



# **Citrix Secure Private Access - On premises**

## Contents

<b>Technical overview</b>	<b>3</b>
<b>What's new</b>	<b>4</b>
<b>Fixed issues</b>	<b>5</b>
<b>Known issues</b>	<b>7</b>
<b>System requirements</b>	<b>9</b>
<b>Sizing guidelines</b>	<b>14</b>
<b>Install Secure Private Access</b>	<b>17</b>
<b>Components</b>	<b>22</b>
<b>StoreFront</b>	<b>23</b>
<b>NetScaler Gateway</b>	<b>25</b>
<b>NetScaler Gateway configuration for Web/SaaS applications</b>	<b>29</b>
<b>NetScaler Gateway configuration for TCP/UDP applications</b>	<b>35</b>
<b>Contextual tags</b>	<b>39</b>
<b>License server</b>	<b>44</b>
<b>Citrix Secure Access client</b>	<b>45</b>
<b>Director</b>	<b>47</b>
<b>Web Studio</b>	<b>49</b>
<b>Deploy Secure Private Access as a cluster</b>	<b>49</b>
<b>Configure Secure Private Access plug-in</b>	<b>51</b>
<b>Set up Secure Private Access</b>	<b>51</b>
<b>Configure Web/SaaS applications</b>	<b>59</b>
<b>Configure TCP/UDP apps</b>	<b>62</b>
<b>Configure access policies for the applications</b>	<b>66</b>

<b>Access restriction options</b>	<b>69</b>
<b>End user flow</b>	<b>87</b>
<b>Upgrade</b>	<b>91</b>
<b>Upgrade your Secure Private Access installer</b>	<b>92</b>
<b>Upgrade the database using scripts</b>	<b>94</b>
<b>Manage configurations</b>	<b>95</b>
<b>Manage settings after installation</b>	<b>95</b>
<b>Manage applications and policies</b>	<b>97</b>
<b>Unsanctioned websites</b>	<b>99</b>
<b>Uninstall Secure Private Access</b>	<b>101</b>
<b>Monitor and troubleshoot</b>	<b>102</b>
<b>Dashboard overview</b>	<b>103</b>
<b>Basic troubleshooting</b>	<b>105</b>
<b>Troubleshooting using Director</b>	<b>112</b>
<b>SIEM integration</b>	<b>115</b>
<b>Scout integration</b>	<b>116</b>
<b>Logs retention settings</b>	<b>117</b>
<b>Logs and telemetry cleanup</b>	<b>118</b>
<b>Third-party notifications</b>	<b>119</b>

## Technical overview

September 5, 2024

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

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

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

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

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

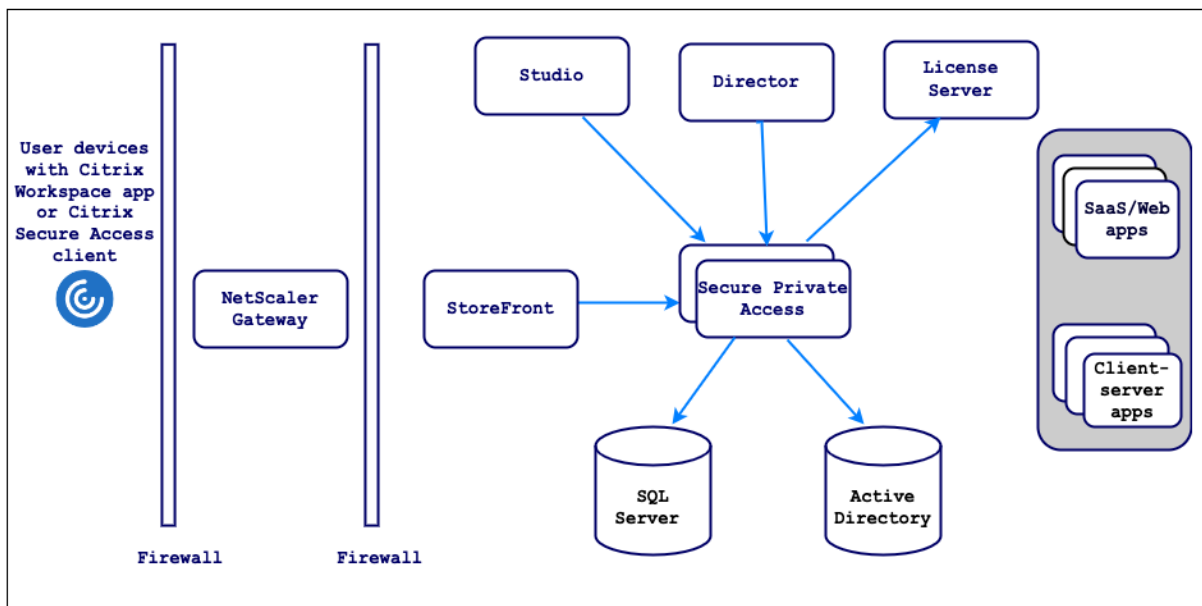
---

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

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

## Components

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



For information about each component, see [Key components](#).

## What's new

September 5, 2024

### July 2024

#### Support for TCP/UDP apps

Secure Private Access is enhanced to support TCP/UDP applications in addition to Web/SaaS applications. End users can now access these applications through the Citrix Secure Access client installed on their devices.

For details see the following topics:

- [Citrix Secure Access client](#)
- [Configure TCP/UDP apps](#)
- [Configure access policies for the applications](#)

### **Integration with the Citrix Scout**

Citrix Secure Private Access is now integrated with Citrix Scout. This integration helps administrators collect logs and metrics for troubleshooting. For details, see [Scout integration](#).

### **Enhancements to the Web Studio integration**

The integration of Citrix Secure Private Access with the Web Studio console is now enhanced to enable users seamlessly access the service through Web Studio. For details, see [Integrate Secure Private Access with Web Studio](#).

### **Enhancements to usage telemetry reporting**

The telemetry reporting functionality is enhanced to gather and analyze data on license usage for Citrix products, components, and features within customer-managed environments managed by customers. This enhancement ensures compliance with licensing agreements for the deployment of Citrix products.

To use this feature, you must update to the latest version of the license server. For more information, see the following topics:

- [Citrix licensing telemetry](#)
- [Required license server updates](#)
- [Citrix license telemetry FAQ](#)
- [Citrix Licensing Telemetry data elements](#)

### **Fixed issues**

September 5, 2024

The following issues are addressed in release 2407.

## Domain Controller configuration

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

## Admin management

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

## 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.

## 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.

- While adding an app, if the app name contains a comma, a warning is displayed. However, the app is created.
- If an app URL contains `www`, then the URL is saved in the routing domain table (**Settings > Application Domain**) without the prefix `www`.

## Upgrades

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).

## Known issues

September 5, 2024

The following issues exist in release 2407.

**Note:**

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

### 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.

[SPAOP-2031]

- If the machine’s domain where Secure Private Access for on-premises is installed is different than the domain of the administrator logged in to Secure Private Access, then you must do the following:

Add a different domain service account as an identity in the IIS Application pool for both the Secure Private Access admin and runtime service.

- Distribution groups are not supported in Secure Private Access. Therefore, policies cannot search for distribution groups to add user and group conditions.
- Secure Private Access does not capture the domain details in the admin console or service. Hence, it relies completely on the domain that the user provided. Therefore, if the corresponding domain is not accessible or if the domain name is not a valid name, then that domain is not supported.

### NetScaler Gateway

- The SSL virtual server with SSL profile configuration isn’t supported in the following scenario.
  - The customer is using NetScaler Gateway 13.1–48.47 and later or 14.1–4.42 and later.
  - The `ns_vpn_enable_spa_onprem` toggle is enabled.



### **Workaround:**

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

For details on the toggle, see [Support for smart access tags](#).

### **RfWeb / Workspace for web**

- RfWeb / Workspace for web isn't supported and hence the apps are not enumerated. For details, see [When using StoreFront version 2311 or later](#).

[SPAOP-2487]

### **Application launch**

- If the `ns_vpn_enable_spa_onprem` and `toggle_vpn_enable_securebrowse_client_mode` knobs are not enabled or if these knobs are not supported in your NetScaler Gateway, then app launch fails after the `CustomHeaderCryptoKey` rotation. The `CustomHeaderCryptoKey` rotation happens automatically after 30 days.

[SPAOP-4528]

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

[SPAOP-1412]

### **StoreFront**

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

### **Logging**

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

## Enable feature flag for TCP/UDP monitoring

- The **SPAOP-3315-EnableZTNAApplications** feature flag is disabled by default in 2407. As a result, the TCP/UDP monitoring data is not stored and hence the Director integration fails.

Workaround: If you are using TCP/UDP apps and want to enable Director integration, manually update the database to enable this feature flag.

[SPAOP-5587]

## Upgrade

- After you upgrade to 2407 and edit an existing app whose URL starts with [www](#), then the **App Connectivity** field does not populate the previous state. You must select the app connectivity type again. This is a one-time action post-upgrade after which the configuration is saved and continues to persist.

[SPAOP-4216]

- After you upgrade to 2407, though you can log on to the admin console, you cannot manage applications and policies. An error message appears.

Workaround: You must upgrade the database using the scripts. For details, see [Upgrade the database using scripts](#).

[SPAOP-5255]

- After you upgrade to 2407, application enumeration and application launch fail.

Workaround: You must upgrade the database using the scripts. For details, see [Upgrade the database using scripts](#).

[SPAOP-5255]

- You cannot upgrade the Secure Private Access plug-in from earlier versions to 2407 if the plug-in was installed using the Delivery Controller.

[SPAOP-4505]

## System requirements

September 27, 2024

Ensure that your product meets the minimal version requirements.

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

**Communication ports:** Ensure that you have opened the required ports for the Secure Private Access plug-in. For details, see [Communication ports](#).

**Note:**

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

## Prerequisites

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

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

- Authentication profile name configured on NetScaler.
- SSL server certificate configured on NetScaler.
- Domain name.
- Certificate configurations are complete. Admins must ensure that the certificate configurations are complete. The Secure Private Access installer configures a self-signed certificate if no certificate is found in the machine. However, this might not always work.

**Note:**

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

### Admin account requirements

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

- Install Secure Private Access: You must be logged in with a local machine administrator account.
- Set Up Secure Private Access: You must sign into the Secure Private Access admin console with a domain user which is also a local machine administrator for the machine where Secure Private Access is installed.
- Manage Secure Private Access: You must sign into the Secure Private Access admin console with a Secure Private Access administrator account.

### Communication ports

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

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

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

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

## References

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

## Sizing guidelines

September 5, 2024

### 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, up to 20 levels of nesting

---

Configuration	Details
Troubleshooting log retention period	7 days (default)
Troubleshooting Log level	Error (default)
Secure Private Access server log retention	90 days or 600 files

---

## Host storage

The host storage details for a benchmark of 5000 users are as follows:

Size - 127 Gig

IOPS - 500

Maximum throughput - 100

## 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 size of 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 Secure Private Access

September 27, 2024

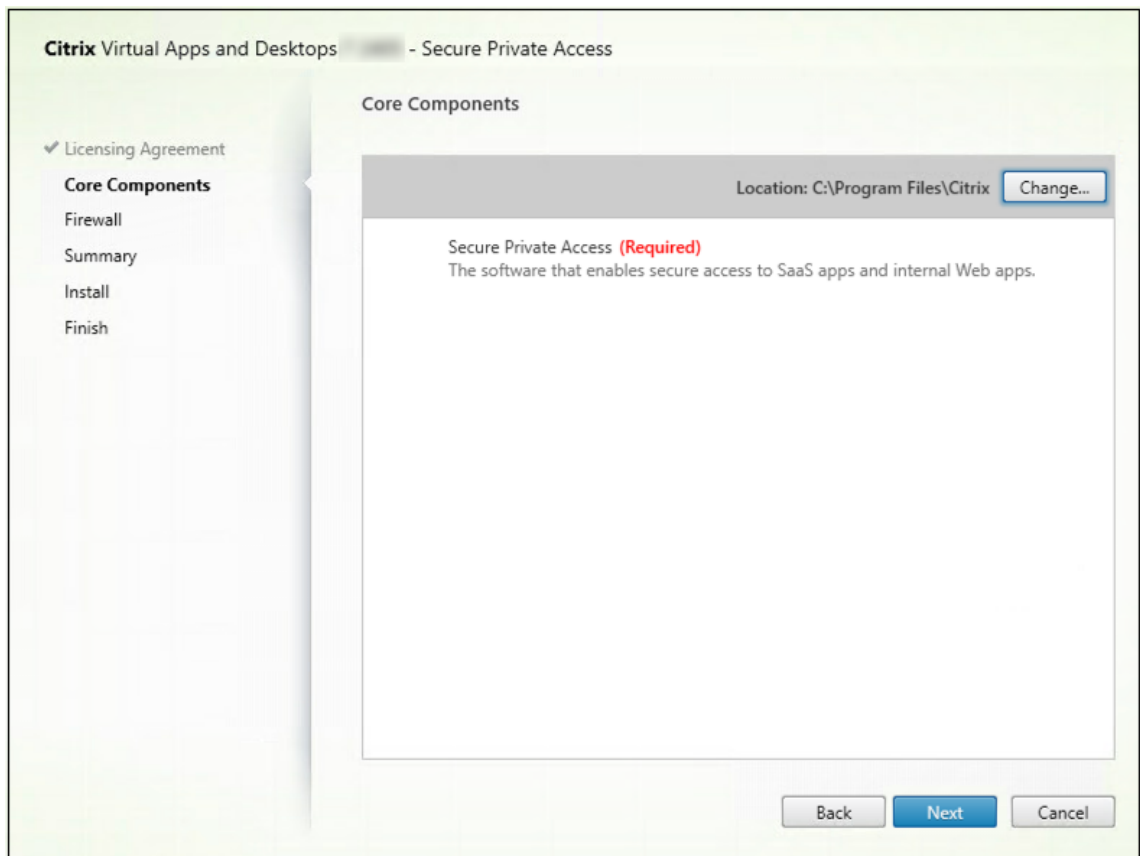
The secure Private Access installer is available as a standalone installer or as part of the integrated Citrix Virtual Apps and Desktops installer.

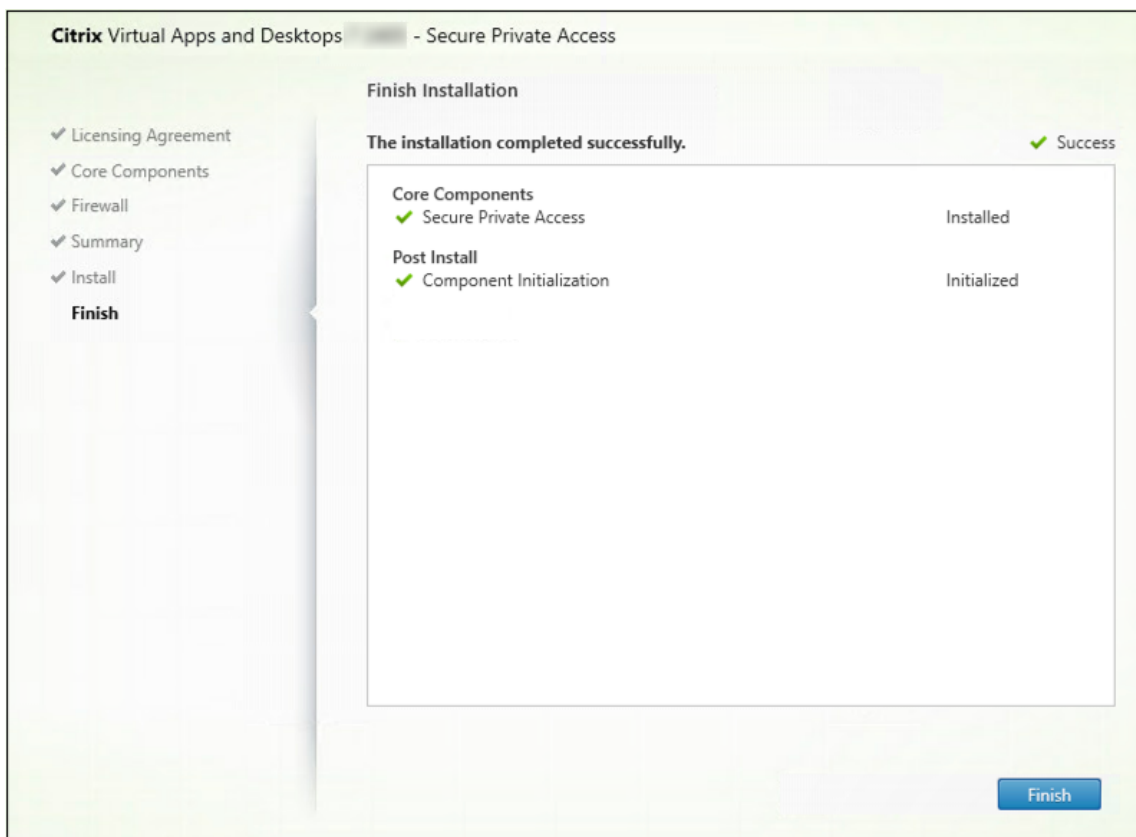
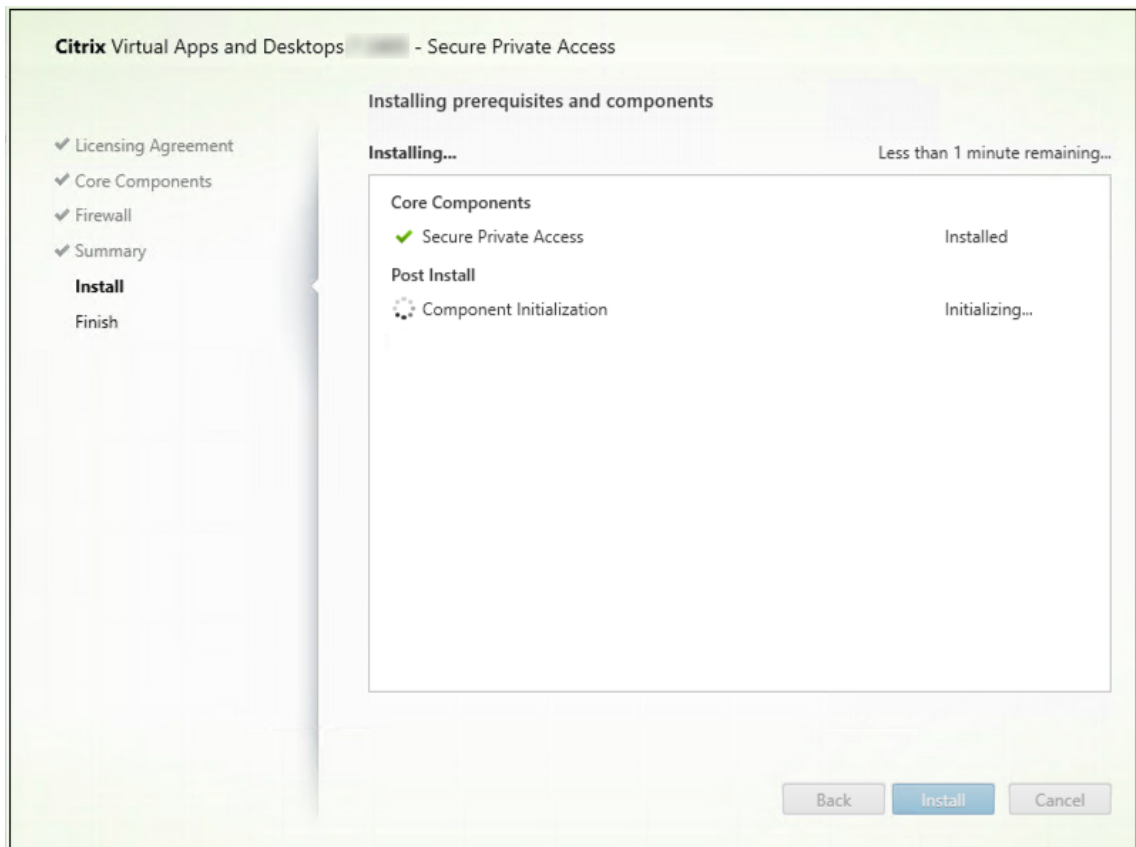
### Admin account requirements to install and manage Secure Private Access

- 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.

### Perform the following steps to install Secure Private Access:

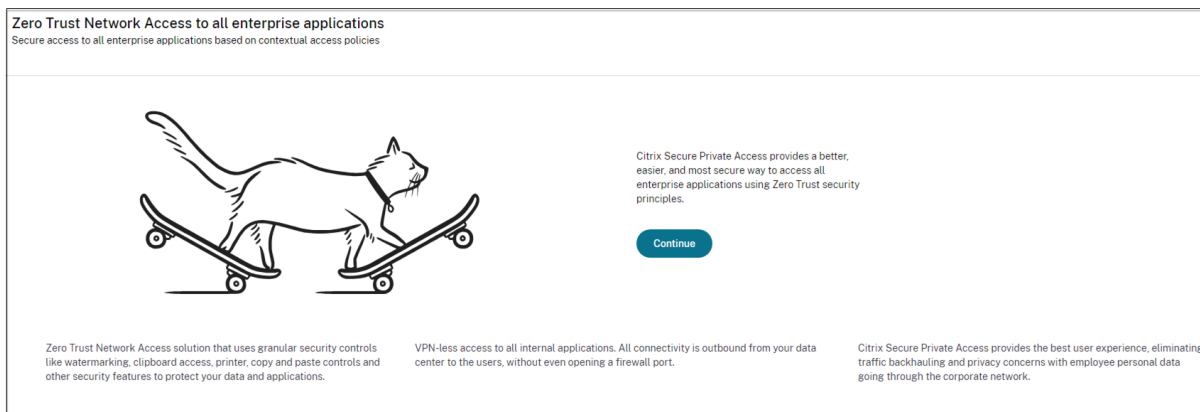
1. Download the Citrix Virtual Apps and Desktops product software from <https://www.citrix.com/downloads/citrix-virtual-apps-and-desktops/> and launch the wizard.
2. Click **Start** next to the product to install: Virtual Apps or Virtual Apps and Desktops.
3. Choose **Secure Private Access** and follow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



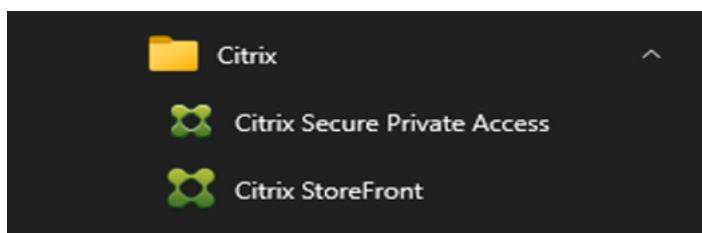


For detailed step-by-step instructions, see [Install core components](#) and [Install using the command line](#).

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.

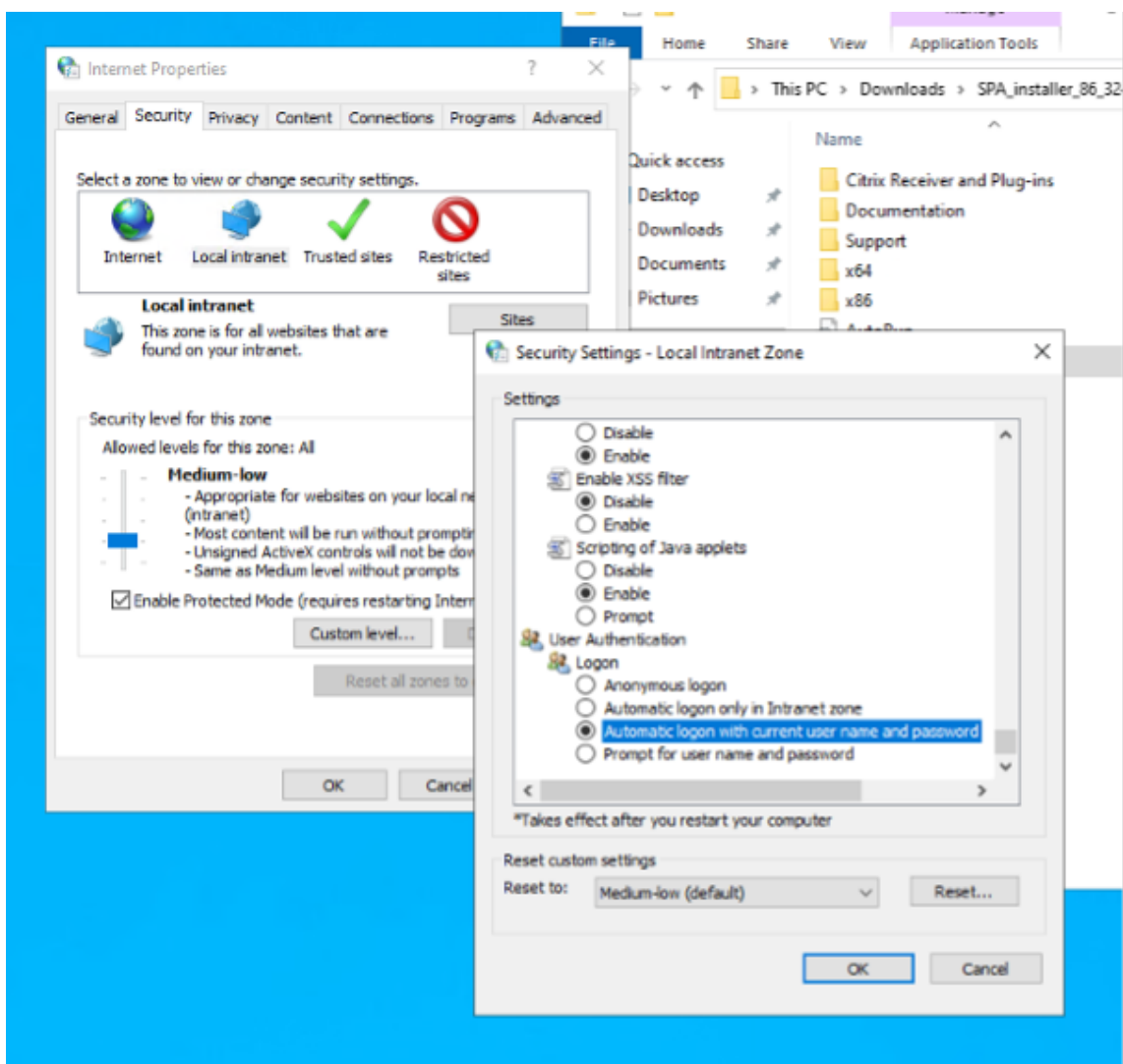
You must sign into the admin console to continue with the Secure Private Access setup. You can set up Secure Private Access with any user who belongs to the same domain as the installation machine, if the user has local administrator privileges on the installation machine.

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](https://*.fabrikam.local)".

4. Click **Custom Level**.
5. In **User Authentication > Logon**, select **Automatic logon with current user name and password**.



**Note:**

- If using Chrome Incognito sessions, create a DWORD registry key Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE and set to value 1.

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

## Next steps

- [Set up Secure Private Access](#)
- [Configure NetScaler Gateway](#)
- [Configure applications](#)
- [Configure access policies for the applications](#)

## Components

September 27, 2024

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

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

For information about the minimum versions requirements of these products, see [System requirements](#).

**Note:**

Director and License Server are integrated with Secure Private Access starting from release 2402.

## StoreFront

September 5, 2024

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 plugin configuration can be seen in the StoreFront admin UI (**Manage Delivery Controllers** screen).

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



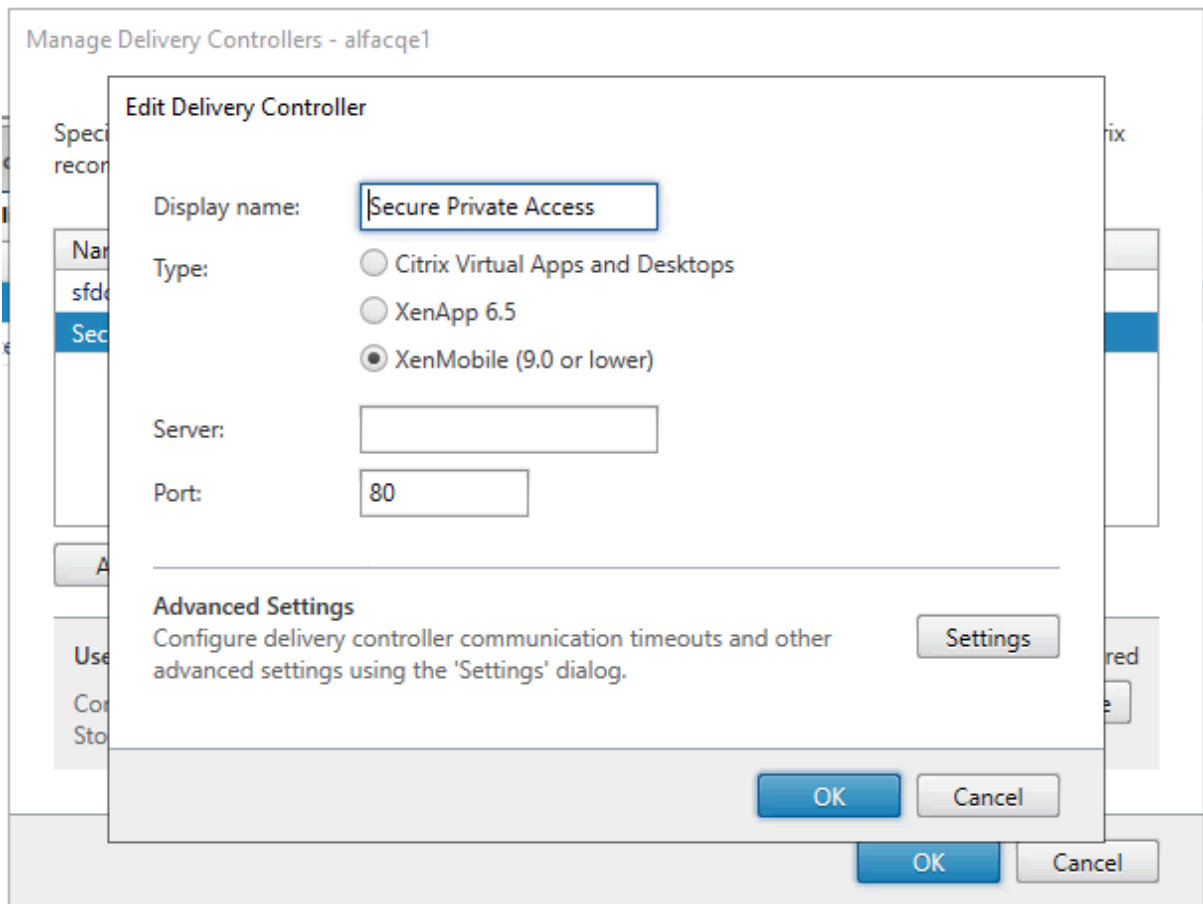
**Important:**

- It is recommended to use the StoreFront script downloaded from the Secure Private Access admin UI to configure StoreFront for Secure Private Access only. Do not configure Secure Private Access from the StoreFront admin UI as the UI does not cover all the required configuration on StoreFront. The script must be run to complete all the necessary configurations.
- One Secure Private Access site can be configured on multiple StoreFront deployments (either on another store on the same StoreFront or a different StoreFront deployment) as well. StoreFront can be added from the **Settings > Integrations** page.
- The StoreFront auto configuration doesn't work from **Settings > Integration** page even if Secure Private Access is co-hosted with StoreFront. Autoconfiguration is done only 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.

## NetScaler Gateway

September 27, 2024

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

**Important:**

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

- [NetScaler Gateway configuration for Web/SaaS applications](#)
- [NetScaler Gateway configuration for TCP/UDP applications](#)

## Compatibility with the ICA apps

NetScaler Gateway created or updated to support the Secure Private Access plug-in can also be used to enumerate and launch ICA apps. In this case, you must configure Secure Ticket Authority (STA) and bind it to the NetScaler Gateway.

**Note:**

STA server is usually a part of Citrix Virtual Apps and Desktops deployment.

For details, see the following topics:

- [Configuring the Secure Ticket Authority on NetScaler Gateway](#)
- [FAQ: Citrix Secure Gateway/ NetScaler Gateway Secure Ticket Authority](#)

## Support for smart access tags

**Note:**

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

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

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

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

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

- You can toggle with command (FreeBSD shell):

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

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

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

- Enable redirection to the “Access restricted” page if access is denied.

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

- Use the “Access restricted” page hosted on CDN.

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

- To disable, run the same command again.
- To verify whether the toggle is on or off run the `nsconmsg` command.
- To configure smart access tags on NetScaler Gateway, see [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_wr.sh -ys call=ns_vpn_enable_spa_onprem
```

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

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

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

3. Save the file.

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

## Enable Secure Private Access plug-in on NetScaler Gateway

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

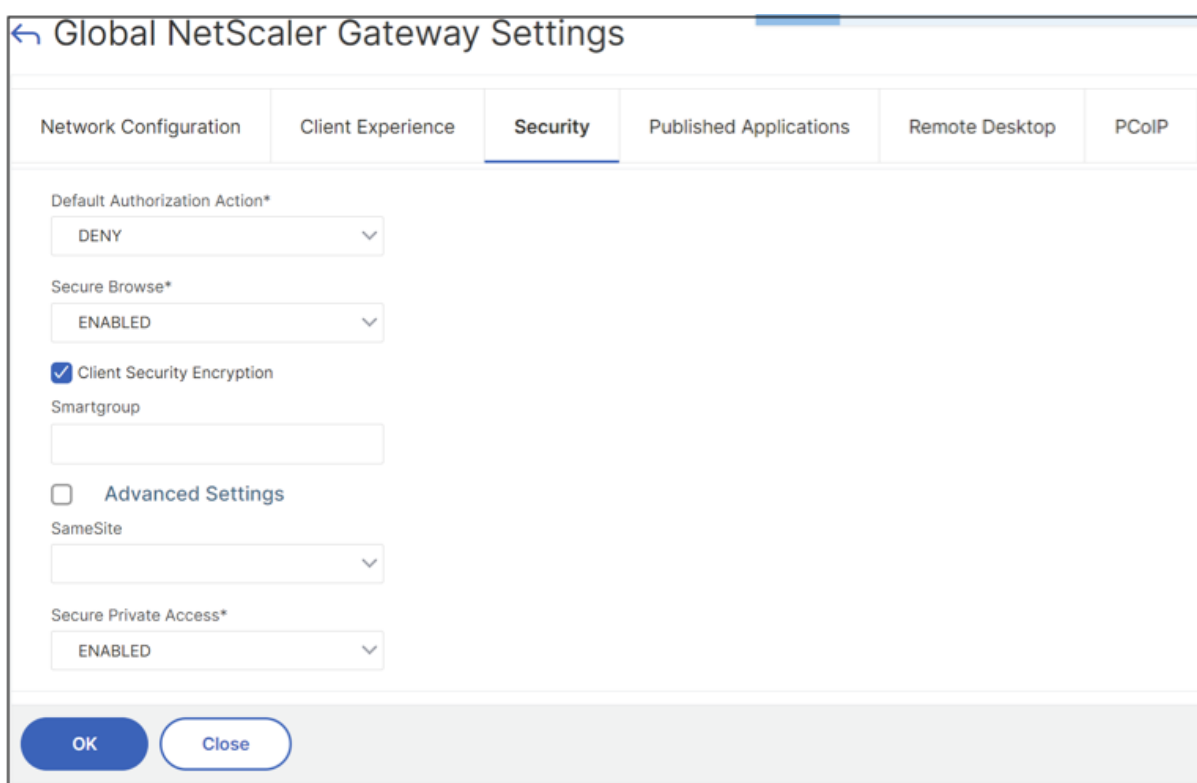
### CLI:

At the command prompt, type the following command:

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

### GUI:

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



The screenshot shows the 'Global NetScaler Gateway Settings' window with the 'Security' tab selected. The settings are as follows:

Network Configuration	Client Experience	Security	Published Applications	Remote Desktop	PCoIP
Default Authorization Action*					
DENY					
Secure Browse*					
ENABLED					
<input checked="" type="checkbox"/> Client Security Encryption					
Smartgroup					
<input type="checkbox"/> Advanced Settings					
SameSite					
Secure Private Access*					
ENABLED					

Buttons: OK, Close

## 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.
- Do not use ICA Proxy on NetScaler Gateway. This feature is disabled when NetScaler Gateway is configured.
- If you use NetScaler deployed in the cloud, you must make changes in the network. For example, allow communications between NetScaler and other components on certain ports.
- If you enable SSO on NetScaler Gateway, make sure that NetScaler communicates to StoreFront using a private IP address. You might have to add a StoreFront DNS record to NetScaler with a StoreFront private IP address.

## NetScaler Gateway configuration for Web/SaaS applications

September 27, 2024

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

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

Forexample, `*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@nsbeta# ./ns_gateway_secure_access.sh
NetScaler Gateway vserver name (Default: _SecureAccess_Gateway):
NetScaler Gateway IP:
NetScaler Gateway FQDN: gateway.mydomain.com
SPA Plugin IP:
SPA Plugin FQDN: spa.mydomain.com
StoreFront Store URL (including protocol http/https): https://
NetScaler authentication profile name: auth_prof
NetScaler authentication vserver: auth_vs
NetScaler SSL server certificate name: star.mydomain.com
Domain: mydomain.com

***** Gateway configuration *****
NetScaler Gateway name: _SecureAccess_Gateway
NetScaler Gateway IP:
NetScaler Gateway FQDN: gateway.mydomain.com
SPA Plugin FQDN: spa.mydomain.com
SPA Plugin IP:
StoreFront Store URL: https://store
NetScaler authentication profile name: auth_prof
NetScaler authentication vserver: auth_vs
NetScaler Gateway server certificate name: star.mydomain.com
Domain: mydomain.com

Checking SPA Plugin support....
NetScaler supports SPA Plugin
Enabling SPA Plugin support.....SUCCESS
Enabling ns_vpn_securebrowse_client_mode_enabled feature.....SUCCESS
Enabling ns_vpn_redirect_to_access_restricted_page_on_deny feature.....SUCCESS
Enabling ns_vpn_use_cdn_for_access_restricted_page feature.....SUCCESS
Persisting SPA Plugin setting nsapimgr_wr.sh -ys call=ns_vpn_enable_spa_onprem in /nsconfig/rc.netscaler file.
Persisting SPA Plugin setting nsapimgr_wr.sh -ys call=toggle_vpn_enable_securebrowse_client_mode in /nsconfig/rc.netscaler file.
Persisting SPA Plugin setting nsapimgr_wr.sh -ys call=toggle_vpn_redirect_to_access_restricted_page_on_deny in /nsconfig/rc.netscaler file.
Persisting SPA Plugin setting nsapimgr_wr.sh -ys call=toggle_vpn_use_cdn_for_access_restricted_page 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

root@nsbeta# █

```

6. Enter **N** for the **Enable TCP/UDP App type support** parameter if you intend to configure gateway only for Web and SaaS applications.
7. Input the required parameters. For the list of parameters, see [Prerequisites](#).

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

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

**Note:**

During script execution, NetScaler and Secure Private Access plug-in compatibility is checked. If NetScaler supports the Secure Private Access plug-in, the script enables NetScaler features to support smart access tags sending improvements and redirection to a new Deny Page when access to a resource is restricted. For details about smart tags, see [Support for smart access tags](#).

The Secure Private Access plug-in features persisted in the /nsconfig/rc.netscaler file allow to keep them enabled after NetScaler is restarted.

```
#####
#1. Upload file to NetScaler (e.g. to /var/tmp)
#2. Run batch command (e.g. batch -filename /var/tmp/ns_gateway_secure_access -outfile /var/tmp/ns_gateway_secure_access_output)
#3. Analyze output (e.g. cat /var/tmp/ns_gateway_secure_access_output)
#####
# Enable NetScaler features
enable ns feature Ssl SSLVpn AAA SWSMITE ID

# Add NetScaler gateway vserver
add vpn vsrvr01_SecureAccess_Gateway Ssl 100.100.100.100 443 -listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile -deploymentType ICA_STOREFRONT -vserverFqdn gateway.mydomain.com -authProfile auth_prof -icaOnly OFF

# Add default AAA group for authenticated users
add aaa Group SecureAccessGroup

# Add excluded domains
bind policy pattern ns_cvpn_default_bypass_domains storefront.mydomain.com
bind policy pattern ns_cvpn_default_bypass_domains spa.mydomain.com
bind policy pattern ns_cvpn_default_bypass_domains citrix.com

# Add session actions
add vpn sessionAction AC_WB_SecureAccess_Gateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useMIE NS -useSIP OFF -icaProxy OFF -whome "https://storefront.mydomain.com" -ClientChoice OFF -ntdom
mydomain.com -defaultAuthzAction ALLOW -authorizationGroup SecureAccessGroup -clientlessVpnMode ON -clientlessModeOfEncoding TRANSPARENT -secureBrowsE ENABLED -storefronturl "https://storefront.mydomain.com" -stogatewayAuth
type domain
add vpn sessionAction AC_WB_SecureAccess_Gateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useMIE NS -useSIP OFF -icaProxy OFF -whome "https://storefront.mydomain.com" -ClientChoice OFF -ntdom
mydomain.com -defaultAuthzAction Allow -authorizationGroup SecureAccessGroup -clientlessVpnMode ON -clientlessModeOfEncoding TRANSPARENT -secureBrowsE ENABLED -storefronturl "https://storefront.mydomain.com" -stogatewayAuth
type domain

# Add session policies
add vpn sessionPolicy PL_WB_SecureAccess_Gateway "HTTP_REQ_HEADER("User-Agent").CONTAINS("CitrixReceiver")" AC_WB_SecureAccess_Gateway
add vpn sessionPolicy PL_WB_SecureAccess_Gateway "HTTP_REQ_HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT" AC_WB_SecureAccess_Gateway

# Add rewrite policies for Citrix headers
add rewrite action Add_X-Citrix-Via insert_Http_Header X-Citrix-Via "gateway.mydomain.com"
add rewrite action Add_X-Citrix-Via-VIP insert_Http_Header X-Citrix-Via-VIP "1"
add rewrite action Add_X-OW-SessionId insert_Http_Header X-OW-SessionId AAA.OSSessionID
add rewrite policy Add_X-Citrix-ViaLabel "HTTP_REQ_HEADER("Host").CONTAINS("spa.mydomain.com") && HTTP_REQ_HEADER("X-Citrix-Via").EXISTS.NOT" Add_X-Citrix-Via
add rewrite policy Add_X-Citrix-Via-VipLabel "HTTP_REQ_HEADER("Host").CONTAINS("spa.mydomain.com") && HTTP_REQ_HEADER("X-Citrix-Via-VIP").EXISTS.NOT" Add_X-Citrix-Via-VIP
add rewrite policy Add_X-OW-SessionIdLabel "HTTP_REQ_HEADER("Host").CONTAINS("spa.mydomain.com") Add_X-OW-SessionID

# Add SSO traffic policy for SPA Plugin
add vpn trafficAction_SecureAccess_Gateway_Traffic_Action Http -SSO ON
add vpn trafficPolicy_SecureAccess_Gateway_Traffic_Policy "HTTP_REQ_HEADER("Host").CONTAINS("spa.mydomain.com")" SecureAccess_Gateway_Traffic_Action

# Bind policies to NetScaler gateway vserver
bind vpn vserver_SecureAccess_Gateway policy PL_WB_SecureAccess_Gateway -priority 100 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver_SecureAccess_Gateway policy PL_WB_SecureAccess_Gateway -priority 100 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver_SecureAccess_Gateway policy Add_X-Citrix-ViaLabel -priority 120 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver_SecureAccess_Gateway policy Add_X-Citrix-Via-VipLabel -priority 130 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver_SecureAccess_Gateway policy Add_X-OW-SessionIdLabel -priority 140 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver_SecureAccess_Gateway policy Add_X-OW-SessionIdLabel -priority 140 -gotoPriorityExpression NEXT -type REQUEST

# Bind SSL cert to NetScaler Gateway
bind ssl vserver_SecureAccess_Gateway sslcertName star.mydomain.com
```

8. 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.

9. Ensure that all commands are successfully completed.

**Note:**

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



## Update existing NetScaler Gateway configuration for Web and SaaS apps

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

### Note:

Starting from NetScaler Gateway 14.1–25.56 and later, you can enable the Secure Private Access plug-in on NetScaler Gateway by using the NetScaler Gateway CLI or the GUI. For details, see [Enable Secure Private Access plug-in on NetScaler Gateway](#).

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

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

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

## NetScaler Gateway virtual server settings

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

### Add a virtual server:

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

### Update a virtual server:

- `tcpProfileName`: `nstcp_default_XA_XD_profile`
- `icaOnly`: `OFF`

## NetScaler Gateway session policy settings

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

- `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

### Example commands to update an existing NetScaler Gateway configuration

Add/update a virtual server:

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

Add a session action:

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

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

Add a session policy:

- `add vpn sessionPolicy PL_OSspaonprem "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")"AC_OSspaonprem`
- `add vpn sessionPolicy PL_WBspaonprem "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT && HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"plugin\").NOT"AC_WBspaonprem`

Bind the session policy to the VPN virtual server:

- `bind vpn vserver SecureAccess_Gateway -policy PL_OSspaonprem -priority 111 -gotoPriorityExpression NEXT -type REQUEST`
- `bind vpn vserver SecureAccess_Gateway -policy PL_WBspaonprem -priority 110 -gotoPriorityExpression NEXT -type REQUEST`

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

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

For details on session action parameters, [vpn-sessionAction](#).

## Additional information

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

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

## NetScaler Gateway configuration for TCP/UDP applications

September 27, 2024

You can use the procedure outlined in [NetScaler Gateway configuration for Web/SaaS applications](#) to configure TCP/UDP applications. To configure gateway for TCP/UDP applications, you must enable the TCP/UDP support by entering **Y** for the **Enable TCP/UDP App type support** parameter in the script.

The following figure displays the **Enable TCP/UDP App type support** parameter enabled for TCP/UDP support.

```
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
```

```
root@ns32201# cat ns_gateway_secure_access
#####
#1: Upload file to NetScaler (e.g. to /var/tmp) #
#2: Run batch command (e.g. batch -fileName /var/tmp/ns_gateway_secure_access -outfile /var/tmp/ns_gateway_secure_access_output) #
#3: Analyze output (e.g. cat /var/tmp/ns_gateway_secure_access_output) #
#####

# Enable NetScaler features
enable ns features SSL SRVVPN AAA REWRITE IC

# Add NetScaler Gateway vserver
add vpn vserver _NS_SecureAccess_Gateway SSL 333.333.333.443 -listenpolicy NONE -topProfileName natop_default_XA_XD_profile -deploymentType ICA_STOREFRONT -vserverFqdn gateway.domain.com -authProfile authn_prof -icaOnly OFF

# Add default AAA group for authenticated users
add aaa group SecureAccessGroup

# Add excluded domains
bind policy patset ns_cvpn_default_bypass_domains storefront.domain.com
bind policy patset ns_cvpn_default_bypass_domains spa.domain.com
bind policy patset ns_cvpn_default_bypass_domains citrix.com

# Add session actions
add vpn sessionAction AC_08_SecureAccess_Gateway -transparentInterception OFF -SSO_ON -ssoCredential PRIMARY -useNIP NS -useIIP OFF -icaProxy OFF -wihome "https://storefront.domain.com/Citrix/SPAstoreMS
?control=https://storefront.domain.com" -defaultAuthorizationAction ALLOW -authorizationGroup SecureAccessGroup -clientlessVpnMode ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -sto
reFront "https://storefront.domain.com" -sfGatewayAuthType domain

add vpn sessionAction AC_WB_SecureAccess_Gateway -transparentInterception OFF -SSO_ON -ssoCredential PRIMARY -useNIP NS -useIIP OFF -icaProxy OFF -wihome "https://storefront.domain.com/Citrix/SPAstoreMS
?control=https://storefront.domain.com" -defaultAuthorizationAction ALLOW -authorizationGroup SecureAccessGroup -clientlessVpnMode ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -sto
reFront "https://storefront.domain.com" -sfGatewayAuthType domain

# Add session policies
add vpn sessionPolicy PL_08_SecureAccess_Gateway "HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver(*)" AC_08_SecureAccess_Gateway
add vpn sessionPolicy PL_WB_SecureAccess_Gateway "HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver(*)" NOT AC_WB_SecureAccess_Gateway

# Add rewrite policies for Citrix headers
add rewrite action Add_X-Citrix-Via insert_http_header X-Citrix-Via "*"gateway.domain.com""
add rewrite action Add_X-Citrix-Via-VIP insert_http_header X-Citrix-Via-VIP "*"333.333.333.333""
add rewrite action Add_X-GW-SessionId insert_http_header X-GW-SessionId AAA.USER.SESSIONID
add rewrite policy Add_X-Citrix-Via01 "HTTP.REQ.HOSTNAME.CONTAINS("spa.domain.com")" is HTTP.REQ.HEADER("X-Citrix-Via(*)".EXISTS_NOT" Add_X-Citrix-Via
add rewrite policy Add_X-Citrix-Via-VIP01 "HTTP.REQ.HOSTNAME.CONTAINS("spa.domain.com")" is HTTP.REQ.HEADER("X-Citrix-Via-VIP(*)".EXISTS_NOT" Add_X-Citrix-Via-VIP
add rewrite policy Add_X-GW-SessionID01 "HTTP.REQ.HOSTNAME.CONTAINS("spa.domain.com")" Add_X-GW-SessionId

# Add SSO traffic policy for SPA Plugin
add vpn trafficAction _SecureAccess_Gateway_Traffic_Action http -SSO_ON
```

## Update existing NetScaler Gateway configuration for TCP/UDP apps

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

### NetScaler Gateway virtual server settings

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

#### Add a virtual server:

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

#### Update a virtual server:

- `tcpProfileName`: `nstcp_default_XA_XD_profile`
- `icaOnly`: `OFF`

For details on the virtual server parameters, see [vpn-sessionAction](#).

### NetScaler Gateway session policy settings

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

- `transparentInterception`: `ON`
- `SSO`: `ON`
- `ssoCredential`: `PRIMARY`
- `useMIP`: `NS`
- `useIIP`: `OFF`
- `icaProxy`: `OFF`
- `ClientChoices`: `ON`
- `ntDomain`: `mydomain.com` - used for SSO (optional)

- `defaultAuthorizationAction`: ALLOW
- `authorizationGroup`: SecureAccessGroup
- `clientlessVpnMode`: OFF
- `clientlessModeUrlEncoding`: TRANSPARENT
- `SecureBrowse`: ENABLED

### Example commands to update an existing NetScaler Gateway configuration

#### Note:

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

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

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

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

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

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

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

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

```
add policy httpCallout SecureAccess_httpCallout_TCP -IPAddress
  192.0.2.24 -port 443 -returnType BOOL -httpMethod POST -hostExpr
  \\"spa.example.corp\\" -urlStemExpr \\"/secureAccess/authorize\\"
  -headers Content-Type(\\"application/json\")X-Citrix-SecureAccess-
  Cache(\\"dstip="+HTTP.REQ.HEADER("CSIP").VALUE(0)+"&sessid="+aaa.
  user.sessionid)-bodyExpr q/{ "+"\\"userName\":"\\"+aaa.USER.NAME
  .REGEX_REPLACE(re#\|#, "\\|", ALL)+"\\" , "+"\\"domain\":"\\"+aaa.
  USER.DOMAIN+"\\", "+"\\"customTags\":"\\"+http.REQ.HEADER("X-Citrix
```

```
-AccessSecurity").VALUE(0)+"\","+"\"gatewayAddress\":\\"ns224158
.example.corp\", "+"\"userAgent\":\\"CitrixSecureAccess\", "+"\"
applicationDomain\":\\"" + http.REQ.HEADER("CSHOST").VALUE(0)+"\",
"+"\"smartAccessTags\":\\"" + aaa.user.attribute("smartaccess_tags
")+ "\" , \"applicationType\":\\"ztna\", \"applicationDetails\":{
\"destinationIp\":\\"" + HTTP.REQ.HEADER("CSIP").VALUE(0)+"\", \"
destinationPort\":\\"" + HTTP.REQ.HEADER("PORT").VALUE(0)+"\", \"
protocol\":\\"TCP\" } } "/ -scheme https -resultExpr "http.RES.
HEADER(\\"X-Citrix-SecureAccess-Decision\").contains(\\"ALLOW\")"
```

where

- **192.0.2.24** is the Secure Private Access plug-in IP address
  - **spa.example.corp** is the FQDN of the Secure Private Access plug-in
  - **ns224158.example.corp** is the FQDN of the gateway VPN virtual server
- Add an authorization policy to support TCP/UDP based connections.
 

```
add authorization policy SECUREACCESS_AUTHORIZATION_TCP "HTTP.REQ
.URL.EQ(\\"/cs\")==& HTTP.REQ.HEADER(\\"PRTCL\").EQ(\\"TCP\")==& sys.
HTTP_CALLOUT(SecureAccess_httpCallout_TCP)"ALLOW
```
  - Bind the authorization policy to the authentication and authorization group to support TCP/UDP based applications.
 

```
bind aaa group SecureAccessGroup -policy SECUREACCESS_AUTHORIZATION_TCP
-priority 1010 -gotoPriorityExpression END
```
  - Bind the Secure Private Access plug-in to the VPN virtual server.
 

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

## Additional information

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

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

## Contextual tags

September 5, 2024

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.



Dashboard Configuration Reporting Documentation Downloads

### Create Preauthentication Profile

Name\*  
win10\_profile ⓘ

Action\*  
ALLOW ▾

Processes to be cancelled

Files to be deleted

Default EPA Group  
spaopdev ⓘ

Create Close

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.

Dashboard Configuration Reporting Documentation Downloads

### Create Preauthentication Policy

Name\*  
Windows10 ⓘ

Request Action\*  
 ▾ Add Edit

Expression\*  
Select ▾ Select ▾ Select ▾

CLIENT.OS(win10).HOTFIX == EXISTS

Create Close

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

## Add Expression

Select Expression Type: Client Security ▾

Component  
Operating System ▾

Name\*  
Windows 10 ▾

Qualifier  
Hotfix ▾

Operator  
== ▾

Value\*

Frequency (min)

Error Weight

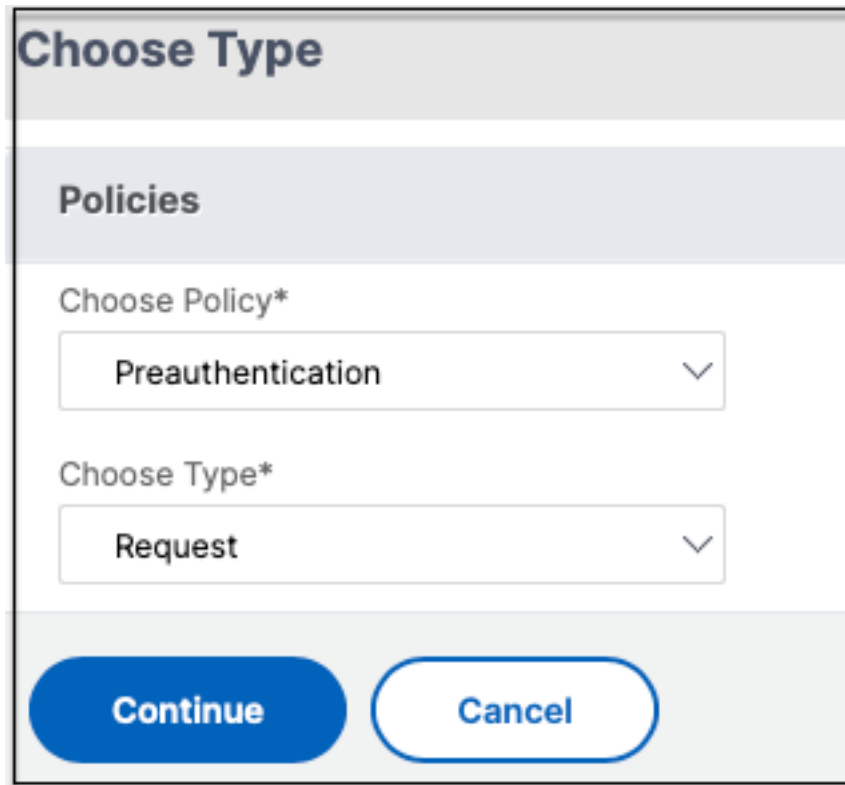
Freshness

Done Cancel

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**.



The screenshot shows a modal dialog titled "Choose Type". Under the "Policies" section, there are two dropdown menus. The first, labeled "Choose Policy\*", has "Preauthentication" selected. The second, labeled "Choose Type\*", has "Request" selected. At the bottom of the dialog, there are two buttons: "Continue" (a solid blue button) and "Cancel" (a white button with a blue border).

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

## 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`).

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

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

- If all EPA actions in an nFactor EPA policy results in action **DENY** and a quarantine group is configured in the last action, the quarantine group name is sent as the smart access.

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

Authentication EPA Action						
	NAME	DEFAULT GROUP	QUARANTINE GROUP	KILL PROCESS	DELETE FILES	EXPRESSION
<input type="checkbox"/>	epallowact	allow_app				sys.client_expr("proc_0_notepad.exe")
<input type="checkbox"/>	epadenyact		deny_app			sys.client_expr("proc_0_notepad.exe")
<input type="checkbox"/>	devCertAct					sys.client_expr("device-cert_0_0")
<input checked="" type="checkbox"/>	preAuthDeviceCertAct					sys.client_expr("device-cert_0_0")
<input type="checkbox"/>	deviceCert					sys.client_expr("device-cert_0_0")
<input type="checkbox"/>	3rdpaact					sys.client_expr("proc_0_chrome.exe")
<input type="checkbox"/>	chromscan					sys.client_expr("proc_0_chrome.exe")

In this example, when the action is denied, *deny\_app* is sent as the smart access tag to the Secure Private Access plug-in. When the action is allowed, *epallowact* and *allow\_app*, are sent as the smart access tags to the Secure Private Access plug-in.

## References

- [Configure access policies for the applications.](#)
- [Support for smart access tags.](#)

## License server

September 27, 2024

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

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

### Note:

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

For more information about the licensing server, see [Licensing Server](#).

## Citrix Secure Access client

September 12, 2024

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

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

### How it works

End users can easily access all their sanctioned private apps by just installing the Citrix Secure Access client on their client devices.

- For Windows, the client version (24.6.1.17 and later) can be downloaded from <https://www.citrix.com/downloads/citrix-gateway/plugin-ins/citrix-secure-access-client-for-windows.html>.
- For macOS, the client version (24.06.2 and later) can be downloaded from the App

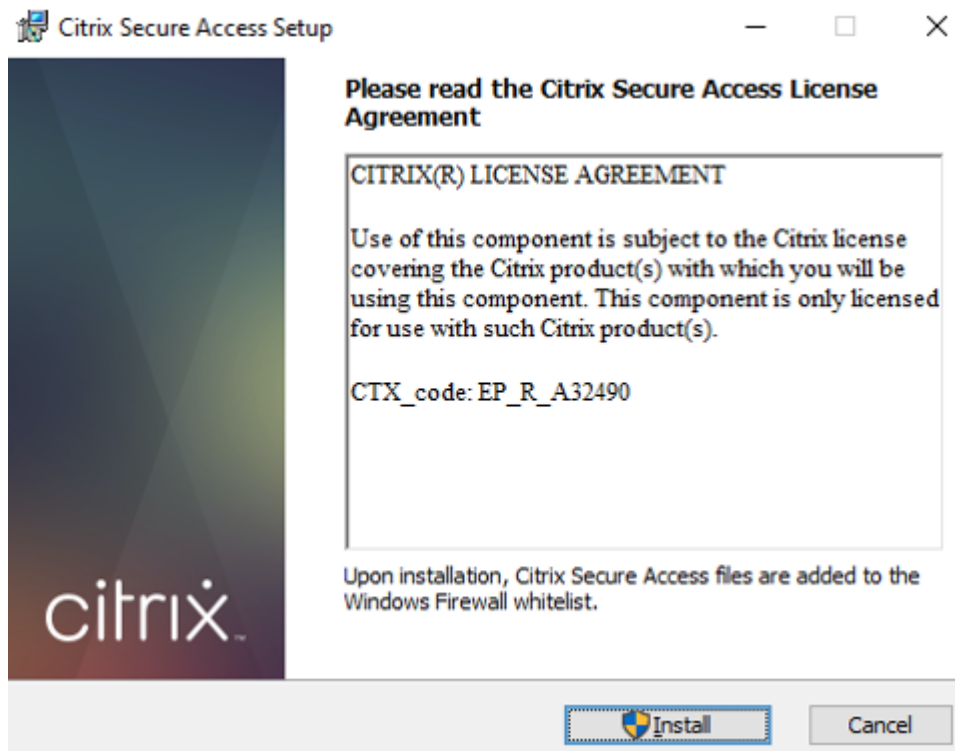
### Install Citrix Secure Access client on a Windows machine

#### Supported OS versions:

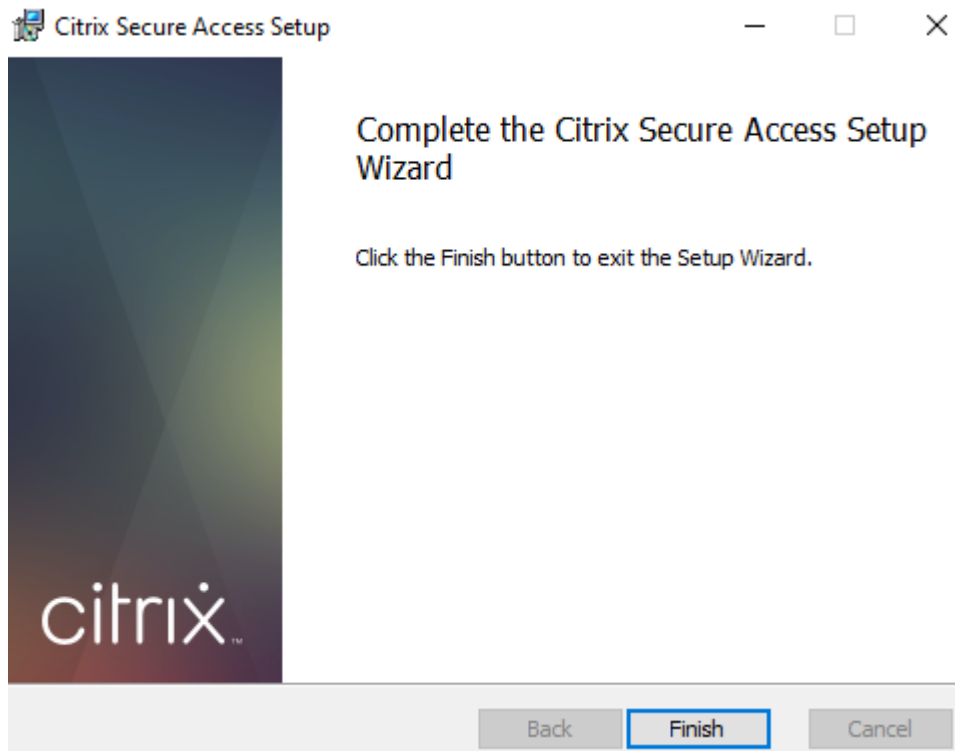
Windows –Windows 11, Windows 10, Windows Server 2016, and Windows Server 2019.

Following are the steps to install the Citrix Secure Access client on a Windows machine.

1. Download the Citrix Secure Access client from <https://www.citrix.com/downloads/citrix-gateway/plugin-ins/citrix-secure-access-client-for-windows.html>.
2. Click **Install** to install the client on your Windows machine. If you have an existing Citrix Gateway client, the same gets upgraded.



3. Click **Finish** to complete the installation.



**Note:**

Multi-user sessions in Windows are not supported.

## Install Citrix Secure Access client on a macOS machine

### Prerequisites:

- Download the Citrix Secure Access client for macOS from the App Store. This app is available from macOS 10.15 (Catalina) and later.
- Preview builds are available in the TestFlight app only for macOS Monterey (12.x).
- If you are switching between the App Store app and the TestFlight preview app, you must recreate the profile you want to use with the Citrix Secure Access app. For example, if you have been using a connection profile with `blr.abc.company.com`, delete the VPN profile, and create the same profile again.

### Supported OS versions:

macOS - 14.x (Sonoma), 13.x (Ventura), 12.x (Monterey)

### Unsupported features

The following features are not supported by the Secure Private Access for on-premises solution.

- Always On before Windows Logon (machine tunnel)
- IntranetIP
- Server initiated connections
- DNS-TCP

### Unsupported client platforms

The following platforms are not supported by the Secure Private Access for on-premises solution.

- Linux
- iOS
- Android

## Director

September 5, 2024

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](#).

## Web Studio

September 5, 2024

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

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

For details, see [Integration of Secure Private Access with Web Studio](#).

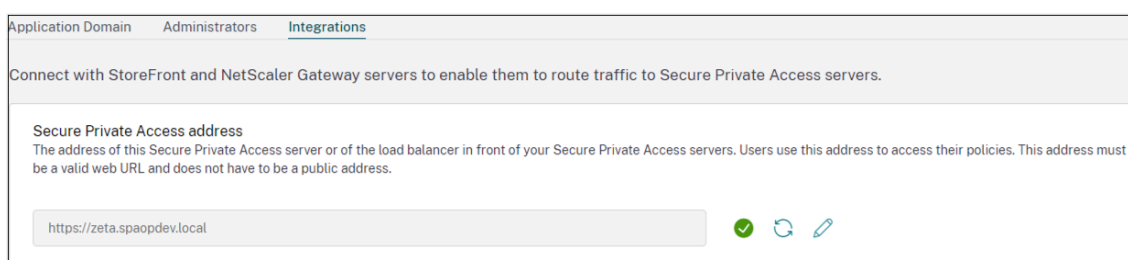
## Deploy Secure Private Access as a cluster

September 5, 2024

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

### 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](#).



The screenshot shows the 'Integrations' tab in the Web Studio console. At the top, there are three tabs: 'Application Domain', 'Administrators', and 'Integrations'. Below the tabs, there is a heading 'Connect with StoreFront and NetScaler Gateway servers to enable them to route traffic to Secure Private Access servers.' Underneath, there is a section titled 'Secure Private Access address' with a descriptive text: 'The address of this Secure Private Access server or of the load balancer in front of your Secure Private Access servers. Users use this address to access their policies. This address must be a valid web URL and does not have to be a public address.' A text input field contains the URL 'https://zeta.spaopdev.local'. To the right of the input field are three icons: a green checkmark, a circular refresh icon, and a pencil icon.

## Load balancer configuration

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

- The FQDNs used to access StoreFront are included in the DNS field as subject alternative name (SAN). If you are using a load balancer, then include both the individual server's FQDN and the load balancer FQDN. This is applicable for SSL certificates. For Secure Private Access, configuring a load balancer is sufficient. For details, see [Load balancing with NetScaler](#). Before configuring Secure Private Access, the StoreFront Store must be configured. If using a load balancer, configure the base URL with the load balancer name and use HTTPS for secure communication. For details, see [Securing StoreFront with HTTPS](#).
- Secure Private Access services are recommended to run as HTTPS but this is not a mandatory requirement. Secure Private Access services can be deployed as HTTP as well.
- SSL offload or SSL bridge is supported, so any load balancer configuration can be used. When using SSL bridge, ensure to configure the same server certificates in each Secure Private Access node. Also, the certificate subject common name or subject alternative name (SAN) must match the load balancer FQDN. Also, SAN must be configured in the Load Balancer service.
- The correct SSL certificate is bound to the IIS server and NetScaler.
- Secure ciphers are used.
- Secure Private Access services (both admin and runtime) are stateless, and so persistency is not required.
- Load balancers (for example NetScaler) have default built-in monitors (probes) for back-end servers. If you must configure a custom HTTP based monitor (probe) for Secure Private Access on-premises servers, the following endpoint can be used:

`/secureAccess/health`

Expected response:

```
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](#).

## Configure Secure Private Access plug-in

September 27, 2024

After you install the Citrix Secure Access plug-in, you can set up the Secure Private Access environment and then configure applications and access policies for applications. Secure Private Access supports Web/SaaS and TCP/UDP apps. Access policies allow you to enable or disable access to the apps based on the user or user groups. In addition, you can enable restricted access to the apps (HTTP/HTTPS and TCP/UDP) by enabling the appropriate security restrictions.

- [Configure HTTP/HTTPS applications](#)
- [Configure TCP/UDP apps](#)
- [Configure access policies for the applications](#)
- [Access restriction options](#)

## Set up Secure Private Access

September 5, 2024

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

- [Set up Secure Private Access by creating a new site](#)
- [Set up Secure Private Access by joining an existing site](#)

## Prerequisites

- You must sign into the Secure Private Access admin console with a domain user which is also a local machine administrator for the machine where Secure Private Access is installed.

- The SQL database server must be installed before creating a site.

## Set up Secure Private Access by creating a new site

### Step 1: Set up a Secure Private Access site

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

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

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

1 Site  
2 Database  
3 Integrations  
4 Summary

Step 1: Creating or joining a site  
A Secure Private Access site is a cluster of servers that all share the same configuration.

Create a new Secure Private Access site  
Select this option if this is your first time installing Secure Private Access.

Join an existing Secure Private Access site  
Select this option to add additional instances to an existing Secure Private Access site.

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.

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

- Site
- Database
- Integrations
- Summary

**Step 2: Database configuration**

Every site requires its own database, which must be created by the database administrator or the machine identity. You can create the database on the same SQL server where you host the Citrix Virtual Apps and Desktops databases.

Enter the SQL Server address that will host the database and enter your desired site name.

SQL Server host\* ⓘ

Site name\* ⓘ

[Test connection](#)

Select how you would like to create and/or configure your database:

**Automatically**

With this option, we'll automatically configure the database for you. If the database doesn't exist, we'll automatically create one. For the automatic creation and configuration to work, the machine identity must have Create Table, Read, Write, and Delete privileges.

Note: Your chosen site name determines your database name. If you create the database yourself, make sure the database name is in the format of "CitrixAccessSecurity-<Site Name>".

For example, "CitrixAccessSecurityLTSR2402".

**Manually** [Download script](#)

With this option, you must manually create and configure the database yourself. After creating an empty database, download the script and share it with your database administrator. They must run the script on your chosen SQL Server host. After running the script, test the connection again.

Note: Your chosen site name determines your database name. If you create the database yourself, make sure the database name is in the format of "CitrixAccessSecurity-<Site Name>".

For example, "CitrixAccessSecurityLTSR2402".

[Back](#)
[Next](#)

**Note:**

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

### Automatic configuration:

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

### Manual configuration:

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

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

#### Note:

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

### Step 3: Integrate servers

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

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

3. Click **Next** and then click **Save**.

### 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.

 ✓

**StoreFront Store URL\***  
Enter your complete StoreFront Store URL.

 ✓  
[+ 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.

 ✓  
[+ 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](#)

<b>Virtual IP address*</b> ⓘ	<b>Callback URL*</b> ⓘ
<input type="text" value="10.80.174.225"/>	<input type="text" value="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](#).

 ✓

**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.

 ✓

**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.

#### Zero Trust Network Access to all enterprise applications

Secure access to all enterprise applications based on contextual access policies

- ✓ Site
- ✓ Database
- ✓ Integrations
- ✓ Summary

### Step 4: Summary

Review the summary of your Secure Private Access setup.

#### Administration


You are a full administrator on this site and can add other administrators if needed.

#### Configurations

- SQL Server Database has been configured. ✓
- StoreFront has been configured. ✓
- NetScaler Gateway connected. ✓
- Director connected. ✓
- License Server connected. ✓
- Secure Private Access server connected. ✓

[Close](#)

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



### You're almost done setting up




Finish the following tasks to complete the setup. These items are essential for publishing applications and policies.

- Configure Gateway**  
You must configure your Citrix Gateway for use with Secure Private Access by downloading the necessary scripts from the Gateway Downloads page.  
[Get Gateway scripts](#)  
[Mark as done](#)
- Configure StoreFront**  
You must configure StoreFront for use with Secure Private Access by downloading and running the necessary scripts.  
[Download StoreFront scripts](#)
- Director**  
To connect with Director for real-time diagnostics, you must use the configuration tool to configure Director with Secure Private Access as described in the product documentation.  
[Go to Director documentation](#)  
[Mark as done](#)

#### Service overview

<b>Active users</b> <span>⌵</span> <b>65</b>	<b>Applications</b> <span>⌵</span> <b>319</b>	<b>Application launch count</b> <span>⌵</span> <b>316</b>	<b>Access policies</b> <span>⌵</span> <b>30</b>
---	--	--	--

#### Troubleshooting resources

 <b>Troubleshooting and Logs</b> View app access status and information for apps configured within Secure Private Access. <a href="#">Go to Troubleshooting Logs</a>	 <b>Director</b> Search by end user in Director to view and triage Secure Private Access session activity. <a href="#">Go to Director</a>	 <b>Gateway</b> Log into your Gateway appliance to track sessions and manage single sign-on across all applications. <small>Activate Windows Go to Settings to activate Windows.</small>
---	--	---

### 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**.

### Zero Trust Network Access to all enterprise applications

Secure access to all enterprise applications based on contextual access policies

✓ Site

② Database

③ Summary

#### Step 2: Database configuration

Enter the database information for the existing Secure Private Access site. This machine identity must have Read and Write permissions for this database.

SQL Server host\* ⓘ  Site name\* ⓘ

**Test connection**

Select how you would like to create and/or configure your database:

**Automatically**

With this option, we'll automatically configure the database for you. For the automatic configuration to work, the machine identity must have Create Table, Read, Write, and Delete privileges.

**Manually** **Download script**

With this option, you must download the script to give Read and Write permissions to the machine. After downloading the script, share it with your database administrator. They must run the script on your chosen SQL Server host. After running the script, test the connection again.

**Back** **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.

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

1 Site

2 Database

3 Summary

### Step 2: Database configuration

Enter the database information for the existing Secure Private Access site. This machine identity must have Read and Write permissions for this database.

SQL Server host\* ⓘ  Site name\* ⓘ

Select how you would like to create and/or configure your database:

**Automatically**

With this option, we'll automatically configure the database for you. For the automatic configuration to work, the machine identity must have Create Table, Read, Write, and Delete privileges.

**Manually**

With this option, you must download the script to give Read and Write permissions to the machine. After downloading the script, share it with your database administrator. They must run the script on your chosen SQL Server host. After running the script, test the connection again.

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

5. Click **Save**.

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

### Next steps

- [Configure NetScaler Gateway](#)
- [Configure applications](#)
- [Configure access policies for the applications](#)

## Configure Web/SaaS applications

September 24, 2024

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**.

The screenshot shows the 'Add an app' dialog box. The 'App Details' section is expanded. The 'Where is the application located?' field has 'Inside my corporate network' selected. The 'App type' is 'HTTP/HTTPS'. The 'App name' is 'google-translate'. The 'App description' field is empty. The 'App icon' field has a cloud icon and links for 'Change icon' and 'Use default icon'. The 'App category' field contains 'Ex.: Category\SubCategory\SubCategory'. The 'URL' field contains 'https://translate.google.co.in'. The 'App Connectivity' dropdown is set to 'Internal'. The 'Related Domains' field contains '\*.google2.com'. There is also another 'App Connectivity' dropdown set to 'Internal'. At the bottom, there are 'Save' and 'Cancel' buttons.

- **App name** –Name of the application.
- **App description** - A brief description of the app. This description is displayed to your users in the workspace. You can also enter keywords for the applications in the format **KEYWORDS:** <keyword\_name>. You can use the keywords to filter the applications. For details, see [Filter resources by included keywords](#).

- **App category** - Add the category and the subcategory name (if applicable) under which the app that you are publishing must appear in the Citrix Workspace UI. You can add a new category for each app or use existing categories from the Citrix Workspace UI. Once you specify a category for a web or a SaaS app, the app shows up in the Workspace UI under the specific category.

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

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

- **App icon** –Click **Change icon** to change the app icon. The icon file size must be 128x128 pixels and only the Ico format is supported. If you do not change the icon, the default icon is displayed.
- **Do not display application to users** - Select this option if you do not want to display the app to the users.
- **URL** –URL of the application.
- **Related Domains** –The related domain is auto-populated based on the application URL. Administrators can add more related internal or external domains.

**Note:**

- Ensure that an app's related domain does not overlap with another app's related domain. If this occurs, remove the related domain from all apps and create a new app with this domain and then set access accordingly in the access policy. You can also consider if you want to display this app in StoreFront or hide it. You can hide the app in StoreFront using the option **Do not display application to users** while publishing the app.
- Similarly, a published app's URL must not be added as another app's related domain.
- For more details, see [Best practices for Web and SaaS application configurations](#).

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

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

- **Allow user to remove from favorites** –Click this option to allow app subscribers to remove the app from the favorites apps list in Citrix Workspace app. When you select this option, a yellow star icon appears at the top left-hand corner of the app in Citrix Workspace app.
- **Do not allow user to remove from favorites** –Click this option to prevent subscribers from removing the app from the favorites apps list in Citrix Workspace app.

If you remove the apps marked as favorites from the Secure Private Access console, then these apps must be removed manually from the favorites list in Citrix Workspace. The apps are not automatically deleted from StoreFront if the apps are removed from the Secure Private Access console.

- **App Connectivity** - Select **Internal** for Web apps and **External** for SaaS apps.

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

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

## Next steps

[Configure access policies for the applications](#)

## Configure TCP/UDP apps

September 27, 2024

### Prerequisites:

- Secure Private Access setup is complete. For details, see [Setup Secure Private Access](#).
- Citrix Secure Access client versions meet the following requirements:
  - Windows - 24.6.1.17 and later
  - macOS - 24.06.2 and later

For details about the Citrix Secure Access client, see [Citrix Secure Access client](#).

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

1. In the admin console, click **Applications** and then click **Add an app**.

2. Select the location **Inside my corporate network**.

3. Enter the following details:

- **App type** –Select TCP/UDP.

**Note:**

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

- **App name**–Name of the application.
- **App description** –Description of the app you are adding. This field is optional.



- **Destinations** –IP Addresses or FQDNs of the back-end machines residing in the resource location. One or more destinations can be specified as follows.
  - **IP address v4**
  - **IP address Range** –Example: 10.68.90.10-10.68.90.99
  - **CIDR** –Example: 10.106.90.0/24
  - **FQDN of the machines or Domain name** –Single or wildcard domain. Example: ex.destination.domain.com, \*.domain.com

**Important:**

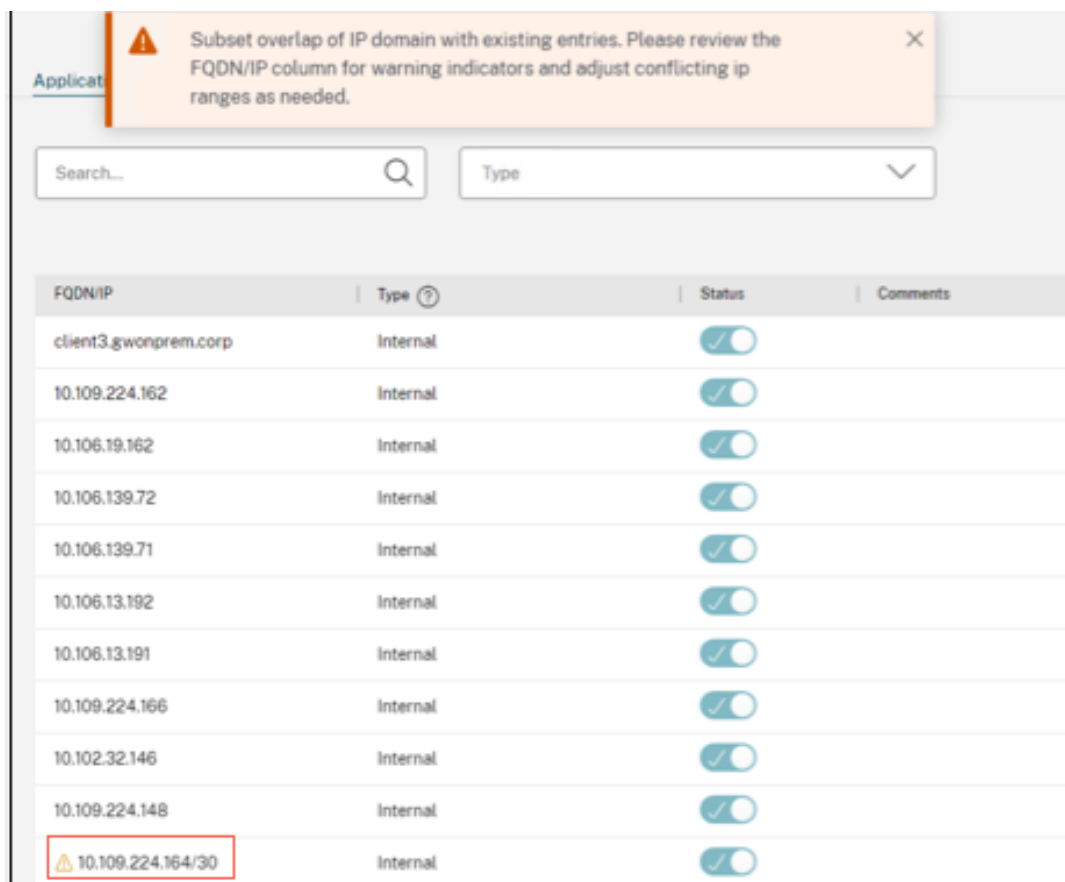
\* End users can access the apps using FQDN even if the admin has configured the apps using the IP address. This is possible because the Citrix Secure Access client can resolve an FQDN to the real IP address.

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

Destination input	How to access the app
10.10.10.1-10.10.10.100	The end user is expected to access the app only through IP addresses in this range.
10.10.10.0/24	The end user is expected to access the app only through IP addresses configured in the IP CIDR.
10.10.10.101	End user is expected to access the app only through 10.10.10.101
*.info.citrix.com	End user is expected to access subdomains of info.citrix.com and also info.citrix.com (the parent domain). For example, info.citrix.com, sub1.info.citrix.com, level1.sub1.info.citrix.com <b>Note:</b> The wildcard must always be the starting character of the domain and only one *. is allowed.
info.citrix.com	End user is expected to access info.citrix.com only and no subdomains. For example, sub1.info.citrix.com is not accessible.

The destination IP address must be unique across resource locations. If a conflicting con-

figuration exists, a warning symbol is displayed against the specific IP address in the Application Domain table (**Settings > Application Domain**).



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

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

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

---

Port input	Description
1300–2400, 42000–43000,22,443	The port number range from 1300 to 2400, 42000–43000, and ports 22 and 443 are supported for the destination.

---

**Note:**

Wildcard port (\*) cannot co-exist with port numbers or ranges.

- **Protocol** –TCP/UDP

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

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

### Configure access policies for TCP/UDP apps

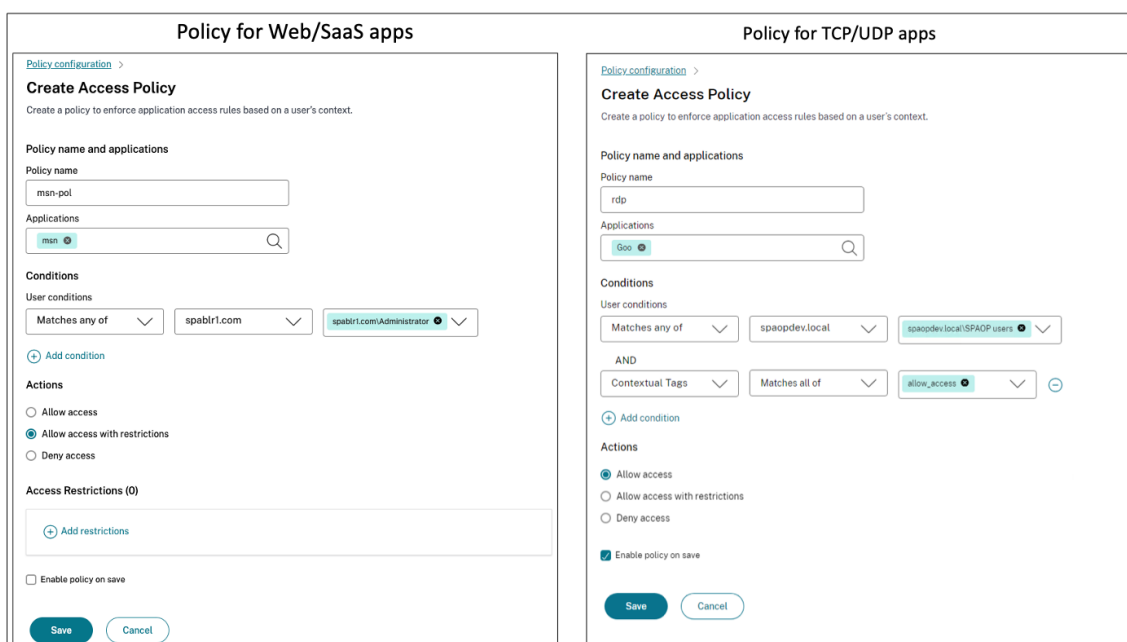
To grant access to the apps for the users, admins are required to create access policies. For details, see [Configure access policies](#).

## Configure access policies for the applications

September 5, 2024

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

1. In the admin console, click **Access Policies**.
2. Click **Create Policy**.



3. a) In **Policy name**, enter a name for the policy.
4. In **Applications**, select the apps for which you want to enforce the access policies.
5. In **Users conditions** –Select the conditions and users or user groups based on which app access must be allowed or denied.
  - **Matches any of:** Only the users 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.
6. Click **Add condition** to add another condition based on contextual tags. These tags are derived from the NetScaler Gateway.
7. In **Actions**, select one of the following actions that must be enforced on the app based on the condition evaluation.
  - **Allow access**
  - **Allow access with restriction**
  - **Deny access**

**Note:**

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

**Add/edit restrictions**
✕

0 selected
 View selected only

Search 🔍

		Access Settings	Current Value
>	<input type="checkbox"/>	Clipboard	Enabled
>	<input type="checkbox"/>	Copy	Enabled
>	<input type="checkbox"/>	Download restriction by file type	Multiple options
>	<input type="checkbox"/>	Downloads	Enabled
>	<input type="checkbox"/>	Insecure content	Disabled
>	<input type="checkbox"/>	Keylogging protection	Enabled
>	<input type="checkbox"/>	Microphone	Prompt every time
>	<input type="checkbox"/>	Notifications	Prompt every time
>	<input type="checkbox"/>	Paste	Enabled
>	<input type="checkbox"/>	Personal data masking	Multiple options
>	<input type="checkbox"/>	Popups	Always block pop-ups
>	<input type="checkbox"/>	Printer management	Multiple options
>	<input type="checkbox"/>	Printing	Enabled
>	<input type="checkbox"/>	Screen capture	Enabled
>	<input type="checkbox"/>	Upload restriction by file type	Multiple options
>	<input type="checkbox"/>	Uploads	Enabled
>	<input checked="" type="checkbox"/>	Watermark	Disabled
>	<input type="checkbox"/>	Webcam	Prompt every time

Done
Cancel

8. Select the restrictions and then click **Done**.
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).
- For the TCP/UDP apps, validate your configuration from the client machines (Windows and macOS) by logging into the Citrix Secure Access client.

[Sample configuration validation](#)

## Access restriction options

September 5, 2024

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

**Add/edit restrictions**
✕

0 selected
 View selected only

Search 🔍

	Access Settings	Current Value
>	<input type="checkbox"/> Clipboard	Enabled
>	<input type="checkbox"/> Copy	Enabled
>	<input type="checkbox"/> Download restriction by file type	Multiple options
>	<input type="checkbox"/> Downloads	Enabled
>	<input type="checkbox"/> Insecure content	Disabled
>	<input type="checkbox"/> Keylogging protection	Enabled
>	<input type="checkbox"/> Microphone	Prompt every time
>	<input type="checkbox"/> Notifications	Prompt every time
>	<input type="checkbox"/> Paste	Enabled
>	<input type="checkbox"/> Personal data masking	Multiple options
>	<input type="checkbox"/> Popups	Always block pop-ups
>	<input type="checkbox"/> Printer management	Multiple options
>	<input type="checkbox"/> Printing	Enabled
>	<input type="checkbox"/> Screen capture	Enabled
>	<input type="checkbox"/> Upload restriction by file type	Multiple options
>	<input type="checkbox"/> Uploads	Enabled
>	<input checked="" type="checkbox"/> Watermark	Disabled
>	<input type="checkbox"/> Webcam	Prompt every time

Done

Cancel

## Clipboard

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

## Copy

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

**Note:**

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

takes precedence over the **Copy** restriction.

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

## Download restriction by file type

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

### Note:

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

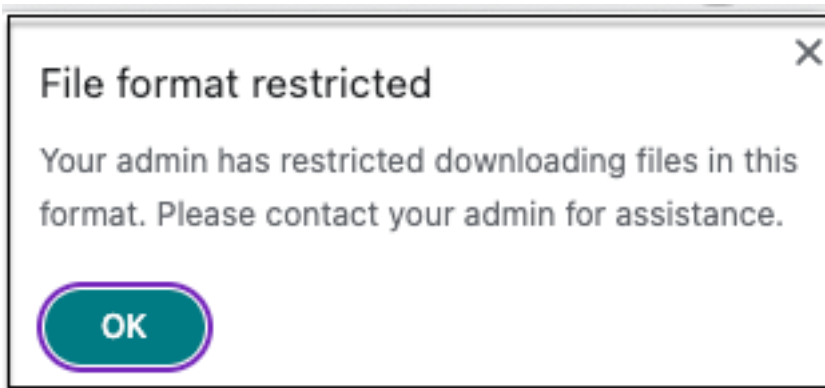
To enable downloading of MIME types, perform the following steps:

1. Create or edit an access policy. For details on creating an access policy, see [Configure access policies](#).
2. In **Actions**, select **Allow with restrictions**.
3. Click **Download restriction by file type** and then click **Edit**.
4. In the **Download restriction by file type settings** page, select one of the following:
  - **Allow all downloads with exceptions** –Select the types that must be blocked and allow all other types.
  - **Block all downloads with exceptions** –Select only the types that can be uploaded and block all other types.
5. If the file type does not exist in the list, then do the following:
  - a) Click **Add custom MIME types**.
  - b) In **Add MIME types**, enter the MIME type in the format `category/subcategory<extension>`. For example, `image/png`.
  - c) Click **Done**.

The MIME type now appears in the list of exceptions.



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



## Downloads

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

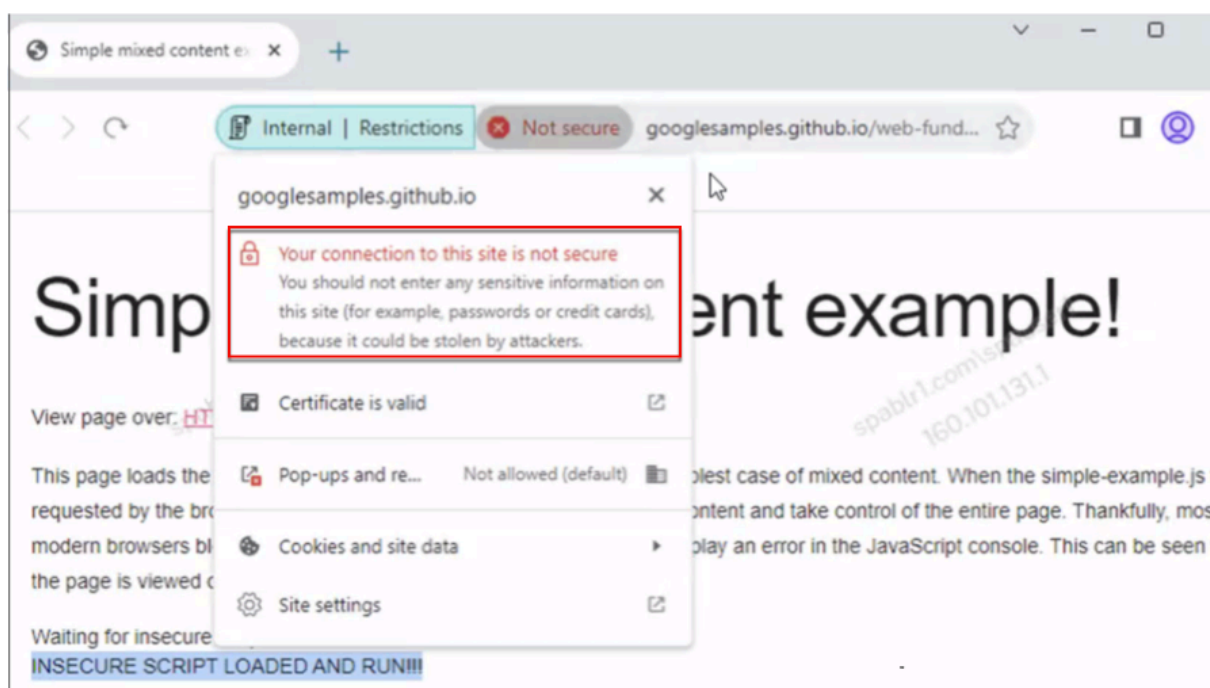
### Note:

If both **Downloads** and **Download restriction by file type** restrictions are enabled in a policy, the **Downloads** restriction takes precedence over the **Download restriction by file type**.

## Insecure content

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

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



## Keylogging protection

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

## Microphone

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

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

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

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

**Note:**

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

For more information on GACS, see [Manage Citrix Enterprise Browser through Global App Configuration service](#).

## Notifications

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

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

To block notifications without prompting, perform the following steps.

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

## Paste

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

**Note:**

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

takes precedence over the **Paste** restriction.

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

## Personal data masking

Enable/disable redacting or masking personally identifiable information (PII) on the SaaS or internal web app with this policy when accessed via Citrix Enterprise Browser. The personal identifiable information can be credit card numbers, social security numbers, dates, and so on. You can also define custom rules for detecting specific types of sensitive information and masking it accordingly. The **Personal data masking** restrictions also provide an option to fully or partially mask the information.

### Note:

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

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

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

If the information type does not appear in the pre-defined list, then you can add a custom information type. For details, see [Add custom information type](#).

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

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

The **Preview** field displays the masking format. This preview is not available for custom policies.

6. Click **Save** and then click **Done**.

### Add custom information type

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

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

### Personal data masking settings ✕

Select information type

Select... ▼ Add

#### Custom 1

Field name

Visa1

Number of characters

12

Regular expression (RE2 library)

`^4[0-9]{12}(?:[0-9]{3})?$`

Select masking type

Full masking

Partial masking

First masked characters

3

Last masked characters

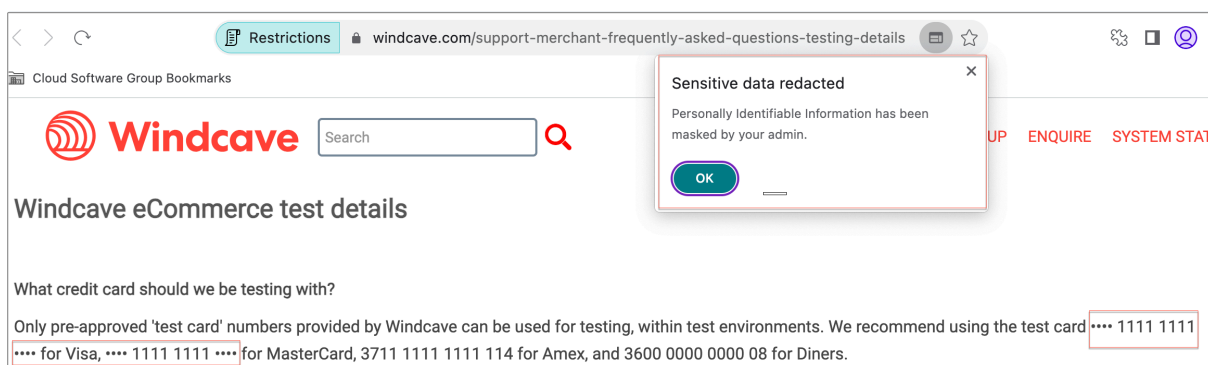
3

i No preview available

Cancel Save

Done Cancel

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



## Popups

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

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

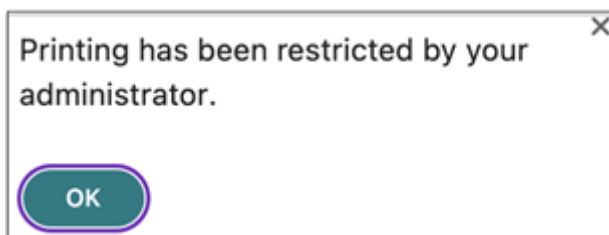
To enable display of popups, perform the following steps:

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

## Printing

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

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



**Note:**

If both **Printing** and **Printer management** restrictions are enabled in a policy, the **Printing** restriction takes precedence over the **Printer management** restriction.

## Printer management

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

**Note:**

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

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

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



### Printer management settings ✕

Specify which printer targets can be selected by end users when printing. If both this setting and the Printing setting are used, the Printing setting takes precedence. Requires Citrix Enterprise Browser v126 or later.

#### Network printers

Disabled  
 Enabled

Enable printers by hostname  
All printers are allowed by default unless specific hostnames are populated.

+

#### Local printers

Disabled  
 Enabled

#### Print using Save as PDF

Disabled  
 Enabled

1. Select the exceptions as per your requirement.

- **Network printers** - A network printer is a printer that can be connected to a network and used by multiple users.
  - **Disabled:** Printing from any printers in the network is disabled.
  - **Enabled:** Printing from all network printers is enabled. If printer host names are specified, then all other network printers apart from the ones specified are blocked.

**Note:** Network printers are identified by their host names.

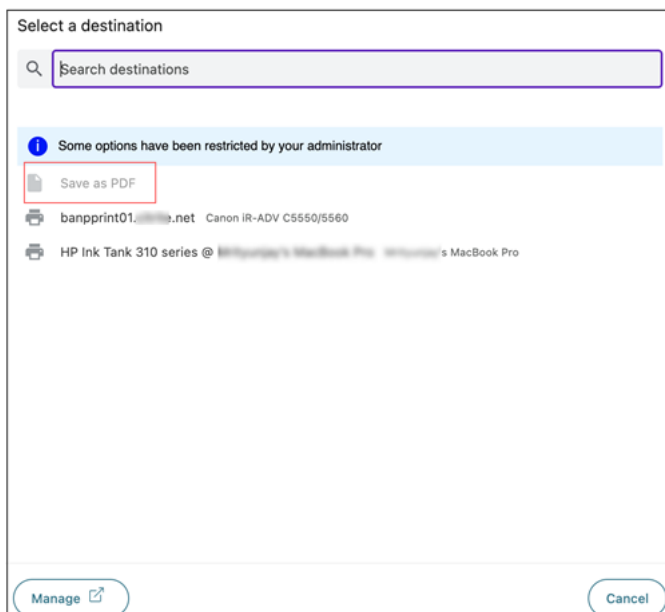
- **Local printers** - A local printer is a device directly connected to an individual computer through a wired connection. This connection is typically facilitated through USB, parallel ports, or other direct interfaces.
  - **Disabled:** Printing from all local printers is disabled.
  - **Enabled:** Printing from all local printers is enabled.
- **Print using Save as PDF**
  - **Disabled:** Saving the content from the application in a PDF format is disabled.
  - **Enabled:** Saving the content from the application in a PDF format is enabled.

2. Click **Save**.

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

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

If the end users rename the network printers, then they cannot use the network printer.



## Screen capture

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

## Upload restriction by file type

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

### Note:

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

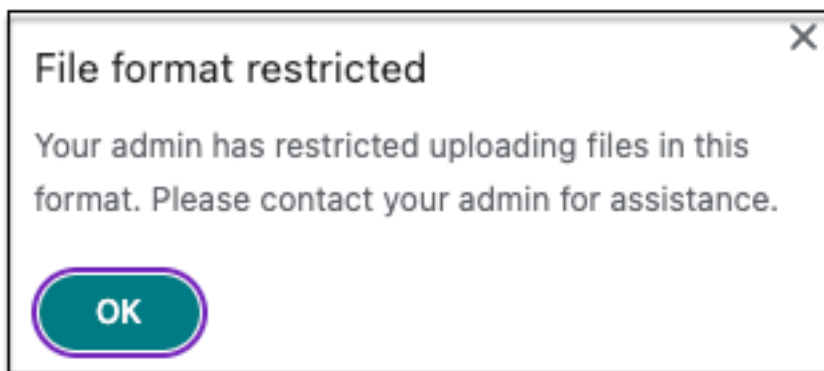
for which this restriction is enabled. Else, the application access is restricted.

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

1. Create or edit an access policy. For details, see [Create access policies](#).
2. In **Actions**, select **Allow with restrictions**.
3. Click **Upload restriction by file type** and then click **Edit**.
4. In the **Upload restriction by file type settings** page, select one of the following:
  - Allow all uploads with exceptions** –Upload all files except the selected types.
  - Block all uploads with exceptions** –Blocks all file types from uploading except the selected types.
5. If the file type does not exist in the list, then do the following:
  - a) Click **Add custom MIME types**.
  - b) In **Add MIME types**, enter the MIME type in the format `category/subcategory<extension>`. For example, `image/png`.
  - c) Click **Done**.

The MIME type now appears in the list of exceptions.

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



## Uploads

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

### Note:

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

## Watermark

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

## Webcam

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

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

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

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

### Note:

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

For more information on GACS, see [Manage Citrix Enterprise Browser through Global App Configuration service](#).

## Clipboard restriction for security groups

You can restrict clipboard access to any designated group of apps. These designated group of apps are created as security groups so that the end users are permitted to copy and paste contents only within that security groups. To enable clipboard access within the apps in a security group, you must just have an access policy configured with the action **allow** or **allow with restrictions** without selecting any access setting.

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

### Note:

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

To create a security group, perform the following steps:

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

Security group name

sec-group-1

Add web or SaaS applications

dribbble × Wikipedia × Pinterest ×

By default, you can copy and paste data between apps within the same security group. Copy and pasting to apps outside of the security group is not allowed.

> Advanced clipboard settings ?

Cancel Save

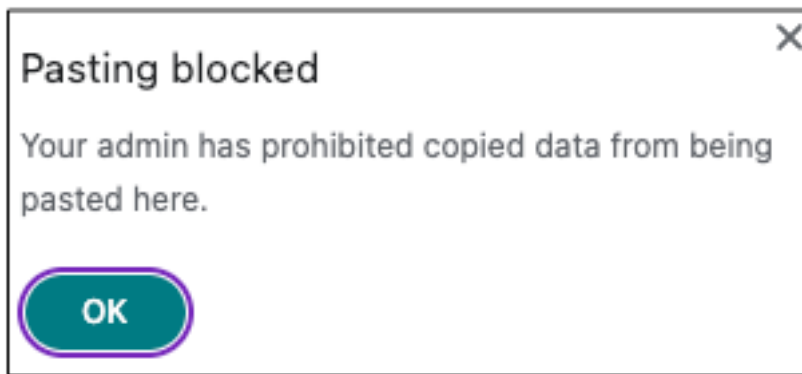
1. Enter a name for the security group.
2. In **Add web or SaaS applications**, choose the applications that you want to group to enable the copy and paste control. For example, Wikipedia, Pinterest and Dribble.

3. Click **Save**.

For details on **Advanced clipboard** settings, see [Enable copy / paste controls for native applications and unpublished apps](#).

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

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



**Note:**

You can copy and paste contents between the apps in a security group and other local apps on the machines or unpublished web apps by using the options in **Advanced clipboard settings**. For details, see [Enable copy / paste controls for native applications and unpublished apps](#).

### Enable granular level copy / paste

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

**Note:**

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

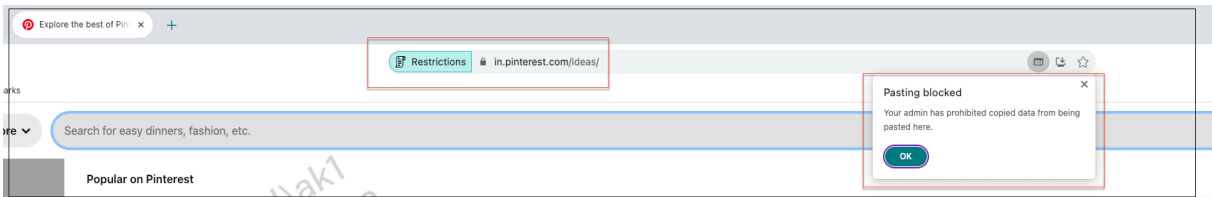
**Example:**

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

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

1. Create or edit an access policy assigned for the application **P**interest. For details on creating an access policy, see [Configure access policies](#).
2. In **Actions**, select **Allow with restrictions**.
3. Select **Paste**.

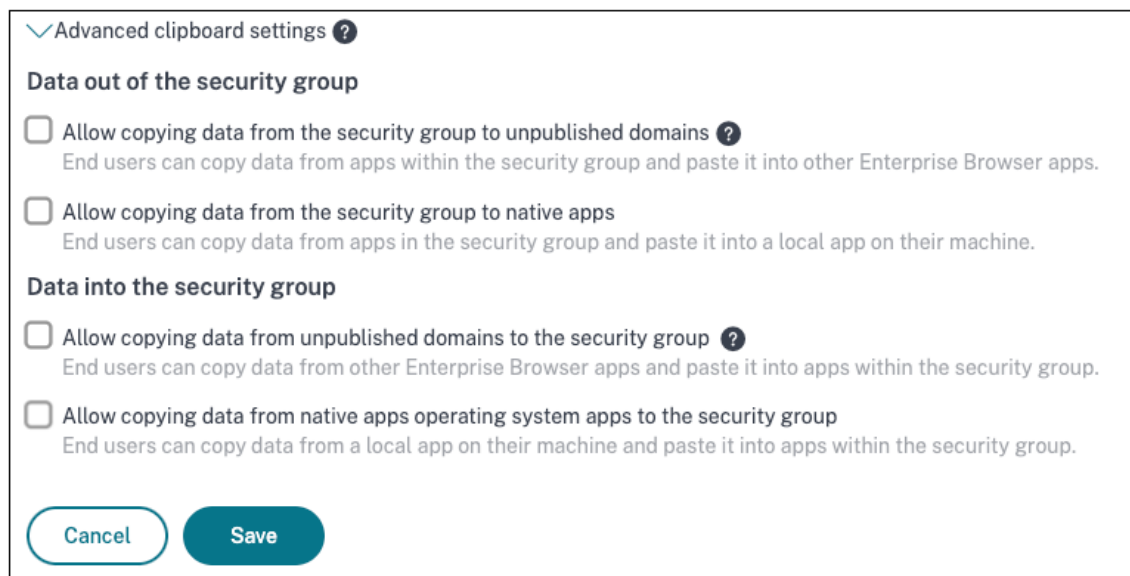
Although Pinterest is part of a security group which also contains Wikipedia and Dribble, users cannot copy content from Wikipedia or Dribble to Pinterest because of the access policy associated with Pinterest in which the **Paste** restriction is enabled.



### Enable copy / paste controls for native applications and unpublished apps

You can copy and paste contents between the apps in a security group and other local apps on the machines or unpublished web apps by using the options in **Advanced clipboard settings**.

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



3. Select the following options as per your requirement:

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

### Known issues

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

For example, assume the following scenario:

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

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

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

### End user flow

September 5, 2024



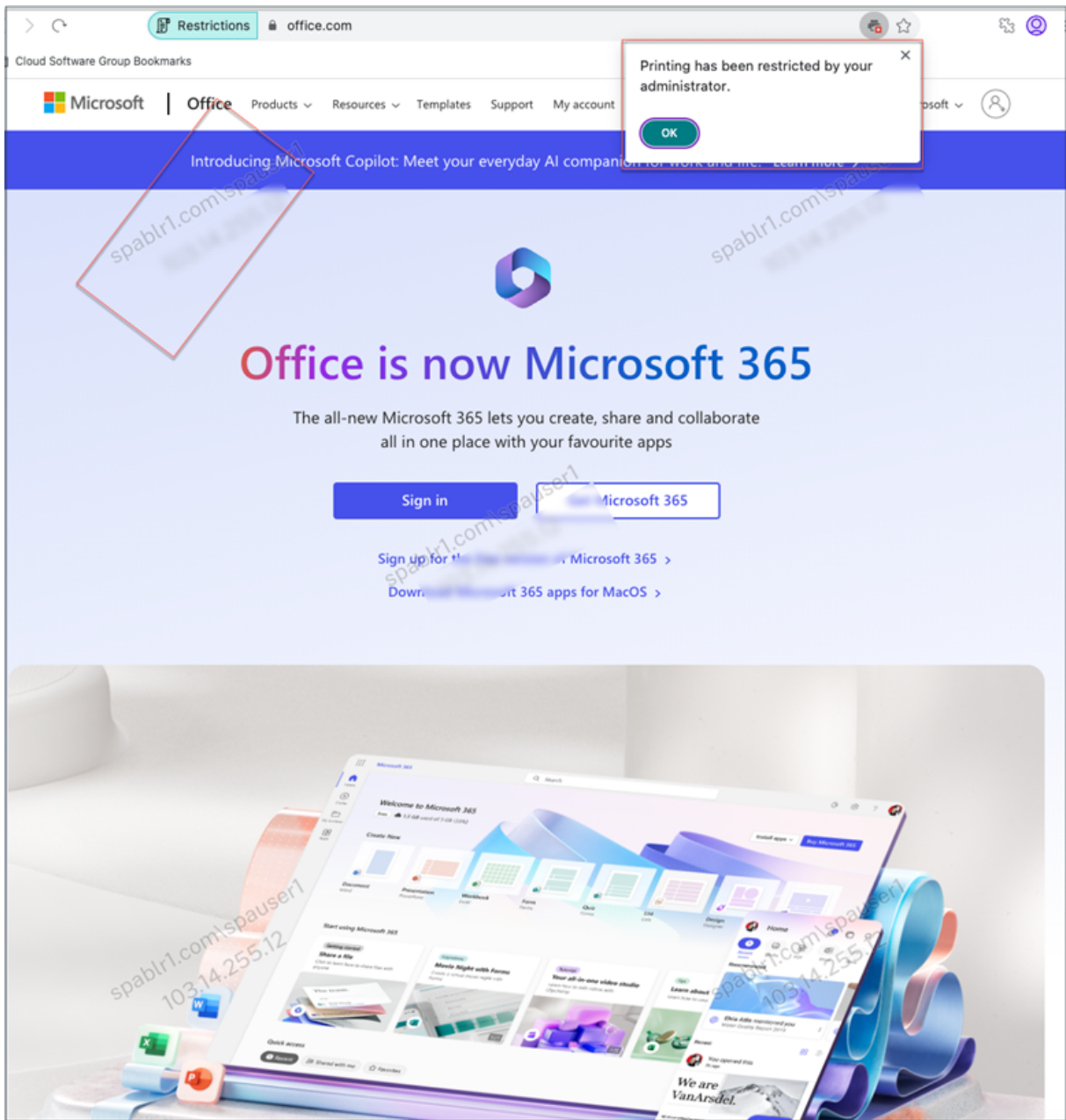
## **SaaS app**

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

The end user must perform the following steps to access the Office 365 app:

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

The end user must now notice that the Office 365 application is launched and contains the watermark. Also, if the end user tries to print some data from the Office 365 application, the print restriction message must be displayed to the user.



**Note:**

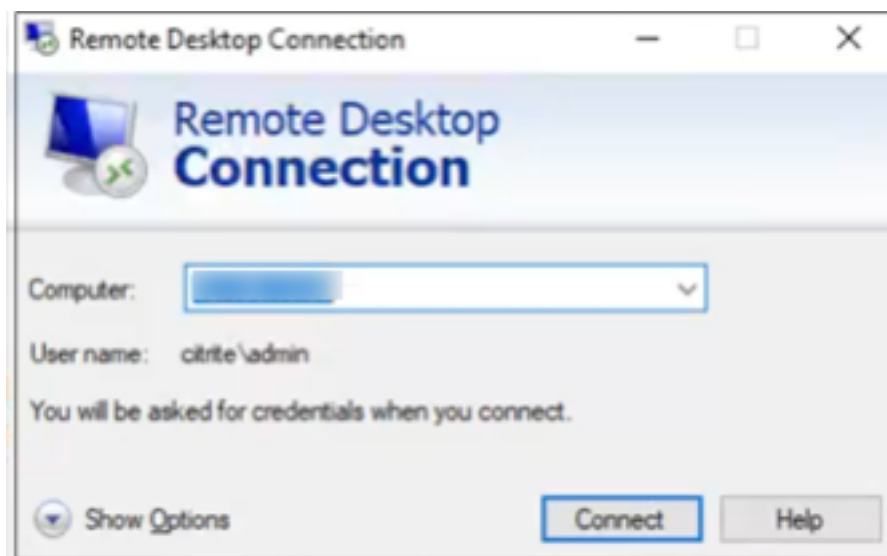
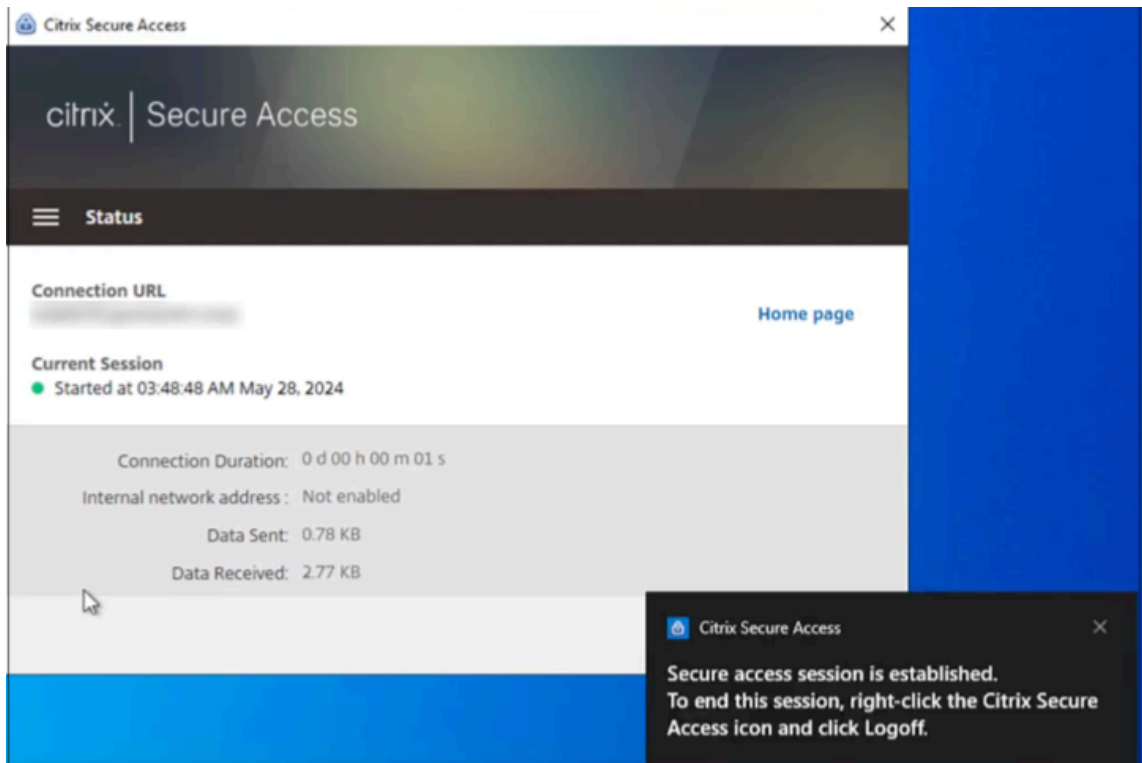
Administrators must provide users with the account information that they need to access virtual desktops and applications. For details, see [Adding store URL to Citrix Workspace app](#).

**TCP/UDP app**

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

1. Log in to the Citrix Secure Access client.

2. After the secure access session is established, start a remote desktop connection.



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

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

## Upgrade

September 27, 2024

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

### Upgrade sequence

The upgrade sequence is as follows:

1. You can upgrade Secure Private Access through the Delivery Controller or through the dedicated Secure Private Access tile in the installer UI based on how you originally installed Secure Private Access.
  - If you have installed Secure Private Access via Delivery Controller, then you cannot upgrade the Secure Private Access component alone. Instead, you must upgrade all the components. For details, see [Upgrade a deployment](#).
  - If you have installed Secure Private Access through the dedicated Secure Private Access tile, then you can upgrade it independently. For details, see [Upgrade your Secure Private Access installer](#).

**Note:**

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

2. Run the database scripts. For details, see [Upgrade the database using scripts](#).
3. Restart the **Default Web Site** and **Citrix Access Security Admin Site** on the **Internet Information Service (IIS) Manager** console to apply changes.
4. Run the StoreFront configuration again. Download the StoreFront scripts from **Settings > Configuration**, and run the scripts on the corresponding StoreFront machines. For details, see [Modify integration settings](#).

**Note:**

If you do not run the scripts, the endpoints are not triggered.

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

## Components upgrade

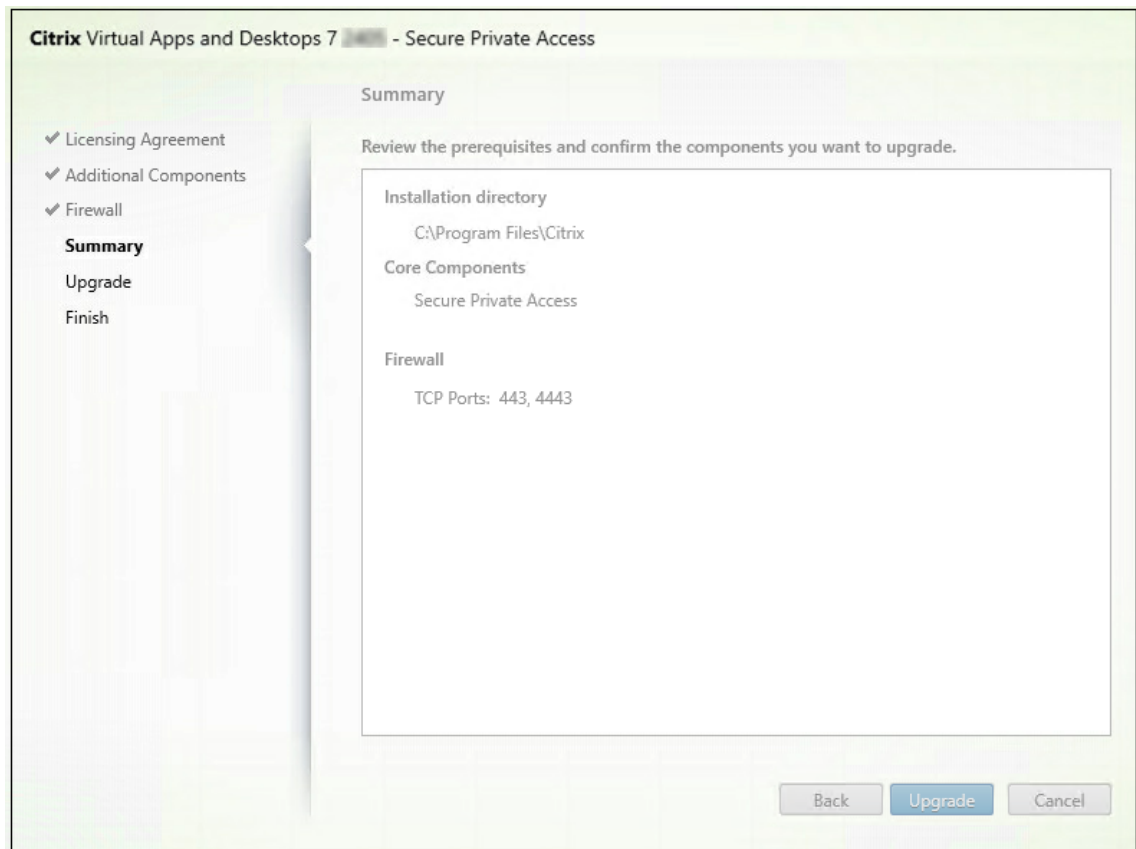
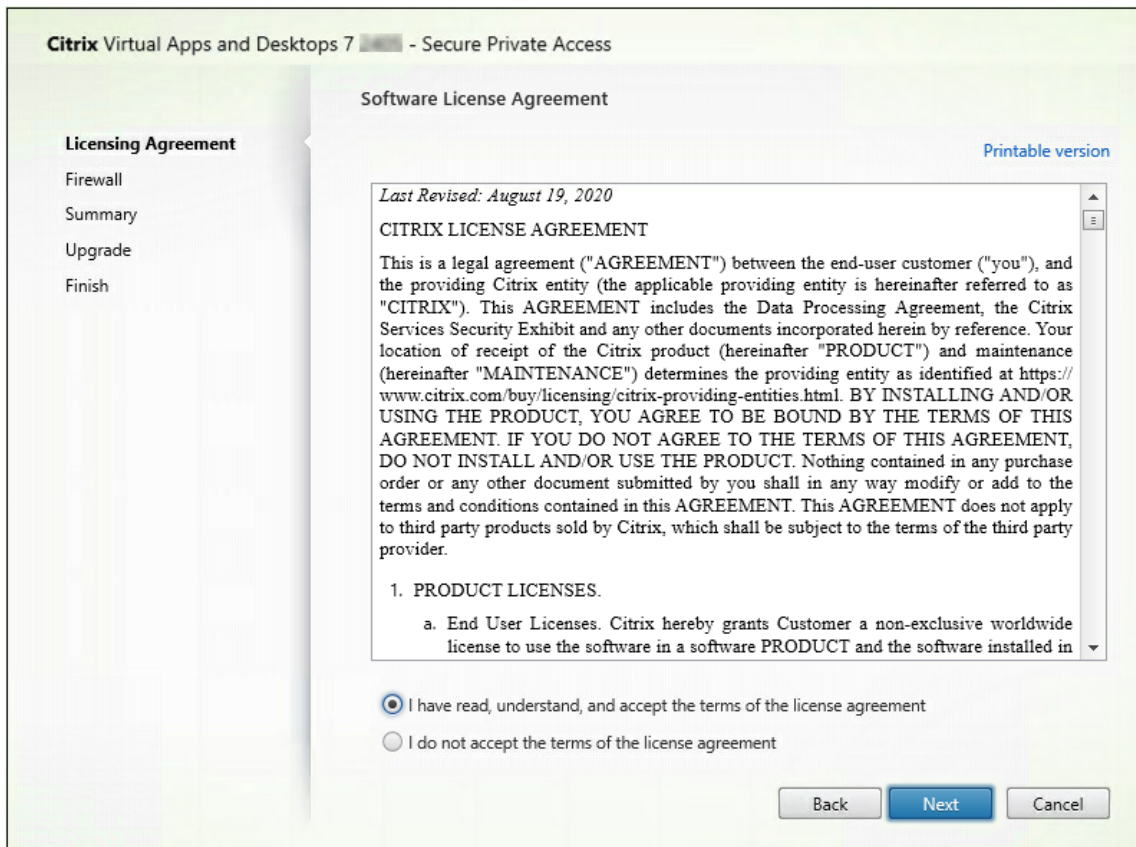
Refer to the following topics for upgrade of the components involved in Secure Private Access on-premises deployment.

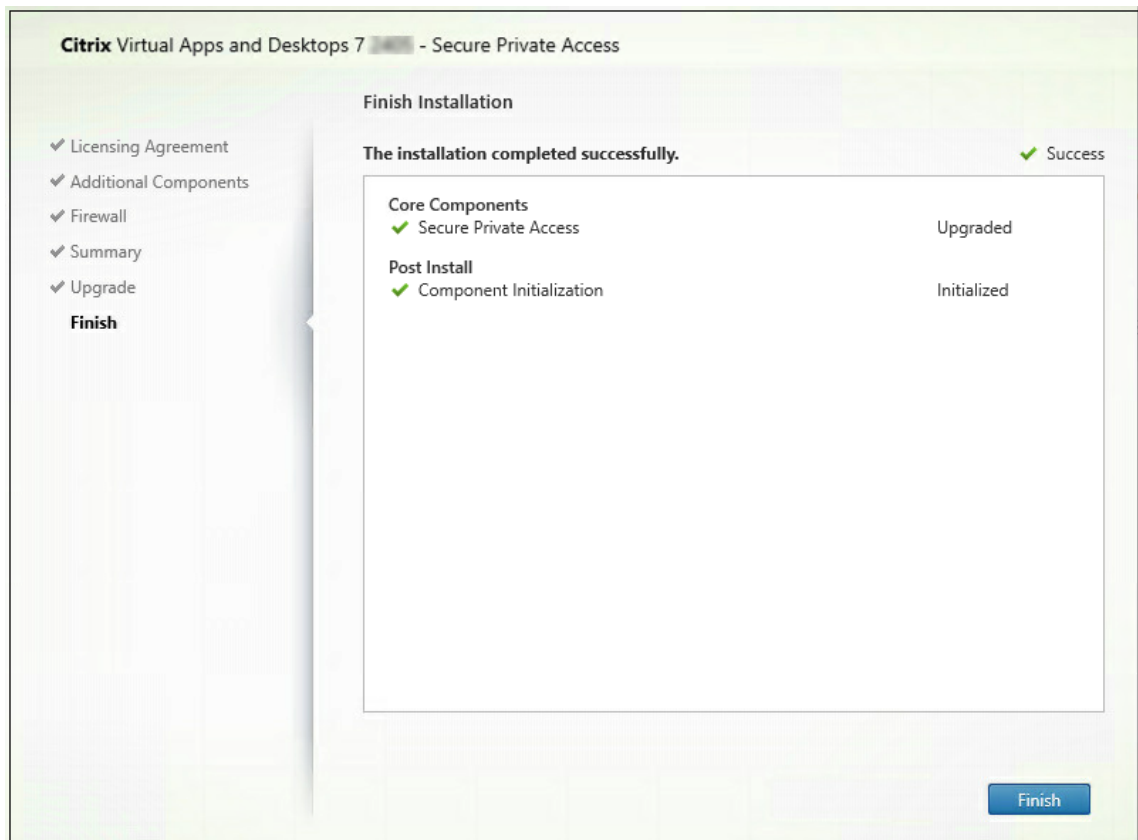
- [Cloud Connector](#)
- [StoreFront](#)
- [NetScaler Gateway](#)
- [License server](#)
- [Web Studio](#)
- [Director](#)

## Upgrade your Secure Private Access installer

September 5, 2024

1. Download the Citrix Secure Private Access 2407 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 2407, you must re-run the StoreFront script so that the new endpoint details are available.

**Next steps**

- [Set up Secure Private Access](#)
- [Configure NetScaler Gateway](#)
- [Configure applications](#)
- [Configure access policies for the applications](#)

**Upgrade the database using scripts**

September 5, 2024

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

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

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

## Manage configurations

September 27, 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 unsanctioned websites

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

## Manage settings after installation

September 5, 2024



## 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.

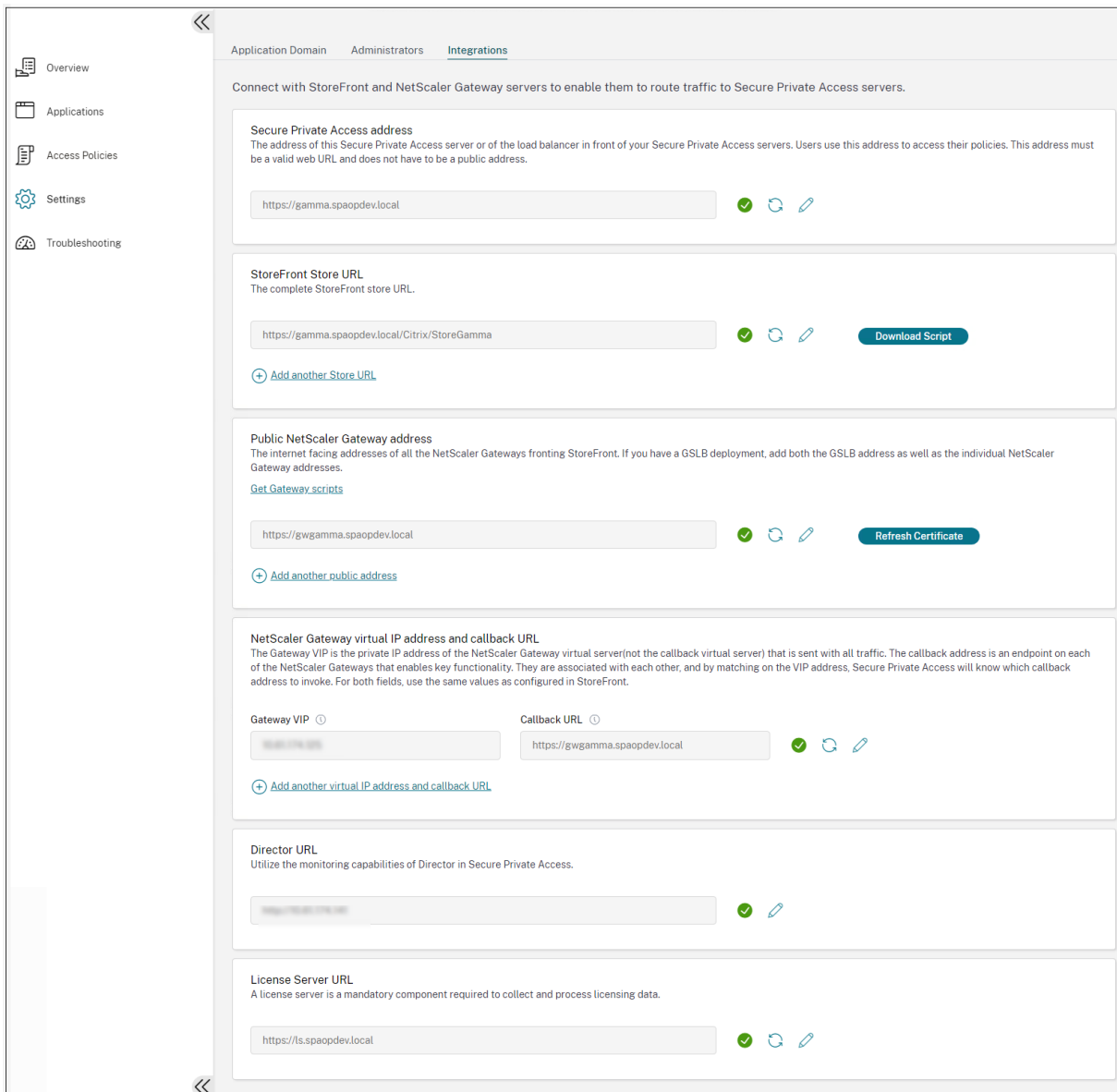
## Modify integration settings

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 than StoreFront, then download the StoreFront script and run it on the StoreFront.



## Manage applications and policies

September 5, 2024

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 **Applications**.

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 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

**App name \***

Slack

**App description**

**App category ?**

Verizon

---

**URL \***

https://csg.enterprise.slack.com

**App Connectivity \* ?**

Internal

**Related Domains \***

\*.csg.enterprise.slack.com

**App Connectivity \* ?**

Internal

**Related Domains \***

\*.slack.com

**App Connectivity \* ?**

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**.

The screenshot shows the 'Add/edit restrictions' dialog box in the Citrix Secure Private Access admin console. The dialog is titled 'Add/edit restrictions' and has a close button (X) in the top right corner. It displays a list of 20 access settings, each with a checkbox, a name, and a current value. Two items are selected: 'Clipboard' (checked) with a current value of 'Disabled', and 'Watermark' (checked) with a current value of 'Enabled'. The other 18 items are not selected. At the bottom of the dialog, there are 'Done' and 'Cancel' buttons.

	Access Settings	Current Value
<input checked="" type="checkbox"/>	Clipboard	Disabled
<input type="checkbox"/>	Copy	Enabled
<input type="checkbox"/>	Download restriction by file type	Multiple options
<input type="checkbox"/>	Downloads	Enabled
<input type="checkbox"/>	Insecure content	Disabled
<input type="checkbox"/>	Keylogging protection	Enabled
<input type="checkbox"/>	Microphone	Prompt every time
<input type="checkbox"/>	Notifications	Prompt every time
<input type="checkbox"/>	Paste	Enabled
<input type="checkbox"/>	Personal data masking	Multiple options
<input type="checkbox"/>	Popups	Always block pop-ups
<input type="checkbox"/>	Printer management	Multiple options
<input type="checkbox"/>	Printing	Enabled
<input type="checkbox"/>	Screen capture	Enabled
<input type="checkbox"/>	Upload restriction by file type	Multiple options
<input type="checkbox"/>	Uploads	Enabled
<input checked="" type="checkbox"/>	Watermark	Enabled
<input type="checkbox"/>	Webcam	Prompt every time

## Unsanctioned websites

September 5, 2024

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

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

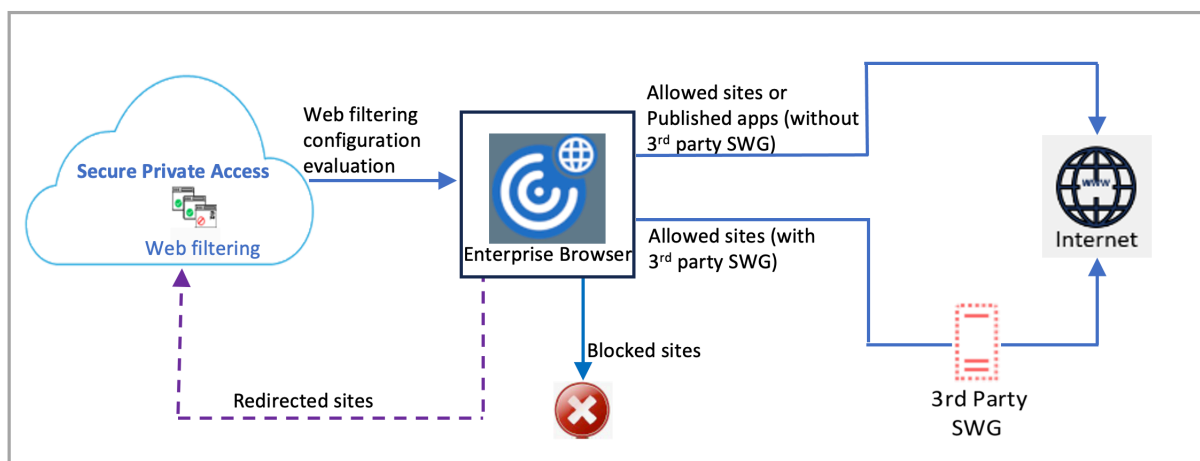
**Note:**

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

**How unsanctioned websites work**

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

The following illustration explains the end user traffic flow.



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

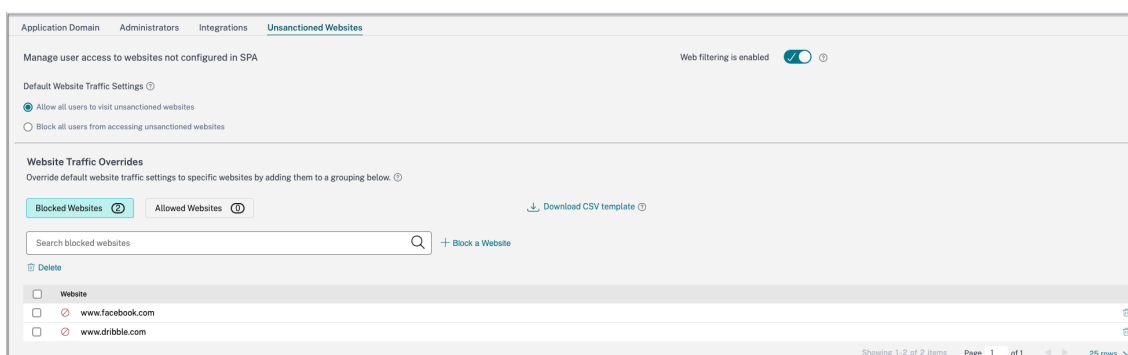
1. Does the request match the global allow list?
  - a) If it matches, the user can access the requested website.
  - b) If it does not match, website lists are checked.
2. Does the request match the configured website list?
  - a) If it matches, the following sequence determines the action.
    - i. Block
    - ii. Allow
  - b) If it does not match, the default action (ALLOW) is applied. The default action cannot be changed.

## Configure rules for unsanctioned websites

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

### Note:

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



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

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

- a) Click the **Allowed Websites** tab, and then click **Allow a Website**.
- b) Add the website address that must be allowed access. You can either manually add the website address or drag and drop a CSV file containing the website address.
- c) Click **Add a URL** and then click **Save**.

The URL is added to the list of allowed websites.

## Uninstall Secure Private Access

September 5, 2024

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

1. Select **Citrix Virtual Apps and Desktops 7 2408 –Secure Private Access**.

2. Click **Uninstall**.
3. Follow the on-screen instructions and complete the uninstallation.

**Note:**

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

To download StoreFrontScripts zip file, follow these steps:

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

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

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

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

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

## Monitor and troubleshoot

September 5, 2024

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](#)
- [List of Secure Private Access session codes in Director](#).
- [Director](#).

## Dashboard overview

September 5, 2024

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

You can add columns to the chart by clicking the + sign depending on what information you want to see in the dashboard. You can export the user logs into CSV format.



TIME	USER NAME	CATEGORY	RESULT	TRANSACTION ID	DETAILS
2024-06-19 13:28:29	spouser@spab1.com	App Enumeration	Success	e441460e-0337-4a25-8f90-e574938f16a4	Total apps enumerated for user spouser@spab1.com
2024-06-19 13:28:29	spouser@spab1.com	App Enumeration	Success	e441460e-0337-4a25-8f90-e574938f16a4	Show Details
2024-06-19 13:28:29	spouser@spab1.com	App Enumeration	Success	e441460e-0337-4a25-8f90-e574938f16a4	SmartAccess tags received PL_OS_SecureAccess
2024-06-19 13:28:29	spouser@spab1.com	App Enumeration	Success	e441460e-0337-4a25-8f90-e574938f16a4	Credential validation succeeded for user spouser@spab1.com
2024-06-19 13:55:52	spouser@spab1.com	App Access	Success	a27ba3a3-7634-41af-91f1-96f86d17015b	Received Gateway callback response successfully
2024-06-19 13:55:52	spouser@spab1.com	App Access	Success	a27ba3a3-7634-41af-91f1-96f86d17015b	Successfully validated the user credentials received from the gateway
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	65963f9b-5849-448e-8906-da5656a90986	Policy evaluation returned access state as ALL
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	65963f9b-5849-448e-8906-da5656a90986	Show Details
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	65963f9b-5849-448e-8906-da5656a90986	SmartAccess tags received PL_OS_SecureAccess
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	6b6a6840-4b84-4218-9241-0437964ee94a	Policy evaluation returned access state as ALL
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	6b6a6840-4b84-4218-9241-0437964ee94a	Show Details
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	566c400b-7a65-418b-8f6c-e1983a5c87e9	Policy evaluation returned access state as ALL
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	566c400b-7a65-418b-8f6c-e1983a5c87e9	Show Details
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	6b6a6840-4b84-4218-9241-0437964ee94a	SmartAccess tags received PL_OS_SecureAccess
2024-06-19 12:55:19	spouser@spab1.com	App Access	Success	566c400b-7a65-418b-8f6c-e1983a5c87e9	SmartAccess tags received PL_OS_SecureAccess
2024-06-19 12:55:17	spouser@spab1.com	App Access	Success	684977eb-9f59-4ec7-8af5-e97ba2a42c97	Successfully generated and sent the policy document
2024-06-19 12:55:17	spouser@spab1.com	App Access	Success	684977eb-9f59-4ec7-8af5-e97ba2a42c97	Show Details
2024-06-19 12:55:17	spouser@spab1.com	App Access	Success	400088ca-5088-4840-b76a-76205841cc7	Policy evaluation returned access state as ALL
2024-06-19 12:55:17	spouser@spab1.com	App Access	Success	400088ca-5088-4840-b76a-76205841cc7	Show Details
2024-06-19 12:55:17	spouser@spab1.com	App Access	Success	684977eb-9f59-4ec7-8af5-e97ba2a42c97	SmartAccess tags received PL_OS_SecureAccess

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

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

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

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

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

### View contextual tags from logs

The **Show Details** link in the **Details** column displays the list of applications associated with the specific access policy and also the contextual tags associated with the policy. If nFactor authentication is configured, the nFactor EPA action names that are validated for the current users are also captured as part of the contextual tags.

The screenshot shows a search interface for Citrix Secure Private Access logs. The search criteria is 'User-Name = "User"'. The results table has columns for TIME, USER NAME, CATEGORY, RESULT, TRANSACTION ID, and DETAILS. A dropdown menu is open over a log entry, showing 'Applications: Wikipedia is ALLOWED by Wikipedia\_spaop\_win10, GoogleI is ALLOWED by Google\_spaop', 'UserName: User A', and 'ContextualTags: Windows10, PL\_OS\_SecureAccess\_Gateway'.

TIME	USER NAME	CATEGORY	RESULT	TRANSACTION ID	DETAILS
2023-09-07 10:29:13	spaopdev.local\usera	App Access	Failure	9c7c2de9-0351-43b1-8...	ERROR: Error in process...
2023-09-07 10:29:13	spaopdev.local\usera	App Access	Success	9c7c2de9-0351-43b1-8...	Show Details
2023-09-07 10:29:12	spaopdev.local\usera	App Access	Success	9c7c2de9-0351-43b1-8...	SmartAccess tags recei...
2023-09-07 10:29:12	spaopdev.local\usera	App Access			DSAuth validation was s...
2023-09-07 09:48:50	spaopdev.local\usera	App Access			Successfully generated ...
2023-09-07 09:48:50	spaopdev.local\usera	App Access			Show Details
2023-09-07 09:48:49	spaopdev.local\usera	App Access			SmartAccess tags recei...
2023-09-07 09:48:49	spaopdev.local\usera	App Access			DSAuth validation was s...
2023-09-07 09:48:40	spaopdev.local\usera	App Access	Success	22592f2f-f17b-4a5f-96...	Show Details
2023-09-07 09:48:40	spaopdev.local\usera	App Access	Success	22592f2f-f17b-4a5f-96...	Policy evaluation return...
2023-09-07 09:48:40	spaopdev.local\usera	App Access	Success	22592f2f-f17b-4a5f-96...	SmartAccess tags recei...
2023-09-07 09:48:40	spaopdev.local\usera	App Access	Success	22592f2f-f17b-4a5f-96...	DSAuth validation was s...
2023-09-07 09:46:27	spaopdev.local\usera	App Access	Failure	6e9d1dd1-5bdb-4474-8...	ERROR: Error in process...

## Basic troubleshooting

September 5, 2024

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](#)

[Public gateway/callback gateway failures](#)

[Secure Private Access Server not reachable](#)

### Certificate errors

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

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

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

## Database creation errors

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

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

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

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

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

**Resolution:** You must create an empty database.

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

**Resolution:** You must manually delete the database.

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

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

- 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.Exception’ 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\CitrixAccessSecurity\Runtime\RuntimeService) update `restrictedToMinimumLevel` 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 }
```

## Troubleshooting using Director

September 5, 2024

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.

### Enumeration related codes

Code	Status	Description
1101	failure	An internal error occurred during the enumeration.
1102	failure	Some apps were enumerated but at least one app evaluation failed.
1103	failure	No apps were enumerated and at least one app evaluation failed.
1000	Success	Enumeration was successful. At least one app was enumerated.
1001	Success	No apps were enumerated because they were all denied by policies.
1002	Success	No apps were enumerated because no policies matched.
1003	Success	No apps were enumerated because some were denied and for others, no policies matched.
1004	Success	No apps were enumerated because no policies to evaluate.

### Session related 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 terminated/inactive.

### App enumeration message codes

Code	Status	Description
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
4000	Allow	App Launch is allowed.
4001	Deny	Application launch was denied because of a policy.

Code	Status	Description
4002	Deny	Application launch was denied because no policy matched.

## SIEM integration

September 5, 2024

The Secure Private Access plug-in supports integration with Security Information and Event Management (SIEM) services. Security events are stored in real time to Windows Event Log (Event Viewer\Applications and Services Logs\Citrix Access Security) and can be collected and analyzed by third-party tools.

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

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

Event ID	Summary	Description	Source
4738	A user account was changed	Event created when new Secure Private Access administrator updated	Citrix Access Security admin service
4726	A user account was deleted	Event created when new Secure Private Access administrator removed	Citrix Access Security admin service
8001	User secure access session	Event created when user session initiated or terminated on endpoint. Contains user, session, and device details, visited internal and external domains during the session	Citrix Access Security admin service
8002	User access authorization request	Event created when Secure Private Access plugin authorizes access to resource. Contains resource FQDN and authorization decision	Citrix Access Security admin service

## References

- [Security Information and Event Management \(SIEM\) integration](#)
- [About Sharing logs to SIEM solutions](#)

## Scout integration

September 5, 2024

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

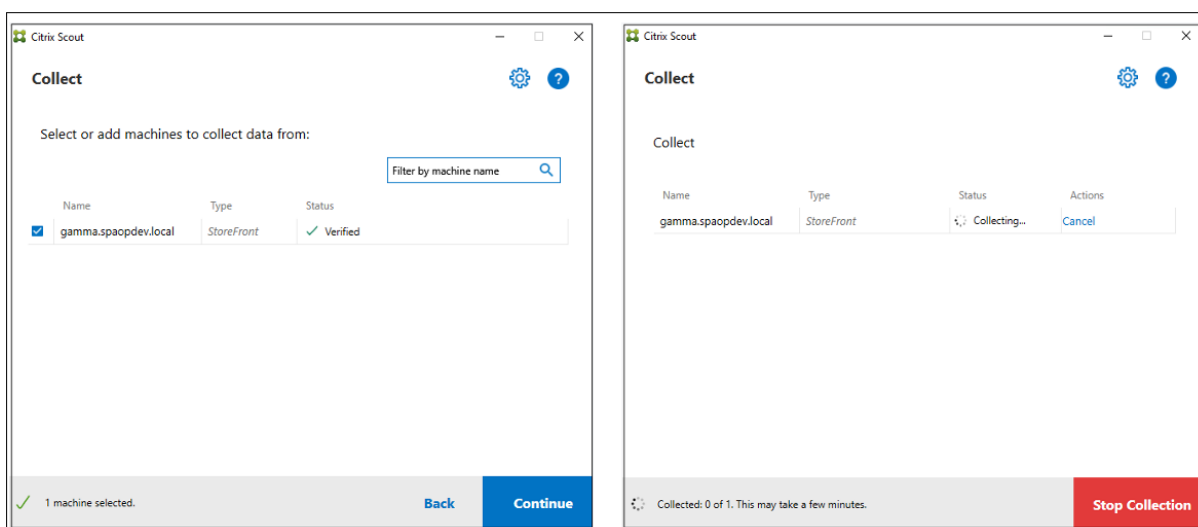
To start collecting the Secure Private Access logs, do the following steps:

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

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

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

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



## Logs retention settings

September 5, 2024

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

September 5, 2024

### 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.

## Third-party notifications

September 5, 2024

[Citrix Secure Private Access for on-premises](#)





© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).