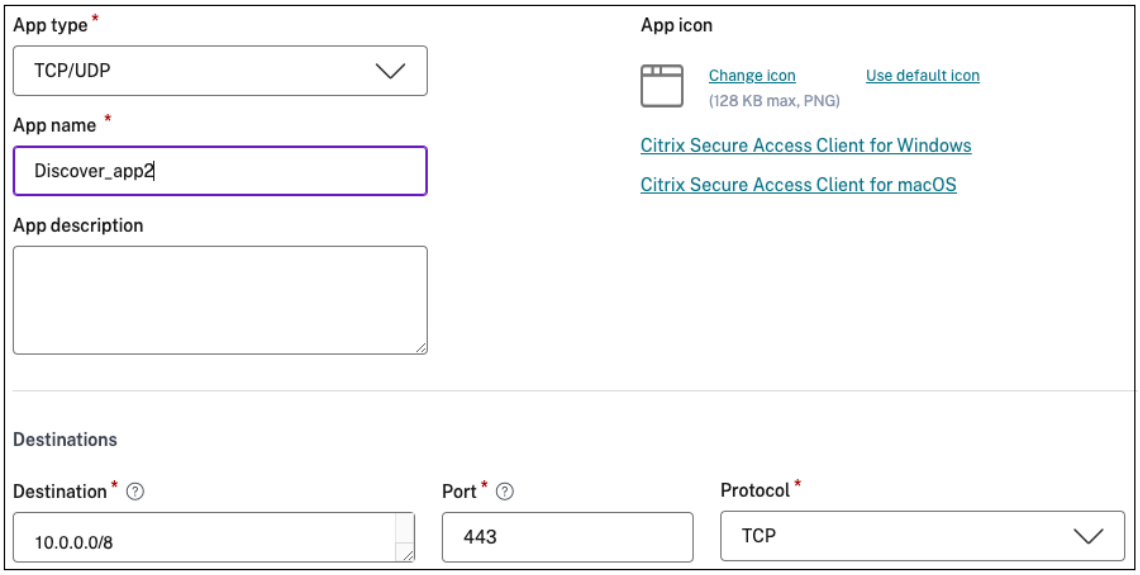


Web app URL: `https://test.citrix.com/`
Related domain: `*.citrix.com`

- For internal TCP/UDP apps, configure an application within Secure Private Access and specify the subnet along with the TCP/UDP protocol and range of ports (enter * to include the entire range). This enables discovering all TCP and UDP apps from the Citrix Secure Access agent. For example, if you want to discover all applications within subnet 10.0.0.0/8, then configure the app with the following details: Example: 10.0.0.0/8:

  Port: (*)

  Protocol: TCP



- Once you have created the applications, you must also define users that are allowed access to apps with the configured domains and IP subnets. Create an access policy and assign users to whom you want to allow access to the FQDNs/IP addresses configured in the applications created. These can be an initial set of test users or a limited number of users you want to give access to initially.
- After creating the applications and corresponding access policies, users can continue to access applications from the Citrix Workspace app and access different domains. All FQDN/IP addresses accessed by the end users start to show up in the Application Discovery page.

> **Note:**
>
> - Once you have discovered and identified most of the applications over a few days/weeks, we recommend deleting the initially created applications so that the wider access given via the wildcard domains and IP subnets can be closed down, and only specific application URLs and IP addresses that are discovered must be allowed access via new applications.
> - Add the prefix `Discover` in the app name to indicate that this is a special app configuration to enable discovery monitoring and reporting. This naming helps you identify to remove the wild card domains or IP subnets or both so you can reduce the overall app access zone to just the specific FQDNs and IP/port combinations later in weeks or a month.
> - To access TCP/UDP apps, users must use the Citrix Secure Access agent. App access from various access methods is monitored based on the apps' domains and subnets configuration and reported within the **App Discovery** page.
> - Even after you have removed the discovered applications, this feature keeps on discovering domains/IP addresses accessed by your users. So at any time, you can come back to the **App Discovery** page to see what is being accessed and if there are any new domains/IP addresses discovered that must be configured as applications.

For details on adding the domains, FQDNs, or IP address, see the following topics.

- Configure HTTP/HTTPS applications
- Configure TCP/UDP apps

Create an application from the App discovery page

To create an application for main domains and unpublished domains from the **App discovery** page, do the following steps:

1. Navigate to **Applications > App discovery**.
2. Select a domain from the list.

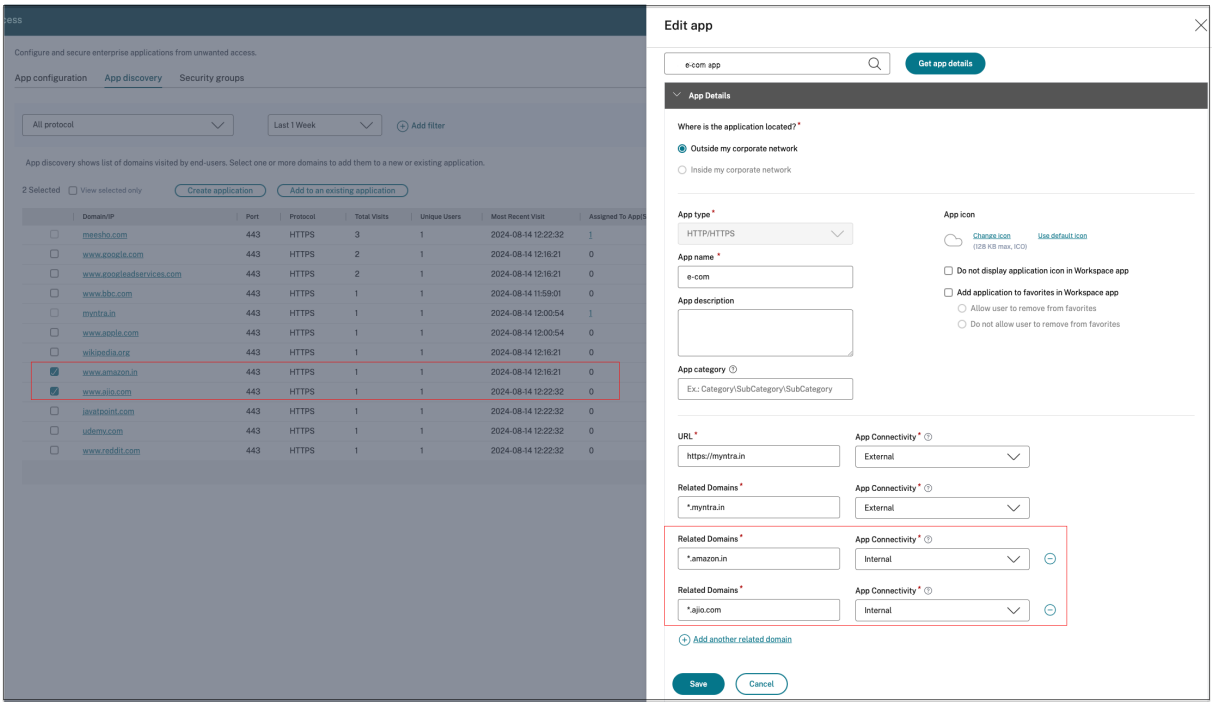
   > **Note:**
   >
   > - You cannot select domains belonging to different protocols to create an application. An error message is displayed when you select domains belonging to different protocols.
   > - If a domain is already associated with an application, you cannot select that domain again to create an application. The checkbox corresponding to that domain appears grayed out and when you hover the mouse over the checkbox, a tooltip appears.

3. Click **Create application**. For details on creating an application, Configure HTTP/HTTPS applications and Configure TCP/UDP apps.

Update an existing application

To add a domain to an existing application, perform the following steps:

1. Select the domain that must be added to an application.
2. Click **Add to an existing application**.
3. In **Applications**, select the application to which you want to add these domains.
4. Click **Get app details**.
5. The **Related Domains** field displays all the domains that you selected earlier in separate rows.
6. Click **Finish**.



Note:

- You can only add a TCP/UDP destination IP address to an existing TCP/UDP application. The **Applications** field lists only the TCP/UDP apps configured in the system.
- You can select an existing HTTP/HTTPS or TCP/UDP app to add domains (main or single entry) whose protocol is HTTP/HTTPS.
- You cannot select a domain that is already associated with an application.

End user flow

September 6, 2025

SaaS app

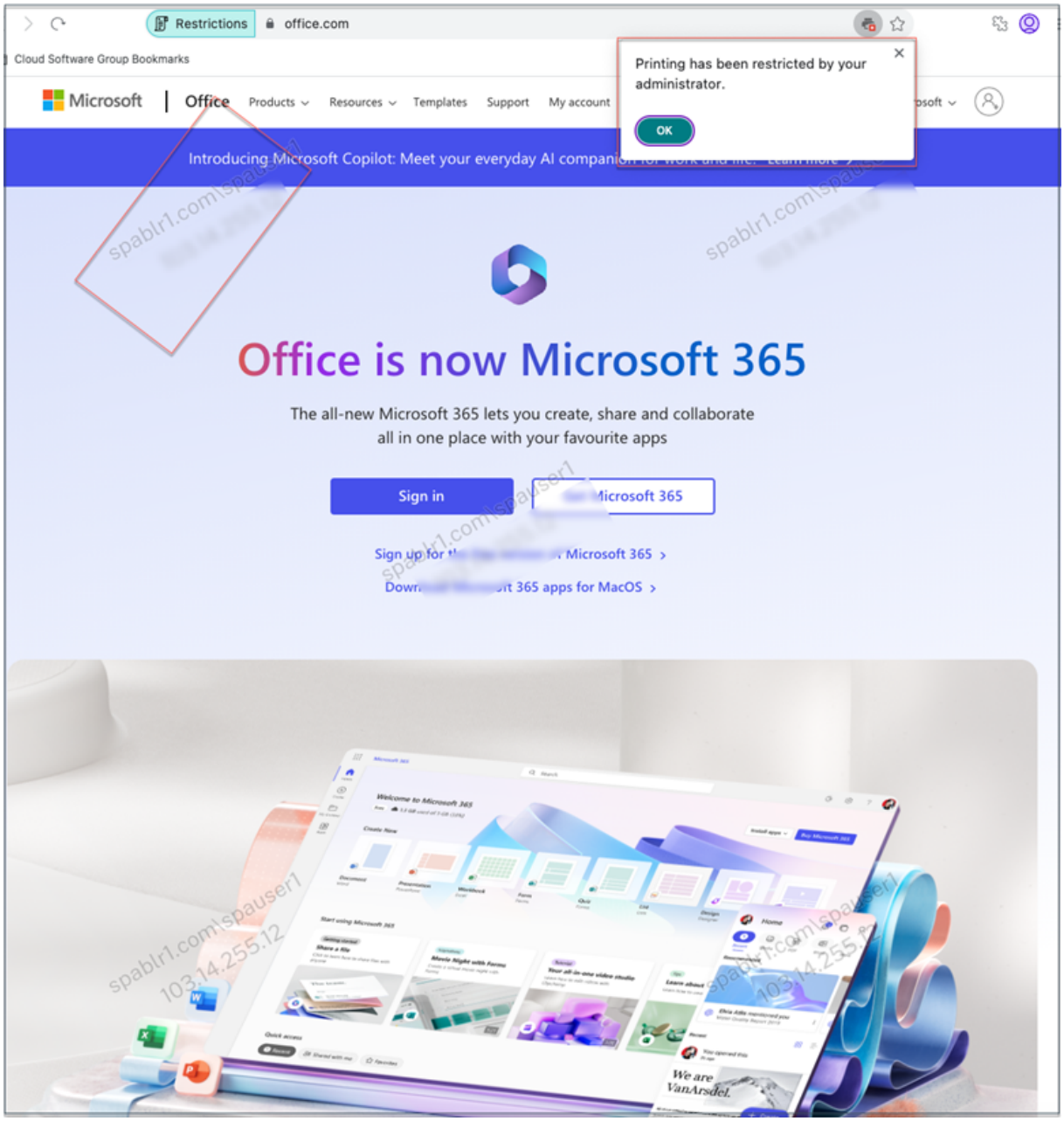
Assume that an admin has configured the Office 365 app with the watermark and print restriction for the end user. Now, when the end user accesses the Office 365 app, the watermark and print restrictions must be applied on the app.

The end user must perform the following steps to access the Office 365 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 Office 365 application is launched and contains the watermark. Also, if the end user tries to print some data from the Office 365 application, the print restriction message must be displayed to the user.



Note:

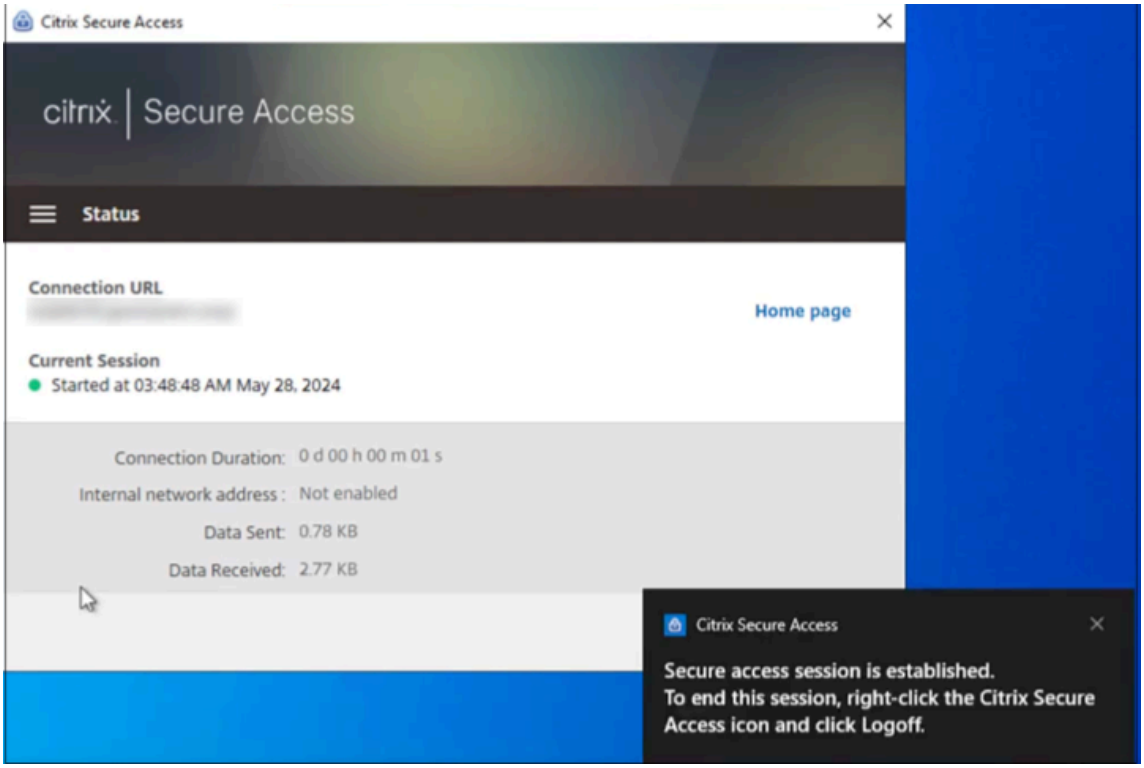
Administrators must provide users with the account information that they need to access virtual

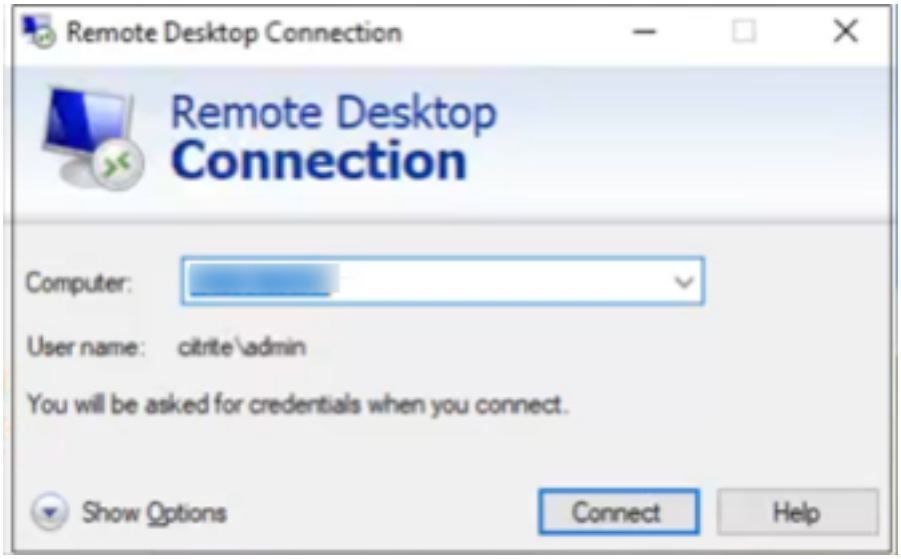
> desktops and applications. For details, see Adding store URL to Citrix Workspace app.

TCP/UDP app

If RDP is configured, end users must perform the following steps to access the TCP/UDP app.

1. Log in to the Citrix Secure Access™ client.
2. After the secure access session is established, start a remote desktop connection.





a) Press the **Windows** key, type **Remote Desktop Connection**, and press **Enter**.
b) Enter the IP address or host name of the computer that you trying to connect to.
c) Click **Connect**. You might be prompted to enter the credentials.
d) Enter the user name and password for the remote computer and then click **OK**.

A remote desktop connection is established now and the end user can interact with the remote computer.

Upgrade

September 6, 2025

You can upgrade your Secure Private Access deployments to a newer version without having to first set up new machines or sites. Before you upgrade, we recommend that you create the snapshots or save the configurations. To start an upgrade, you run the installer from the new version to upgrade the previously installed Secure Private Access plug-in.

Upgrade sequence

The upgrade sequence is as follows:

1. You can upgrade Secure Private Access through the Delivery Controller™ or through the dedicated Secure Private Access tile in the installer UI based on how you originally installed Secure Private Access.

   - If you have installed Secure Private Access via Delivery Controller, then you cannot upgrade the Secure Private Access component alone. Instead, you must upgrade all the components. For details, see Upgrade a deployment.
   - If you have installed Secure Private Access through the dedicated Secure Private Access tile, then you can upgrade it independently. For details, see Upgrade your Secure Private Access installer.

   > **Note:**
   >
   > We recommend that you install Secure Private Access through the Delivery Controller for POC environments, However, for production environments, we recommend that you use the dedicated installer so that you can adapt new features or functionality.

2. Run the database scripts. For details, see Upgrade the database using scripts.
3. Restart the **Default Web Site** and **Citrix Access Security Admin Site** on the **Internet Information Service (IIS) Manager** console to apply changes.

4. Run the StoreFront configuration again. Download the StoreFront scripts from **Settings > Configuration**, and run the scripts on the corresponding StoreFront machines. For details, see Modify integration settings.

   > **Note:**
   >
   > If you do not run the scripts, the endpoints are not triggered.

5. (Optional) Run the NetScaler Gateway script. For details, see NetScaler Gateway.

Components upgrade

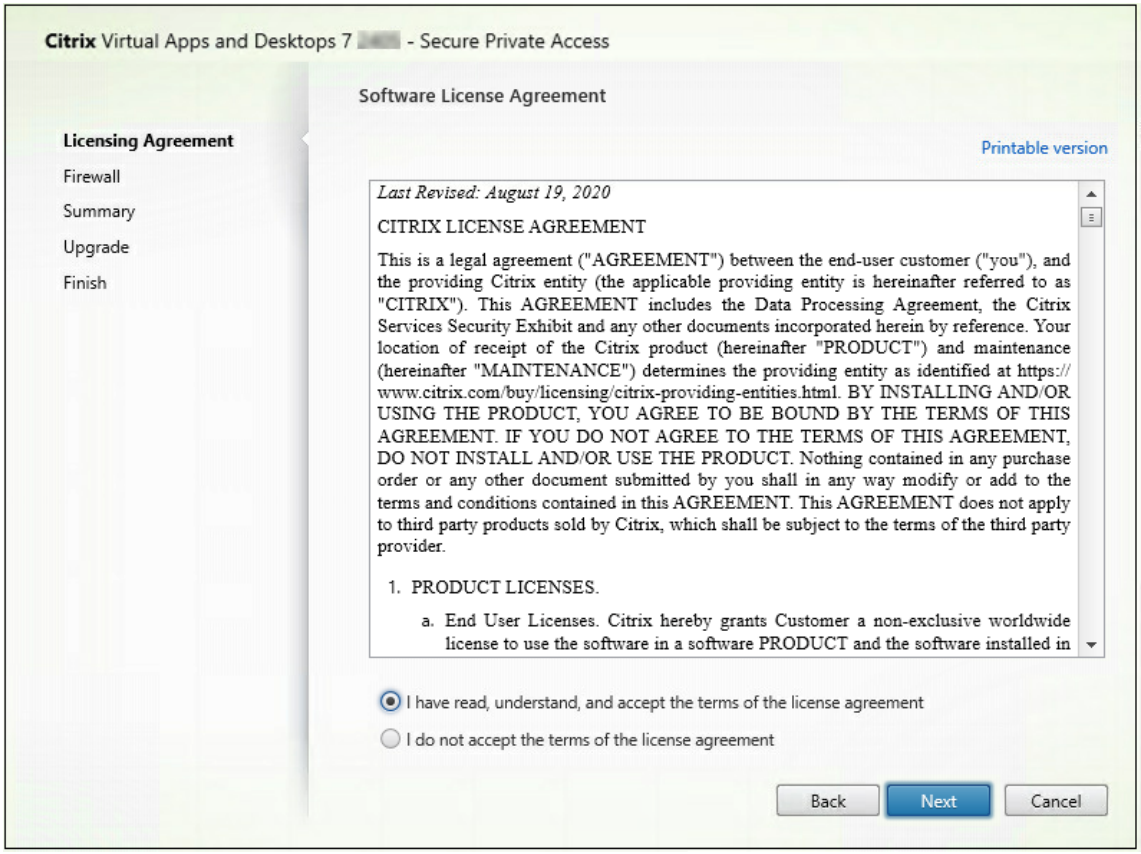
Refer to the following topics for upgrade of the components involved in Secure Private Access on-premises deployment.

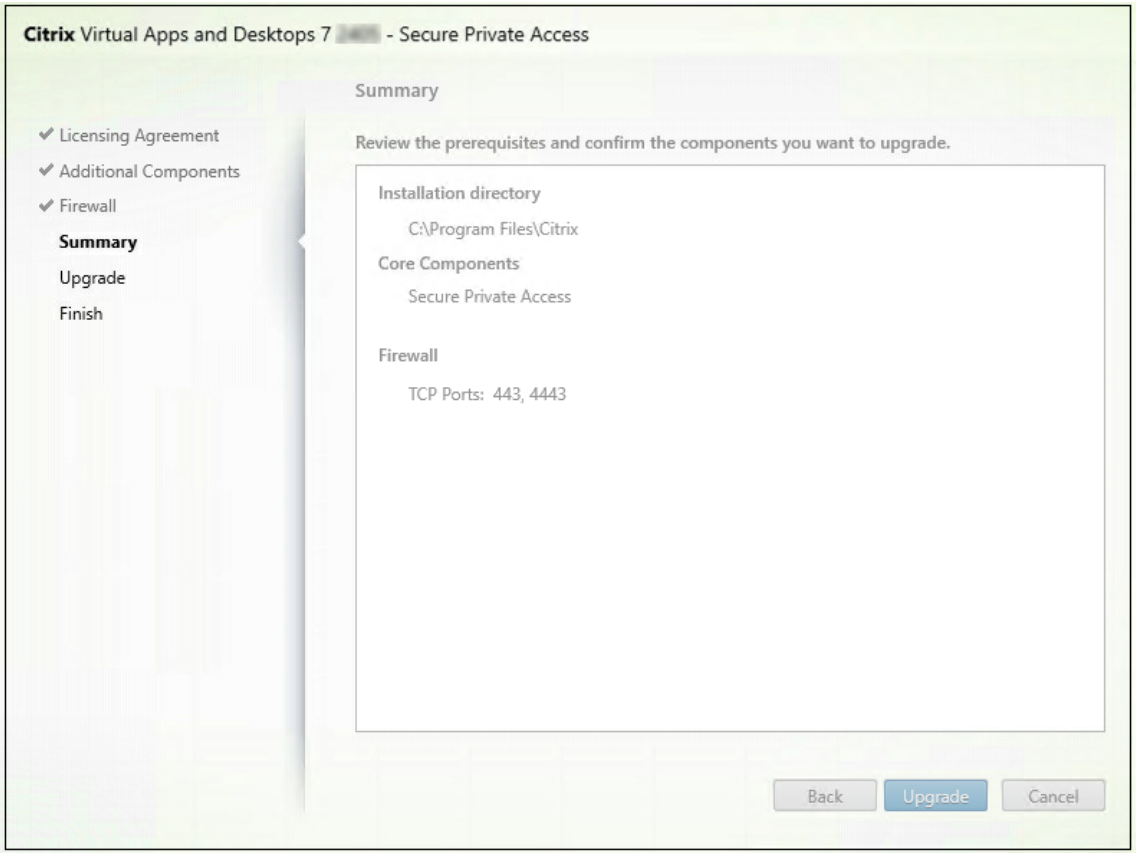
- Cloud Connector
- StoreFront
- NetScaler Gateway
- License server
- Web Studio
- Director

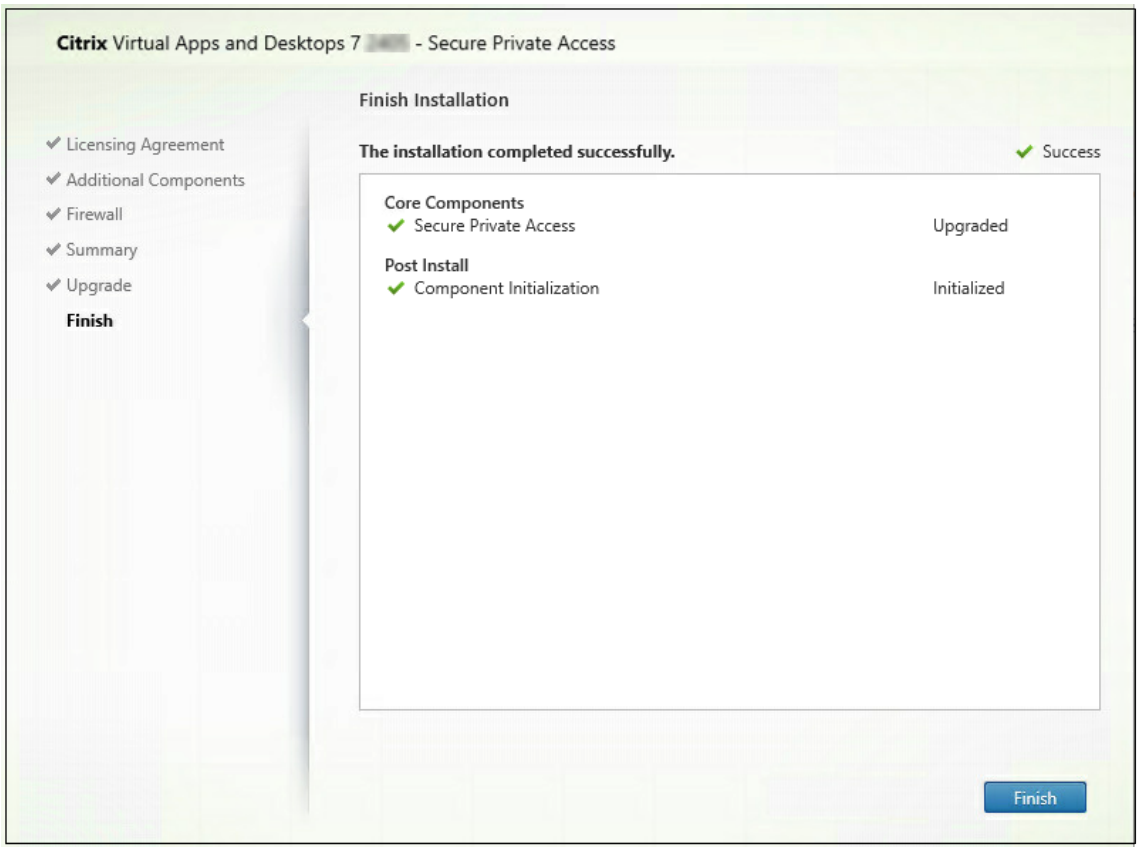
Upgrade your Secure Private Access installer

September 6, 2025

1. Download the Citrix Secure Private Access installer from https://www.citrix.com/downloads/citrix-secure-private-access/spa-onprem-standalone/.
2. Run the .exe as an administrator on a domain joined machine.
3. Follow the on-screen instructions to complete the installation.







> **Important:**
>
> After you upgrade the installer to release the latest release, you must re-run the StoreFront™ script so that the new endpoint details are available.

Next steps

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

Upgrade the database using scripts

September 6, 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>
   ```

Manage configurations

September 6, 2025

After you have installed Secure Private Access, you can modify the settings from the **Settings** page. You can manage routing of application domains, administrators, and modify the integration settings.

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

For details on how to update or modify the settings, see the following topics:

- Manage routing of application domains
- Manage administrators
- Modify integration settings

Manage unsanctioned websites

You can also configure rules for unsanctioned websites. Applications (intranet or internet) that are not configured within Secure Private Access are regarded as "Unsanctioned Websites". For details, see Unsanctioned websites.

Policy modeling tool

The Policy modeling tool provides visibility into the application access result (allowed or allowed with restriction or denied). Admins can check the access results for specific users and user condition. For details, see Policy modeling tool.

Policy modeling tool

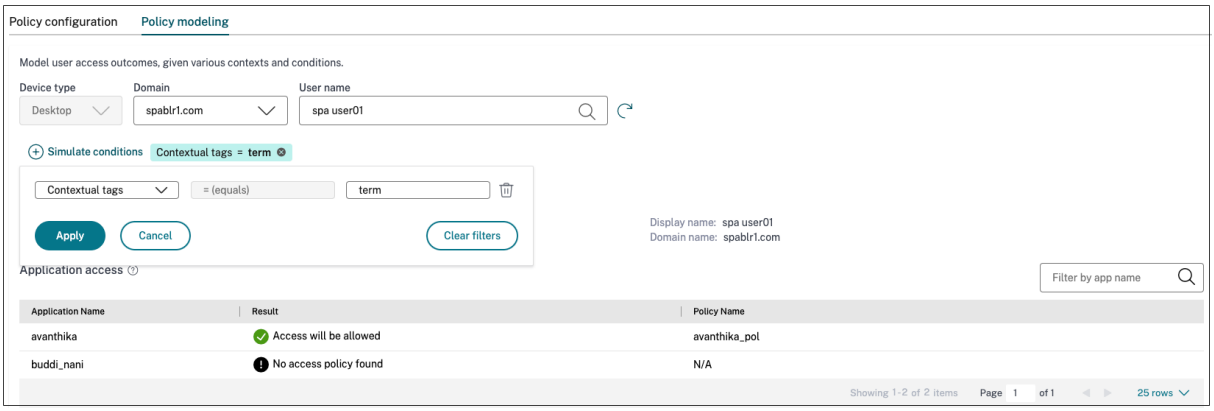
September 6, 2025

Admins can create multiple policies and assign these policies to multiple applications. As a result, it might become difficult for admins to understand the application access results for their end-users. That is, if the end-user is allowed or denied access based on the application and access policy configurations. The policy modeling tool (**Access policies > Policy modeling**) helps resolve these issues by giving the administrators full visibility into the expected application access result (allowed/allowed with restriction/denied). Admins can check the access results for specific users and add a user condition for contextual tags. The tool also displays the list of policies associated with the applications.

To analyze the access policy configuration, perform the following steps.

1. In the Secure Private Access console, click **Access Policies** and then click the **Policy modeling** tab.
2. Add the following details:
   - **Device type**: Desktop is selected by default.
   - **Domain**: Select the domain associated with the user.
   - **User**: Select the user name for which you want to analyze the applications and associated policies.
3. You can also simulate a condition based on contextual tags on the end user and their devices.
   a) Click **Simulate conditions**. The condition **Contextual tags** is selected by default.
   b) Enter the contextual tag in **Value**.
   c) Click the **+** sign to add other conditions.
4. Click **Apply**.

The applications and associated policies for the selected user are displayed in a tabular format.



Unsanctioned websites

September 6, 2025

Applications (intranet or internet) that are not configured within Secure Private Access are regarded as “Unsanctioned Websites”. By default, Secure Private Access denies access to all intranet web applications if there are no applications and access policies configured for those applications.

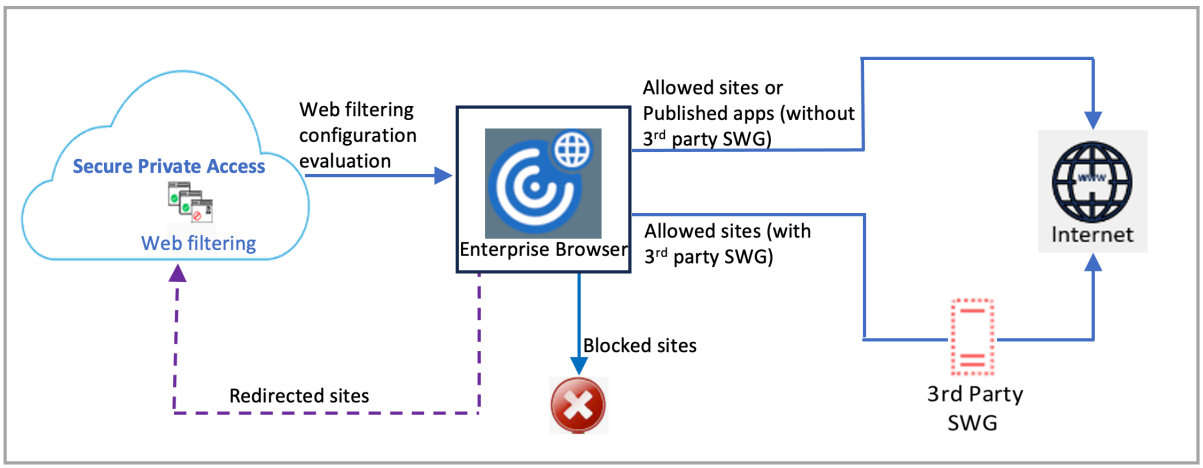
For all other internet URLs or SaaS applications that do not have an app configured, admins can use the **Settings > Unsanctioned Websites** tab from the admin console to allow or deny access via Citrix Enterprise Browser.

> **Note:**
>
> By default, settings are configured to ALLOW access to all internet URLs or SaaS apps via Citrix Enterprise Browser.

How unsanctioned websites work

1. URL analysis check is done to determine if the URL is a Citrix® service URL.
2. The URL is then checked to determine if it is an Enterprise web or SaaS app URL.
3. The URL is then checked to determine if it is identified as a blocked URL or if the URL can be allowed to be accessed.

The following illustration explains the end user traffic flow.



When a request arrives, the following checks are performed, and corresponding actions are taken:

1. Does the request match the global allow list?

    a) If it matches, the user can access the requested website.

b) If it does not match, website lists are checked.

2. Does the request match the configured website list?

   a) If it matches, the following sequence determines the action.

      i. Block

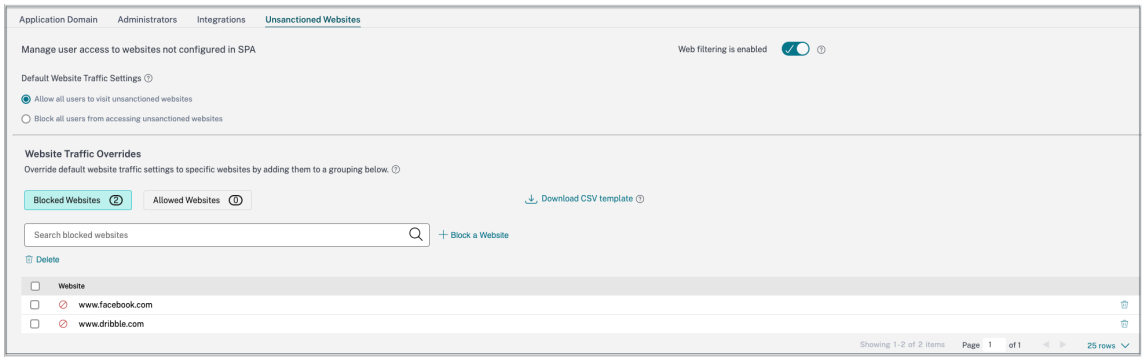
      ii. Allow

   b) If it does not match, the default action (ALLOW) is applied. The default action cannot be changed.

Configure rules for unsanctioned websites

1. In the Secure Private Access admin console, click **Settings > Unsanctioned Websites**.

   > **Note:**
   >
   > - The web filtering feature is enabled by default and access to all unsanctioned internet URLs is allowed.
   > - You can change the setting to **Block all users from accessing unsanctioned websites** to block access to any internet URL via Citrix Enterprise Browser for all users.



   You can also change settings for specific URLs by adding them to blocked websites or allowed websites.

   For example, if you have blocked access to all unsanctioned URLs by default and you want to allow access to only a few specific internet URLs, then you can do so by performing the following steps:

   a) Click the **Allowed Websites** tab, and then click **Allow a Website**.

   b) Add the website address that must be allowed access. You can either manually add the website address or drag and drop a CSV file containing the website address.

c) Click **Add a URL** and then click **Save**.

The URL is added to the list of allowed websites.

Manage settings after installation

September 6, 2025

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 necessary.

Manage administrators

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.

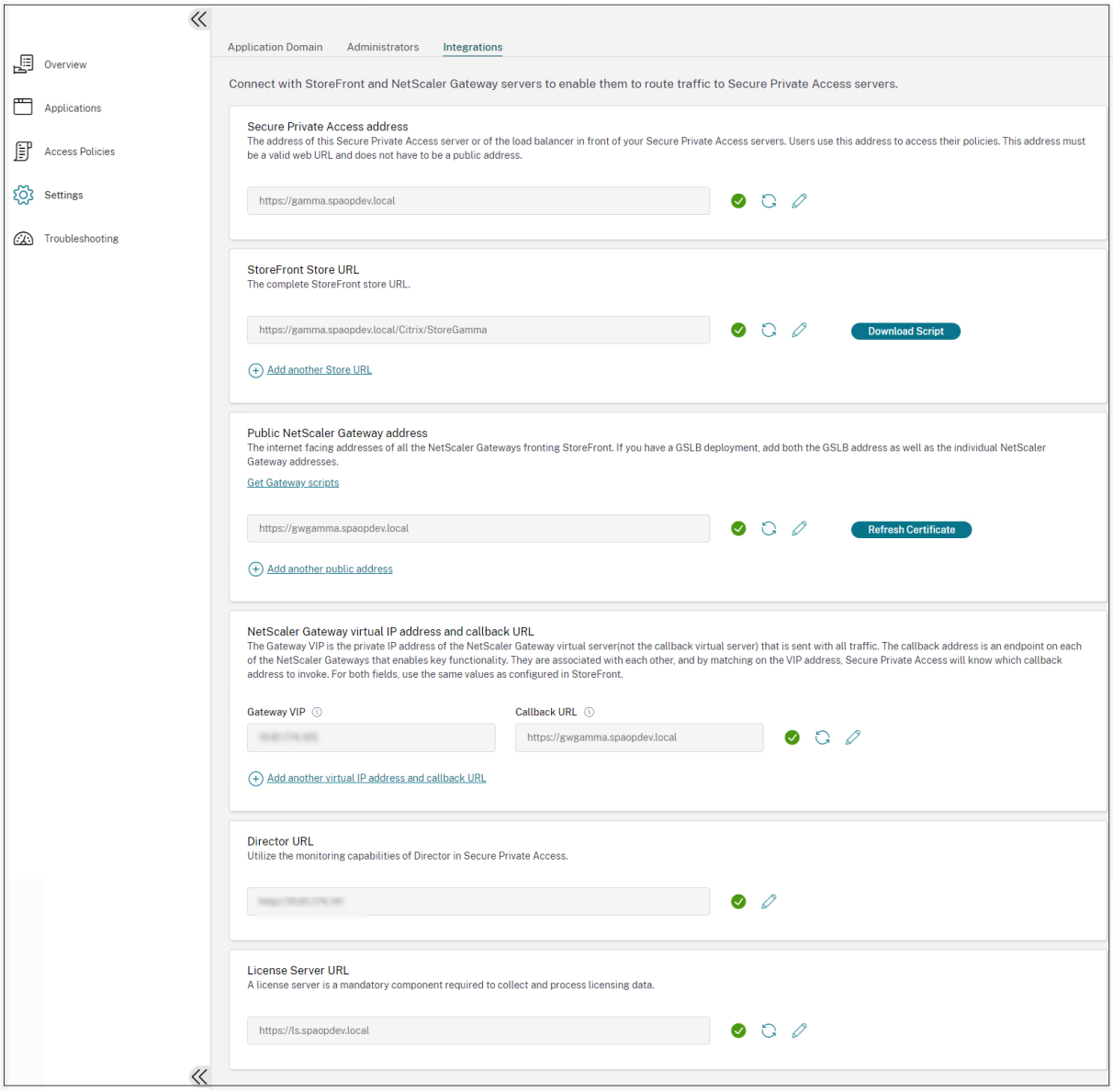
Modify integration settings

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

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 the Secure Private Access address is changed, then download the StoreFront script and run it on the StoreFront host.
- If Secure Private Access is installed on a machine different that StoreFront, then download the StoreFront script and run it on the StoreFront.



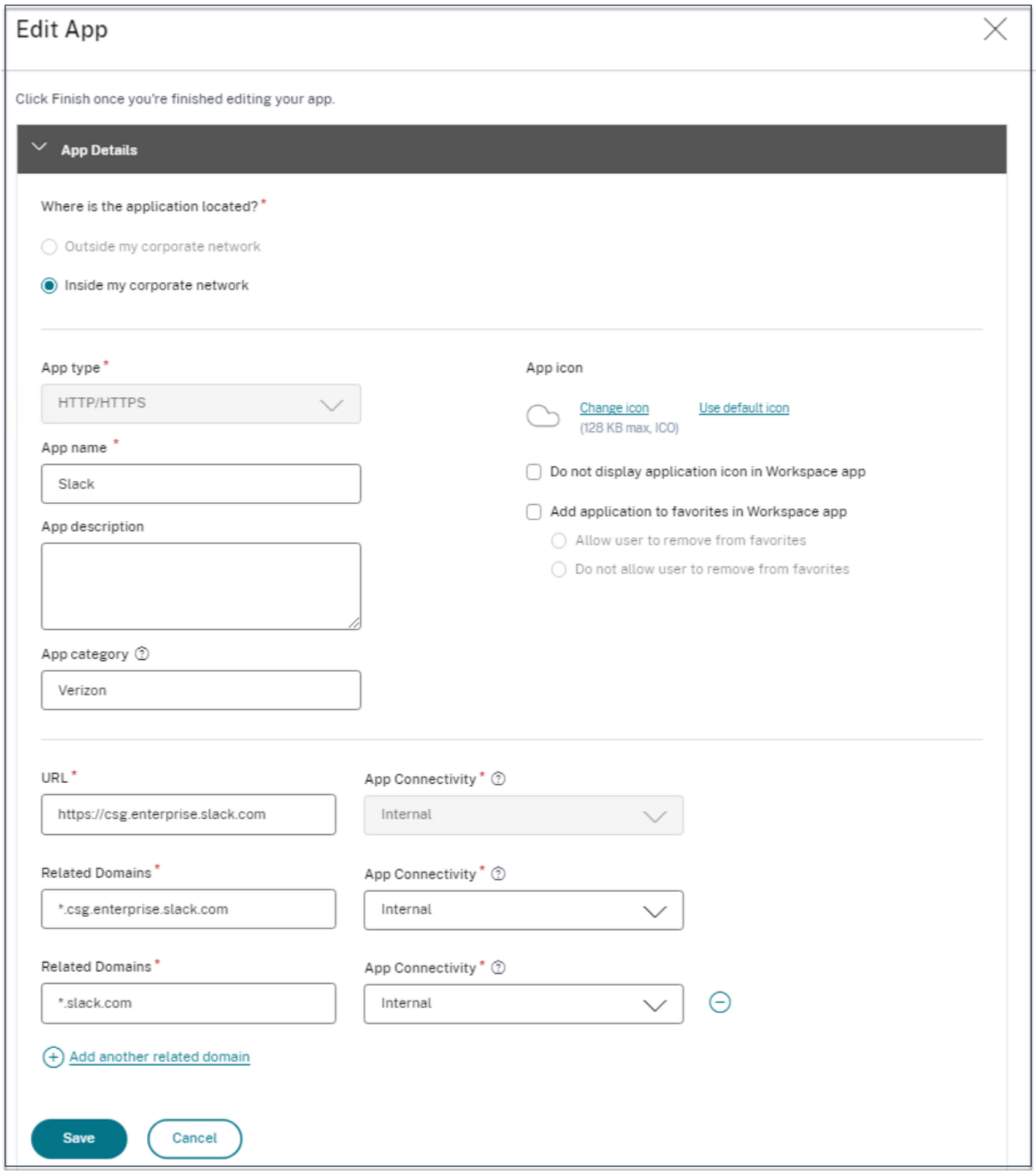
Manage applications and policies

September 6, 2025

After configuring the applications and access policies, you can edit them if necessary.

Edit an application

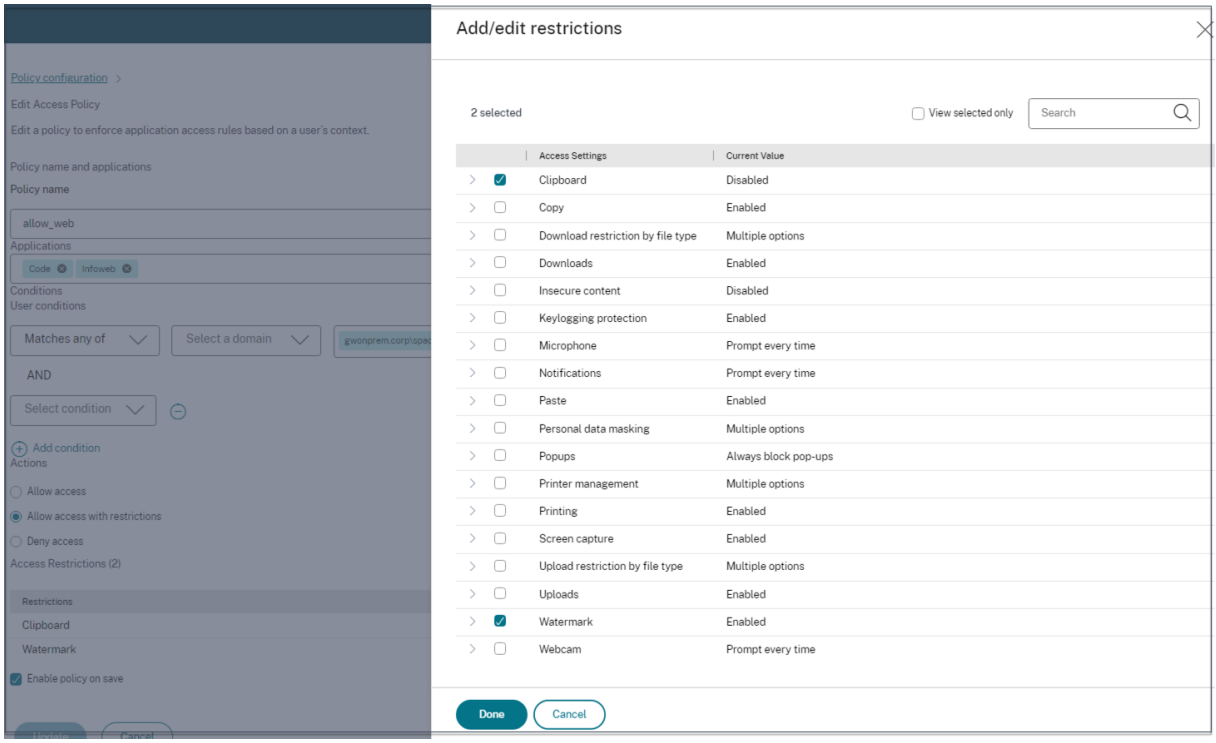
1. In the Secure Private Access admin console, click **Applciations**.
2. Click the ellipsis button in line with the application that you want to modify and then click **Edit Application**.
3. Edit the app details.
4. Click **Save**.



Edit an access policy

1. In the Secure Private Access admin console, click **Access Policies**.
2. Click the ellipsis button in line with the policy that you want to modify and then click **Edit access policy**.
3. Edit the policy details.

4. Click **Update**.



Uninstall Secure Private Access

September 6, 2025

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

1. Select **Citrix Virtual Apps and Desktops™ 7 2507 –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
```

Monitor and troubleshoot

September 6, 2025

The Secure Private Access **Troubleshooting** dashboard displays the logs related to application launch, app enumeration, and their statuses. For details, see Dashboard overview.

Troubleshooting

You might come across issues related to the following while or after setting up Secure Private Access:

- Certificate errors
- Database creation errors
- StoreFront™ failures
- Public gateway/callback gateway failures
- Secure Private Access Server not reachable

For details about fixing these issues, see Basic troubleshooting.

Session related codes in Director

Director integration with Secure Private Access enables effective performance monitoring and troubleshooting as issues from all the components in a Secure Private Access setup are captured in Director. It is recommended that you resolve the failure or exception issues by examining the logs. If that does not resolve the issue, contact support.

References

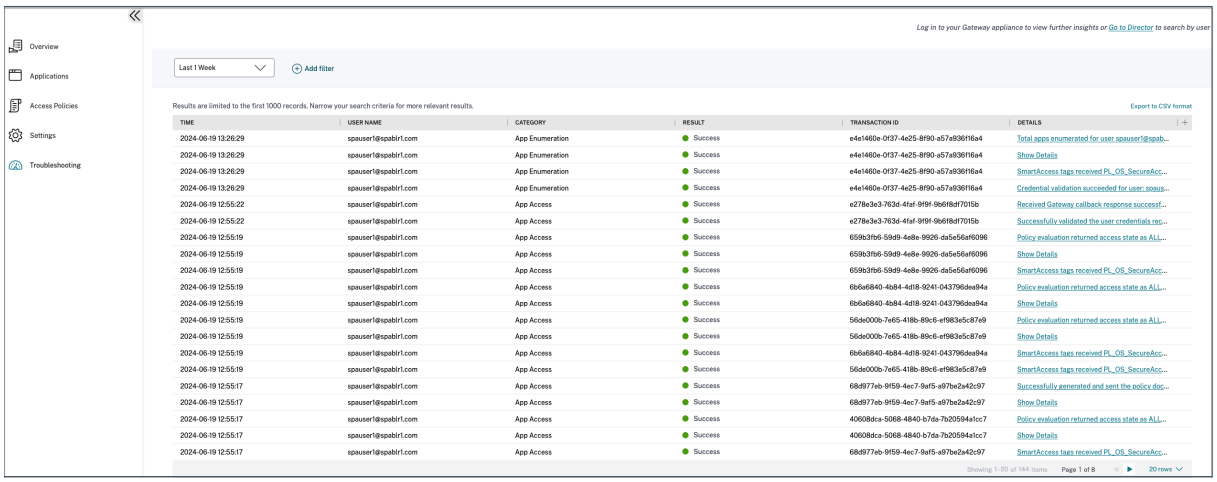
- Configure Director with Secure Private Access
- View a Secure Private Access session in Director
- Secure Private Access session codes in Director.
- Director.

Dashboard overview

September 6, 2025

The Troubleshooting dashboard displays the logs related to application launch, app enumeration, and the status. You can view the logs for the pre-set time or for a custom timeline. You can use the **Add Filter** option to refine you search based on the various criteria such as app category, user name, transaction ID. For example, in the search fields, you can select Transaction-ID, = (equals to some value), and enter 7456c0fb-a60d-4bb9-a2a2-edab8340bb15 in this sequence, to search for all logs related to this transaction ID.

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 following search operators to refine your search by using the **Add Filter** option:

- **= (equals to some value)**: To search for the logs/policies that exactly match the search criteria.
- **!= (not equal some value)**: To search for the logs/policies that do not contain the specified criteria.
- **~ (contains some value)**: To search for the logs/policies that match the search criteria partially.
- **!~ (does not contain some value)**: To search for the logs/policies that do not contain some of the specified criteria.

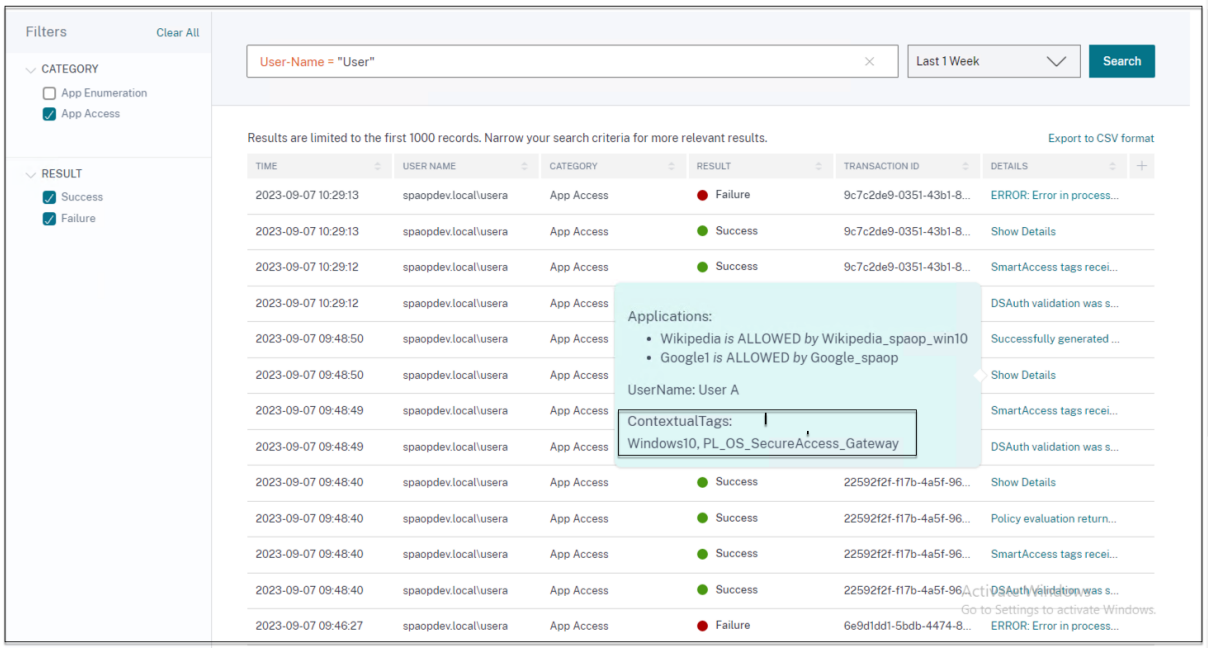
For example, you can search for an event type “Enumeration”by using the string **Event-Type > = (equals to some value) > Enumeration** in the search field.

Similarly, to search for users that partially contain the term “operator”, use the string **User-Name > ~ (contains some value) > 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 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. If nFactor authentication is configured, the nFactor endpoint analysis action names that are validated for the current users are also captured as part of the contextual tags.



Basic troubleshooting

September 10, 2025

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

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.

  - 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.

> **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>

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:

- 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

First-time setup cannot be completed

You might not be able to re-configure license server if the Director configuration failed during the first-time setup.

Resolution:

Manually clean up the license_server table.

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:

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;
   ```

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

Change log level for troubleshooting logs

Troubleshooting logs are the default error log level.

To change the log level for the troubleshooting logs, in the runtime service appsettings.json (C:\Program Files\Citrix\Citrix Access Security\Runtime\RuntimeService) update `restrictedToMinimumLeve` for `TroubleshootingSql` to one of the following values:

```
-  Information
-  Debug
-  Warning
-  Error

"TroubleshootingSql": {

  "restrictedToMinimumLevel": "Error",
  "batchPostingLimit": 50,
  "batchPeriod": "00:00:05" // 5 seconds
 }
```

Application Launch / Citrix Secure Access login failure

Application launch or the Citrix Secure Access login fails if Netscaler Gateway certificate is rotated.

Resolution: Refresh the certificate in the Secure Private Access admin console.

1. Navigate to **Settings > Integrations**.
2. In **Public NetScaler Gateway address** section, click **Refresh Certificate**.

   It might take several minutes for the refresh to complete.

For details, see Modify integration settings.

Secure Private Access sessions codes in Director

September 6, 2025

Director integration with Secure Private Access enables effective performance monitoring and troubleshooting as issues from all components in a Secure Private Access setup are captured in Director. The following tables list the various error codes and the associated conditions that are displayed in Director.

For more information, see the following topics.

- Configure Director with Secure Private Access
- View a Secure Private Access session in Director

> **Note:**
>
> - Codes that contain "0"in the second digit represent a normal execution flow. For example, 1000 represents successful app enumeration.
> - Codes that contain "1"in the second digit represent a failure or exception. For example, 2101 represents a session failure. For a failure or an exception, it is recommended that you resolve such issues by examining the logs. If that does not resolve the issue, contact support.

Session codes

Code	Status	Description
2101	Failure	Session failure.
2102	active/inactive/failure	Session is active or terminated or at least one app launch in the session failed.
2000	Active	The session is active.
2001	Inactive	Session is terminiated/inactive.

App enumeration related codes

Code	Status	Description
1101	failure	An internal error occurred during the enumeration.
1102	failure	Some apps were enumerated but at least one app evaluation failed.
1103	failure	No apps were enumerated and at least one app evaluation failed.
1000	Success	Enumeration was successful. At least one app was enumerated.
1001	Success	No apps were enumerated because they were all denied by policies.
1002	Success	No apps were enumerated because no policies matched.
1003	Success	No apps were enumerated because some were denied and for others, no policies matched.
1004	Success	No apps were enumerated because no policies to evaluate.
3101	Failure	App enumeration - An internal error occurred (currently unused).
3102	Failure	App was not enumerated because there was an exception during policy evaluation.
3103	Failure	App enumeration status is null - An internal error occurred during policy evaluation.
3104	Allow/deny/failure	Error retrieving policy details for the app.
3000	Allow	App enumeration is allowed.
3001	Deny	App enumeration is denied by policy.

Code	Status	Description
3002	Deny	App was not enumerated because no policies matched.
3003	Unknown	App enumeration status is unknown.
3004	App launch from CEB	App launch attempt from Citrix Enterprise Browser.

App launch message codes

Code	Status	Description
4101	Failure	Application launch error - An internal error occurred during application launch.
4102	Failure	Application launch error (internal).
4103	Allow/deny/failure	Error retrieving policy details for the app.
4104	Failure	Application Launch Error - No application configuration found.
4000	Allow	App Launch is allowed.
4001	Deny	Application launch was denied because of a policy.
4002	Deny	Application launch was denied because no policy matched.

SIEM integration

December 9, 2024

The Secure Private Access plug-in supports integration with Security Information and Event Management (SIEM) services. Security events are stored in real time to Windows Event Log (Event

Viewer\Applications and Services Logs\Citrix Access Security) and can be collected and analyzed by third-party tools.

The following table lists the Secure Private Access plug-in security events:

Event ID	Summary	Description	Source
4624	An account was successfully logged on	Event created when Secure Private Access administrator logged in to the Secure Private Access admin console	Citrix Access Security Admin service
4625	An account failed to log on	Event created when the Secure Private Access administrator failed to log in to the Secure Private Access admin console	Citrix Access Security Admin service
4634	An account was logged off	Event created when Secure Private Access administrator logged off from the Secure Private Access admin console	Citrix Access Security admin service
4720	A user account was created	Event created when new Secure Private Access administrator added	Citrix Access Security admin service
4738	A user account was changed	Event created when new Secure Private Access administrator updated	Citrix Access Security admin service
4726	A user account was deleted	Event created when new Secure Private Access administrator removed	Citrix Access Security admin service

Event ID	Summary	Description	Source
8001	User secure access session	Event created when a user session initiated or terminated on the endpoint. Contains user, session, and device details, visited internal and external domains during the session	Citrix Access Security admin service
8002	User access authorization request	Event created when the Secure Private Access plug-in authorizes access to a resource. Contains resource FQDN and authorization decision	Citrix Access Security admin service

References

- Security Information and Event Management (SIEM) integration
- About Sharing logs to SIEM solutions

Scout integration

September 6, 2025

Citrix Scout is integrated with Secure Private Access to enable administrators to collect logs and metrics for troubleshooting. For information on what information is collected, see What is collected.

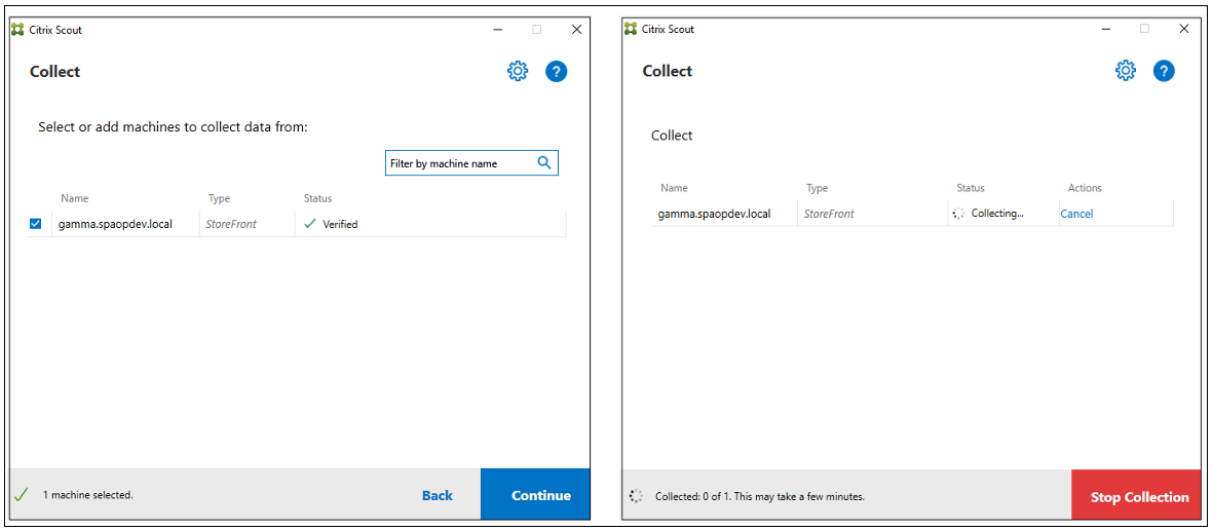
To start collecting the Secure Private Access logs, do the following steps:

1. Select a Secure Private Access machine to start the collection.
2. Click **Continue**.

You can click the **Stop Collection** anytime to stop the collection.

Citrix Scout also retrieves the following logs. These logs are stored in a bundle in the local machine and can be uploaded to Citrix Cloud.

- C:\Program Files\Citrix\Citrix Access Security\Admin\AdminService\logs\spa-admin
- C:\Program Files\Citrix\Citrix Access Security\Runtime\RuntimeService\logs\spa-runtime



Logs retention settings

September 6, 2025

The logs are stored in the Secure Private Access database for seven 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": 7,
  "CleanupOldestDataIfEntriesCountAbove": 0
 }
```

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.

> **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

September 6, 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
     }
```

> **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.

Third-party notifications

September 6, 2025

Citrix Secure Private Access for on-premises