Citrix Secure Private Access™ - On premises

Contents

Technical overview

August 18, 2025

Citrix Secure Private Access™ on-premises is a customer-managed Zero Trust Network Access (ZTNA) solution that provides VPN less access to Internal web and SaaS applications with the following along with a seamless end-user experience:

- Least privilege principle
- Single sign-on (SSO)
- Multifactor authentication
- Device posture assessment
- Application-level security controls
- App protection features

The solution leverages the StoreFront on-premises and Citrix Workspace™ app to enable a seamless and secure access experience to access web and SaaS apps within Citrix Enterprise Browser. This solution also leverages the 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 and SaaS apps) using the StoreFront™ on-premises portal as a unified access portal to web and SaaS 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
Configuration and Management	Secure Private Access

Functionality	Service/Component providing the functionality
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.
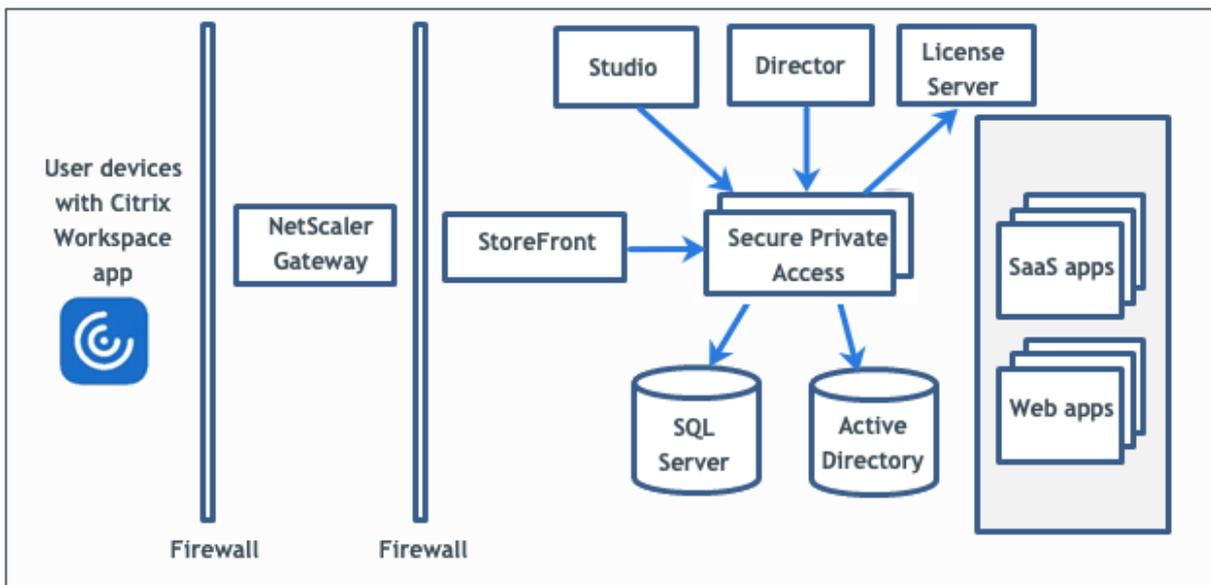
For information about each component, see Key components.

What's new

August 18, 2025

December 2024

- **Support for Secure Private Access on-premises solution on FIPS platform**

  The Secure Private Access on-premises solution is now supported on NetScaler platforms that comply with Federal Information Processing Standards (FIPS) and running the 13.1-37.219 and later FIPS builds. For more information, see Federal Information Processing Standards.

February 2023

Citrix Secure Private Access™ integration with Director

Citrix Secure Private Access is now integrated with Director for performance management and enhanced troubleshooting. For details, see Secure Private Access integration with Director.

View Secure Private Access user sessions in Director

You can now view the View Secure Private Access user sessions in Director. You can view details regarding the active and failed sessions. You can also information related to apps, policies, and session details of the failed and successful sessions. For details, see View a Secure Private Access session by user.

Citrix Secure Private Access integration with the license server

Citrix Secure Private Access is now integrated with the License Server to collect and process licensing data. For details, see License server with Secure Private Access.

Fixed issues

August 18, 2025

The following issues are addressed in release 2402.

Admin management

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

Admin console

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

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

Known issues

September 13, 2025

The following issues exist in release 2402.

Domain Controller configurations

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

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

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

- The alternate UPN suffix is not supported by Secure Private Access for Intranet (StoreFront) login and Internet/Extranet (gateway) app enumeration.

- 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.

```
1  [SPAOP-2487]
```

Application icons

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

Application launch

Application launch fails if all of the following conditions are met:

- Netscaler version 13.0.x, 13.1 prior to 13.1-48.47, 14.1 prior to 14.1−4.42 are used.
- LDAP UPNs are configured with a different suffix than the actual domain.
- LDAP UPN and sAMAccountName are different.

Upgrades

- Upgrade of 2308 to 2402 and later is not supported.

- If custom SSL certificate is used for the Secure Private Access admin service, the certificate must be bound again to the "Citrix Access Security Admin" site on Internet Information Service (IIS).

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.

Admin console

- While adding an app, if the app name contains a comma, a warning is displayed. However, the app is created.

Installer display in Uninstall or change a program page

When you upgrade Secure Private Access from 2311 to 2402 by using the ISO file, the **Uninstall or change a program** page (**Control Panel > Programs > Programs and Features**) displays two entries for the Secure Private Access installer instead of replacing the initial entry.

- **Citrix Virtual Apps and Desktops™ 7 2402 LTSR**
- **Citrix Virtual Apps and Desktops 7 2311 - Secure private access**

You can uninstall the 2311 build installer by selecting **Citrix Virtual Apps and Desktops 7 2311 - Secure private access**.

> **Note:**
>
> This issue is not observed when the Secure Private Access 2311 standalone installer is upgraded using the 2402 standalone installer.

System requirements

August 18, 2025

Ensure that your product meets the minimal version requirements.

- Citrix Workspace™ app

    - Windows –2309 and later
    - macOS –2309 and later

- Operating system for Secure Private Access plug-in server - Windows Server 2019 and later.
- StoreFront™ –LTSR 2203 or CR 2212 and later.

- NetScaler −13.0, 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.
- Director 2402 or later.
- NetScaler FIPS - 13.1-37.219 and later FIPS builds.
- Communication ports: Ensure that you have opened the required ports for the Secure Private Access plug-in. For details, see Communication ports.

> **Note:**
>
> The Secure Private Access for on-premises is not supported on Citrix Workspace app for iOS and Android.

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.

- 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 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
	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)

Source	Destination	Type	Port	Details
		TCP	636	LDAP over SSL (LDAPS)
		TCP, UDP	464	Native Windows authentication protocol to allow users to change expired passwords
	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

August 18, 2025

Database storage requirements

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

The following figure displays the server storage requirements:

Number of users	Number of Secure Private Access server nodes	Secure Private Access node configuration			SQL Server (Secure Private Access Database only)			Active Directory		StoreFront	
		CPU	Memory (GB)	Storage (GB)	CPU	Memory (GB)	Storage (GB)	CPU	Memory (GB)	CPU	Memory (GB)
1000	3	8	16	80	4	16	250	4	16	4	16
5000	8	8	16	80	16	16	750	16	16	4	16

> **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, Settings to retain event logs.

Server configuration

The following table displays the server configuration details:

Configuration	Details
Total number of applications	250
Total number of policies	50
Number of apps per user	15
AD configuration	Users are part of 20 groups, upto 20 levels of nesting
Troubleshooting log retention period	7 days (default)
Troubleshooting Log level	Error (default)
Secure Private Access server log retention	90 days or 600 files

Traffic Profile

The following table displays the traffic profile details per day per user.

Profile	Details
Enumerations	10
Enterprise browser policy sync	20
App launch from Citrix Workspace™ app	4
App access from Citrix Enterprise Browser™	500
Help desk troubleshooting requests (per day), through Citrix Director	1000

Deployment guidelines

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

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

Note:

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

Other components configuration

Component	vCPUs	Memory
Secure Private Access plug-in	8	16 GB
Secure Private Access SQL server	8	16 GB
StoreFront	16	8 GB
Gateway	4	8 GB
Active Directory	8	14 GB
Client	4	8 GB

Install and configure

August 18, 2025

The secure Private Access installer is available as a standalone installer or as part of the integrated Citrix Virtual Apps and Desktops installer. For details, see Install core components or 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™**).

Admin account requirements to install and manage Secure Private Access

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

Set up Secure Private Access

You can set up Secure Private Access by completing the following steps:

- Set up Secure Private Access by creating a new site or Set up Secure Private Access by joining an existing site
- Configure databases
- Integrate StoreFront, NetScaler Gateway, Director, and License servers

Configure applications and access policies

After you set up the Secure Private Access environment, you must configure applications and access policies for applications.

- Configure applications
- Configure access policies for the applications

Secure Private Access installer

August 18, 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.
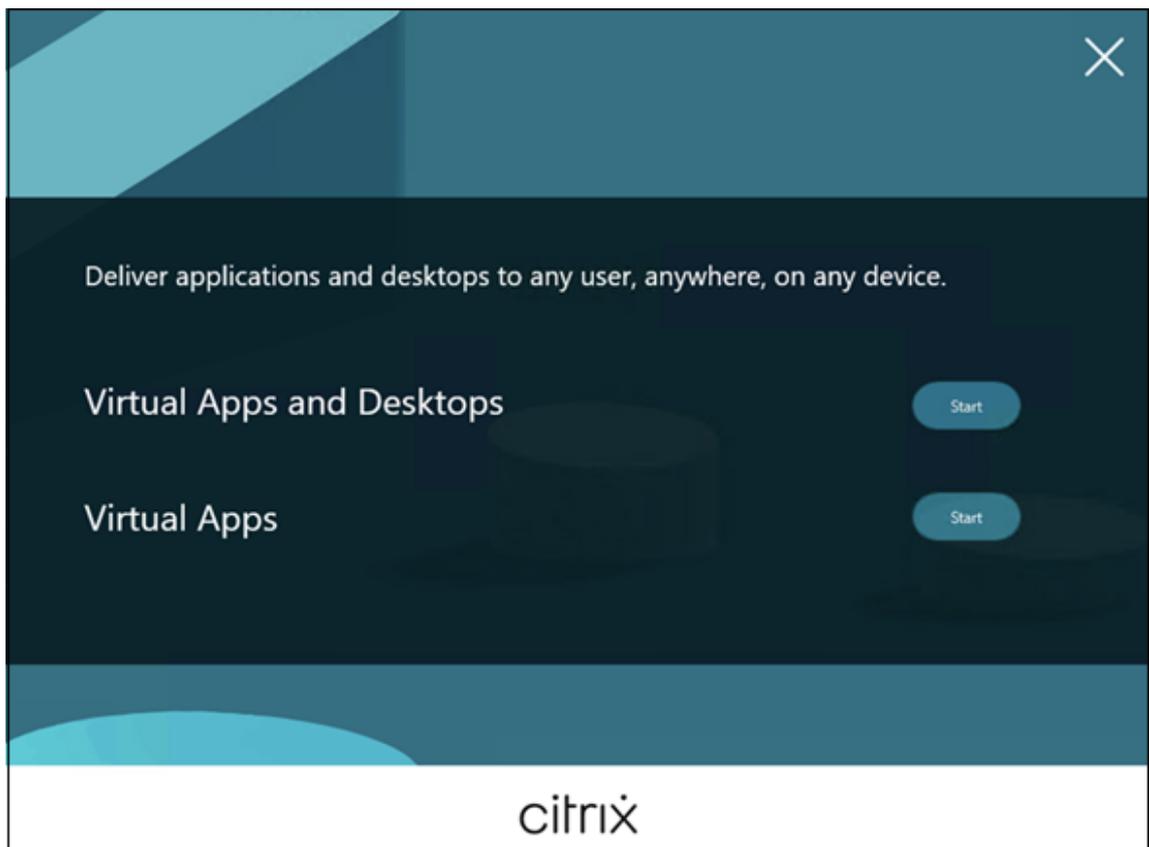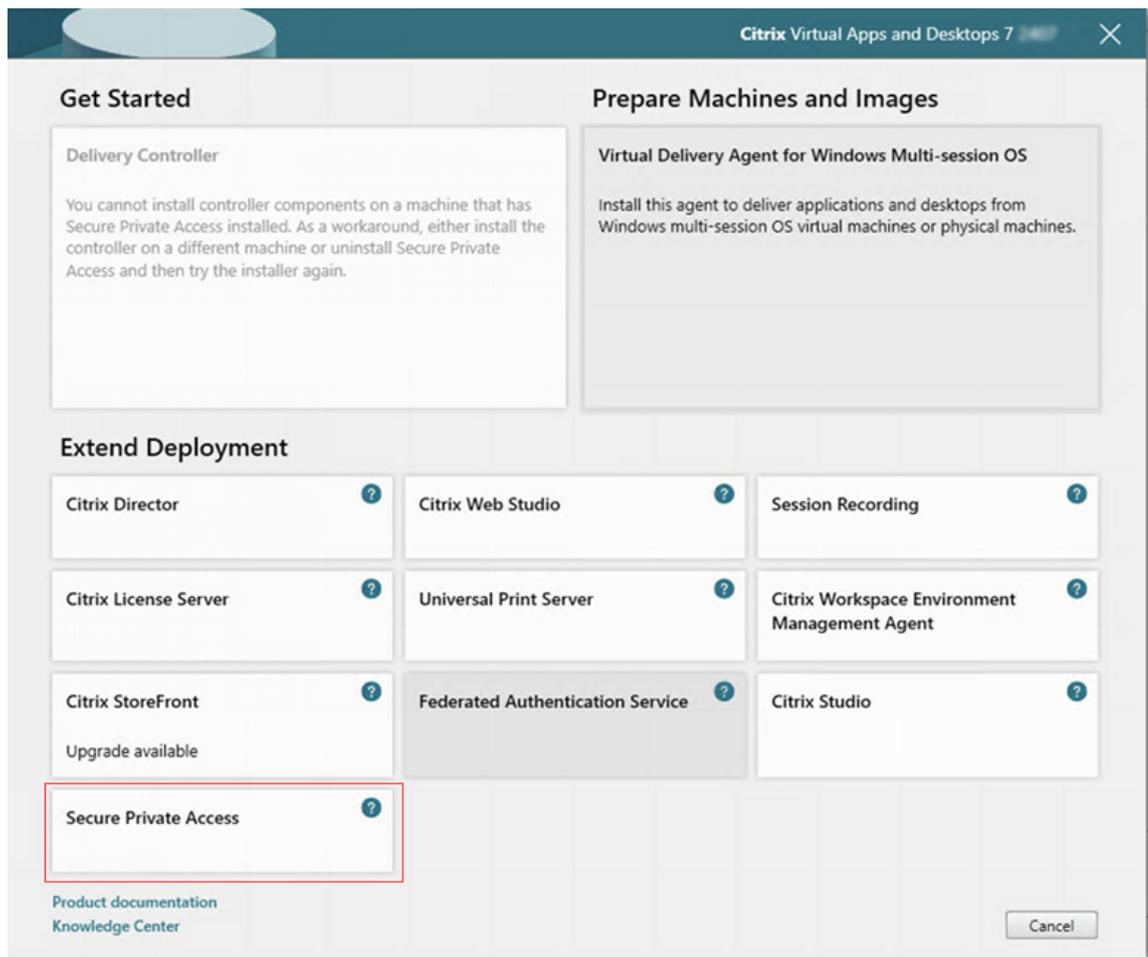
For detailed instructions, see the following topics:

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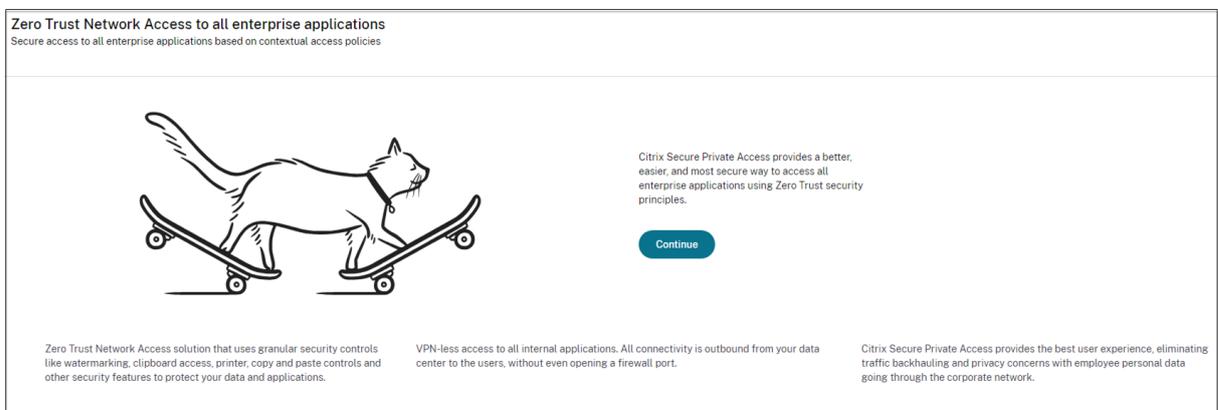
You can also see the Secure Private Access shortcut on the desktop Start menu (**Citrix > Citrix Secure Private Access™**).

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** and in **User Authentication > Logon**, select **Automatic logon with current user name and password**.
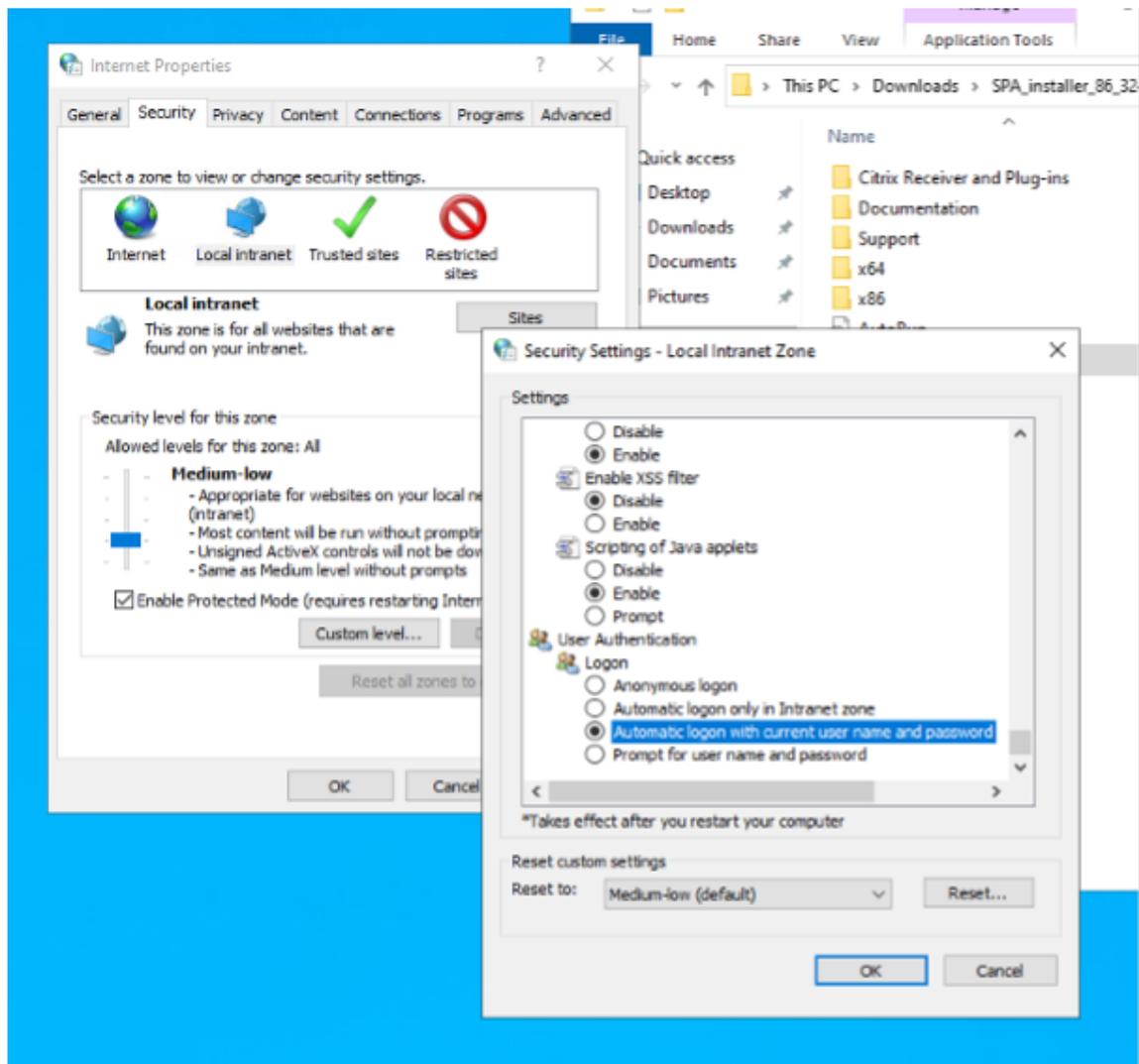
Note:

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

Set up Secure Private Access

September 4, 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 need to 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 Store-Front 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:** - 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**.

Zero Trust Network Access to all enterprise applications
Secure access to all enterprise applications based on contextual access policies

- ✓ Site
- ✓ Database
- ③ Integrations
- ④ Summary

Step 3: Integrations
Connect with StoreFront and NetScaler Gateway servers so they can route traffic to Secure Private Access servers.

Secure Private Access address*
Enter the address of your Secure Private Access server or the load balancer managing traffic for your Secure Private Access servers. The address doesn't need to be a public address.

https://gamma.spaopdev.local ✓

StoreFront Store URL*
Enter your complete StoreFront Store URL.

https://gamma.spaopdev.local/Citrix/StoreGamma ✓

⊕ Add another Store URL

Public NetScaler Gateway address*
Enter all the addresses of the NetScaler Gateways accessing StoreFront. If you have a Global Server Load Balancing (GSLB) deployment, add the GSLB addresses as well.

https://gwgamma.spaopdev.local ✓

⊕ Add another public address

NetScaler Gateway virtual IP address and callback URL*
Enter the callback URL and virtual IP (VIP) address from each NetScaler Gateway. Each entry must match the values configured in StoreFront.
Learn more

Virtual IP address* ⓘ   Callback URL* ⓘ

10.61.174.125   https://gwgamma.spaopdev.local ✓

⊕ Add another virtual IP address and callback URL

Director URL*
Utilize the monitoring capabilities of Director in Secure Private Access.
Enter the Director URL to configure Director for use in Secure Private Access. You must also use the configuration tool for Director as described in the product documentation.

http://10.61.174.141 ✓

License Server URL*
A license server is a mandatory component required to collect and process licensing data.
Enter the License Server URL to configure this component.

https://ls.spaopdev.local ✓

[Test all URLs]

[Back]   [Next]

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.
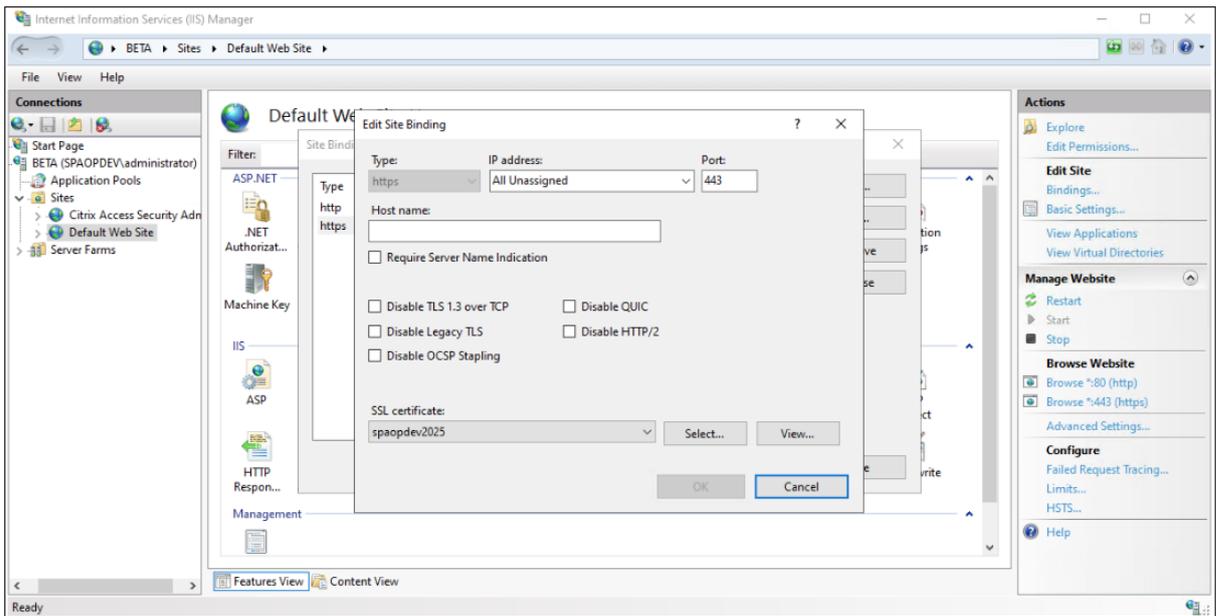
Multi-domain environments

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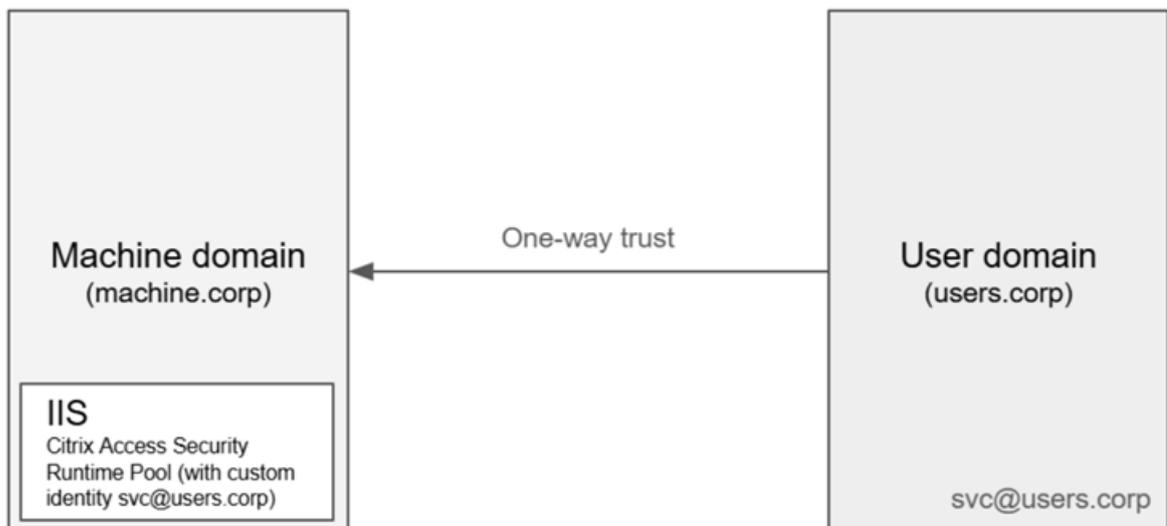
To establish domain trust for Secure Private Access on-premises deployment in multi-domain environments, the following prerequisites must be met:

- 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**.
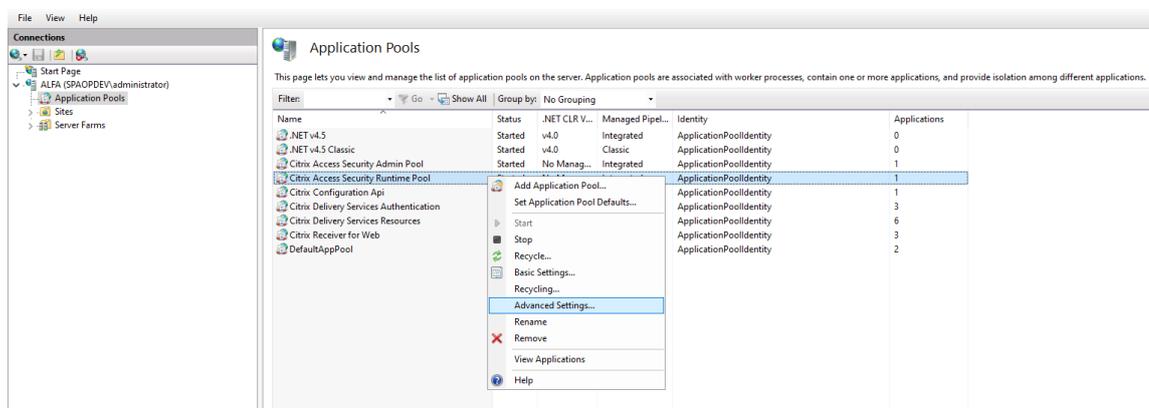
3. Click the edit icon in **Identity > ApplicationPoolIdentity**.
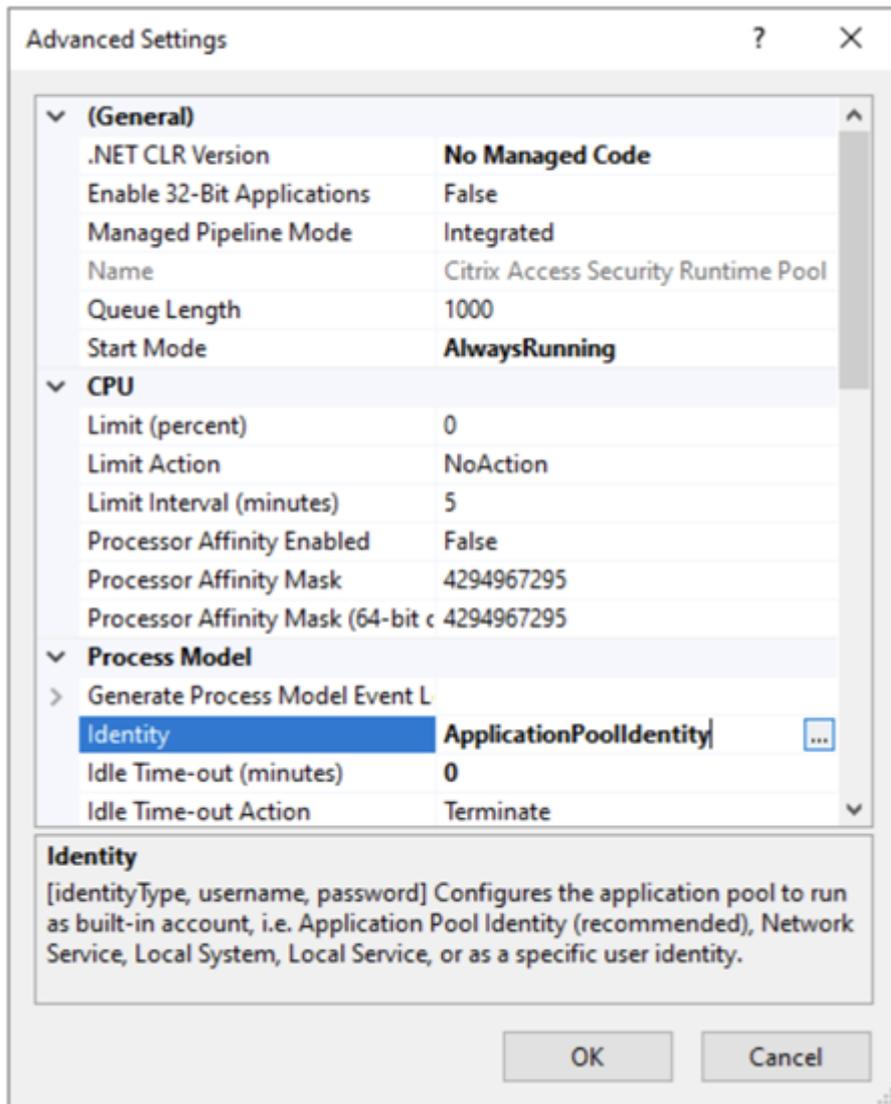
4. In **Custom account:** click **Set**.
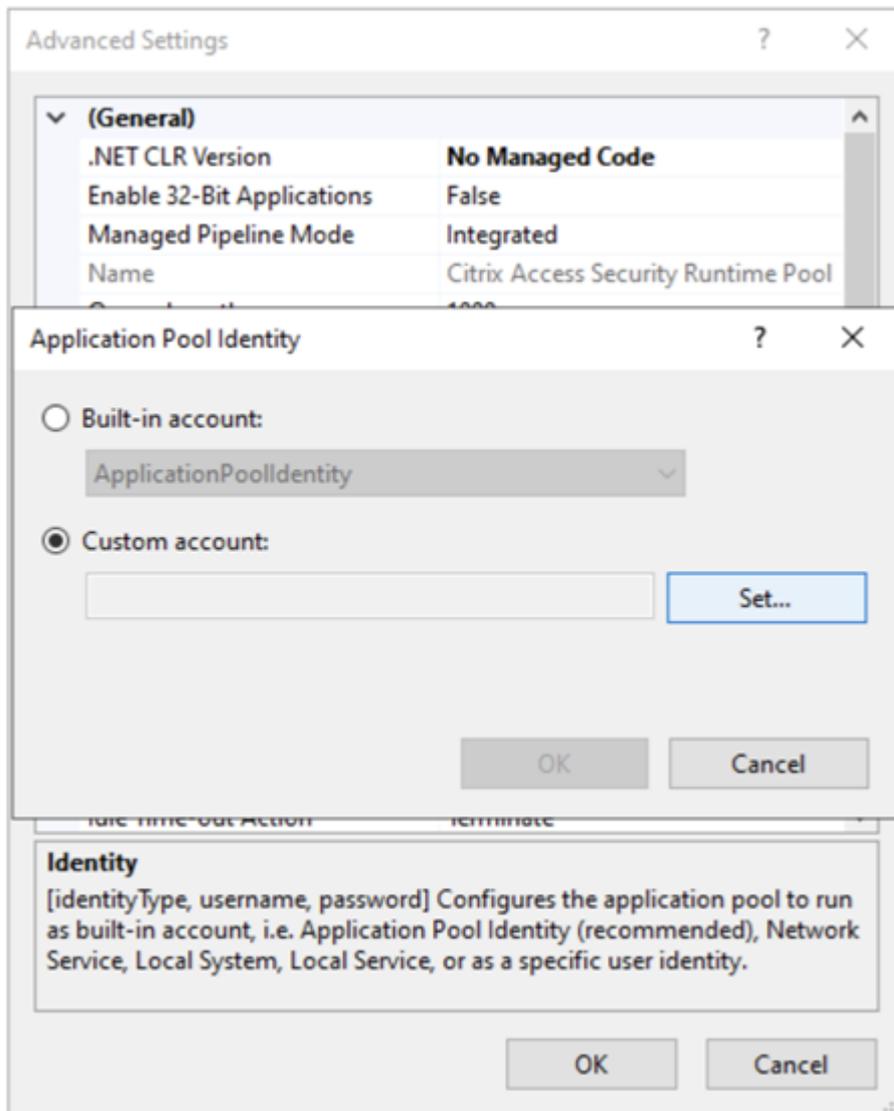
5. Set credentials for the user.

6. Click **OK**.
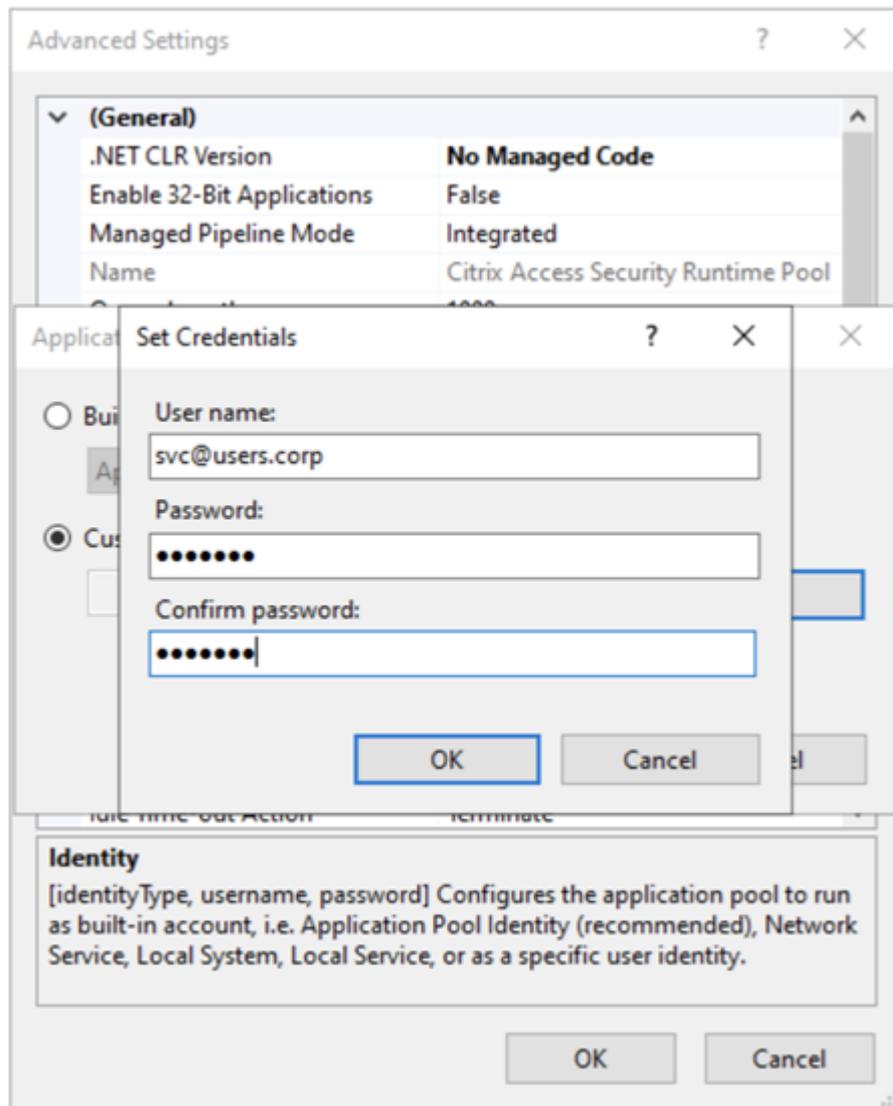
Next steps

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

Components

August 18, 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 keeps track of 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 Store-Front 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:** 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:** 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.

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

NetScaler Gateway

August 18, 2025

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

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

   To create a new NetScaler Gateway, use ns_gateway_secure_access.sh.

To update an existing NetScaler Gateway, use ns_gateway_secure_access_update.sh.

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

   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.

```
root@ns32201# ./ns_gateway_secure_access_2405.sh
NetScaler Gateway vserver name (default: _SecureAccess_Gateway): spaonprem
NetScaler Gateway IP:
NetScaler Gateway FQDN: ns32205.cgwsanity.net
SPA Plugin IP:
SPA Plugin FQDN:
StoreFront Store URL (including protocol http/https):
NetScaler authentication profile name: authnprof
NetScaler SSL server certificate name: ns32205
Domain: cgwsanity.net
Enable TCP/UDP Apptype support (Y/N): Y

************ Gateway configuration ********************
NetScaler Gateway name: spaonprem
NetScaler Gateway IP:
NetScaler Gateway FQDN: ns32205.cgwsanity.net
SPA Plugin FQDN: spa.cgwsanity.net
SPA Plugin IP:
StoreFront Store URL:
NetScaler authentication profile name: authnprof
NetScaler Gateway server certificate name: ns32205
Domain: cgwsanity.net
Enable App type TCP/UDP:
********************************************************

Checking SPA Plugin support....
NetScaler supports SPA CLI, skipping nsapimgr commands
Number of PEs running: 3
Changing ns_vpn_enable_spa_tcp_udp_apps from 0 to 3 Done.
Changing ns_vpn_enable_spa_tcp_udp_apps from 0 to 3 Done.
Changing ns_vpn_enable_spa_tcp_udp_apps from 0 to 3 Done.
TCP/UDP Apptype support is enabled
Persisting TCP/UDP Apptype support setting: nsapimgr_wr.sh -ys ns_vpn_enable_spa_tcp_udp_apps=3 in /nsconfig/rc.netscaler file.

NetScaler Gateway creation script ns_gateway_secure_access created
Please copy it to NetScaler (e.g. /var/tmp folder) and run command:
batch -fileName /var/tmp/ns_gateway_secure_access -outfile /var/tmp/ns_gateway_secure_access_output
Check ns_gateway_secure_access_output file for output
```

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

For 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/up-

---

> dates/binds resources. Therefore, if you see an unexpected error because of one of the parameters being incorrect, it's recommended to redo the configuration from the start.

Configure Secure Private Access on a NetScaler Gateway with existing configuration

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

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

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

Settings on NetScaler Gateway virtual server

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

Add a virtual server:

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

Update a virtual server:

- tcpProfileName: nstcp_default_XA_XD_profile
- icaOnly: OFF

Examples:

To add 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
```

To update a virtual server:

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

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

NetScaler Gateway session action

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

- `transparentInterception`: OFF
- `SSO`: ON
- `ssoCredential`: PRIMARY
- `useMIP`: NS
- `useIIP`: OFF
- `icaProxy`: OFF
- `wihome`: `"https://storefront.mydomain.com/Citrix/MyStoreWeb"` - replace with real store URL. 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, it's used to bind Secure Private Access specific authorization policies)
- `clientlessVpnMode`: ON
- `clientlessModeUrlEncoding`: TRANSPARENT
- `SecureBrowse`: ENABLED
- `Storefronturl`: `"https://storefront.mydomain.com"`
- `sfGatewayAuthType`: domain

Examples:

To add a session action:

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

To update a session action:

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

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

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

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

Compatibility with the ICA® apps

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

For details, see the following topics:

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

Support for smart access tags

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

- 13.1–48.47 and later
- 14.1–4.42 and later

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

Toggle name	Description
`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.

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.
- We recommend that you set **ICA Proxy** to OFF in the Secure Private Access enabled VPN virtual server.
- 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.

Configure contextual tags

August 18, 2025

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

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

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

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

Configure custom tags using the GUI

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

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

Configure a classic gateway preauthentication policy

1. Navigate to **NetScaler Gateway > Policies > Preauthentication** and then click **Add**.

2. Select an existing policy or add a name for the policy. This policy name is used as the custom tag value.

3. In **Request Action**, click **Add** to create an action. You can reuse this action for multiple policies, for example, use one action to allow access, another to deny access.

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**.

Choose Type

Policies

Choose Policy*

Preauthentication

Choose Type*

Request

Continue   Cancel

5. Select the policy name and the priority for the policy evaluation.

6. Click **Bind**.

Citrix Secure Private Access™ - On premises

Configure custom tags using the CLI

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

Example:

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

Adding new contextual tag

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

References

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

StoreFront

August 18, 2025

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

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

Perform the following steps to configure StoreFront manually.

1. Download the script from the Secure Private Access admin console (**Settings > Integrations**).

2. Click **Download Script** corresponding to the StoreFront entry for which the configuration changes have to be done.

   The downloaded zip file contains a configuration script, a README file, and a configuration cleanup script. The cleanup script can be used in case integration between StoreFront and Secure Private Access is to be removed.

3. Run the script as an admin on a PowerShell 64-bit instance by using the command `./ConfigureStorefront.ps1`.

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

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

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

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

ther on another store on the same StoreFront or a different StoreFront deployment) as well. StoreFront can be added from the **Settings > Integrations** page.

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

When using StoreFront version 2308 or earlier

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

- The Secure Private Access plug-in type is shown as XenMobile.
- The Secure Private Access server URL is not displayed.
- The Secure Private Access port is always shown as 80.
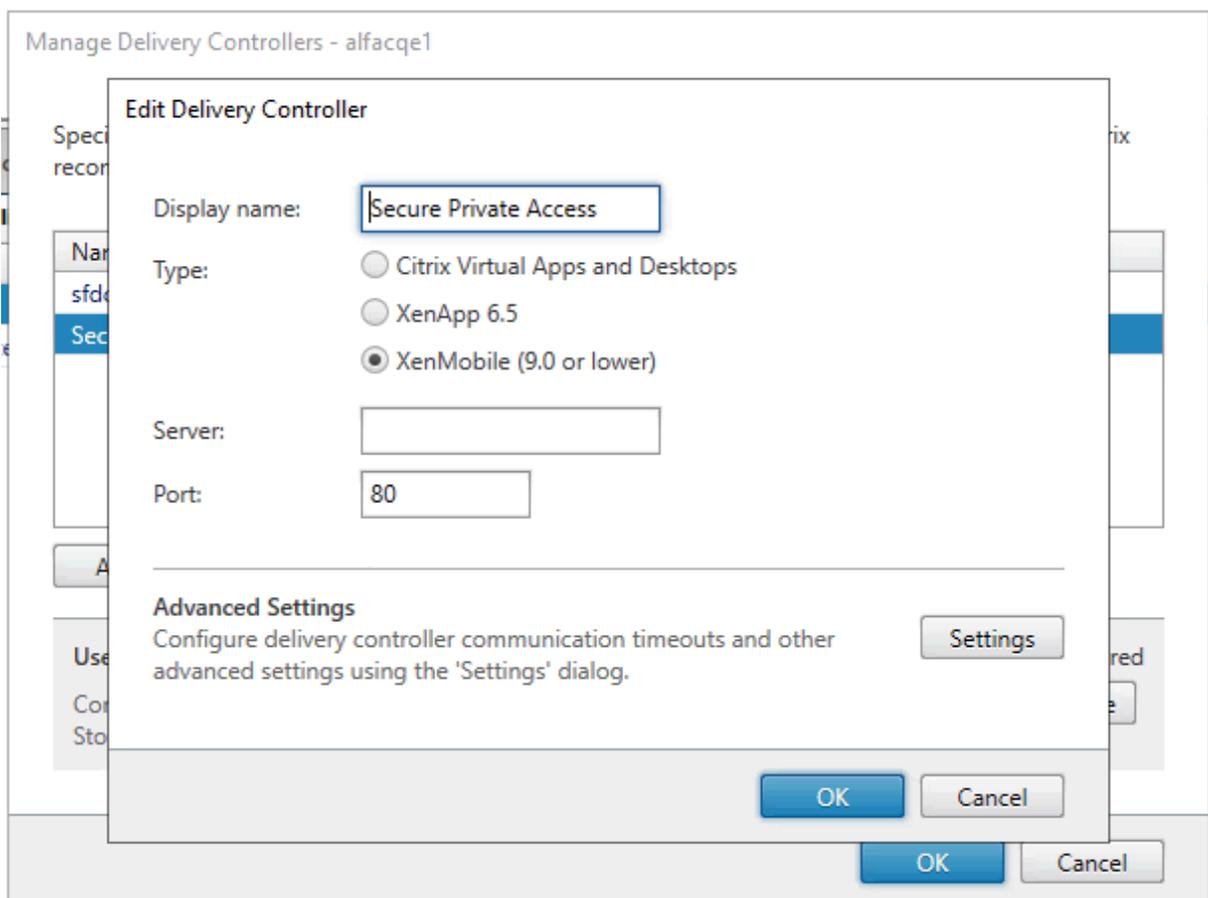
When using StoreFront version 2311 or later

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.

Director

August 18, 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:**
>
> - 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.

License server

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 and Manage settings after installation.

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.

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

Web Studio

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

You must install Web Studio version 2308 or later.

Perform the following steps to enable Web Studio integration:

1. Install Citrix Web Studio by using the Citrix Virtual Apps and Desktops™ installer or the integrated DDC installer.

2. Follow the onscreen instructions and complete the installation. When prompted for a controller address, enter the DDC FQDN as the controller address.

3. After successful installation, navigate to the folder C:\Program Files\Citrix\Web Studio\Site\studio\assets\json and modify the content of the spa-config.json file.

   If a non-default location was used for the Web Studio installation, replace the default installation location in C:\Program Files\Citrix with the correct location.
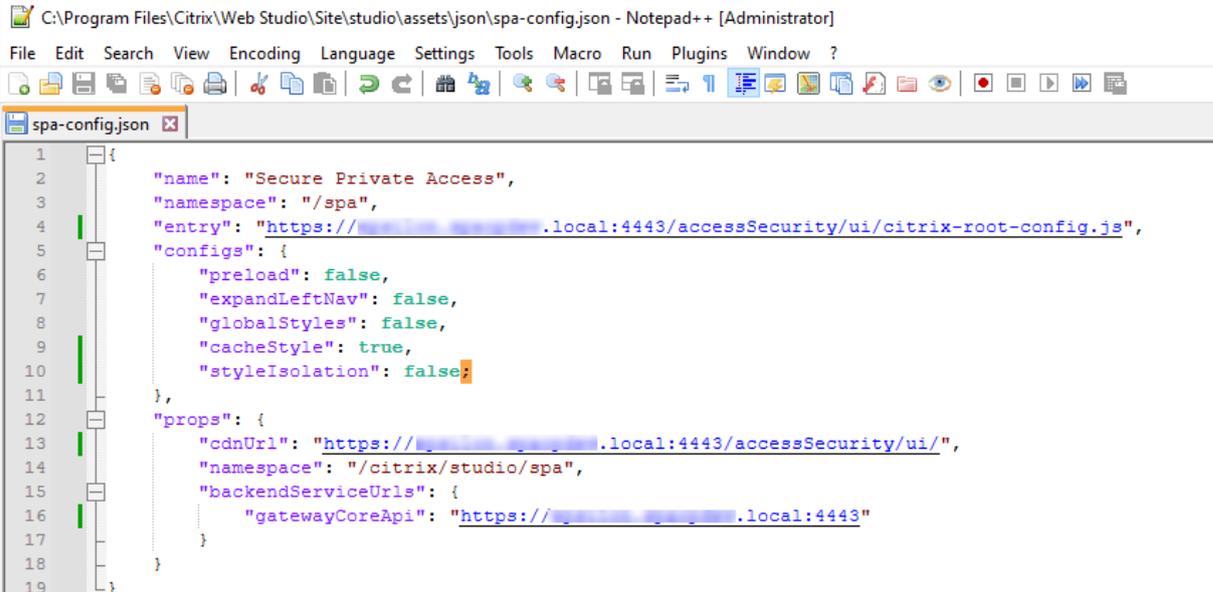
1. Replace ''SpaServer''with the FQDN of your Secure Private Access plug-in.
2. Log in to Web Studio.
3. On the left navigation menu, click **Secure Private Access** to access the Secure Private Access admin console from Web Studio.

Configure applications

August 18, 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.

- **Add application to favorites automatically** – Click this option to add this 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 access policies for the applications

August 18, 2025

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

1. In the admin console, click **Access Policies**.

2. Click **Create Policy**.

3. In **Applications**, select the apps for which you want to enforce the access policies.

4. In **Users/User groups** —Select the conditions and users or user groups based on which app access must be allowed or denied.

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

5. Click **Add condition** to add another condition based on contextual tags. These tags are derived from the NetScaler® Gateway.

6. Select **Conditional Tags** and then select the conditions based on which app access must be

allowed or denied.

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

- **Allow access**

- **Allow access with restriction**

- **Deny access**

When you select **Allow access with restrictions**, you must click **Add restrictions** to select the restrictions. For more information on each restriction, see Available access restrictions

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

> **Note:**
>
> The action **Allow access with restriction** is not applicable for the TCP/UDP apps.

8. In **Policy name**, enter a name for the policy.

9. Select **Enable policy on save**. If you do not select this option, the policy is only created and not enforced on the applications. Alternatively, you can also enable the policy from the Access Policies page by using the toggle switch.

Access policy priority

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

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

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

Next steps

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

Sample configuration validation

Deploy Secure Private Access as a cluster

August 18, 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.
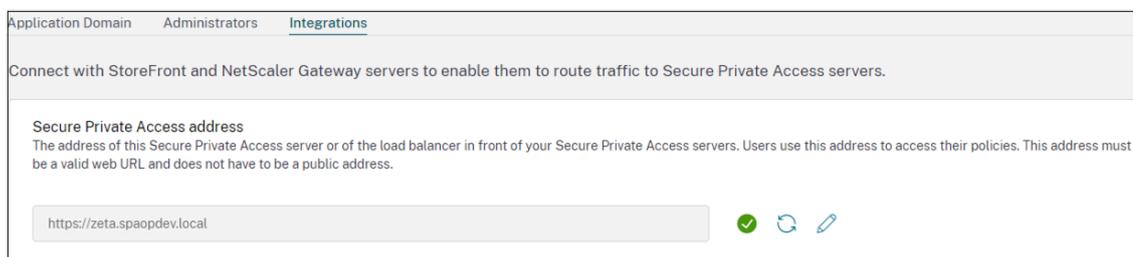
Load balancer configuration

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 the 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:

```
1    Http status code: 200 OK
2
3    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.

Uninstall Secure Private Access

August 18, 2025

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

1. Select **Citrix Virtual Apps and Desktops™ 7 2402** –**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
```

Upgrade

August 18, 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. 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.

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

Upgrade your Secure Private Access installer

August 18, 2025

1. Download the Citrix Secure Private Access 2402 installer from https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/.

2. Run the .exe as an administrator on a domain joined machine.

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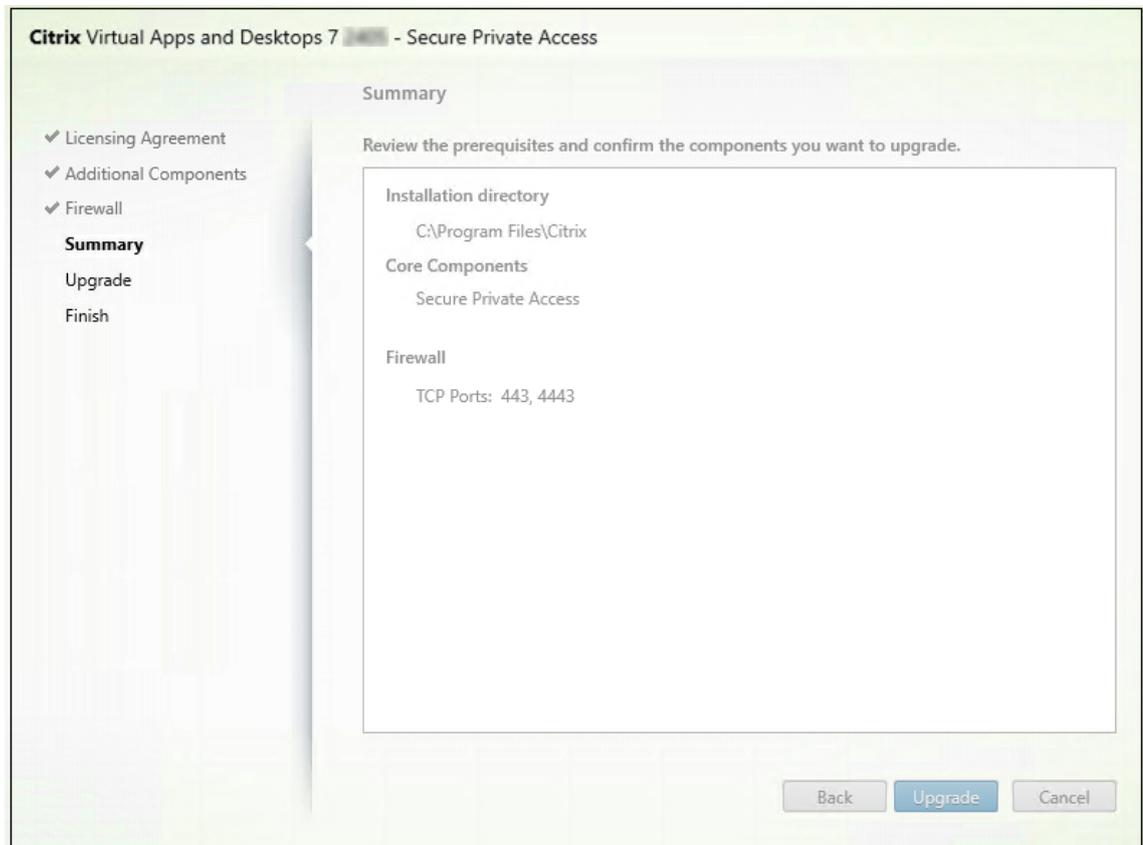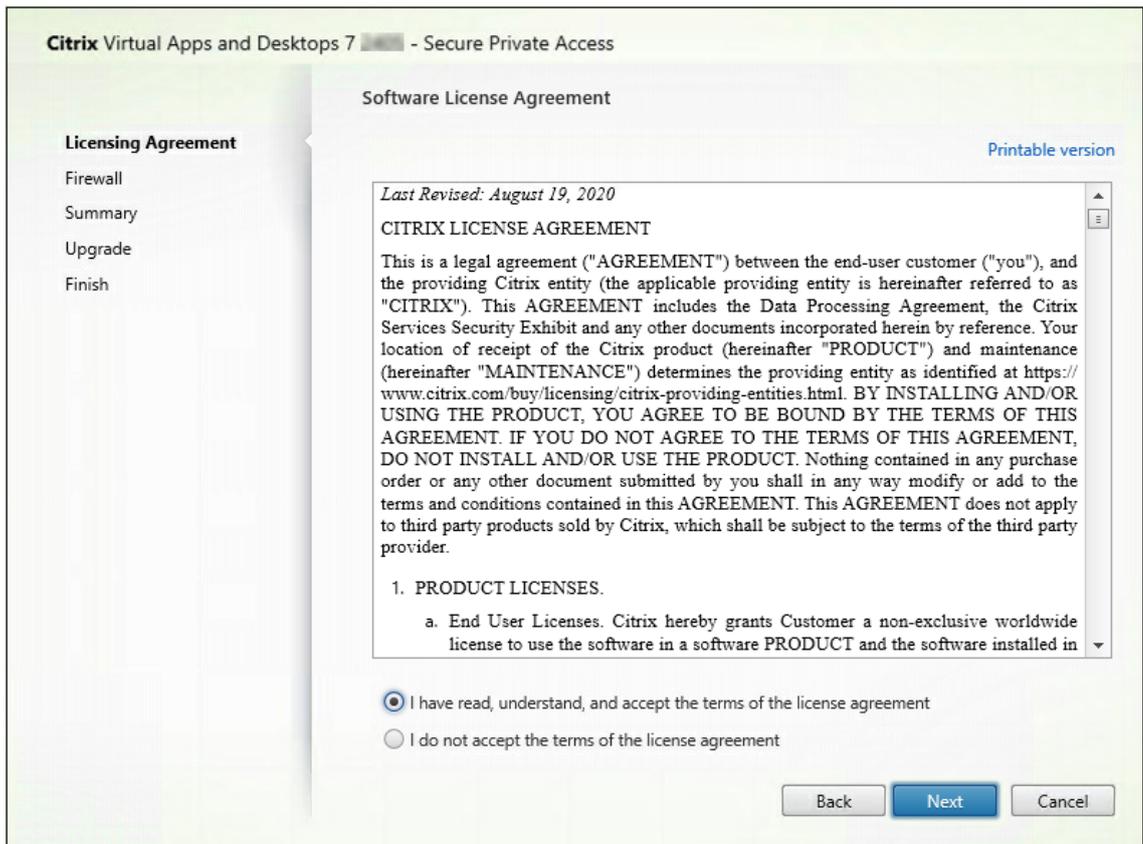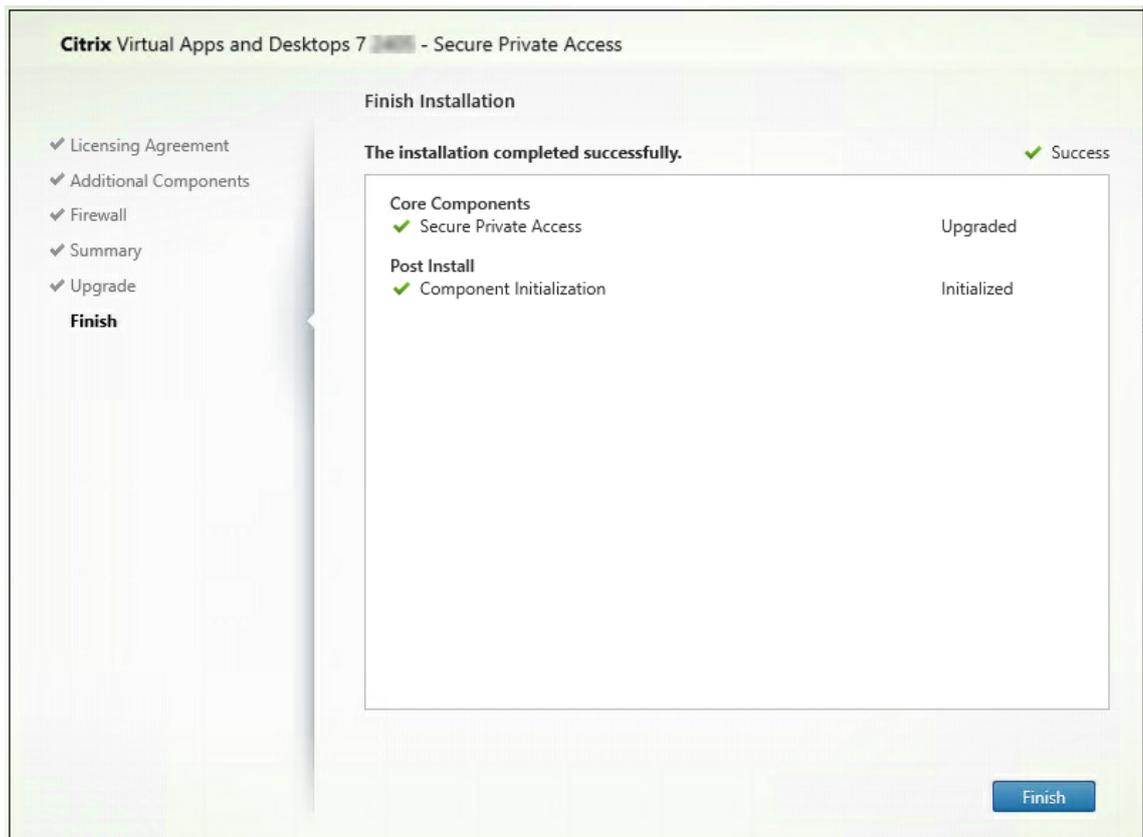
Important:

After you upgrade the installer to release 2402, 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

August 18, 2025

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

1. Open the PowerShell or the command prompt window with admin privileges.

2. Change the directory to the Admin\AdminConfigTool folder under the Secure Private Access installation folder (for example, cd "C:\Program Files\Citrix\Citrix Access Security\Admin\AdminConfigTool").

3. Run the following command:

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

Manage

August 1, 2024

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 settings after installation

August 18, 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 required.

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 Secure Private Access is installed on a machine different that StoreFront, then download the StoreFront script and run it on the StoreFront.
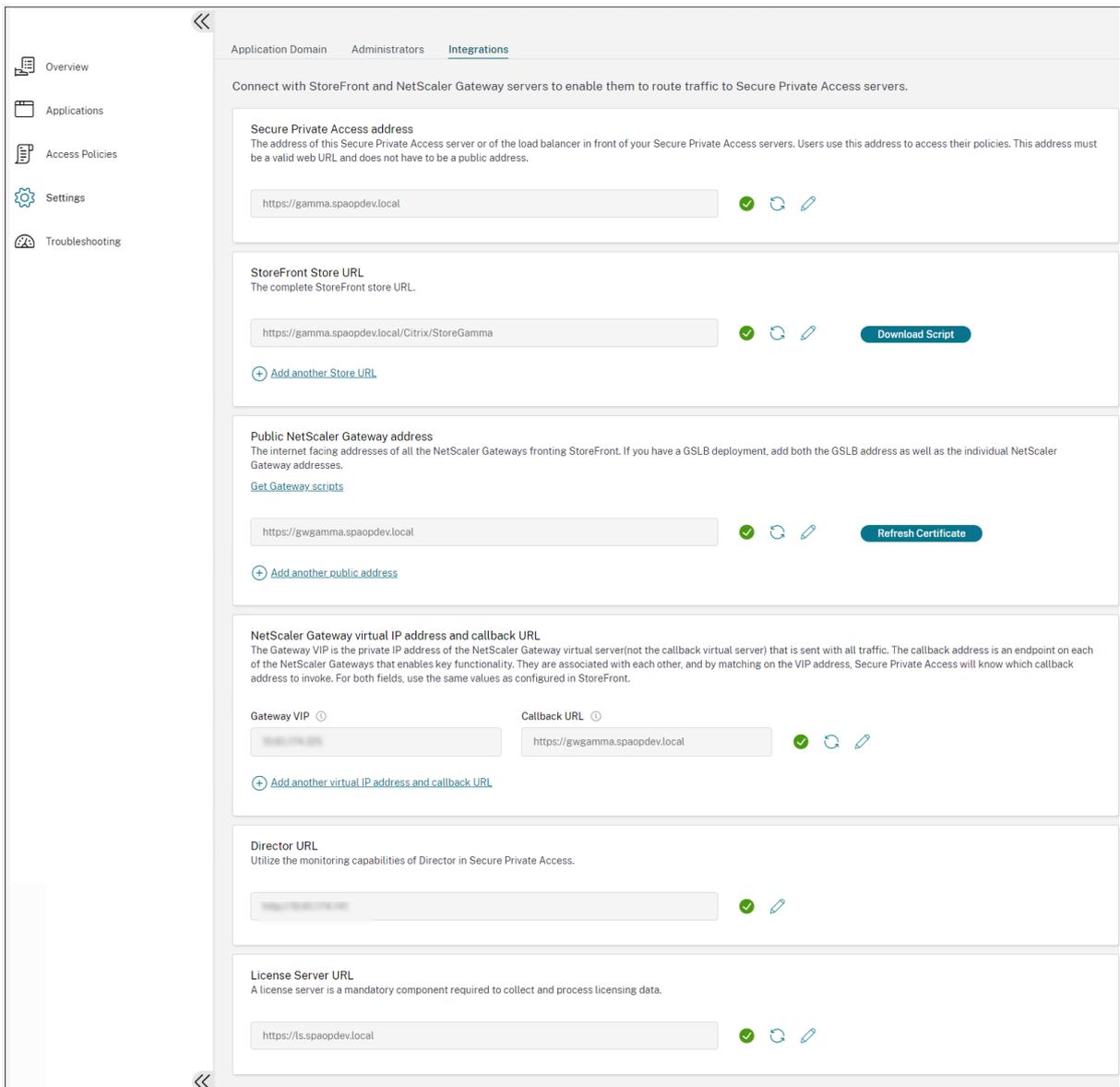
Manage applications and policies

August 18, 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 App ✕

Click Finish once you're finished editing your app.

∨ App Details

Where is the application located? *

○ Outside my corporate network

● Inside my corporate network

App type *

| HTTP/HTTPS ∨ |

App name *

| Slack |

App description

| |

App category ⑦

| Verizon |

App icon

☁ Change icon   Use default icon
(128 KB max, ICO)

☐ Do not display application icon in Workspace app

☐ Add application to favorites in Workspace app

○ Allow user to remove from favorites

○ Do not allow user to remove from favorites

URL *

| https://csg.enterprise.slack.com |

App Connectivity * ⑦

| Internal ∨ |

Related Domains *

| *.csg.enterprise.slack.com |

App Connectivity * ⑦

| Internal ∨ |

Related Domains *

| *.slack.com |

App Connectivity * ⑦

| Internal ∨ | ⊖

⊕ Add another related domain

Save   Cancel

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**.
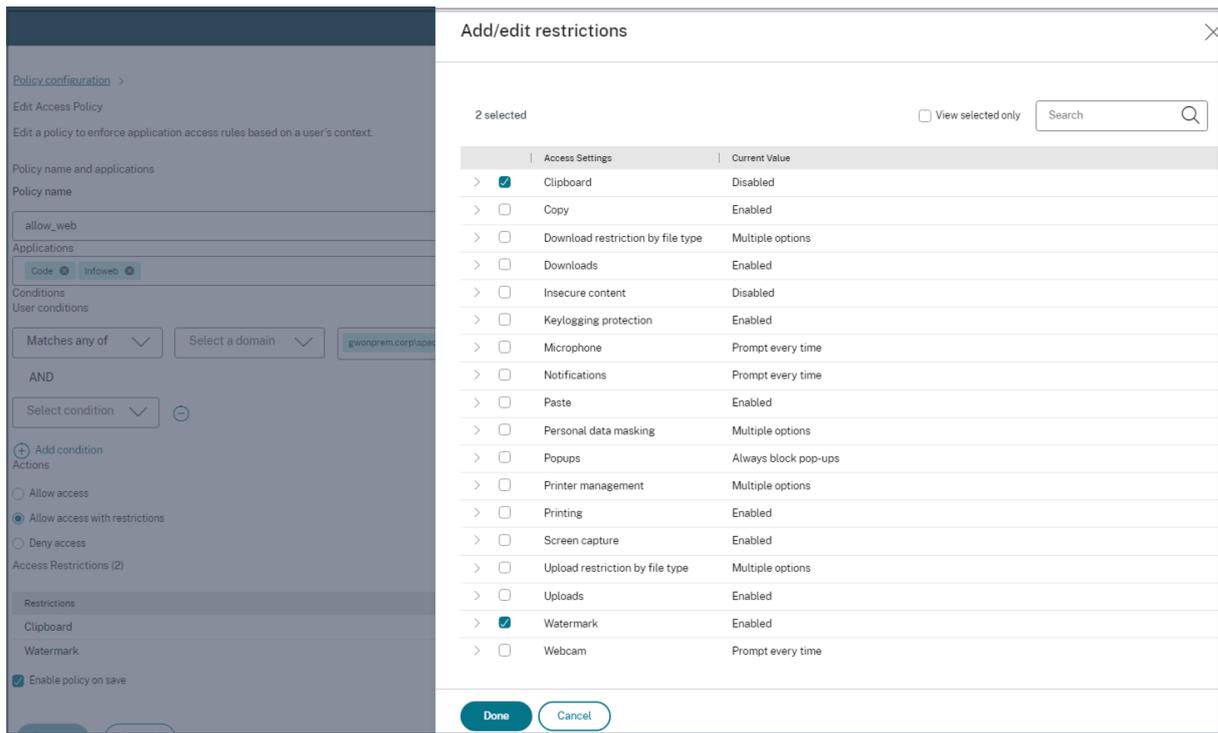
End user flow

August 18, 2025

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

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

1. Access the StoreFront™ store from the Citrix Workspace™ app.

2. Log on to the store.

3. Click the **Apps** tab, and then click the **Office365** application.

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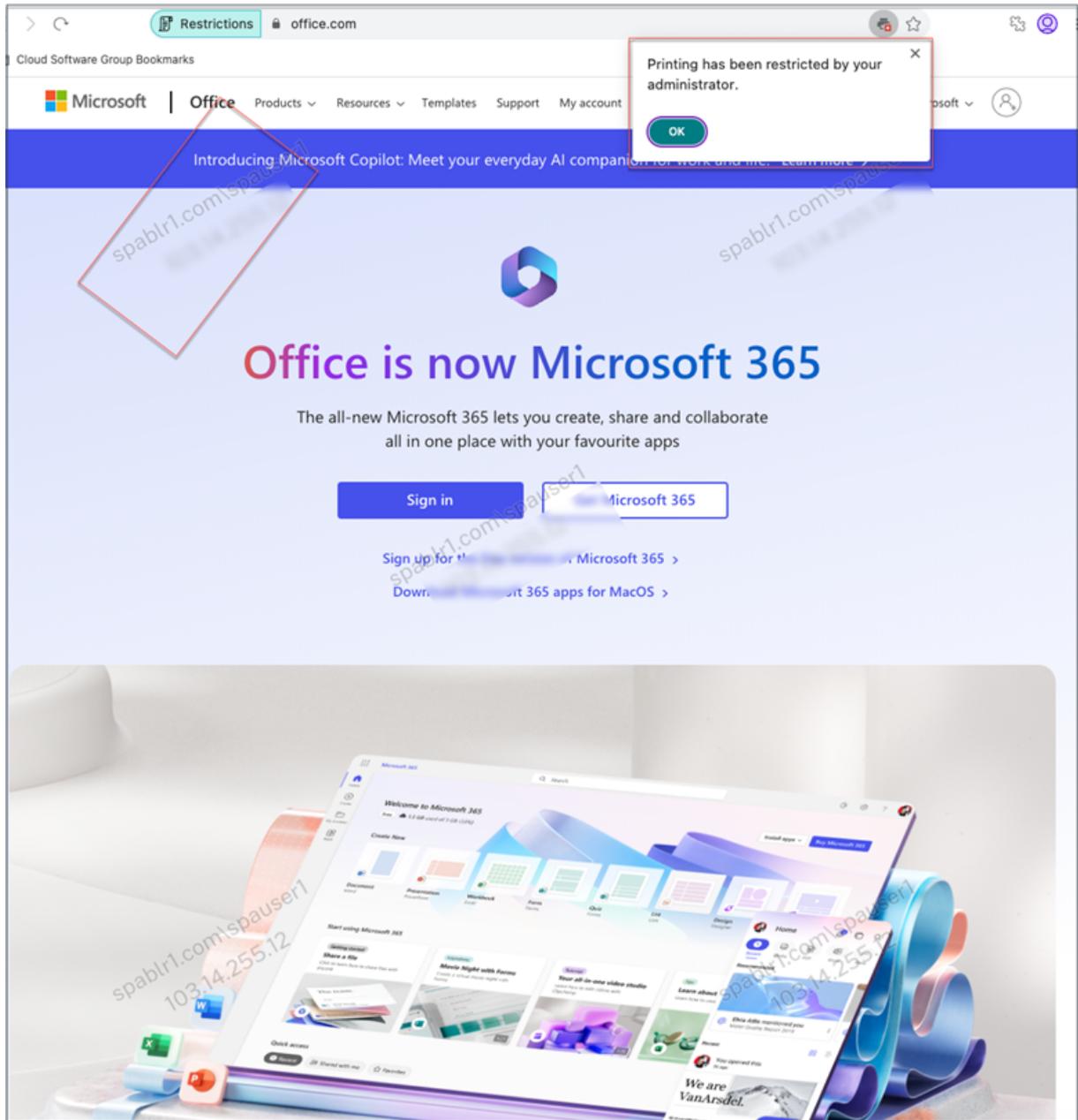
Note:

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.

Monitor and troubleshoot

August 18, 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

August 18, 2025

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

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

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

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

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

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

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

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

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

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

View contextual tags from logs

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

Basic troubleshooting

August 18, 2025

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

Certificate errors

Database creation errors

StoreFront failures

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 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:

```
 1  -   Information
 2  -   Debug
 3  -   Warning
 4  -   Error
 5
 6  "TroubleshootingSql": {
 7
 8    "restrictedToMinimumLevel": "Error",
 9    "batchPostingLimit": 50,
10    "batchPeriod": "00:00:05" // 5 seconds
11  }
```

Secure Private Access sessions codes in Director

August 18, 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.

Code	Status	Description
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.
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.

Logs retention settings

August 18, 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:

```
1    "TroubleshootingLogs": {
2
3      "CleanupPeriodInHours": 12,
4      "CleanupDataOlderThanDays": 7,
5      "CleanupOldestDataIfEntriesCountAbove": 0
```

```
6        }
```

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

August 18, 2025

Telemetry data cleanup

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

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

CDF logs cleanup

CDF logs are stored on the Secure Private Access installation machine, inside the installation folders for the Admin and the runtime service. The CDF logs are placed in .csv files with a 10MB size limit

applied to each file.

The Admin service can retain up to 90 CDF log files at once, after which it deletes the oldest files to clear space for the new CDF log files to be created.

The Runtime service works in the same way as the Admin service but can retain a larger number of files at once, up to 600.

Custom cleanup of CDF logs

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

```
1  "CdfFile": {
2
3      "fileSizeLimitBytes": 10485760, // 10 MB
4      "retainedFileCountLimit": 600
5    }
```

> **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.

Secure Private Access licensing telemetry data elements

August 18, 2025

Event header

Field	Description	Example
ver	Header version. Hardcoded.	1.0 "ver": "1.0"
id	Unique event ID (GUID)	1fced2a0-52e7-4c48-bf4e-6f2e06136e11
type	Event type name. Hardcoded.	PolicyDocument.Download "type": "PolicyDocument.Download"

Field	Description	Example
st	UTC formatted timestamp	2011-08-12T20:17:46.384Z
prod	Product name. Hardcoded.	AccessSecurity.OnPrem "prod": "AccessSecurity.OnPrem"
prodVer	Product version	2402
$schema	Reference to schema. Hardcoded.	`https://cas.citrix.com/schemas/event.json` "$schema": `"https://cas.citrix.com/schemas/event.json"`

tenant	Organization (customer) identification info.
	"tenant": {
	"id": ""
	}
		"tenant": {
		"id": ""
		}

user	User identification mapping info, UPN only
	"UPN": <username (optionally encoded)>
	Encoded if scrambling enabled (see Event Payload enabledFeatures)
		The Secure Private Access plug-in does not track the customer ID/org ID. It must be empty.
		
		clear text
		"user": {
		"UPN": `"userx@domain.com"`
		}
		hashed
		"user": {
		"UPN": "Mzc0NDJkODAxZjl0MDZkMGI2=="
		}

Event payload

Field	Description	Example
actualtemplatecode	Payload template version. Hardcoded. "actualtemplatecode": "1.0"	1.0
ngsUsername	Username in UPN format (clear text/encoded) Encoded if scrambling enabled (see Event Payload enabledFeatures)	user@domain.com; Mzc0NDJkODAxZjl0MDZkMGI2==
ngsProductName	Product name. Hardcoded. "ngsProductName": "AccessSecurity.OnPrem	AccessSecurity.OnPrem
transportProtocolType	Connection type: tcp or udp or 0 (for web\saas)	tcp
ngsRecordType	Application type: websaas or tcpudp	websaas
tenantName	Tenant name for multitenant deployments (service providers) or site name for single tenant	SPAOPDEVSite
enabledFeatures	Denotes the features that are enabled for the session. Currently not used.	1

Third-party notifications

August 18, 2025

Citrix Secure Private Access for on-premises