# Citrix Secure Private Access™ Hybrid Deployment

## Contents



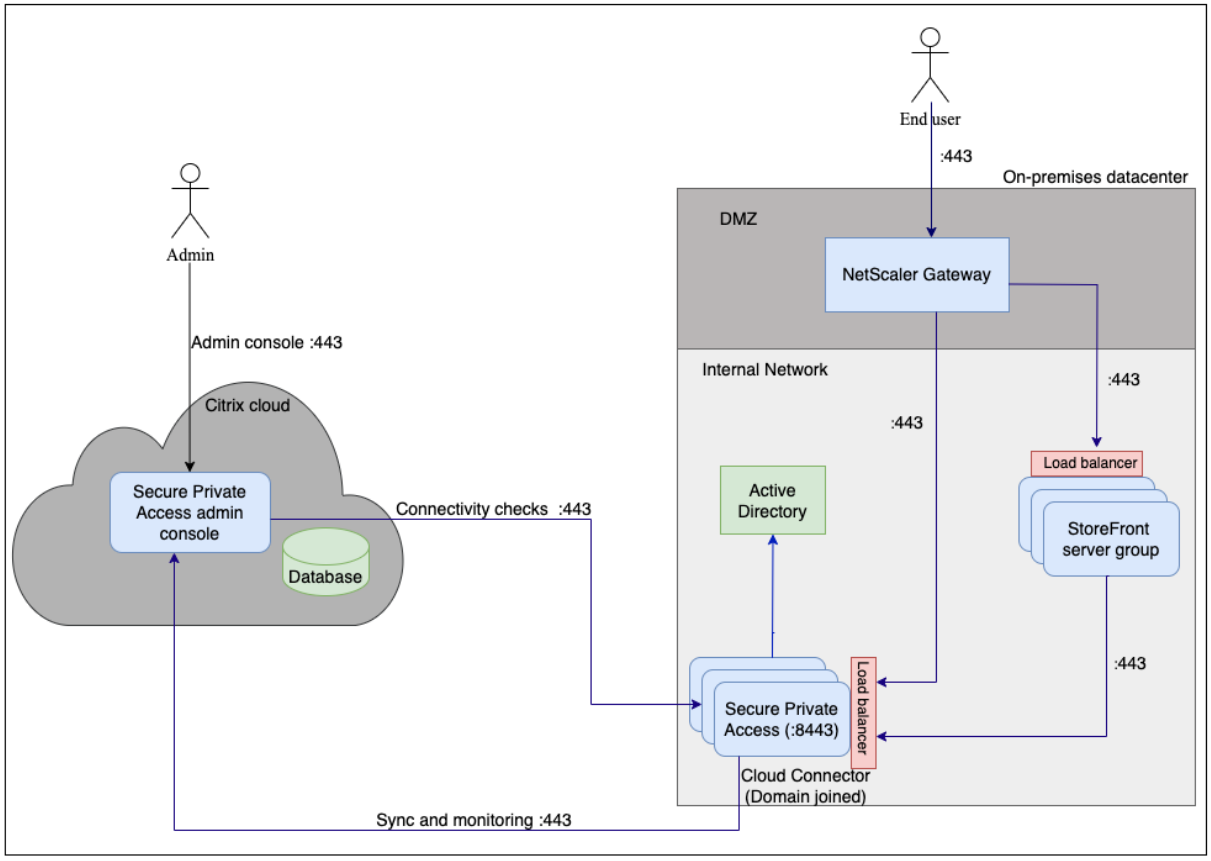
 

# Citrix Secure Private Access™ hybrid deployment

September 6, 2025

Citrix Secure Private Access for hybrid deployment allows customers to implement a Zero Trust Network Access (ZTNA) solution using on-premises StoreFront and NetScaler Gateway components and use the Citrix Cloud™ for managing the configuration, administration, and monitoring functions. This means customers can leverage existing NetScaler Gateway on-premises to control user traffic routing while using Citrix Cloud hosted UI for management of configurations and policies. Also, use Citrix Monitor hosted in the Citrix Cloud for monitoring and troubleshooting functions.

The key components of the Secure Private Access hybrid deployment are:




**Cloud Connector:** Pulls and caches all the configuration data, which allows app launches and access even when Citrix Cloud is unavailable. No user traffic is sent to the cloud. Cloud Connector is installed on a Windows server within your on-premises network. The Secure Private Access provider is part of the Cloud Connector. For details, see Cloud Connector for hybrid deployment.

**StoreFront:** Handles the enumeration and delivery of applications and desktops to the end users. StoreFront remains on-premises and you can continue to use your existing StoreFront setup without migrating to the cloud. For details, see StoreFront.

**NetScaler Gateway:** Provides secure remote access to applications and desktops. NetScaler Gateway remains on-premises, ensuring that users can securely connect to their resources from outside the corporate network. For details, see Configure NetScaler Gateway.

**Secure Private Access admin console:** Provides access to administrative and management functions, such as onboarding new users, configuring applications, and setting up policies. Site management tasks are centralized and administration is streamlined without requiring on-premises infrastructure for these functions. For details, see Access the Secure Private Access admin console.

> **Note:**
>
> For details on the system requirements and supported product versions for Secure Private Access hybrid deployment, see System requirements and prerequisites.

## What's new

September 6, 2025

### August 2025

- **Generate Secure Private Access site configuration reports**

  Customer administrators can now generate configuration reports to gain insights into the Secure Private Access site's setup. The configuration reports can be used in the following scenarios:

  - Identify and resolve configuration issues.
  - Share with the Citrix Support team for investigation and troubleshooting purposes.
  - Use the report as a reference to set up new sites or modify existing site details.

  For details, see Configuration reports.

  - **Additional dashboard widgets**

  The Secure Private Access dashboard for hybrid deployments is now enhanced to include the following widgets to provide deeper insights and improved monitoring:

  - Device Posture logs
  - Connector status
  - Top applications by launch count
  - Top discovered applications by total visits
  - Top access policies by enforcement

For more information, see Dashboard overview.

## May 2025

- **Integration of Citrix Secure Private Access™ with Google Chrome Enterprise Premium**

  The integration of Citrix Secure Private Access with Google Chrome Enterprise Premium enables customers to use Google Chrome Enterprise Premium as the enterprise browser solution for secure access to private web apps and SaaS applications along with secure connectivity provided by Citrix Secure Private Access. For details, see Integration of Citrix Secure Private Access with Google Chrome Enterprise Premium.

## April 2025

- **Device Posture checks on on-premises NetScaler® Gateway**

  Citrix Device Posture checks can now be configured to work with on-premises NetScaler Gateway. This integration allows administrators to evaluate the security posture of devices attempting to access network resources and ensure that only trusted devices can access corporate resources.

  For details, see the following topics:

  - Device Posture
  - Device Posture checks on on-premises NetScaler Gateway
  - Citrix Device Posture service for NetScaler Gateway authentication

- **Key-based authentication for StoreFront™ to Secure Private Access communication**

  A security key-based authentication method is introduced for StoreFront to Secure Private Access communication. Key based authentication is enabled by default for the new customers whereas it is disabled for the existing customers. Existing customers must enable the security key and run the StoreFront configuration script again. For details, see Configure StoreFront.

- **Support for Web/SaaS apps in ICA Proxy mode**

  The ICA Proxy mode now supports enumeration and launching of Web/SaaS applications. This also enables the use of the new StoreFront UI to enumerate apps.

  The ICA Proxy mode support is only available in NetScaler Gateway release 14.1 build 43.x and later. For details on configuration, see NetScaler Gateway session actions settings.

- **Enforce application rules based on the machine's context**

  You can now enforce application access rules based on the machine's context in addition to the user's context. You can select the machine or user context when creating an access policy. For details, see Configure access policies for the applications.

- **Exclude domains from being tunneled through NetScaler Gateway**

  You can now configure domains that can be excluded from being intercepted and tunneled through NetScaler Gateway. You can set the application connectivity type as Internal or External to allow or exclude domains from being intercepted and tunneled respectively. For details, see Configure TCP/UDP apps.

- **DNS over TCP support for Secure Private Access hybrid deployments**

  DNS over TCP is now supported for Secure Private Access hybrid deployments. The application FQDNs can now be resolved using TCP.

## December 2024

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

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

## October 2024

### Initial release

Citrix Secure Private Access for hybrid deployment allows customers to implement a Zero Trust Network Access (ZTNA) solution using on-premises StoreFront and NetScaler Gateway components and use Citrix Cloud™ for managing the configuration, administration, and monitoring functions.

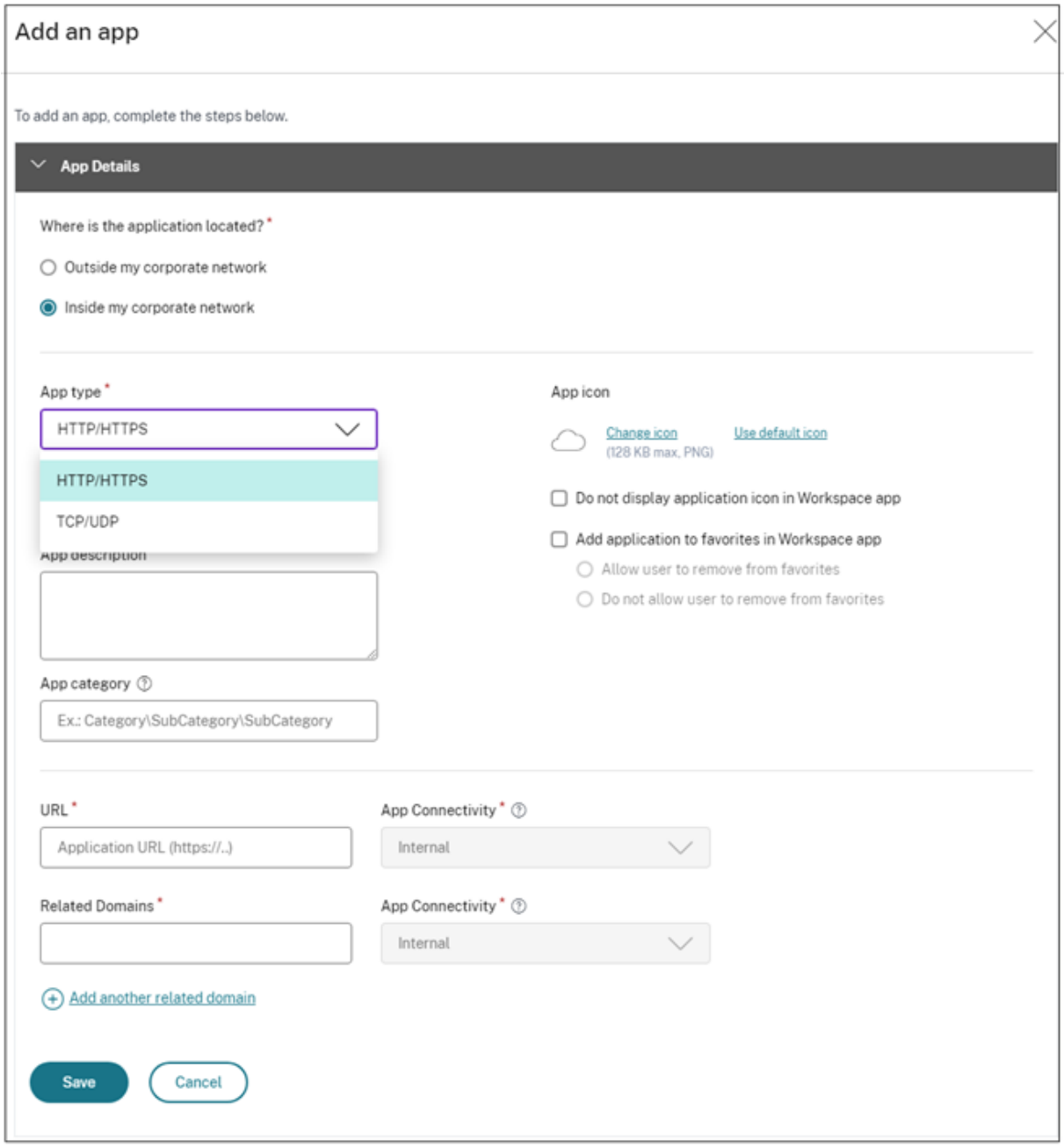
The following are some of the key features of the Citrix Secure Private Access for hybrid deployment.

- **Web/SaaS and TCP/UDP support:**

  Citrix Secure Private Access for hybrid deployment supports Web/SaaS and TCP/UDP apps. For details, see the following topics:

  - System requirements and prerequisites.
  - Configure Web/SaaS applications
  - Configure TCP/UDP apps

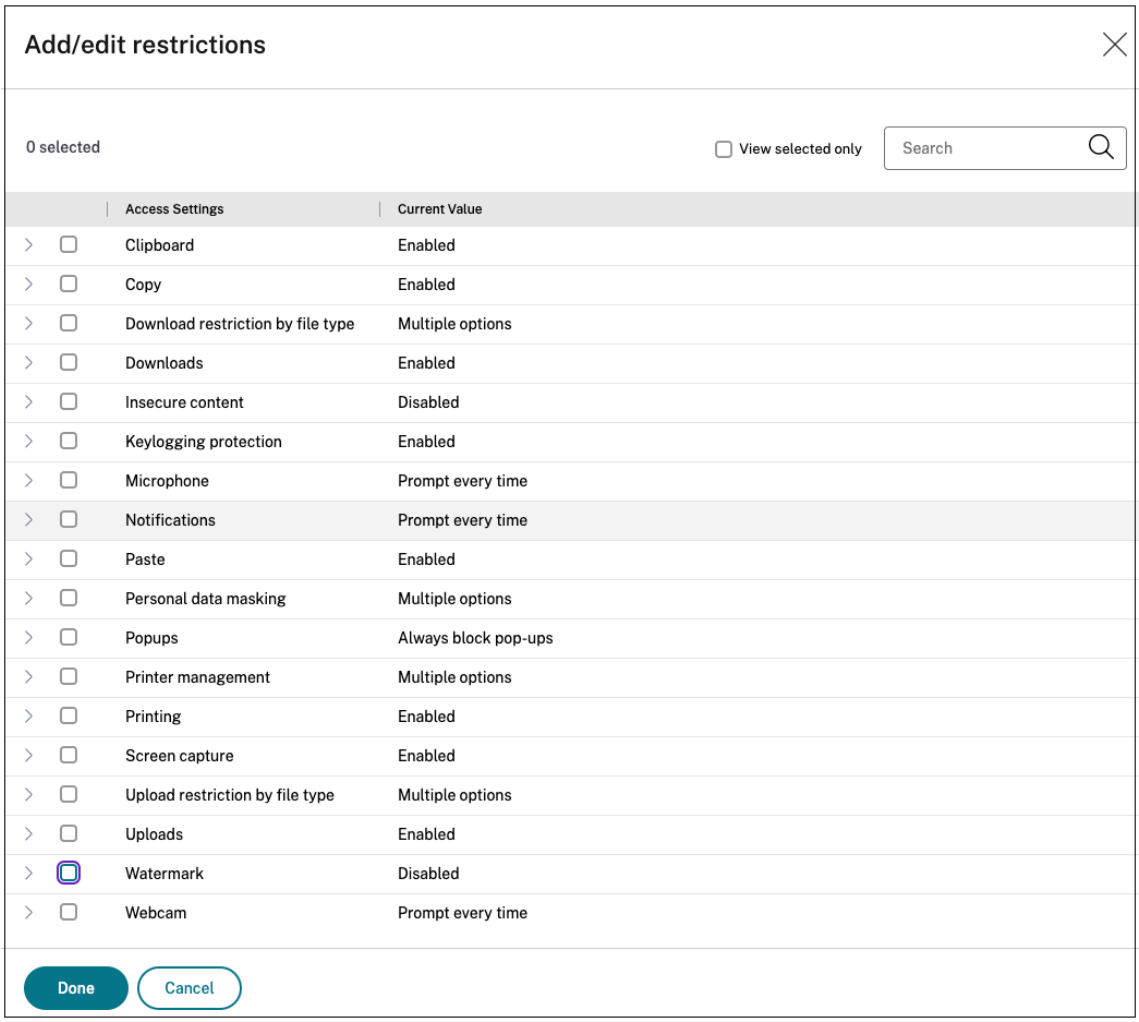
 




- **Enhanced access restriction options:**

  While creating access policies for applications, you can select access restrictions that must be enforced on the applications. These security restrictions are predefined in the system. Admins cannot modify or add other combinations. For details, see Access restriction options.



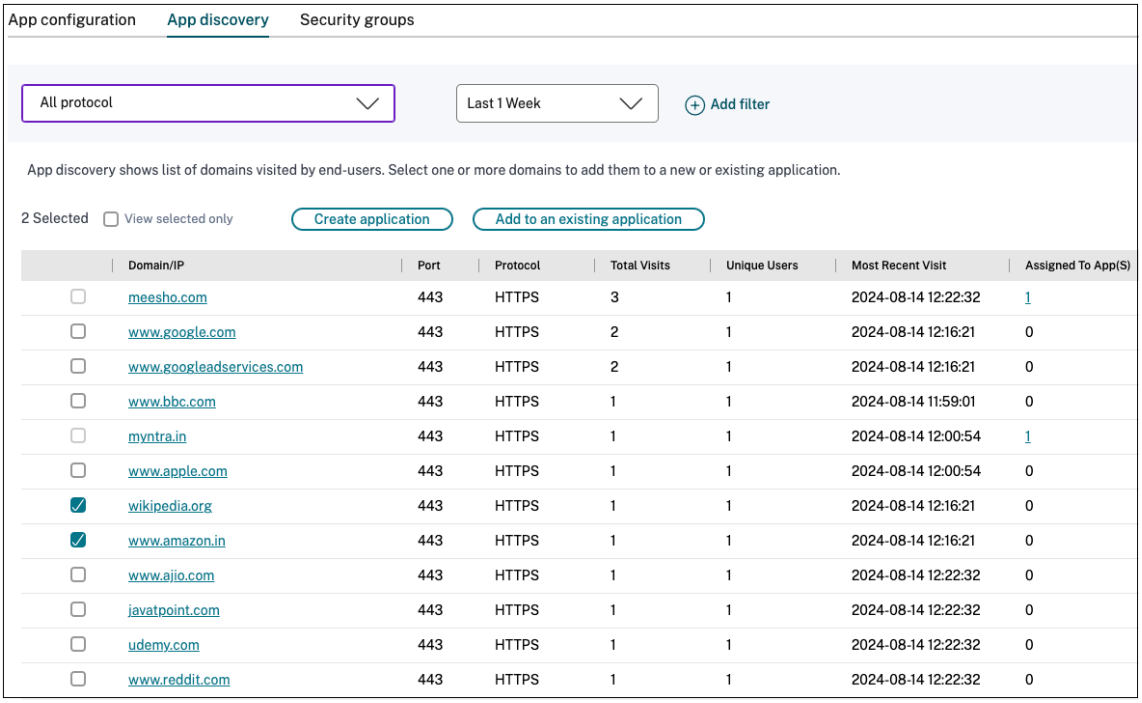

- **Secure Private Access integration with DaaS Monitor:**

  Secure Private Access is integrated with Monitor, the monitoring and troubleshooting console for Citrix DaaS. Administrators and help-desk personnel can monitor and troubleshoot Web/SaaS and TCP/UDP app sessions and events from the DaaS Monitor. For details, see Secure Private Access integration with DaaS monitor.

- **Application Discovery:**

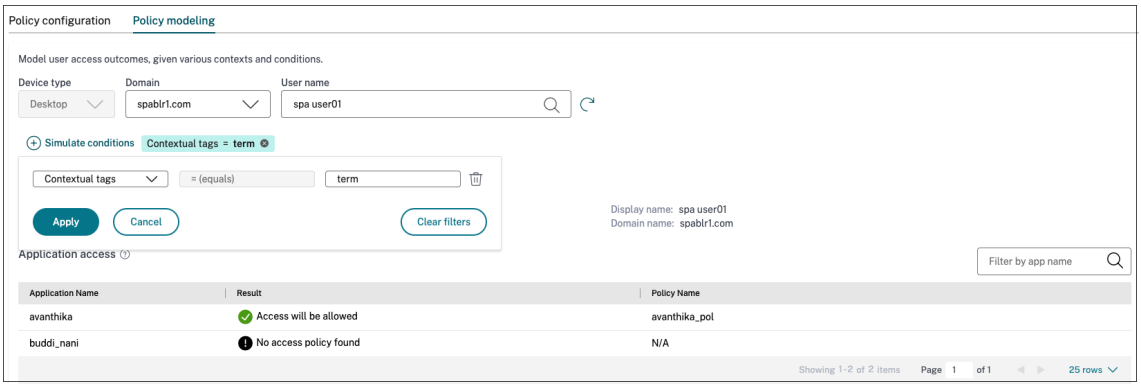
  The Application Discovery feature helps an admin get visibility into the external and internal applications (HTTP/HTTPS and TCP/UDP apps) that are being accessed in an organization. This feature discovers and lists all the domains/IPs addresses, published or unpublished. Thus, admins can see what domains/IP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




- **Policy modeling tool:**

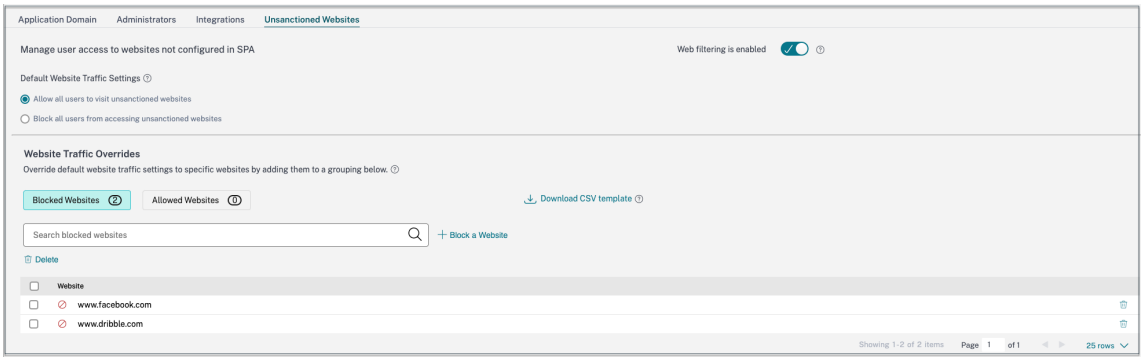
  The policy modeling tool **(Access policies > Policy modeling**) provides the administrators full visibility into the expected application access result (allowed/allowed with restriction/denied). Admins can check the access results for specific users and add a user condition for contextual tags. For details, see Policy modeling tool.




- **Support for Unsanctioned websites:**

  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. For details, see Unsanctioned websites.




## System requirements and prerequisites

September 6, 2025

Ensure that your product meets the minimal version requirements.

| Product | Minimum version |
|---|---|
| Citrix Workspace™ app | Windows –2403 and later<br>macOS –2402 and later |
| StoreFront™ | 2402, 2407 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.<br>**Note:**<br>The NetScaler Gateway minimum version required for Web/SaaS apps is 13.1.<br>The TCP/UDP apps in hybrid deployments are supported from NetScaler Gateway version 14.1–34.42 and later. |
| NetScaler FIPS | 13.1-37.219 and later FIPS builds |
| Citrix Secure Access client | Windows client - 24.6.1.17 and later<br>macOS client - 24.06.2 and later |

Though support for TCP/UDP apps along with Web/SaaS apps is available starting from NetScaler Gateway version 14.1-25.56, the 14.1-34.42 version significantly streamlines the configuration process.

| Product | Minimum version |
| --- | --- |
| | For details, see Citrix Secure Access client.<br>Also, see Features and platforms supported by Citrix Secure Access client. |
| Citrix Cloud Connector | See Cloud Connector for hybrid deployment. |
| Communication ports | Ensure that you have opened the required ports for the Secure Private Access provider. For details, see Communication ports. |

## Prerequisites

- **For the Secure Private Access admin console access, ensure that the following requirements are met:**
  - Citrix Cloud account. For details, see Create a Citrix Cloud account.
  - Secure Private Access service entitlement.
- **Ensure to get the Secure Private Access service in Cloud Connector enabled.**

  Once the Cloud Connector is updated, the Secure Private Access service is disabled. To enable the feature, customers must contact Citrix Support. Once enabled, the service status changes to **Running** and the Secure Private Access service automatically starts on the connector machine.
- **For creating or updating an existing NetScaler® Gateway, ensure that you have the following details:**
  - 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 virtual IP address, FQDN, and NetScaler Gateway callback URL (optional) that are required for versions 13.0, 13.1.48.47 and later, 14.1.4.42 and later.
  - IP address and FQDN of the Secure Private Access provider host machine (or a load balancer if the Secure Private Access provider is deployed as a cluster).
  - Authentication profile name and authentication virtual server 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 and the certificates are trusted. The Secure Private Access provider

configures a self-signed certificate if no certificate is found in the machine.

### Communication ports

The following table lists the communication ports that are used by the Secure Private Access provider.

| Source | Destination | Type | Port | Details |
|---|---|---|---|---|
| NetScaler Gateway | Secure Private Access provider | HTTPS | 443 | Application authorization validation |
| | StoreFront | HTTPS | 443 | Authentication and Application enumeration |
| | Web applications | HTTPS | 443 | NetScaler Gateway communication to configured Secure Private Access applications (Ports can differ based on the application requirements) |
| StoreFront | Cloud Connector | TCP | 443 | Unless the customer is using custom ports |
| Secure Private Access provider | Cloud Connector | TCP | 8443 | Unless the customer is using custom ports |
| Cloud Connector | Internet | TCP | 443 | See Connectivity requirements |
| User device | NetScaler Gateway | HTTPS | 443 | Communication between the end-user device and NetScaler Gateway |

### Features and platforms supported by Citrix Secure Access™ client

**Unsupported features:** The following features are not supported by the Citrix Secure Access client in the hybrid deployment.

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

**Unsupported platforms:** The following platforms are not supported by the Citrix Secure Access client in the hybrid deployment.

- Linux
- iOS
- Android

## Sizing guidelines

September 6, 2025

This document provides the recommended sizing guidelines for deploying a Secure Private Access site in a hybrid deployment model. The following guidance is based on validation with production-like configurations and user scenarios, and is intended specifically for Secure Private Access workloads. For environments that include both Citrix DaaS™ and Secure Private Access, use these guidelines to estimate the additional resources required for Secure Private Access.

### Test inputs

The following parameters were used in the tests that validated these recommendations:

| Parameter | Value |
|---|---|
| Concurrent access (users) | Up to 20,000 |
| Login ramp-up time | 20 minutes (1,000/min) |
| Active Directory domains | 10 |
| Group membership per user | 150 |
| Total published applications | 250 (200 HTTP, 50 TCP/UDP) |

| Parameter | Value |
|---|---|
| Application launches per user/hour | 25 |
| Number of access policies | 50 |

## Cloud Connector sizing

The following table outlines the minimum recommended CPU and memory configurations for Cloud Connectors based on the site sizes.

| | Medium | Large | Maximum |
|---|---|---|---|
| Concurrent Users | 5,000 | 10,000 | 20,000 |
| Connectors for high availability | 2 | 2 | 3 |
| vCPUs for Cloud Connectors | 4 | 4 | 4 |
| Memory for Cloud Connectors | 8 GB | 8 GB | 8 GB |

> **Note:**
>
> For environments exceeding 20,000 concurrent users, scale out connector instances proportionally. If your requirements fall between the two recommended values, use the larger size as your guideline.

## NetScaler® Gateway sizing

During testing, NetScaler Gateway with 4 vCPUs and 16 GB RAM was used for workloads ranging from 5,000 to 20,000 users.

Note the following recommendations:

- It is recommended to allocate 4 GB RAM per vCPU.
- For user counts exceeding 20,000, it is recommended to use a global server load balancing (GSLB) deployment with additional NetScaler instances.
- Deploy NetScaler Gateway in a high availability (HA) mode to ensure continuous service and minimum downtime.

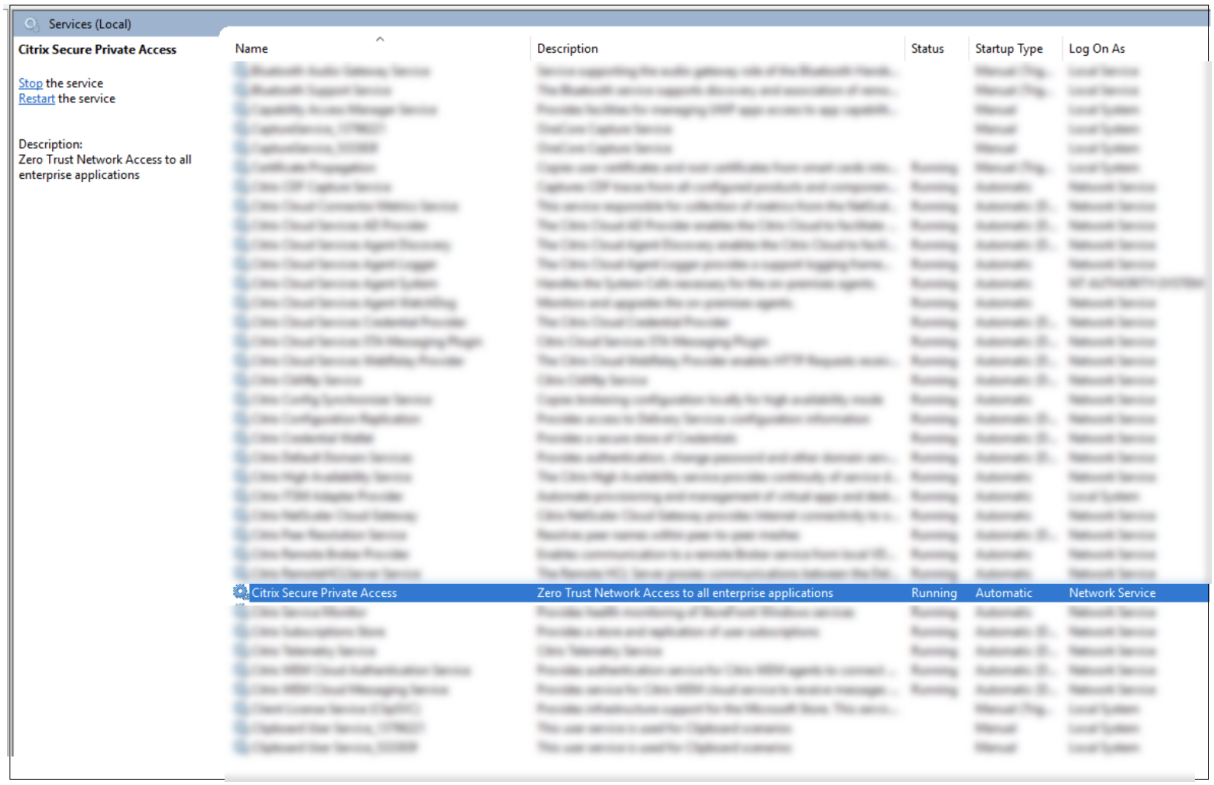
> **Note:**
>
> These tests and recommendations are guidelines to help you begin your testing. We recommend that you perform the testing in your environment to validate the correct Cloud Connector and NetScaler Gateway sizing. Regular monitoring of CPU and memory usage for all components is recommended, along with periodic performance validations.

## Cloud Connector for hybrid deployment

September 6, 2025

The Secure Private Access provider for the hybrid deployment is installed as part of Citrix Cloud Connector. After Citrix Cloud Connector is installed, the Citrix Secure Private Access™ service can be found in the Windows services. The Secure Private Access service operates under the network service account.

> **Important:**
>
> Once the Cloud Connector is updated, the Secure Private Access service is disabled. To enable the feature, customers must contact Citrix Support. Once enabled, the service status changes to **Running** and the Secure Private Access service automatically starts on the connector machine.



For details on Cloud Connector installation, see Cloud Connector Installation.

### Port configuration for Citrix Secure Private Access

**Points to note:**

- By default, Citrix Secure Private Access uses port 8443 as a plain HTTP service. Ensure that you add the inbound rule for port 8443 from the data center network.
- The internal load balancer for Citrix Secure Private Access adds the Cloud Connector back-end service using port 8443.
- The port 8443 can be opened by manually configuring the firewall rules or by running the Citrix Secure Private Access config tool.

  Perform the following steps to run the config tool:

  1. Navigate to the Citrix Secure Private Access installation folder (default path - C:\Program Files\Citrix\AccessSecurityService).
  2. Run the command `.\Citrix.AccessSecurityService.exe /ENABLE_SPA_PORTS 8443`.

  After the command is run successfully, the firewall is configured automatically.

## Load balancer and TLS for Secure Private Access

September 6, 2025

We recommend that you configure load balancers for the Secure Private Access service. Citrix Secure Private Access uses HTTP on port 8443 on the Cloud Connector. This setup is suitable when a load balancer is configured with full SSL offload and a TLS/SSL certificate. Alternatively, you can configure a load balancer with SSL bridge to forward encrypted traffic to the Secure Private Access service.

### Load balancer with SSL bridge

To configure NetScaler load balancer with SSL bridge, see Configure SSL bridging.

> **Note:**
>
> In this case it is required to enable TLS for Secure Private Access service on Cloud Connector.

### Load balancer with SSL offload

To configure NetScaler load balancer with SSL offload, see Configure SSL offloading.

The virtual server intercepts and decrypts the incoming SSL traffic and forwards it to the bound service. To enable SSL offloading, you must import a valid certificate and key and bind the pair to the virtual server.

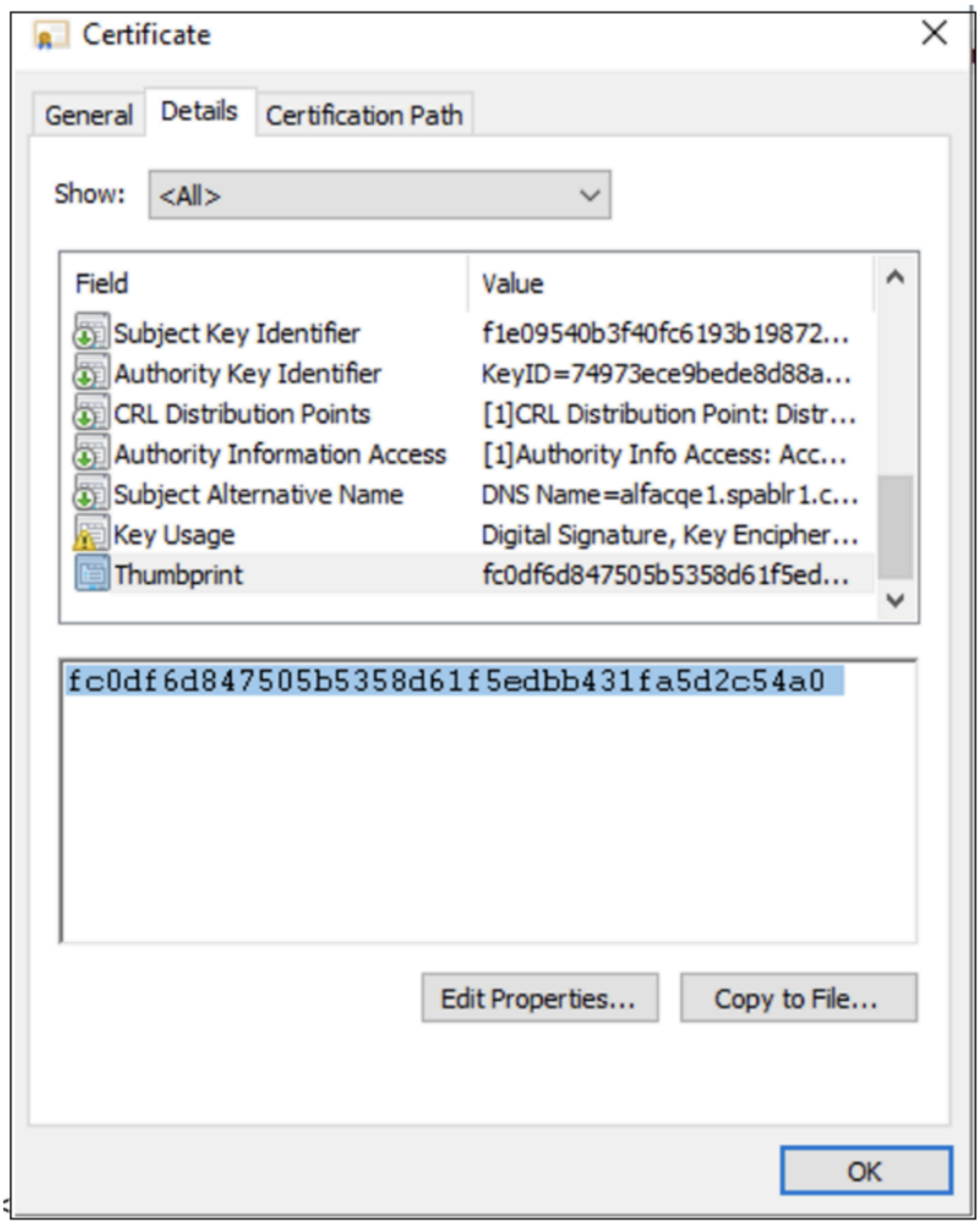
> **Note:**
>
> In an SSL offload configuration, the traffic between the load balancer and the Secure Private Access service is unencrypted HTTP.

### Enable TLS for Secure Private Access

Perform the following steps to configure Citrix Secure Private Access™ service over TLS:

1. Install the TLS certificate in the Cloud Connector local machine personal certificate store.
2. Grant Network Service account permission to access the installed certificate. You can do this by using the Microsoft Management Console (MMC).
   a) Open the Microsoft Management Console.
   b) Add certificate snap-in for local computer account, follow the wizard, and click **OK**.
   c) In the Microsoft Management Console, go to **Console Root -> Certificates -> Personal -> Certificates**.
   d) Right-click the certificate that is required to configure for Secure Private Access.
   e) Click **All Tasks -> Manage Private Keys**.



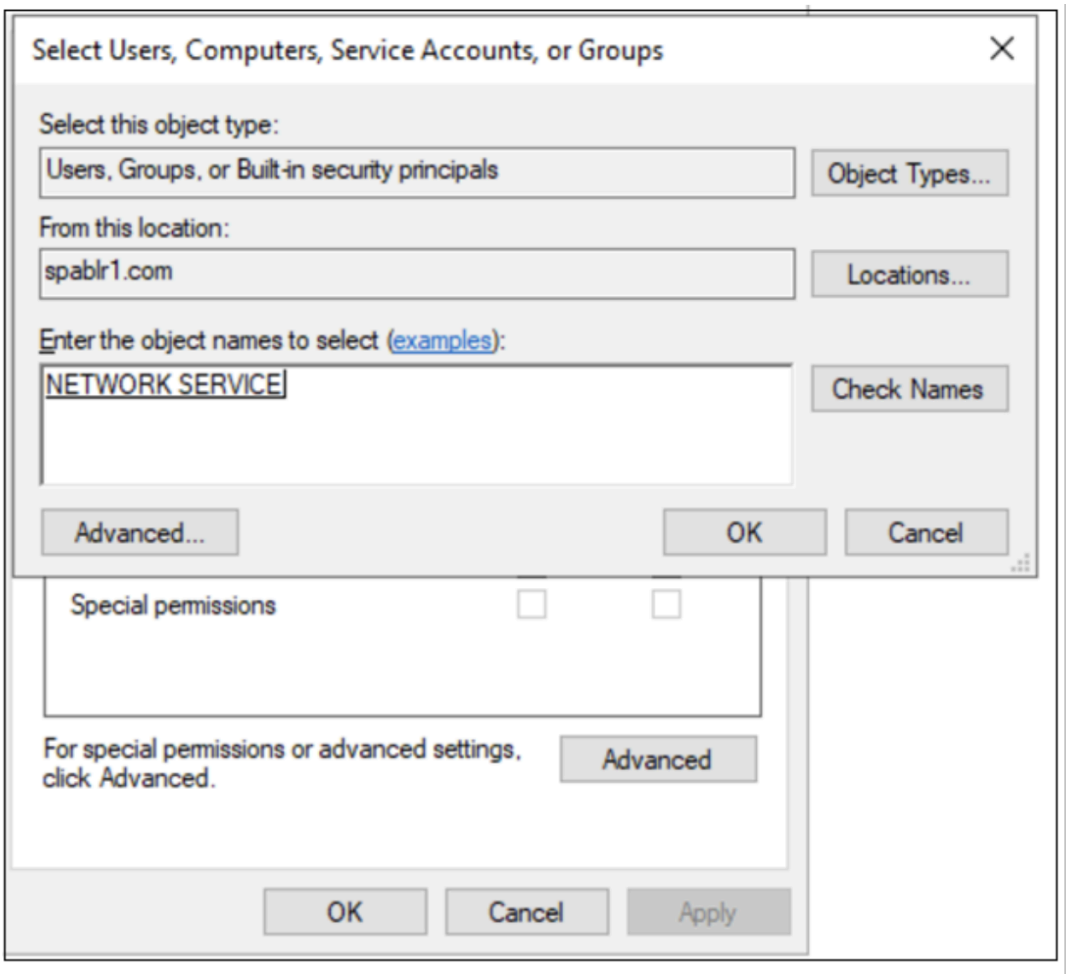

f) In the Permissions window, click **Add** and then search for the Network Service account.

g) Choose the permission **Read only**.

h) Click **OK**.

i) Copy the thumbprint from Certificate Details.




3. After copying the thumbprint, perform the following steps to enable TLS.

   a) Navigate to the Citrix Secure Private Access installation folder (default path - C:\Program Files\Citrix\AccessSecurityService).

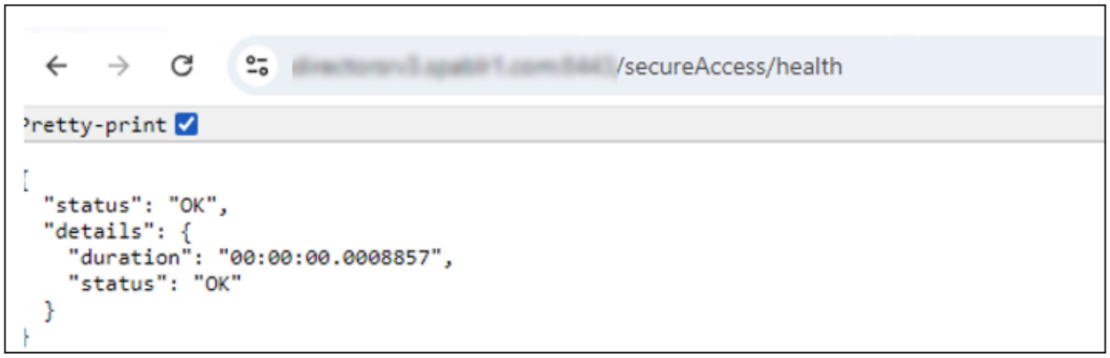
   b) Run .\Citrix.AccessSecurityService.exe /CERTIFICATE_THUMBPRINT <`ThumbprintValue`>.

   c) Restart the Citrix Secure Private Access service.

   d) After the command is run successfully, the Secure Private Access service must be running as a TLS service. To confirm, enter the following URL in the browser:

```
https://<Cloud connector address>:<port>/secureAccess/health
```




## Setup and configure for hybrid deployment

September 6, 2025

As part of the Secure Private Access hybrid deployment onboarding and setup process, the following steps must be completed.

1. Access to the Secure Private Access service admin console
2. Onboard and setup
3. Configure StoreFront
4. Configure NetScaler Gateway
5. Configure applications
    - Configure Web/SaaS applications
    - Configure TCP/UDP apps
    - Configure TCP/UDP - server to client apps
6. Configure access policies for applications

## Access the Secure Private Access admin console

September 6, 2025

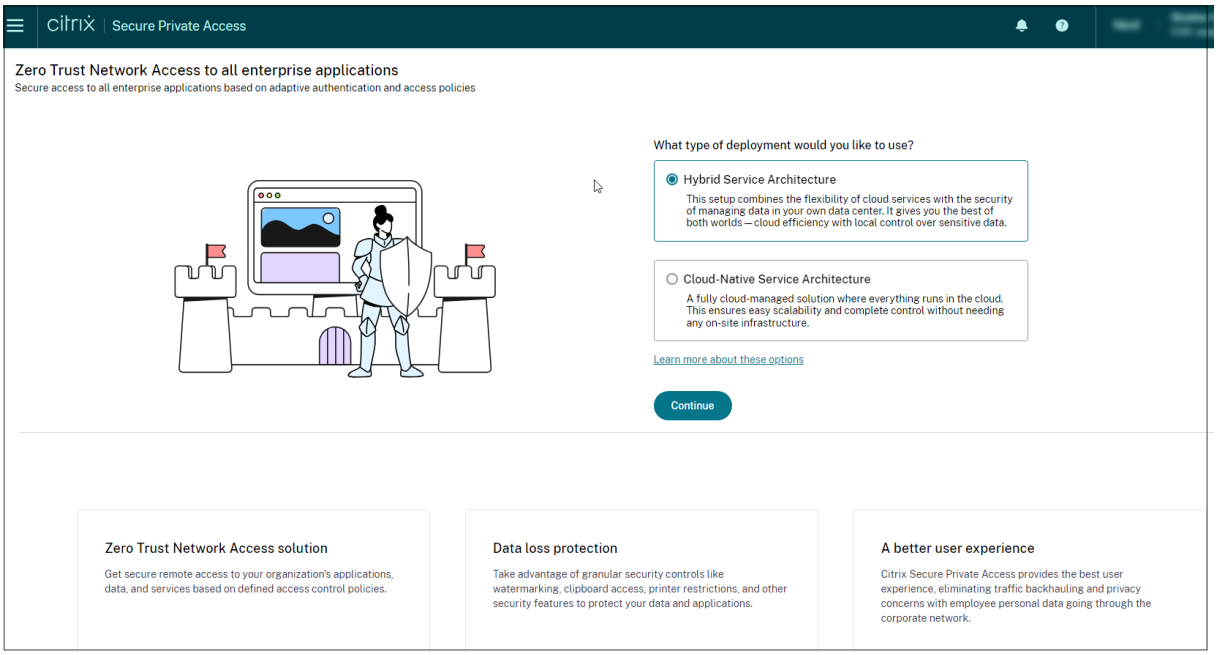
Ensure that the following requirements are met to access the Secure Private Access service admin console.

- Secure Private Access service entitlement.
- Citrix Cloud account. For details, see Create a Citrix Cloud account.

Perform the following steps to access the Secure Private Access admin console.

1. Log on to Citrix Cloud.
2. Click **Manage** on the Secure Private Access tile to access the admin console.
3. Select **Hybrid Service Architecture** and then click **Continue**.




## Onboard and setup

September 6, 2025

As part of the onboarding process, you must first define the Secure Private Access site and specify the servers associated with this deployment.

**Step1 - Define your site:**

A Secure Private Access site is a group of cloud connectors that collaboratively handle the evaluation of policies, application access, and security restrictions. To facilitate this, a single private address is required to create an internal load balancer that distributes traffic among these servers. This load balancer distributes traffic among multiple cloud connectors to ensure load balancing, high availability, and efficient resource utilization.

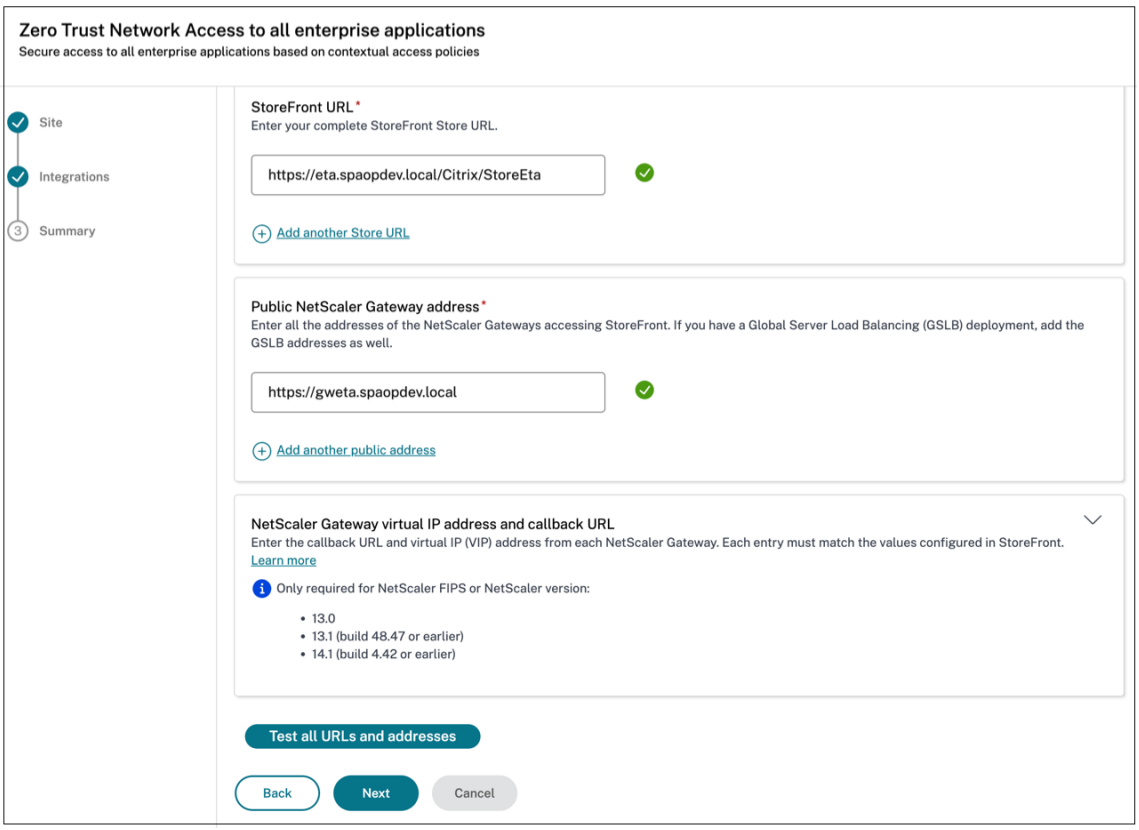
In **Secure Private Access URL,** enter the URL of the load balancer.


**Step 2 - Integrate servers:**

1. Enter the following details.

   - 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`.
   - NetScaler Gateway virtual IP address –This virtual IP address must be the same as the one configured in StoreFront™ for callbacks.
   - NetScaler Gateway Callback URL (Optional) –This URL must be the same as the one configured in StoreFront. For example, `https://gateway.domain.com`.



2. Click **Test all URLs and addresses**.

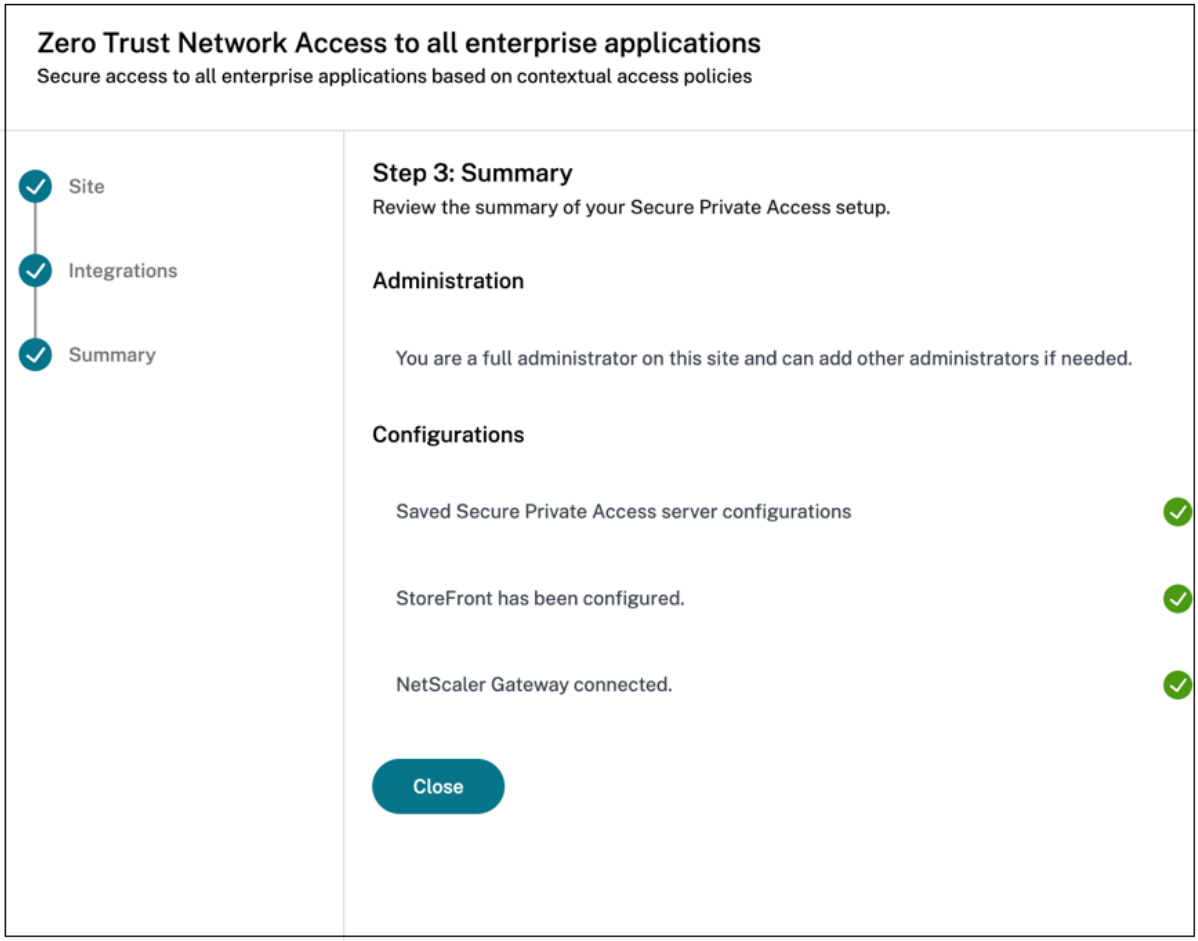
   If any URLs are changed in the on-premises environment, click **Test all URLs and addresses** to confirm that the addresses are reachable.

3. Click **Next**.

**Step 3 - Summary:**

After the configuration is complete, validation must be done to ensure that all servers that are configured are reachable.

If an error is found during validation, an error message is displayed against that component. After resolving the issue, run the validation checks again to ensure that all components are correctly configured and reachable.




Click **Close**.

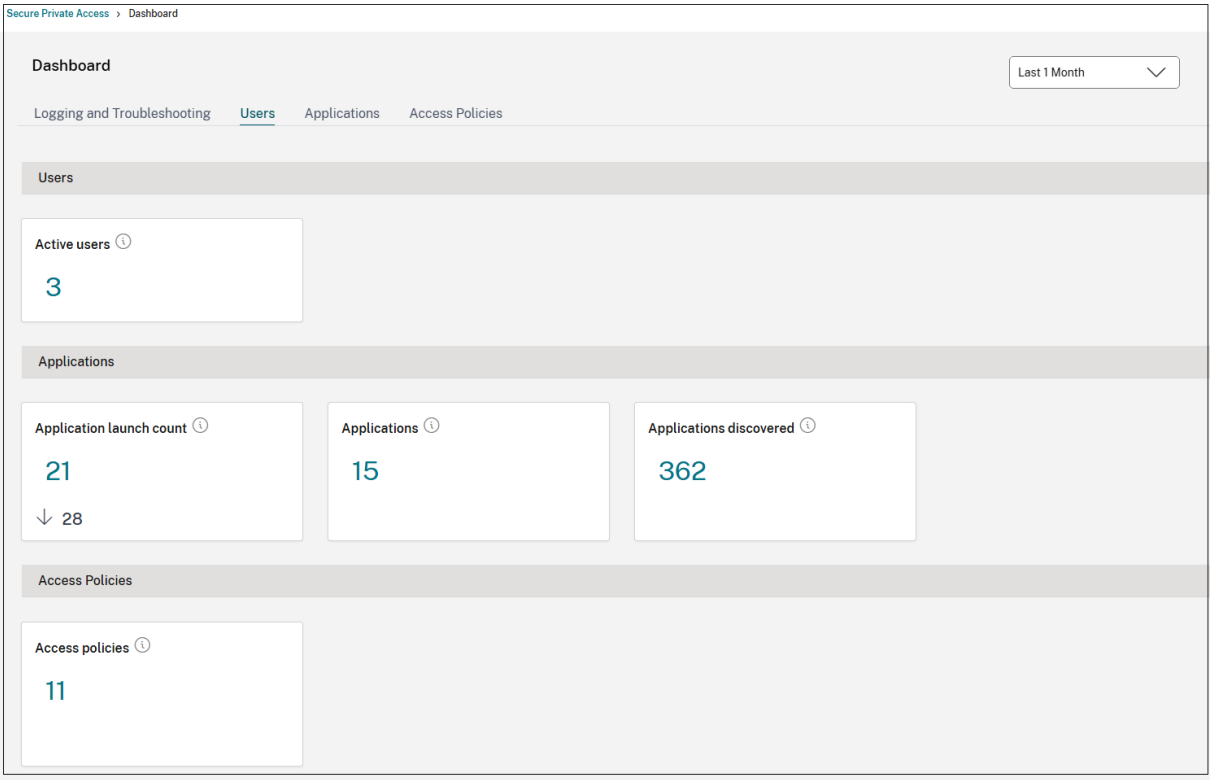
> **Note:**
>
> - You are prompted to download and run the StoreFront and NetScaler® Gateway scripts to

> configure these components, if not already done. Once you run the scripts, click **Mark as done**. However, it is not mandatory to download and run the StoreFront and NetScaler Gateway scripts immediately after the initial setup. It is recommended to run these scripts to ensure that the configuration is complete.

Once you are done with the onboarding, you can create applications and associate access policies with the applications.

The following figure displays the Secure Private Access dashboard after the onboard and setup is complete.




> **Note:**
>
> From the dashboard, you can click **Go To Monitor** to monitor and troubleshoot app sessions and events from DaaS Monitor. For details, see Integration with DaaS monitor.

## Configuration synchronization

All cloud configurations in the Secure Private Access console are automatically synced to Cloud Connector every five minutes. This sync occurs only when there are changes in the cloud configuration.

## StoreFront

September 6, 2025

You must download the StoreFront script and manually run the scripts on the StoreFront machine.

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 provider 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.

### Key-based authentication for StoreFront to Secure Private Access communication

In the previous release, communication between StoreFront and Secure Private Access lacked authentication. Starting from version 2502, a security key-based authentication method is introduced for StoreFront to Secure Private Access communication.

**Authentication steps:**

1. StoreFront sends the key value in the HTTP header "X-Citrix-XmlServiceKey".
2. The Secure Private Access plug-in then validates the key by checking it against either the primary key or a grace key.
3. Upon successful key matching, the Secure Private Access plug-in authenticates the StoreFront to Secure Private Access communication.

**Key generation for new and existing customers:**

- **New customers:** The Secure Private Access plug-in automatically generates the StoreFront security key during the initial setup and enables StoreFront to Secure Private Access authentication.
- **Existing customers:** The Secure Private Access plug-in also auto-generates the StoreFront security key after an upgrade. However, the StoreFront to Secure Private Access authentication is disabled by default. A warning message appears on the admin console, prompting customers to enable the security key. Following this, customers must run the StoreFront configuration script. For details see Modify integration settings.

**Key management:**

The security key can be viewed, rotated, and enabled or disabled for StoreFront to Secure Private Access authentication through the admin console.
Key rotation generates a new key, and moves the old key to the grace key position. The grace key is automatically deleted after two weeks.
If the security key is rotated or if there is a change in the StoreFront to Secure Private Access authentication status, customers must download and run the StoreFront configuration script again.

### When using StoreFront version 2402 or later

In StoreFront version 2402 and later, the Citrix Workspace™ for Web client doesn't enumerate the Secure Private Access apps. This is because Secure Private Access doesn't support the Secure Private

Access app launch in the Workspace for Web platform.

## Configure NetScaler Gateway

September 6, 2025

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

> **Note:**
>
> - Support for TCP/UDP apps along with Web/SaaS apps is available starting from NetScaler Gateway version 14.1–25.56. However, Secure Private Access for TCP/UDP apps in hybrid deployments is supported from version 14.1–34.42 and this version significantly streamlines the configuration process.
> - Support for Web/SaaS apps is available from NetScaler Gateway versions 13.1, 14.1 and later. For details about the NetScaler Gateway configuration, see Configure NetScaler Gateway.
> - Secure Private Access for hybrid deployment can be enabled globally or per VPN virtual server. We recommend that you enable Secure Private Access per VPN virtual server. After Secure Private Access is enabled, TCP/UDP and Web/SaaS applications are enabled by default.

**To create NetScaler Gateway for the Web/SaaS or TCP/UDP applications, perform the following steps:**

1. Download the latest script `ns_gateway_secure_access.sh`. from https://www.citrix.com/downloads/citrix-secure-private-access/Shell-Script/.
2. Upload these scripts to the NetScaler machine. You can use the WinSCP app or the SCP command. For example, `scp ns_gateway_secure_access.sh nsroot@nsalfa.fabrikam.local:/var/tmp`.

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

   > **Note:**
   >
   > - It's recommended to use NetScaler /var/tmp folder to store temp data.
   > - Make sure that the file is saved with LF line endings. FreeBSD does not support CRLF.

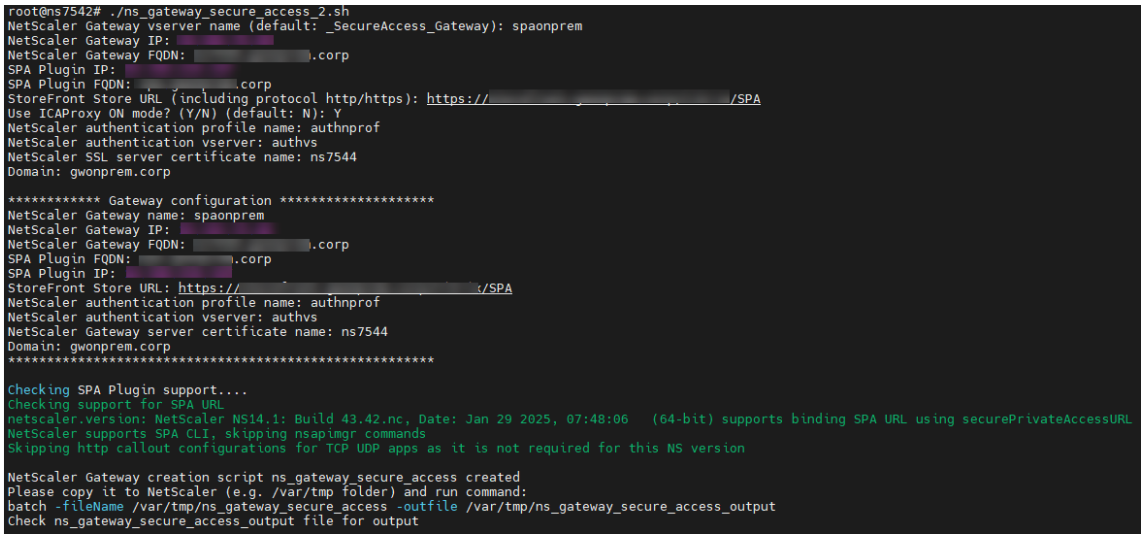
 

> - If you see the error `-bash: /var/tmp/ns_gateway_secure_access.sh : /bin/sh^M: bad interpreter: No such file or directory`, it means that the line endings are incorrect. You can convert the script by using any rich text editor, such as Notepad++.

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

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

5. Run the uploaded script on the NetScaler shell.



```
root@ns7542# ./ns_gateway_secure_access_2.sh
NetScaler Gateway vserver name (default: _SecureAccess_Gateway): spaonprem
NetScaler Gateway IP:
NetScaler Gateway FQDN:                    .corp
SPA Plugin IP:
SPA Plugin FQDN:                    .corp
StoreFront Store URL (including protocol http/https): https://                    /SPA
Use ICAProxy ON mode? (Y/N) (default: N): Y
NetScaler authentication profile name: authnprof
NetScaler authentication vserver: authvs
NetScaler SSL server certificate name: ns7544
Domain: gwonprem.corp

************ Gateway configuration ********************
NetScaler Gateway name: spaonprem
NetScaler Gateway IP:
NetScaler Gateway FQDN:                    .corp
SPA Plugin FQDN:                    .corp
SPA Plugin IP:
StoreFront Store URL: https://                    /SPA
NetScaler authentication profile name: authnprof
NetScaler authentication vserver: authvs
NetScaler Gateway server certificate name: ns7544
Domain: gwonprem.corp
*****************************************************

Checking SPA Plugin support....
Checking support for SPA URL
netscaler.version: NetScaler NS14.1: Build 43.42.nc, Date: Jan 29 2025, 07:48:06   (64-bit) supports binding SPA URL using securePrivateAccessURL
NetScaler supports SPA CLI, skipping nsapimgr commands
Skipping http callout configurations for TCP UDP apps as it is not required for this NS version

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

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

   Enter **Y** for the **Use ICAProxy ON mode?** parameter if you intend to use ICA Proxy mode for enumeration and launching of Web/SaaS applications. Else enter **N.**

   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 provider compatibility is checked. If NetScaler supports the Secure Private Access provider, 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.

```
##################################################################################################################
#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 REWRITE IC

# Add NetScaler Gateway vserver
add vpn vserver _SecureAccess_Gateway SSL [redacted] -Listenpolicy NONE -tcpProfileName nstcp_default_XA_XD_profile -deploymentType ICA_STOREFRONT -vserverFqdn gateway.mydomain.com -authnProfile auth_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.mydomain.com
bind policy patset ns_cvpn_default_bypass_domains spa.mydomain.com
bind policy patset ns_cvpn_default_bypass_domains citrix.com

# Add session actions
add vpn sessionAction AC_OS_SecureAccess_Gateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF -wihome "https://[redacted]" -ClientChoices OFF -ntDomai
n mydomain.com -defaultAuthorizationAction ALLOW -authorizationGroup SecureAccessGroup -clientlessVpnMode ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -storefronturl "https://storefront.mydomain.com" -sfGatewayAuth
Type domain
add vpn sessionAction AC_WB_SecureAccess_Gateway -transparentInterception OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy OFF -wihome "https://[redacted]" -ClientChoices OFF -ntDomai
n mydomain.com -defaultAuthorizationAction ALLOW -authorizationGroup SecureAccessGroup -clientlessVpnMode ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -storefronturl "https://storefront.mydomain.com" -sfGatewayAuth
Type domain

# Add session policies
add vpn sessionPolicy PL_OS_SecureAccess_Gateway "HTTP.REQ.HEADER(\"User-Agent\").CONTAINS(\"CitrixReceiver\")" AC_OS_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 "\"[redacted]\""
add rewrite action Add_X-GW-SessionId insert_http_header X-GW-SessionId AAA.USER.SESSIONID
add rewrite policy Add_X-Citrix-ViaPol "HTTP.REQ.HOSTNAME.CONTAINS(\"spa.mydomain.com\") && HTTP.REQ.HEADER(\"X-Citrix-Via\").EXISTS.NOT" Add_X-Citrix-Via
add rewrite policy Add_X-Citrix-Via-VIPPol "HTTP.REQ.HOSTNAME.CONTAINS(\"spa.mydomain.com\") && HTTP.REQ.HEADER(\"X-Citrix-Via-VIP\").EXISTS.NOT" Add_X-Citrix-Via-VIP
add rewrite policy Add_X-GW-SessionIdPol "HTTP.REQ.HOSTNAME.CONTAINS(\"spa.mydomain.com\")" Add_X-GW-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.HOSTNAME.CONTAINS(\"spa.mydomain.com\")" _SecureAccess_Gateway_Traffic_Action

# Bind policies to NetScaler Gateway vserver
bind vpn vserver _SecureAccess_Gateway -policy PL_OS_SecureAccess_Gateway -priority 100 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver _SecureAccess_Gateway -policy PL_WB_SecureAccess_Gateway -priority 110 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver _SecureAccess_Gateway -policy Add_X-Citrix-ViaPol -priority 120 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver _SecureAccess_Gateway -policy Add_X-Citrix-Via-VIPPol -priority 130 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver _SecureAccess_Gateway -policy Add_X-GW-SessionIdPol -priority 140 -gotoPriorityExpression NEXT -type REQUEST
bind vpn vserver _SecureAccess_Gateway -policy _SecureAccess_Gateway_Traffic_Policy -priority 150 -gotoPriorityExpression NEXT -type REQUEST

# Bind SSL cert to NetScaler Gateway
bind ssl vserver _SecureAccess_Gateway -certkeyName star.mydomain.com
```

7. Switch to the NetScaler CLI and run the resultant NetScaler commands from the new file with the batch command. For example;

   `batch -fileName /var/tmp/ns_gateway_secure_access -outfile /var/tmp/ns_gateway_secure_access_output`

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

   A command can fail if a resource exists or one of the parameters entered in step 6 is incorrect.

8. Ensure that all commands are successfully completed.

> **Note:**
>
> - If a load balancer is configured, ensure that you provide the load balancer URL while binding the Secure Private Access provider to the VPN virtual server. Example: `bind vpn vserver spahybrid -securePrivateAccessUrl "https://spa.example.corp"`
> - 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.

## Points to note

- Existing NetScaler Gateway can be updated with script but there can be a significant number of possible NetScaler configurations that can't be covered by a single script.
- We recommend that you set **ICA® Proxy** to OFF in the Secure Private Access enabled VPN virtual server.
- If you use NetScaler deployed in the cloud, you must make changes in the network. For example, allow communications between NetScaler and other components on certain ports. For details on the ports, see Communication ports.

- If you enable SSO on NetScaler Gateway, make sure that NetScaler communicates to StoreFront™ using a private IP address. You might have to add a StoreFront DNS record to NetScaler with a StoreFront private IP address.

## Update existing NetScaler Gateway configuration

September 6, 2025

If you are updating an existing NetScaler Gateway configuration, it is recommended that you update the configuration manually. For details, see the following sections:

- Update existing NetScaler Gateway configuration for Web and SaaS apps
- Update existing NetScaler Gateway configuration for TCP/UDP apps

### 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
- dtls: OFF

**Update a virtual server:**

- tcpProfileName: nstcp_default_XA_XD_profile
- icaOnly: OFF
- dtls: OFF

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

### 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.

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 session actions settings

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

- `transparentInterception`: OFF
- `SSO`: ON
- `ssoCredential`: PRIMARY
- `useMIP`: NS
- `useIIP`: OFF
- `icaProxy`: ON
- `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`: OFF
- `clientlessModeUrlEncoding`: TRANSPARENT
- `SecureBrowse`: ENABLED
- `Storefronturl`: `"https://storefront.mydomain.com"`
- `sfGatewayAuthType`: domain

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

#### Example commands when ICA® Proxy is disabled

Add/update a virtual server.

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

Add a session action.

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

Add a session policy.

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

Bind the session policy to the VPN virtual server.

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

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

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

For details on session action parameters, vpn-sessionAction.

#### Example commands when ICA Proxy is enabled

Add/update a virtual server.

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

Add a session action.

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

Add authorization policies.

- `add authorization policy ALLOW_STOREFRONT "(HTTP.REQ.HOSTNAME .SET_TEXT_MODE(IGNORECASE).STARTSWITH(\"gateway.example.corp \")|| HTTP.REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE).STARTSWITH (\"storefront.example.corp\"))&& (HTTP.REQ.URL.SET_TEXT_MODE( IGNORECASE).STARTSWITH(\"/Citrix\")|| HTTP.REQ.URL.SET_TEXT_MODE( IGNORECASE).STARTSWITH(\"/AGServices\"))"ALLOW`
- `add authorization policy SECUREACCESS_AUTHORIZATION "(CLIENT. SSLVPN.MODE.EQ(\"SECURE_BROWSE\")|| HTTP.REQ.HEADER(\"X-Citrix -AccessSecurity\").EXISTS || HTTP.REQ.HEADER(\"X-Citrix-Secure- Browser\").EXISTS)&& sys.HTTP_CALLOUT(SecureAccess_httpCallout)" ALLOW`
- `add authorization policy SECUREACCESS_AUTHORIZATION_ICAPROXY " CLIENT.SSLVPN.MODE.EQ(\"ICAPROXY\")&& HTTP.REQ.HOSTNAME.SET_TEXT_MODE (IGNORECASE).STARTSWITH(\"gateway.example.corp\").NOT && HTTP. REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE).STARTSWITH(\"storefront. example.corp\").NOT && sys.HTTP_CALLOUT(SecureAccess_httpCallout) "ALLOW`

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

- `bind aaa group SecureAccessGroup -policy ALLOW_STOREFRONT - priority 100 -gotoPriorityExpression END`
- `bind aaa group SecureAccessGroup -policy SECUREACCESS_AUTHORIZATION -priority 1000 -gotoPriorityExpression END`
- `bind aaa group SecureAccessGroup -policy SECUREACCESS_AUTHORIZATION_ICAPRO -priority 1100 -gotoPriorityExpression END`

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

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

For details on session action parameters, vpn-sessionAction.

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

Support for TCP/UDP apps in addition to Web/SaaS apps is available starting from NetScaler Gateway version 14.1–25.56. For hybrid deployments, it is recommended to use version 14.1–34.42 to fully leverage TCP/UDP features. If you are updating earlier versions, 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 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

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

```
add vpn sessionAction AC_AG_PLGspahybrid -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_PLUGINspahybrid "HTTP.REQ.HEADER
(\"User-Agent\").CONTAINS(\"CitrixReceiver\").NOT && (HTTP.REQ
.HEADER(\"User-Agent\").CONTAINS(\"plugin\")|| HTTP.REQ.HEADER(\"
User-Agent\").CONTAINS(\"CitrixSecureAccess\"))"AC_AG_PLGspahybrid
```

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

```
bind vpn vserver spahybrid -policy PL_AG_PLUGINspahybrid -priority
 105 -gotoPriorityExpression NEXT -type REQUEST
```

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

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

> **Note:**
>
> NetScaler Gateway release 14.1–34.42 and later does not support the App Controller server. You must instead bind the Secure Private Access URL to the VPN virtual server.

## NetScaler Gateway configuration for earlier versions

September 6, 2025

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

> **Important:**
>
> - Support for TCP/UDP apps in addition to Web/SaaS apps is available starting from NetScaler Gateway version 14.1–25.56. However, Secure Private Access for TCP/UDP apps in hybrid deployments is supported from version 14.1–34.42 and this version significantly streamlines the configuration process.
> - Support for Web/SaaS apps is available from NetScaler Gateway versions 13.1, 14.1 and later.
> - For details about the NetScaler Gateway configuration, see Configure NetScaler Gateway.

### 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 provider on NetScaler Gateway by using the CLI or GUI. For details, see Enable Secure Private Access provider 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

The smart access tags are added as a header in the Secure Private Access provider request.

### Configure Secure Private Access toggles

The following table lists the toggles that must be used to support smart access tags for hybrid deployments.

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

| Toggle name | Description |
| --- | --- |
| `nsapimgr -ys call= toggle_vpn_use_cdn_for_access_restricted_page` | Use the “Access restricted”page hosted on CDN. |

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

### Persist Secure Private Access provider settings on NetScaler

To persist the Secure Private Access provider settings on NetScaler, do the following:

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

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

nsapimgr -ys call=toggle_vpn_use_cdn_for_access_restricted_page
```

3. Save the file.

The Secure Private Access provider settings are automatically applied when NetScaler is restarted.

### Enable Secure Private Access provider on NetScaler Gateway

Starting from NetScaler Gateway 14.1–25.56 and later, you can enable the Secure Private Access provider on NetScaler Gateway by using the NetScaler Gateway CLI or the GUI.

**CLI:**

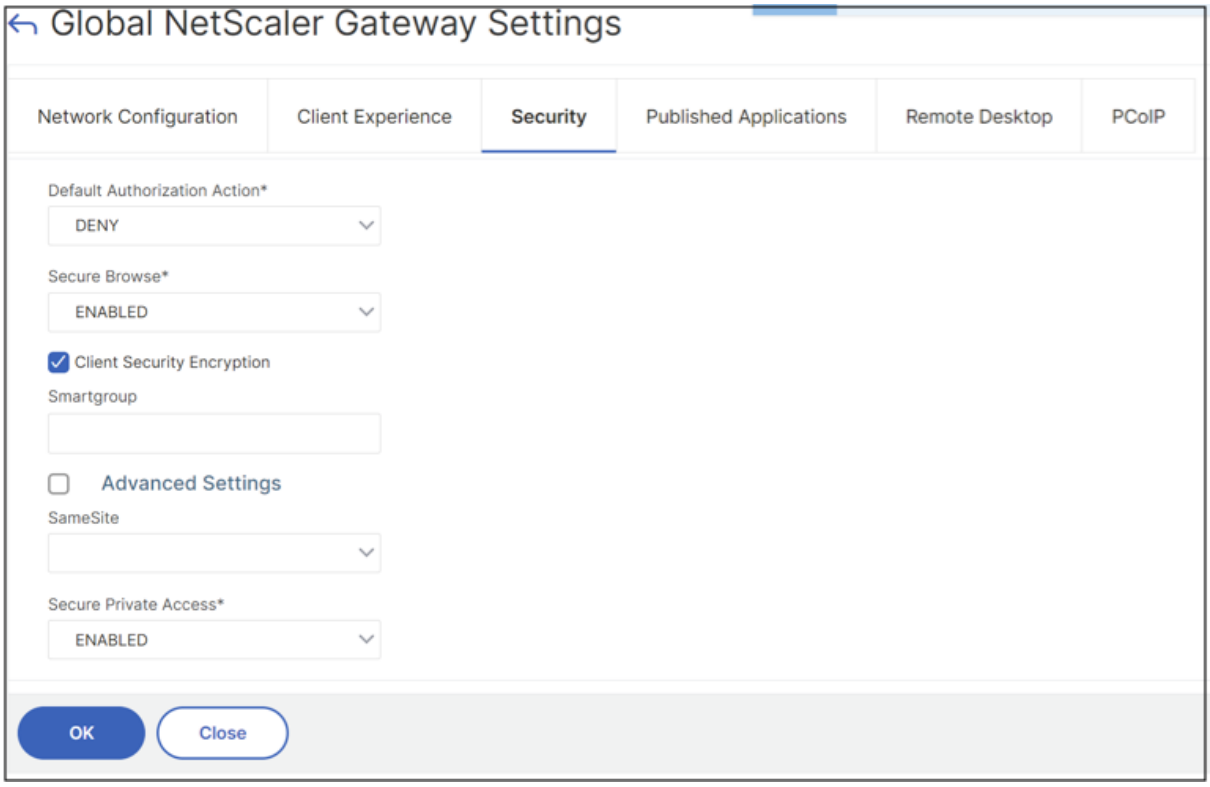
At the command prompt, type the following command:

```
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.**




## Compatibility with the ICA® apps

NetScaler Gateway created or updated to support the Secure Private Access provider 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

### Known limitations

- Existing NetScaler Gateway can be updated with script but there can be a significant number of possible NetScaler configurations that can't be covered by a single script.
- We recommend that you set **ICA Proxy** to OFF in the Secure Private Access enabled VPN virtual server.
- If you use NetScaler deployed in the cloud, you must make changes in the network. For example, allow communications between NetScaler and other components on certain ports. For details on the ports, see Communication ports.
- If you enable SSO on NetScaler Gateway, make sure that NetScaler communicates to StoreFront™ using a private IP address. You might have to add a StoreFront DNS record to NetScaler with a StoreFront private IP address.

## Contextual tags

September 6, 2025

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

### Configure custom tags using the GUI

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

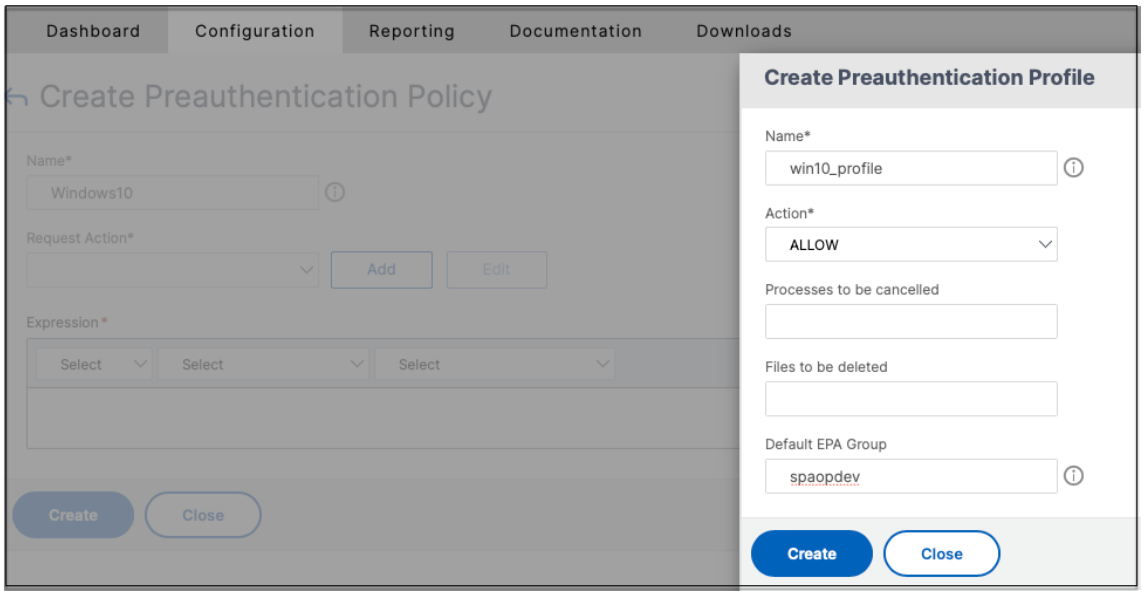
1. Configure a classic gateway preauthentication policy.
2. Bind the classic preauthentication policy to the gateway virtual server.

#### Configure a classic gateway preauthentication policy

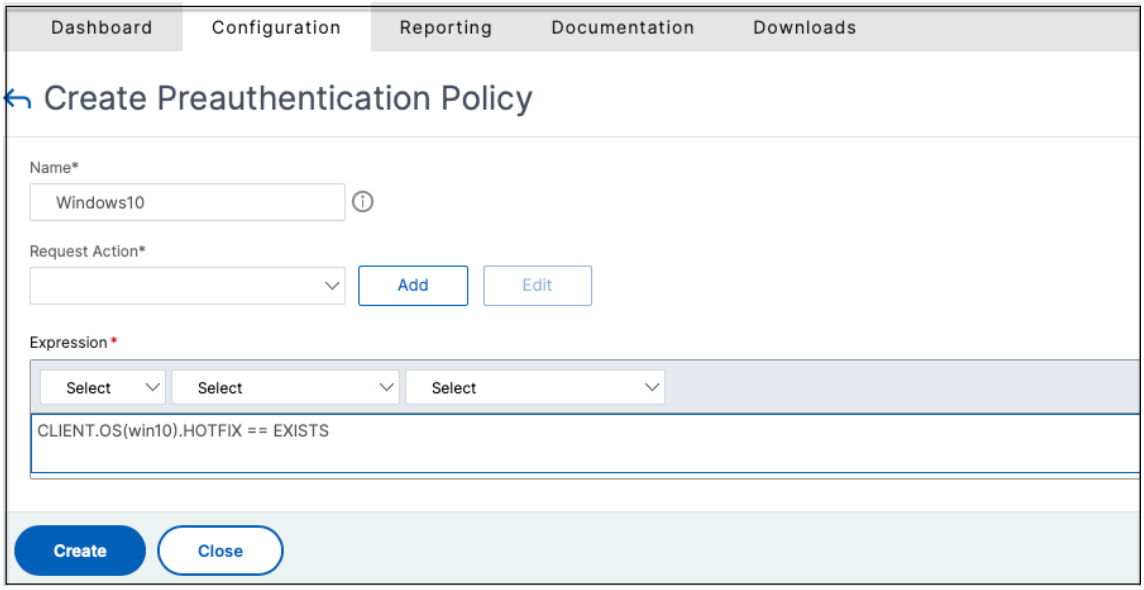
1. Navigate to **NetScaler Gateway > Policies > Preauthentication** and then click **Add**.

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

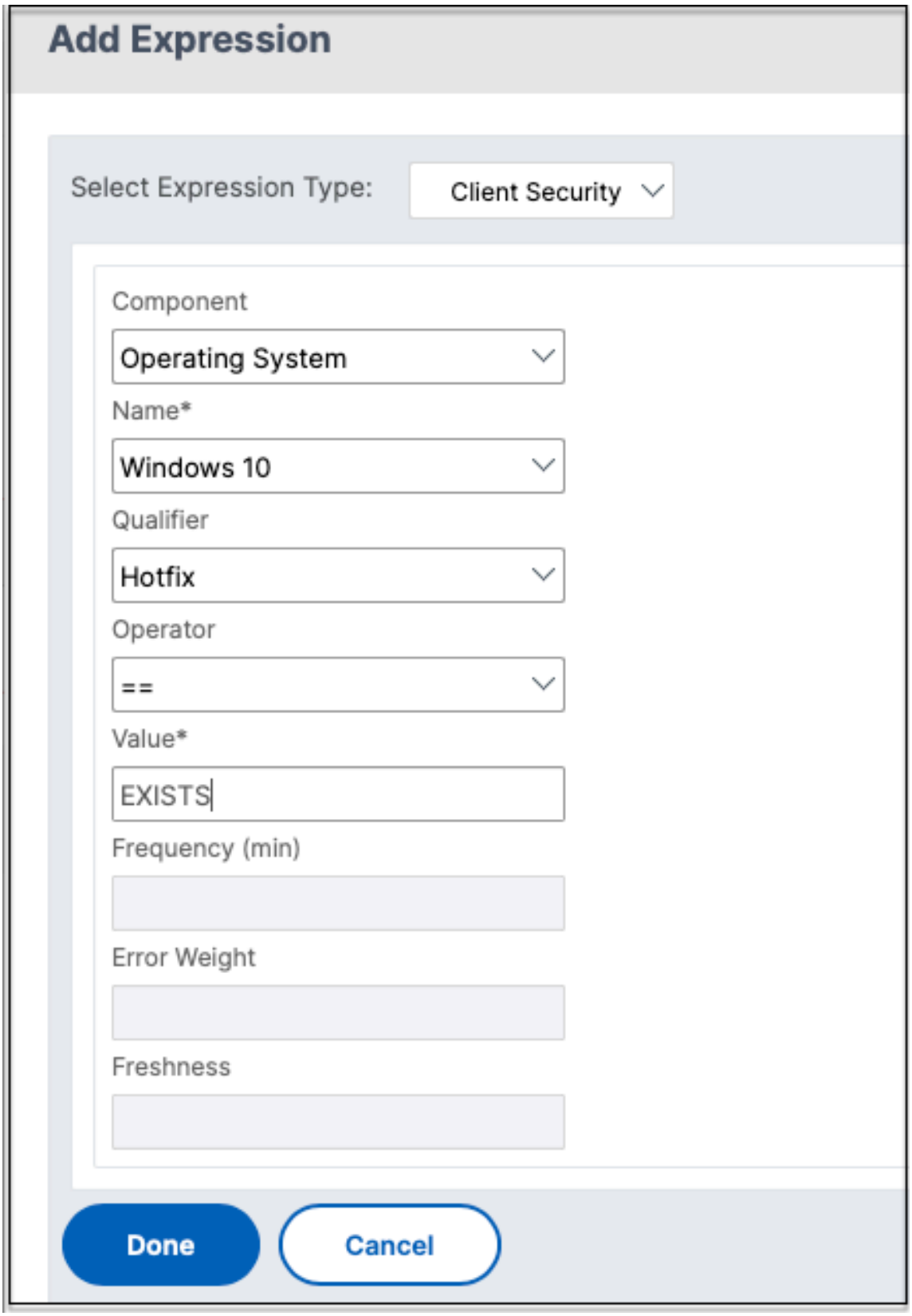



4. Fill in the details in the required fields and click **Create**.
5. In **Expression**, enter the expression manually or use the Expression editor to construct an expression for the policy.




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

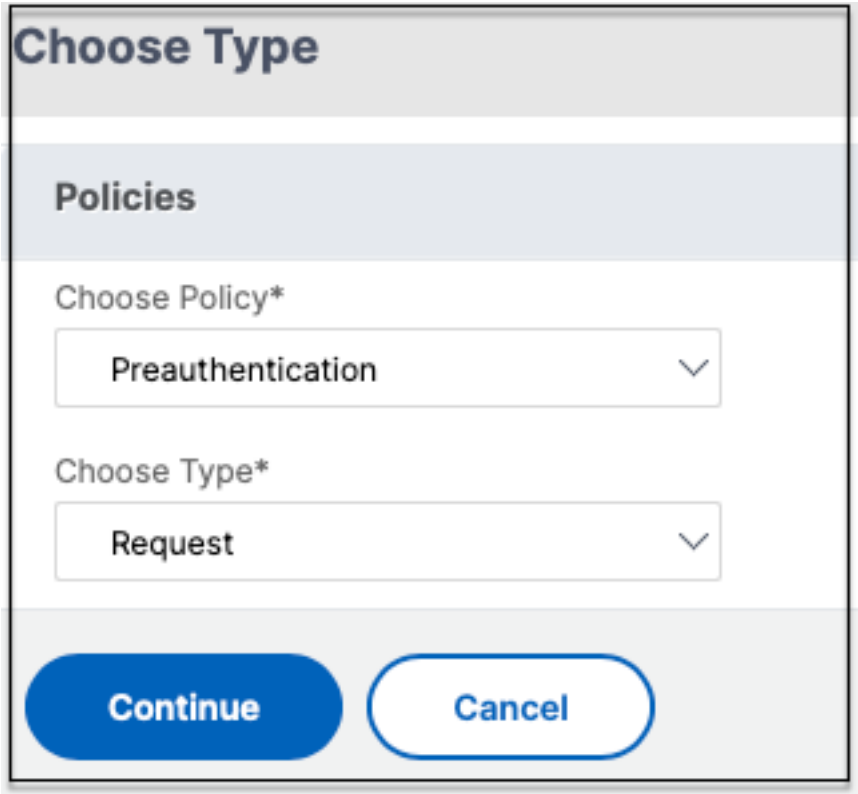



6. Click **Create**.

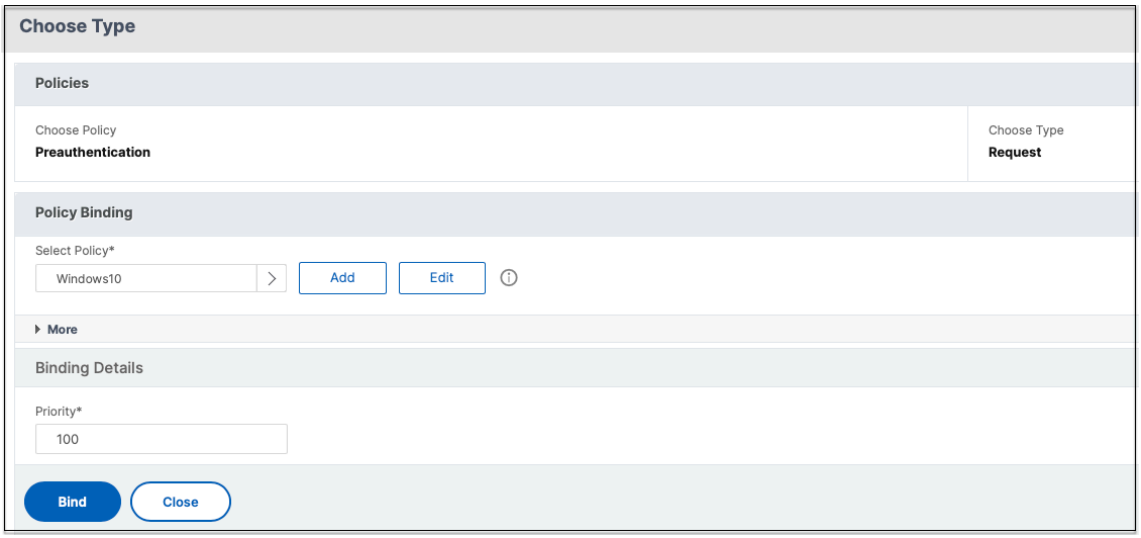
**Bind the custom tag to NetScaler Gateway**

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




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




### Configure custom tags using the CLI

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

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

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

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

### Adding a new contextual tag

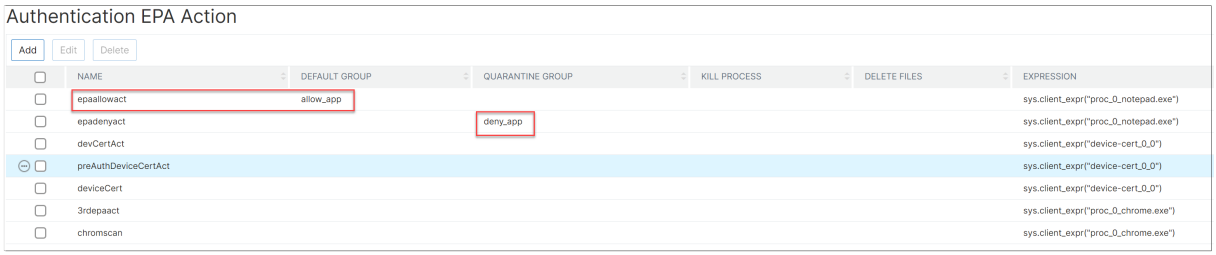
1. Open the Secure Private Access admin console and click **Access Policies**.
2. Create a new policy or edit an existing policy.
3. In the **Condition** section, click **Add condition** and select **Contextual Tags**, **Matches all of**, and then enter the contextual tag name (for example, `Windows10`).

**Note on EPA tags sent to Secure Private Access provider**

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

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




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

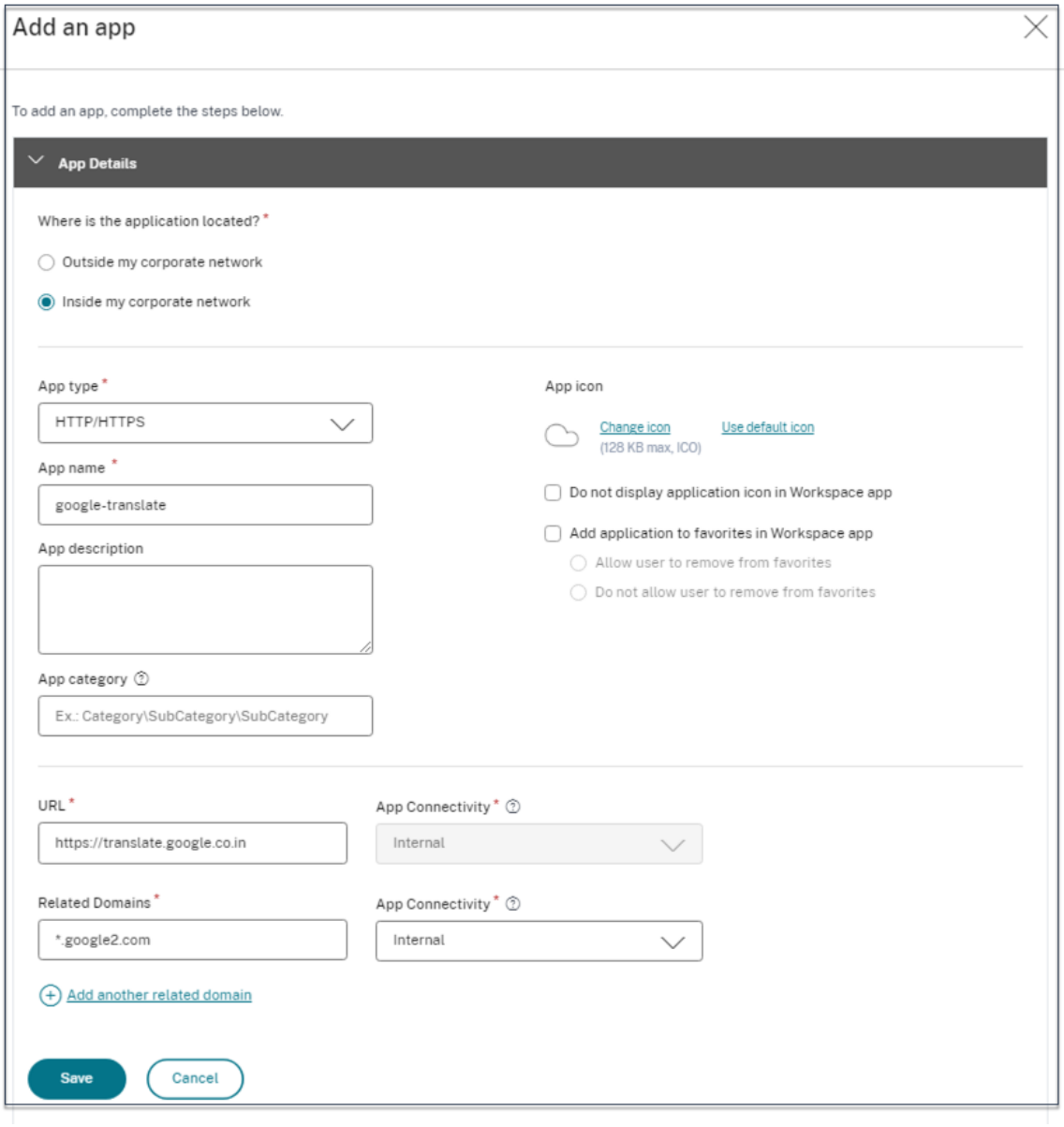
## Configure Web/SaaS applications

September 6, 2025

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

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




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

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

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

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

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

- **Add application to favorites automatically** –Click this option to add the app as a favorite app in Citrix Workspace app. When you select this option, a star icon with a padlock appears at the top left-hand corner of the app in Citrix Workspace app.
  - **Allow user to remove from favorites** –Click this option to allow app subscribers to remove the app from the favorites apps list in Citrix Workspace app.

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

  - **Do not allow user to remove from favorites** –Click this option to prevent subscribers from removing the app from the favorites apps list in Citrix Workspace app.

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

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

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

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

### Next steps

Configure access policies for the applications.

## Configure TCP/UDP apps

September 6, 2025

**Prerequisites:**

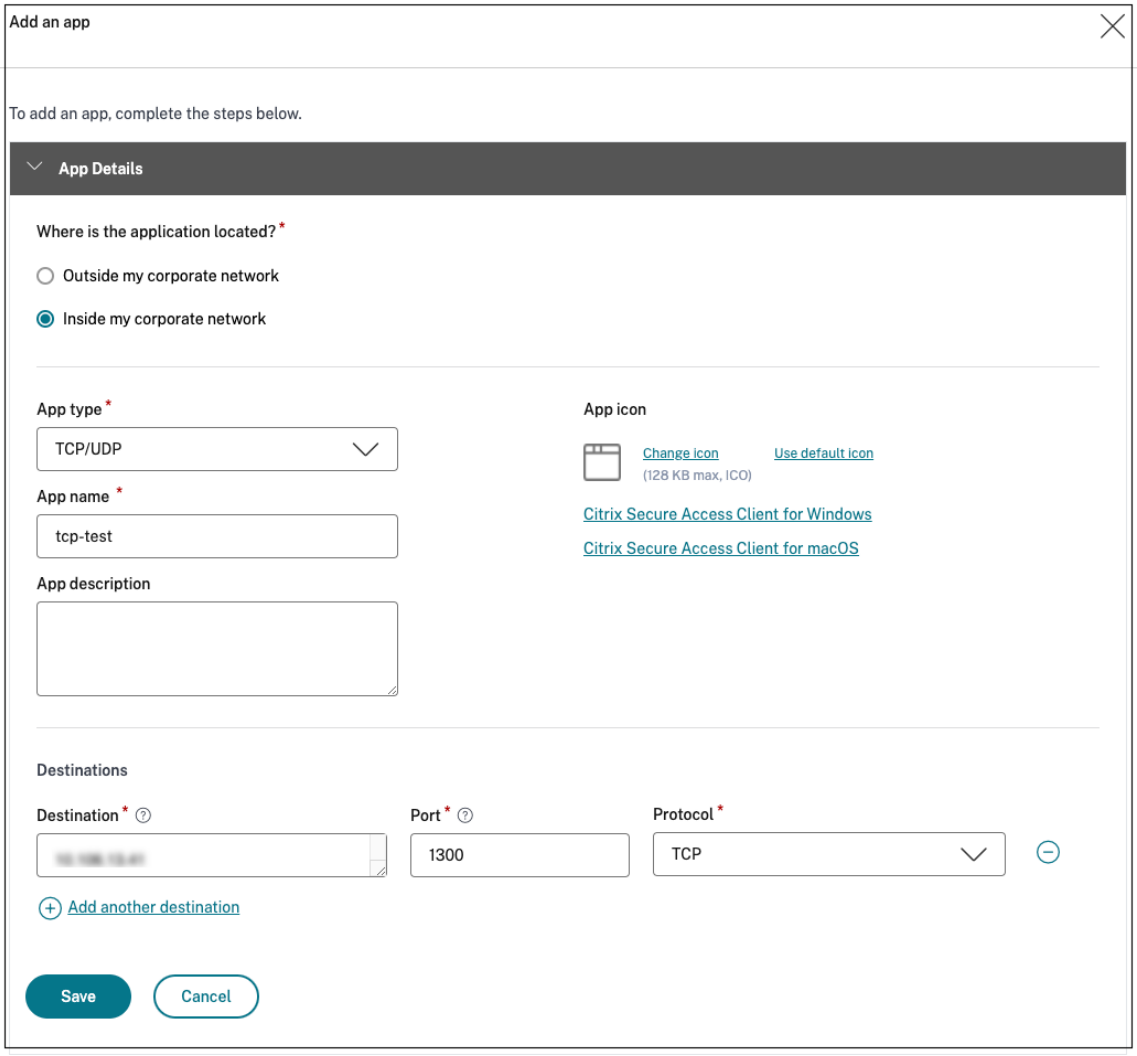
- Secure Private Access setup is complete.
- Client versions meet the following requirements:
  - Windows - 24.8.1.15 and later
  - macOS - 24.09.1 and later

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

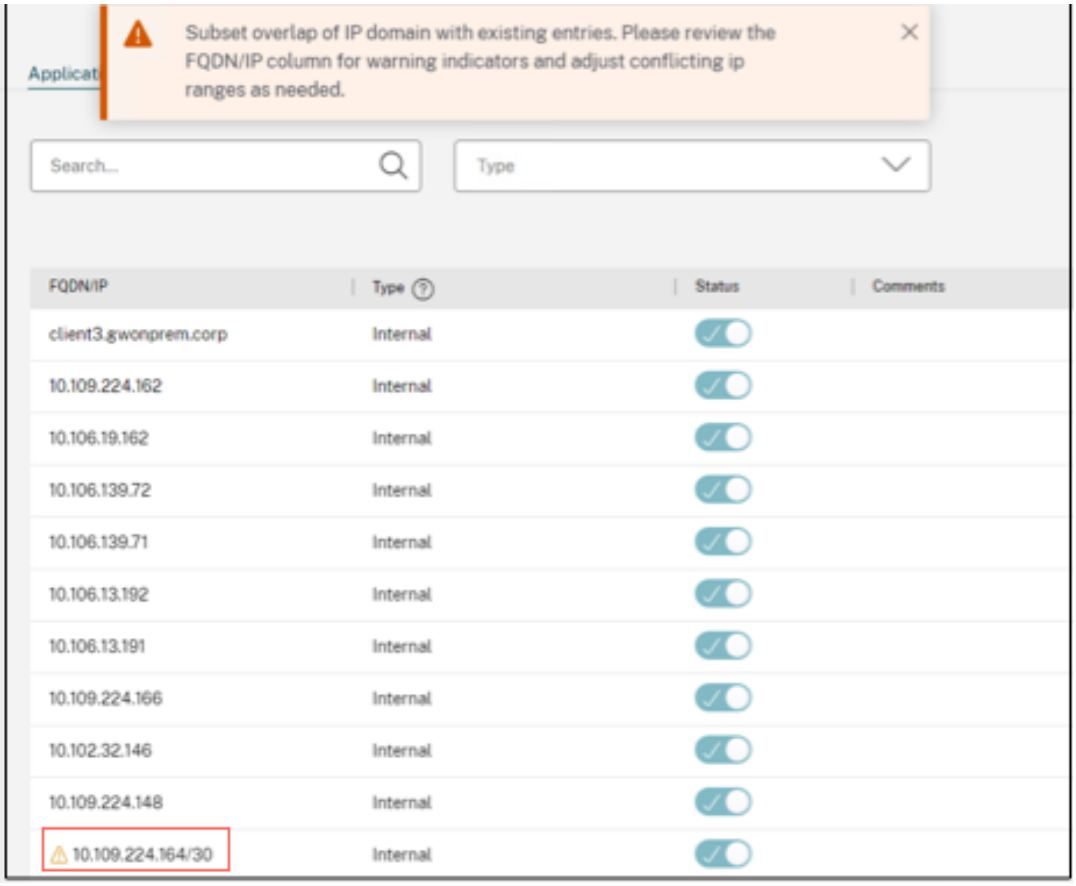
> **Note:**
>
> * End users can access the apps using FQDN even if the admin has configured the apps using the IP address. This is possible because the Citrix Secure Access™ client can resolve an FQDN to the real IP address.

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

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

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




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

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

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

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

- **Protocol** –TCP/UDP

4. **App Connectivity:** Define how your application traffic must be routed.

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

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

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

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

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

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

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

### Next steps

Configure access policies for the applications.

## Configure TCP/UDP - server to client apps

September 6, 2025

The **TCP/UDP - server to client** app type can be used for supporting the following features:

- Software distribution using Microsoft Endpoint Configuration Manager or similar solutions

- Remote policy updates on managed devices using GPO Push
- Remote assistance to troubleshoot and debug user workstations.

**Prerequisites:**

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

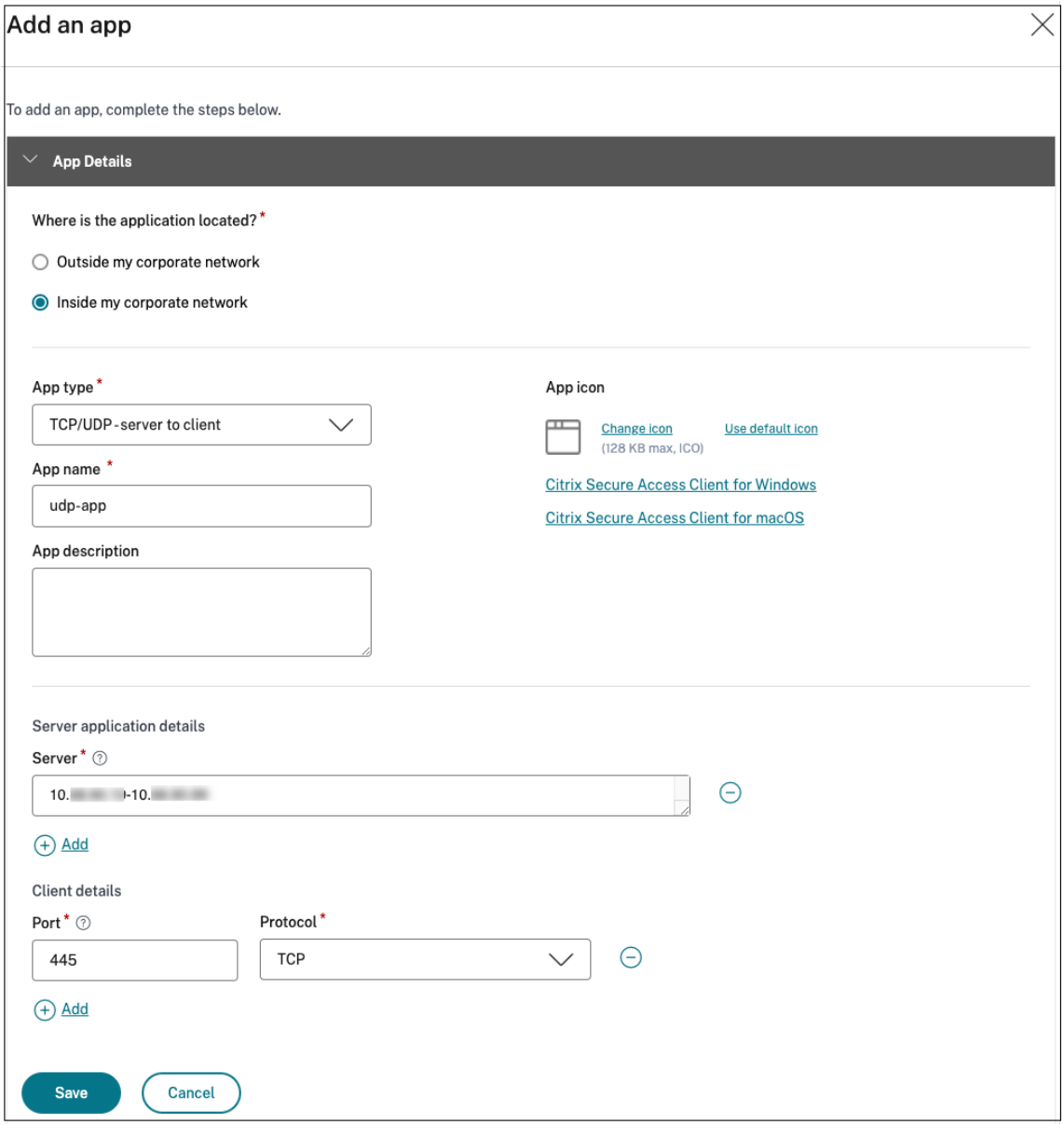
  ```
  set vpn sessionAction AC_AG_PLGspaonprem -useMIP NS -useIIP
  NOSPILLOVER
  ```

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

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

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




3. Enter the following details:

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

4. Click **Add** to add additional servers.

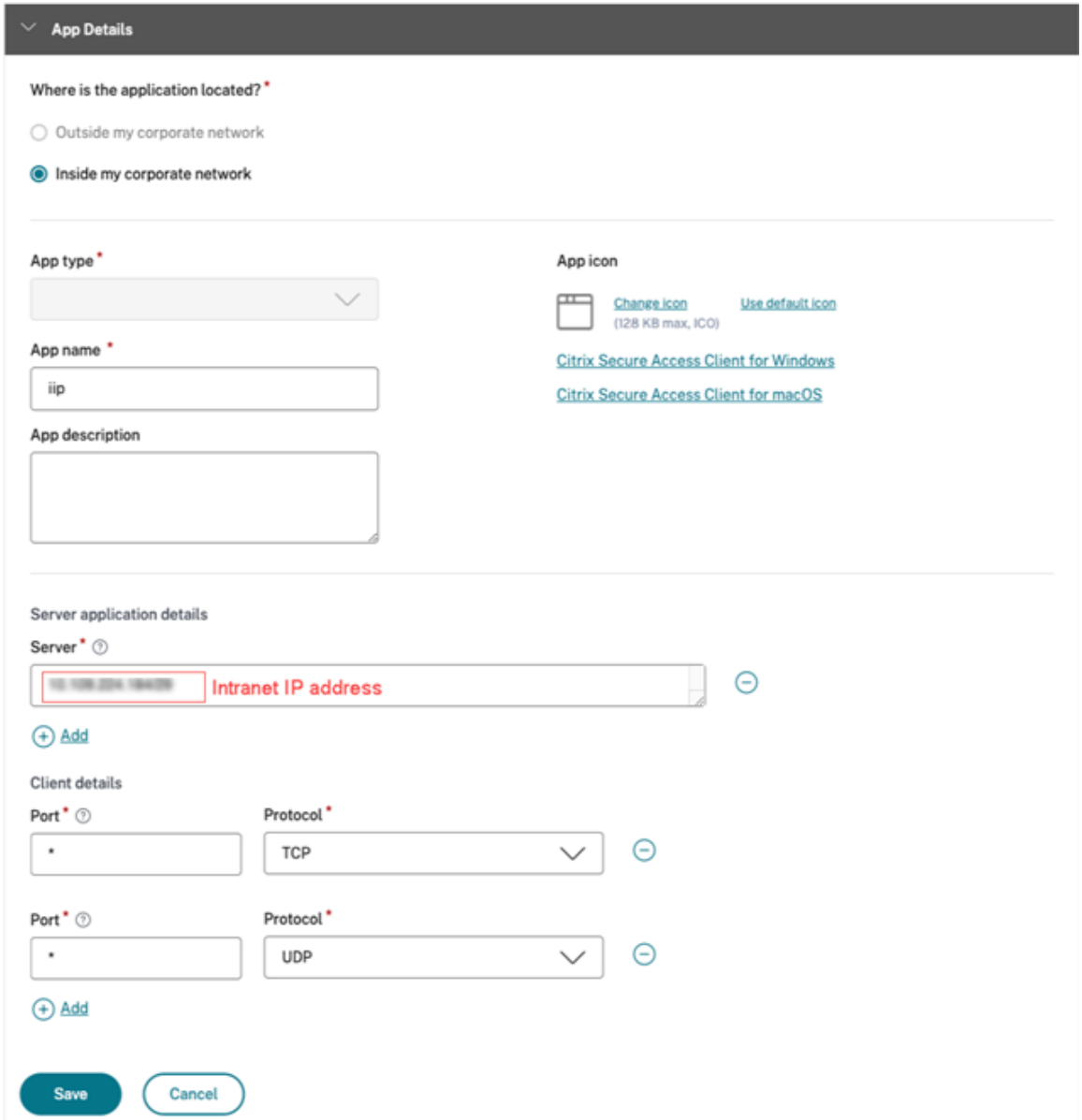
5. Click **Save**. The app is added to the **App Configuration** page. You can edit or delete an app

from the **Applications** page after you have configured the application. To do so, click the ellipsis button in line with the app and select the actions accordingly.

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

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



### Next steps

Configure access policies for the applications.

## Configure access policies for the applications

September 6, 2025

Access policies allow you to enable or disable access to the apps based on the user 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. In the **Create Access Policy** page, select one of the following:

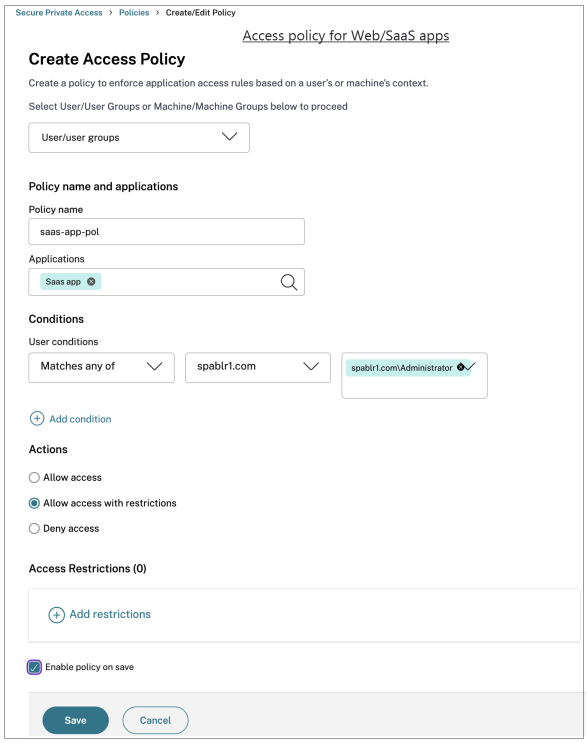
   - **Users/User groups**
   - **Machines/Machine groups**

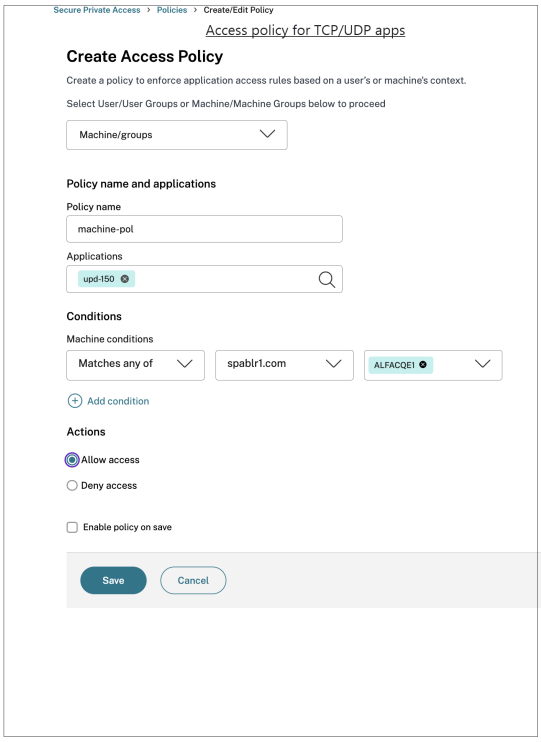
   Application access rules are enforced based on a user's or machine's context, based on the selection in the access policy.

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

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




4. a) In **Policy name**, enter a name for the policy.

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

6. In **Users conditions** –Select the conditions and users or user groups based on which app access must be allowed or denied.

   - **Matches any of**: Only the users 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.

   You can search for users by display name, email ID, or user principal name. This search option allows admins to accurately identify and grant access to the correct user, even if they have multiple accounts.

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

8. You can further refine access control by adding conditions based on contextual tags and Device Posture tags for more granular access control.

   - **Contextual tags** - Click **Add condition** and select **Contextual tags**. Select the logical expression from the drop-down menu and the contextual tag based on which the app access must be allowed or denied.
   - **Device Posture check** - Click **Add condition**. Select **Device Posture check** and the logical expression from the drop-down menu. Enter one of the following values in the custom

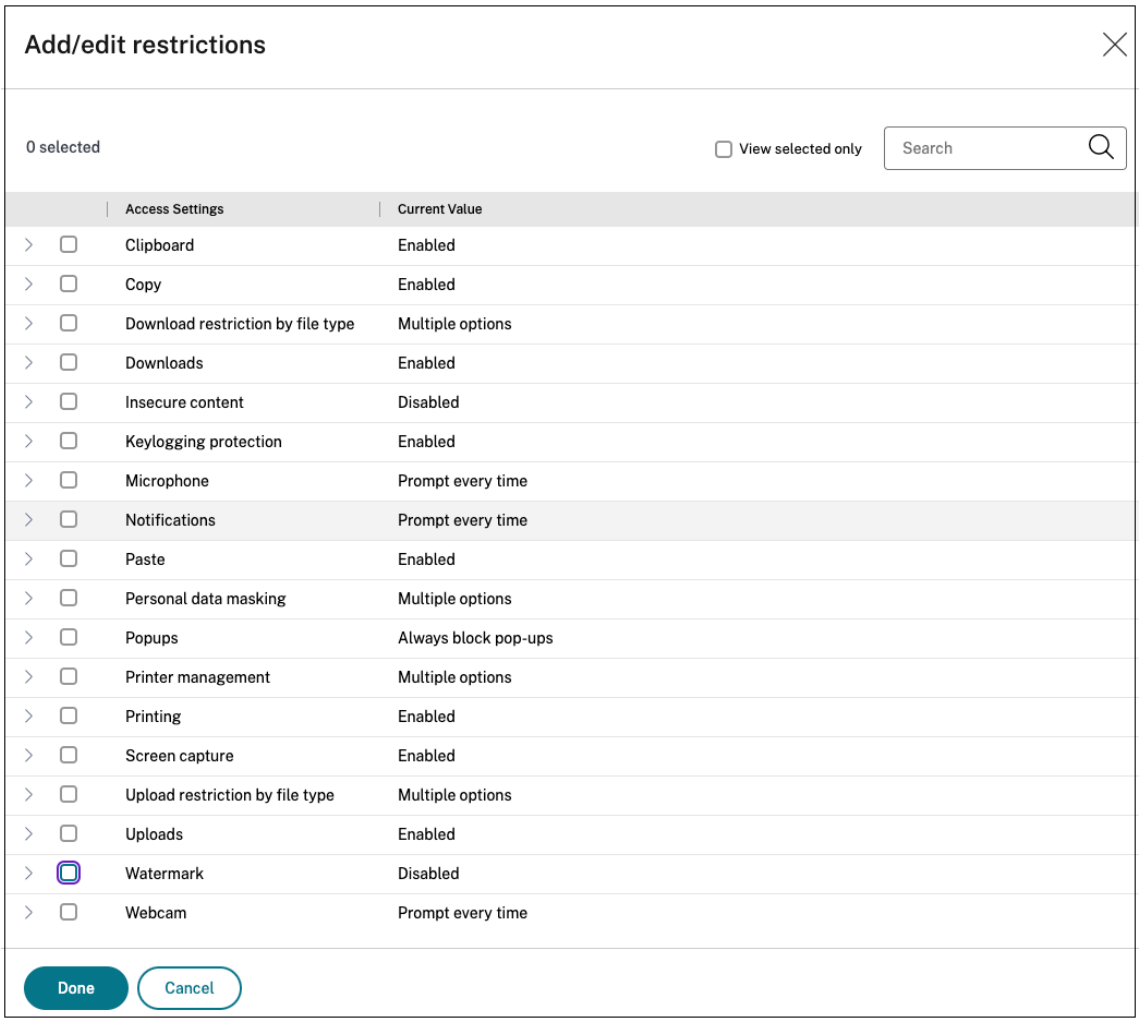
tags:

- **Compliant** - For compliant devices
- **Non-Compliant** - For non-compliant devices

9. 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.



10. Select the restrictions and then click **Done**.
11. 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.

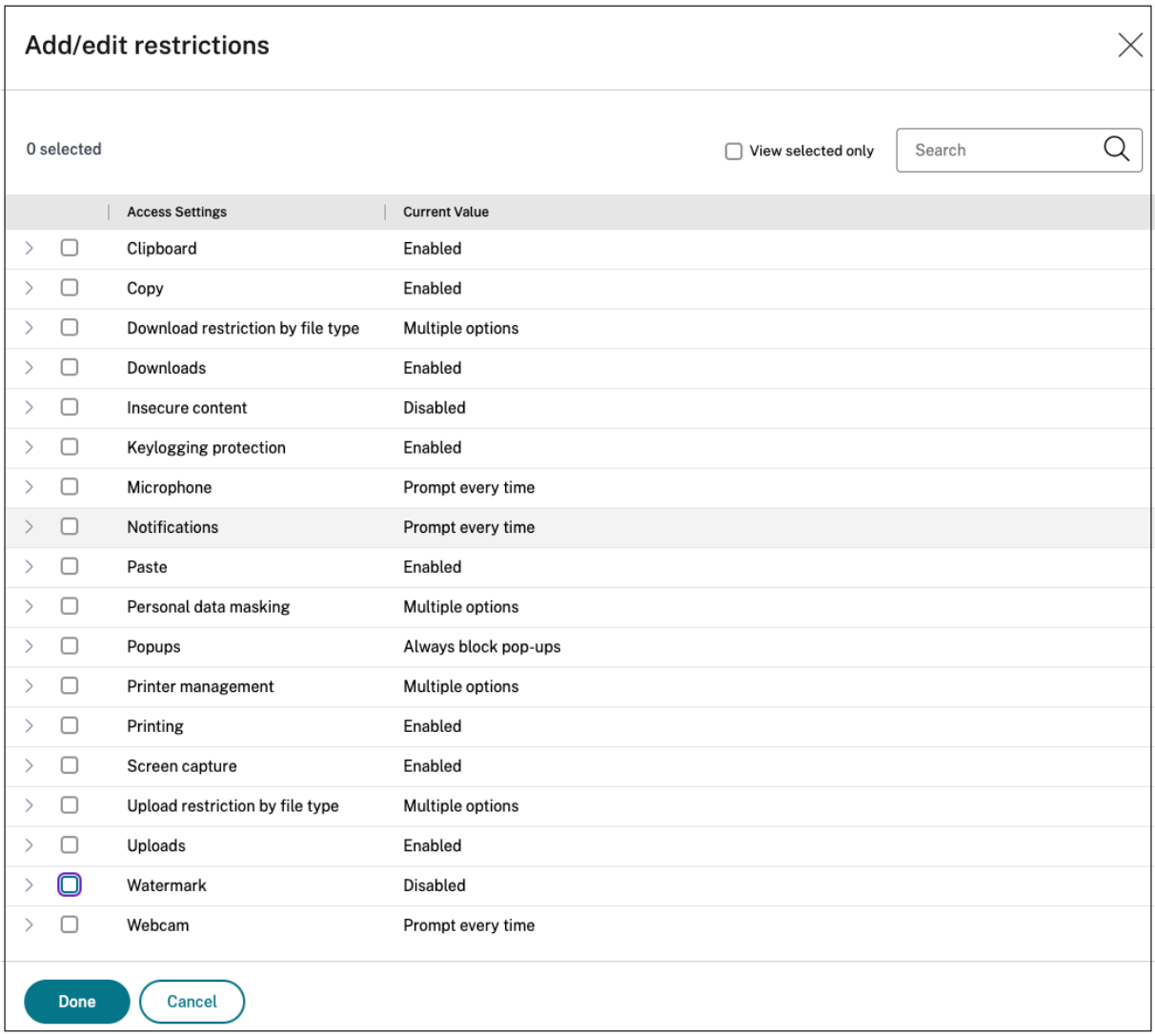
Sample configuration validation

## Access restriction options

September 6, 2025

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




## Clipboard

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

## Copy

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

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

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

### Downloads

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

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

### Download restriction by file type

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

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

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

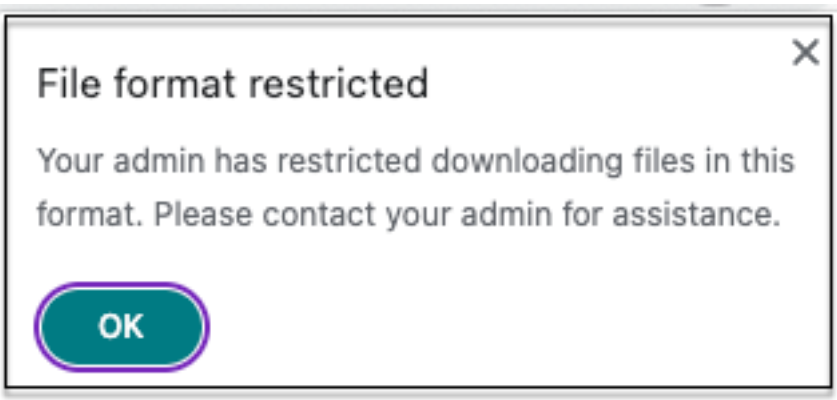
1. Create or edit an access policy. For details on creating an access policy, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Click **Download restriction by file type** and then click **Edit**.

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

   The MIME type now appears in the list of exceptions.

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




### Insecure content

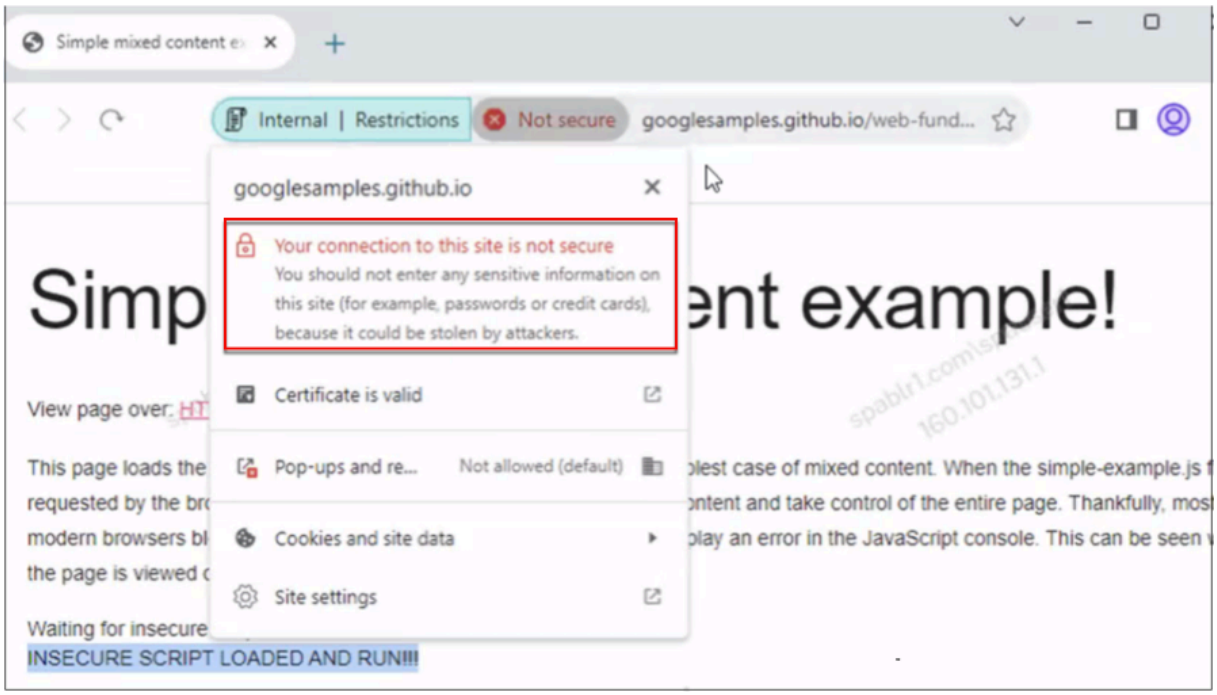
Enable/disable end users from accessing insecure content within the SaaS or internal web app configured with this policy when accessed via Citrix Enterprise Browser. Insecure content is any file linked to from a webpage using an HTTP link rather than an HTTPS link. Default value: Disabled.

To enable viewing insecure content, perform the following steps:

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

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




## Keylogging protection

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

## Microphone

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

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

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

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

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

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

### Notifications

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

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

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

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

### Paste

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

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

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

### Personal data masking

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

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

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

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

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

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

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

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

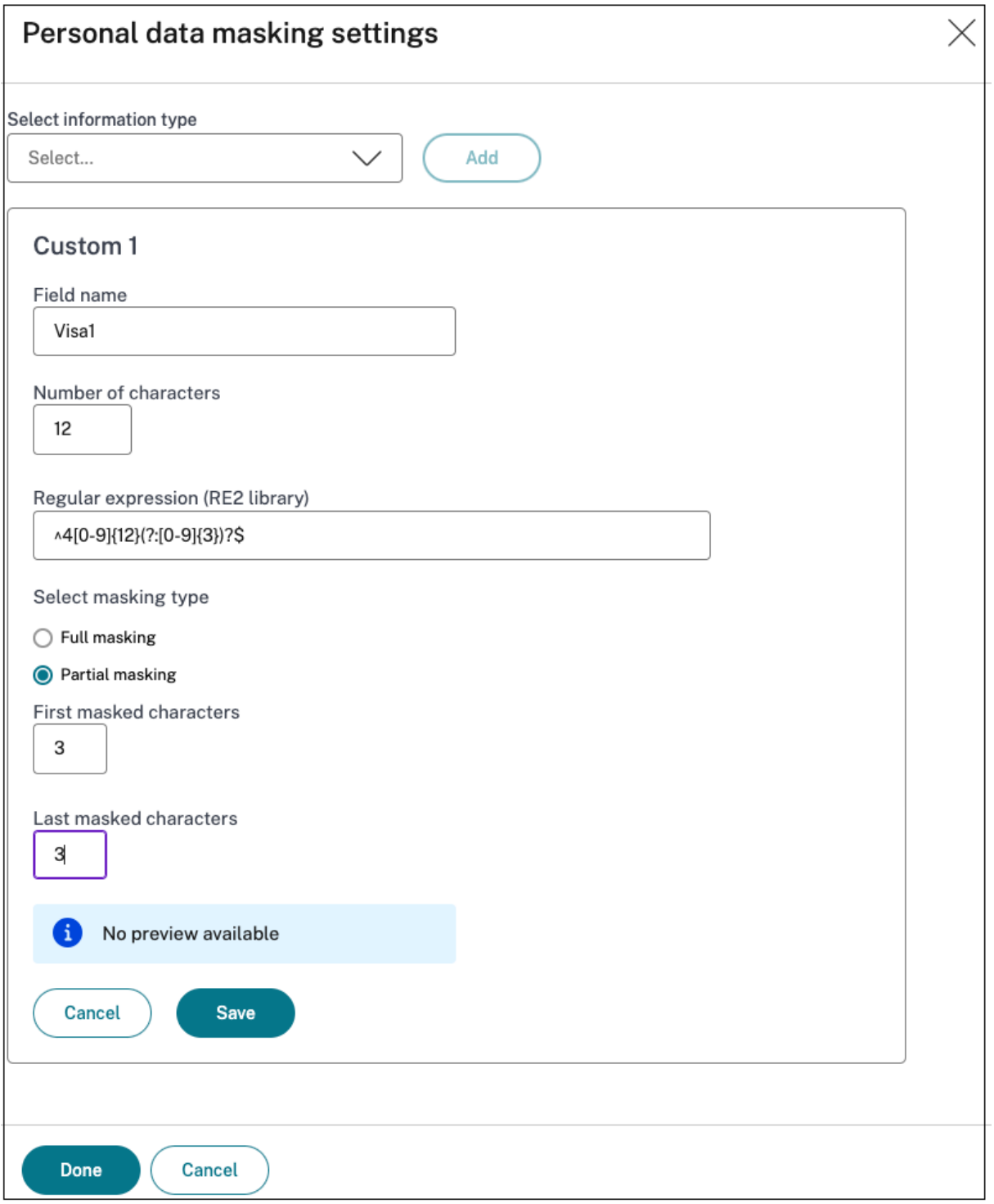
 

### Add custom information type

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

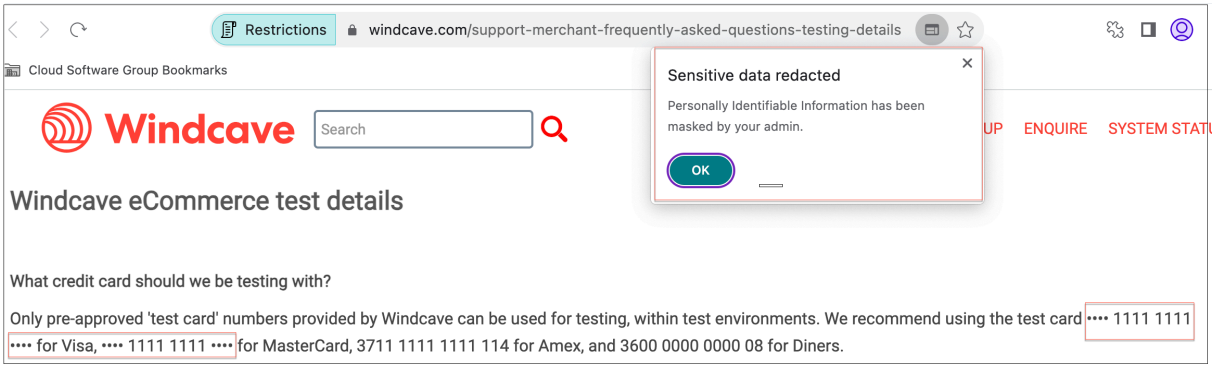
1. In **Select Information type**, select **Custom**, and then click **Add**.
2. In **Field name**, enter the name for the information type that you want to mask.
3. In **Number of characters**, enter the number of characters of the information type.
4. In **Regular Expression (RE2 library)**, enter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




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




## Popups

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

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

To enable display of popups, perform the following steps:

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

## Printing

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

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

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

### Printer management

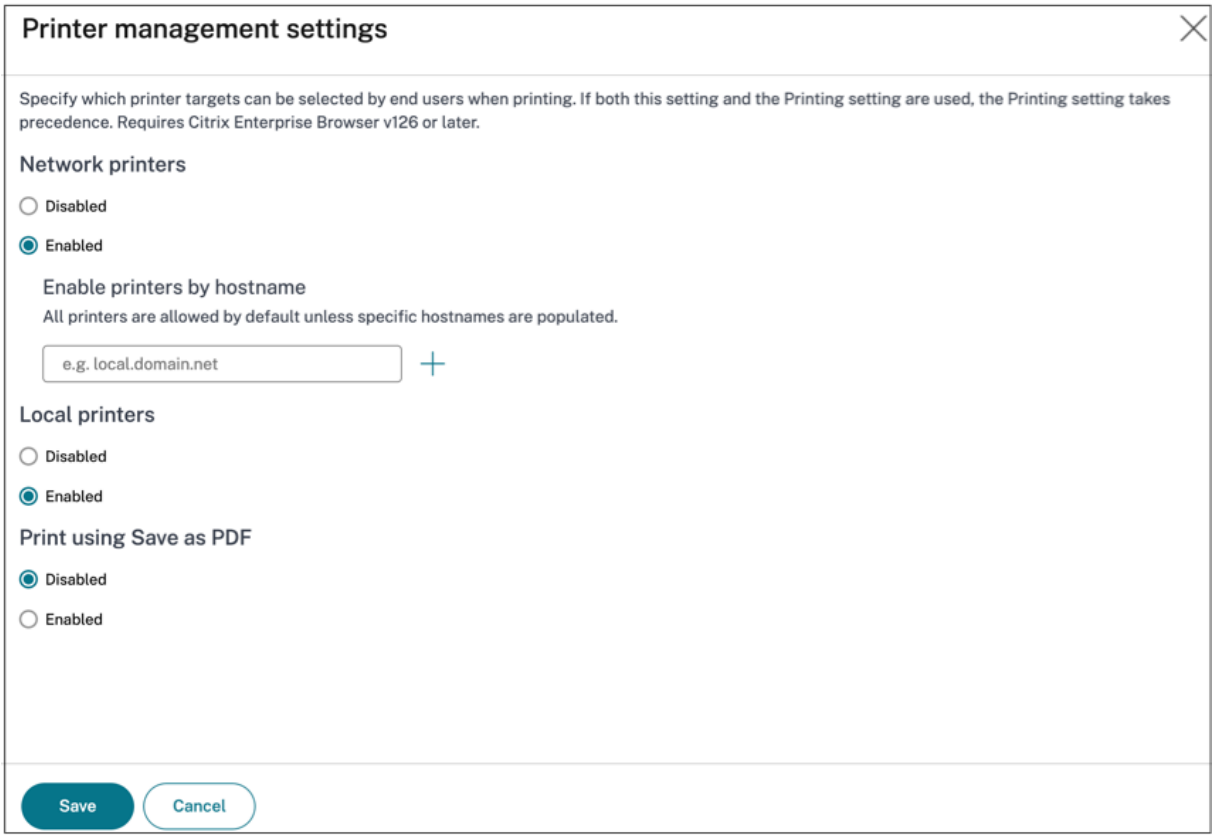
Enable/disable printing data by using the admin-configured printers from the configured SaaS or internal web apps with this policy when accessed via Citrix Enterprise Browser.

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

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

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




1. Select the exceptions as per your requirement.

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

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

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

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

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

   - **Print using Save as PDF**

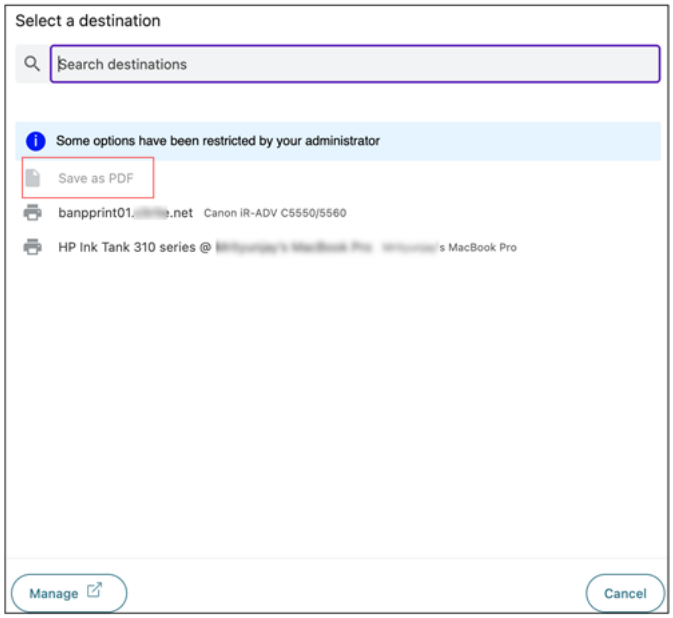
     - **Disabled**: Saving the content from the application in a PDF format is disabled.
     - **Enabled:** Saving the content from the application in a PDF format is enabled.

2. Click **Save**.

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

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




### Screen capture

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

### Upload restriction by file type

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

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

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

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

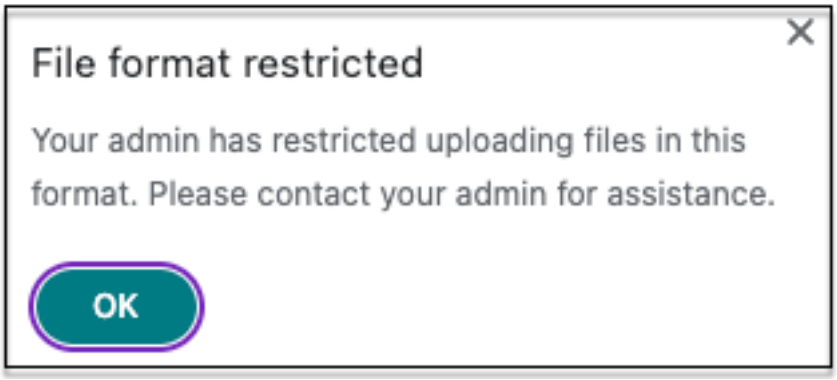
   **Allow all uploads with exceptions** –Upload all files except the selected types.
   **Block all uploads with exceptions** –Blocks all file types from uploading except the selected types.

5. If the file type does not exist in the list, then do the following:

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

   The MIME type now appears in the list of exceptions.

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




### Uploads

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

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

### Watermark

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

### Webcam

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

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

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

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

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

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

### Clipboard restriction for security groups

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

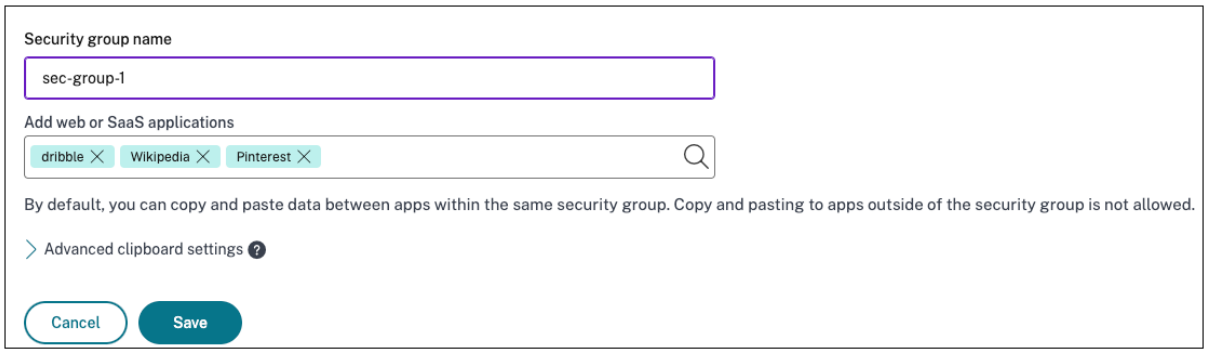
copy and paste operations can be performed. To enable clipboard access within the apps in a security group, you must just have an access policy configured with the action **allow** or **allow with restrictions** without selecting any access setting.

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

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

To create a security group, perform the following steps:

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



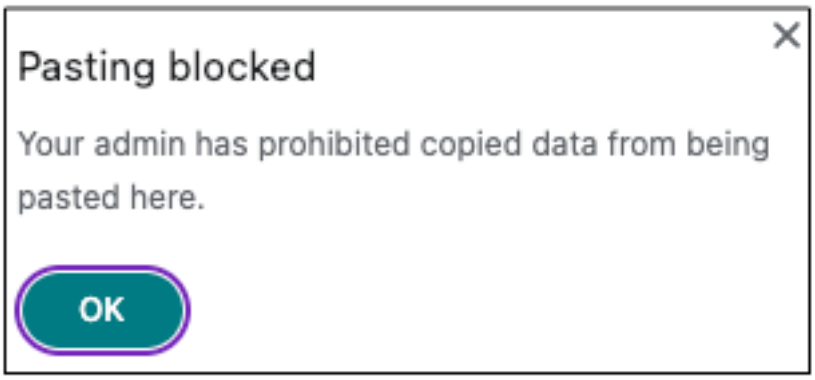

1. Enter a name for the security group.
2. In **Add web or SaaS applications**, choose the applications that you want to group to enable the copy and paste control. For example, Wikipedia, Pinterest and Dribble.
3. Click **Save**.

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

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

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




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

### Enable granular level copy / paste

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

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

**Example:**

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

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

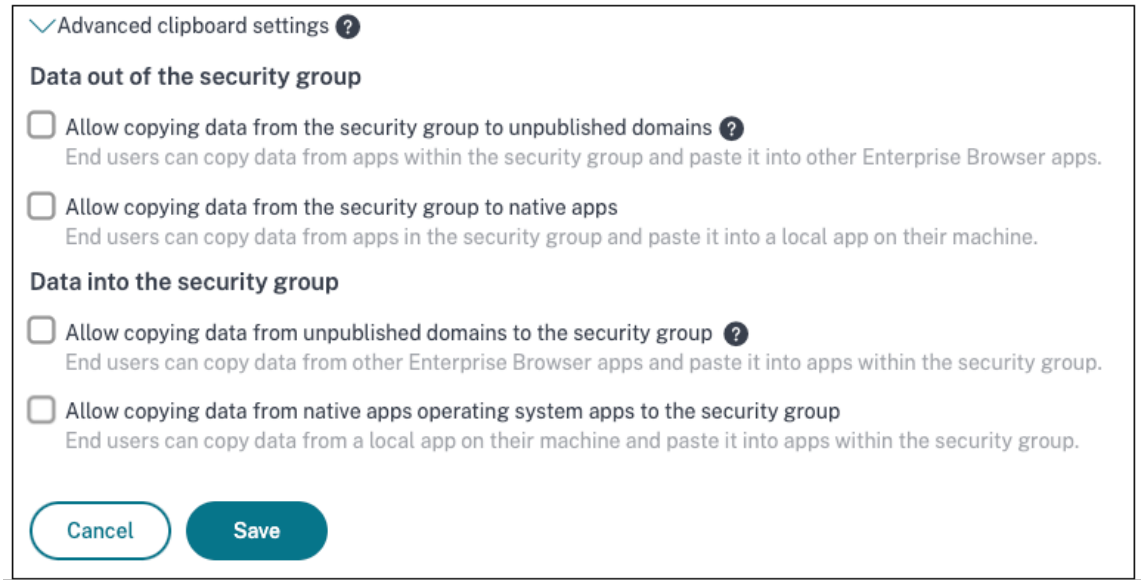
 

1. Create or edit an access policy assigned for the application `Pinterest`. For details on creating an access policy, see Configure access policies.
2. In **Actions**, select **Allow with restrictions**.
3. Select **Paste**.

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


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

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




3. Select the following options as per your requirement:

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

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

### Known issues

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

  For example, assume the following scenario:

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

  In this scenario, if the user tries to copy data from this application into another application in the same security group, the pasting control is disabled. A notification regarding the same is displayed to the user.
- For a SaaS app, the app access can be denied if the application is configured with an access policy with action **Deny access.** The end users can still access the app because the app traffic is not tunneled through Secure Private Access. Also, if the application is part of the security group, the security group settings are not honored and hence you cannot copy / paste content from the application.

## Integration of Citrix Secure Private Access with Google Chrome Enterprise Premium

September 6, 2025

### Solution overview

This integrated solution from Citrix enables customers to use Google Chrome Enterprise Premium as the enterprise browser solution for secure access to private web apps and SaaS applications along

with secure connectivity provided by Citrix Secure Private Access.

The integrated solution is comprised of the following components:

- Google Chrome Enterprise Premium (CEP), which includes features such as Data Leak Prevention (DLP), malware and phishing protection, URL filtering, and Google administration console.
  - The Google Chrome browser running locally on the client machine acts as a managed browser. A managed browser enables a secure browsing experience to the end user and enforces the security controls based on the policies defined by the administrator.
  - The Google Chrome Enterprise Premium console accessed via the Google Cloud portal provides the administration, management, and monitoring console for the Chrome Enterprise Premium security policies.
- Citrix Secure Private Access, which includes Citrix Secure Access™ (CSA), Citrix console including the Secure Private Access console for zero-trust access policies to private applications and Citrix Monitor for monitoring and troubleshooting.
  - The Citrix Secure Access client, running locally on the client machine, enables connectivity to internal applications for the Chrome browser. This client ensures that only traffic originating from the Chrome process is tunneled, as configured by the administrator.
  - The Citrix Secure Private Access service enforces all the access policies configured by the administrator, ensuring that users are only granted access to specific web applications.

### Chrome Enterprise Premium advanced security features

The following are some of the advanced security features offered by Chrome Enterprise Premium:

- **Data loss prevention (DLP):** Implement granular controls and policies to prevent sensitive data from being leaked or accidentally shared.
- **Malware deep scanning:** Advanced scanning techniques are used to detect and quarantine unknown or high-risk files, preventing the execution of malicious code and protecting against zero-day attacks.
- **Phishing protection:** Safeguard users from visiting harmful websites by identifying and blocking phishing attempts, preventing the theft of login credentials and personal information.
- **URL categorization and filtering:** Restricts access to websites based on their content category, preventing users from accessing inappropriate or malicious content.
- **Web usage insights and analytics:** Provides detailed reports and analytics on web traffic, allowing administrators to monitor user activity, identify potential security threats, and optimize network bandwidth.

For more information, see Chrome Enterprise Premium overview.

### Prerequisites for the integrated solution

To ensure optimal integration between the Citrix Workspace™ application and Chrome Enterprise Premium, the following prerequisites must be implemented. Successful completion of these prerequisites will result in a more efficient and seamless experience when launching applications from the Citrix Workspace app or the web-based user interface.

- **Configure Chrome browser to a managed Chrome browser:** Ensure that the users'Chrome browser is managed by the organization. For details, see Enroll cloud-managed Chrome browsers. See the notes on the importance of Chrome being managed for proper integration.
- **Set Chrome as the default browser:** We recommend that you set Chrome as your default browser or remove all other browsers from your device except Chrome. For details, see Set Google Chrome as your enterprise browser. See the notes on the importance of Chrome being the default system browser for proper integration.
- **Use only managed devices:** The devices used to access the applications must be managed by the organization. Otherwise, Chrome enrollment and Chrome being the default browser cannot be enforced at scale. To enforce this policy, administrators can use the Citrix endpoint analysis or the Citrix Device Posture service. These tools can assess the device's management status and compliance with the organization's security requirements.
- **Install Citrix Secure Access client:** To access applications via Google Chrome, users must use managed devices that have the Citrix Secure Access client installed. The Citrix Secure Access client enhances security and control by monitoring and controlling internal web app traffic on devices, permitting access only if the traffic originates from the managed Chrome browser.

  Users without the Citrix Secure Access client installed or those using unmanaged devices, can only access applications via Citrix Enterprise Browser.

  The following client versions support the integration of Chrome Enterprise Premium with Citrix Secure Private Access:

  - Windows - 25.4.1.9 and later
  - macOS - 25.03.1 and later

- **Create or recreate policies and security controls:** Policies and security controls configured in the Secure Private Access console only apply to Citrix Enterprise Browser. When Google Chrome is set as the enterprise browser, security controls must be configured as policies and rules in the Google Admin console.

  - Policies are configured in the **Google Admin console > Devices > Chrome > Settings**. These settings allow you to manage browser settings, such as block javascript and allow list of printers.

  - Rules are configured in **Google Admin console > Rules**. These rules are advanced settings related to DLP, such as adding a watermark, blocking the download of files with social security numbers, and URL filtering.

> **Notes:**
>
> - The Chrome browser must be set as the default browser. Otherwise, the Citrix Workspace app launches the default system browser instead of Chrome Enterprise Premium browser.
> - The Citrix Secure Access client only validates that the traffic originates from the Chrome browser. This implies that the DLP rules cannot be enforced at the granular level of individual user profiles within the browser. Hence, DLP rules must be configured at a managed browser level rather than at a managed profile level. This approach ensures that all traffic passing through the Chrome browser, regardless of the specific user profile in use, is subject to the same set of DLP rules.
> - Access rules for external web/SaaS apps must be configured via Google Chrome policy configuration.
> - Google Chrome's policy configuration is limited to **Allow** or **Deny** access options. The **Allow with restriction** option is supported in Citrix Enterprise Browser but is not supported in Google Chrome and must be functionally interpreted as **Allow.**
>
> For details on creating policies and rules for Google Chrome in the Google Workspace Admin console, see the following topics:
>
> - Set Chrome Enterprise connector policies for Chrome Enterprise
> - Data protection rules

### ICA® Proxy settings in a SPA hybrid deployment

In a hybrid deployment, to use Google Chrome as Workspace for Web (that is, enumerate and launch Secure Private Access apps through the Chrome browser), you must perform the following configuration changes related to ICA Proxy on NetScaler® Gateway:

**Enable ICA Proxy for Workspace for Web:**

**Using the NetScaler GUI:**

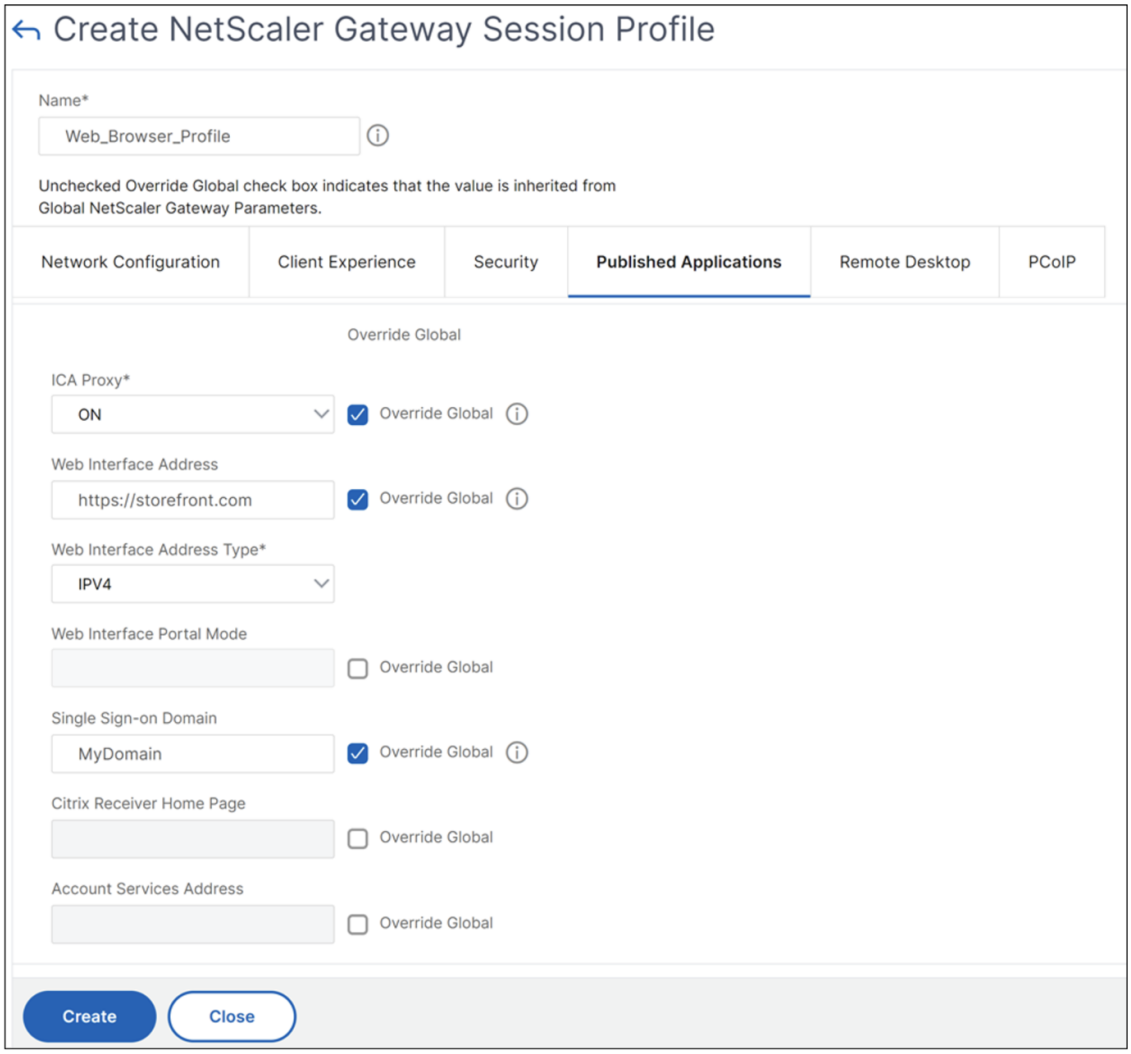
1. Navigate to **Configuration > NetScaler Gateway > Policies > Session**.
2. Create a session profile or edit an existing session profile for Workspace for Web.

> **Note:**
>
> The Workspace for Web session policy usually has the following rule:

> HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("plugin").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixSecureAccess").NOT.

3. In the NetScaler Gateway Session Profile page, click the **Published Applications** tab.
4. In **ICA Proxy**, click **On**.




For details, see Create a session policy for web browser-based access.

**Using the CLI:**

Use the following sample command as a reference to enable ICA Proxy:

```
add vpn sessionAction Web_Browser_Profile -transparentInterception
OFF -SSO ON -ssoCredential PRIMARY -useMIP NS -useIIP OFF -icaProxy
 ON -wihome "https://storefront.mydomain.com/Citrix/MyStoreWeb"-
ClientChoices OFF -ntDomain mydomain.com -defaultAuthorizationAction
```

```
 ALLOW -authorizationGroup SecureAccessGroup -clientlessVpnMode
ON -clientlessModeUrlEncoding TRANSPARENT -SecureBrowse ENABLED -
storefronturl "https://storefront.mydomain.com"-sfGatewayAuthType
domain
```

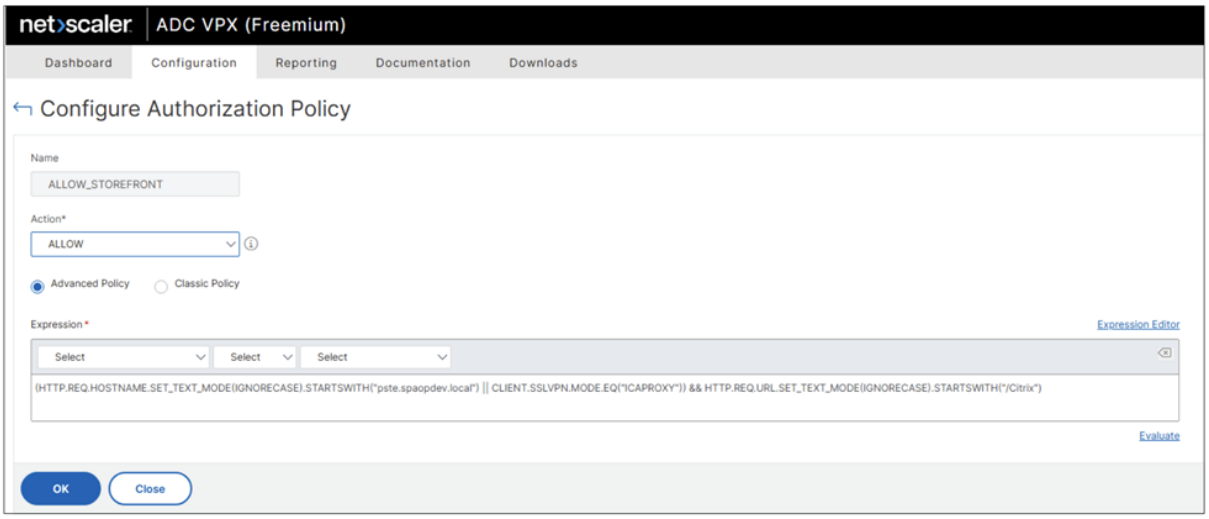
Ensure that this session action is bound to a session policy for Workspace for Web.

**Configure the authorization policy to allow ICA Proxy traffic:**

**Using the GUI:**

1. Navigate to **NetScaler Gateway > Policies > Authorization**.
2. Create an authorization policy or edit an existing policy.
3. In **Action**, select **Allow**.
4. In **Expression**, click **Expression Editor**.
5. Configure the expression - click **Select** and choose the necessary elements.
6. Click **OK**.

For details, see Configuring Authorization Policies.




**Using the CLI:**

Use the following sample command as a reference to allow ICA Proxy traffic:

```
add authorization policy ALLOW_STOREFRONT "(HTTP.REQ.HOSTNAME.SET_TEXT_MODE
(IGNORECASE).STARTSWITH(\"storefront.mydomain.com\")||CLIENT.SSLVPN
.MODE.EQ(\"ICAPROXY\"))&&HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).
STARTSWITH(\"/Citrix\")"ALLOW
```

### Synchronize user directory configured in Citrix Workspace with the Google Cloud user directory

We recommend that you synchronize the user directory configured in Citrix Workspace or StoreFront with the Google Cloud user directory. While it is not a requirement for managing per-user access to web and SaaS apps when using the managed browser configuration in Chrome, it is a requirement for managing some security controls and gathering per-user/user group usage insights within the Google Chrome Enterprise Premium console.

Specifically the following features require synchronization of the user identities from your local user directory configured in Citrix with the Google Cloud user directory:

- Per-user and user group based Data Loss Prevention (DLP) controls and other security policies within Google Chrome Enterprise Premium.
- Per-user and user group based endpoint verification and enforcement within Google Chrome Enterprise Premium.
- Per-user and user group based security insights in the Google Chrome Enterprise Premium console.
- Using a managed profile with a corporate account for Chrome profile synchronization of bookmarks, history, settings, and so on.

For more information, see Google Directory sync.

### Set Google Chrome as your enterprise browser

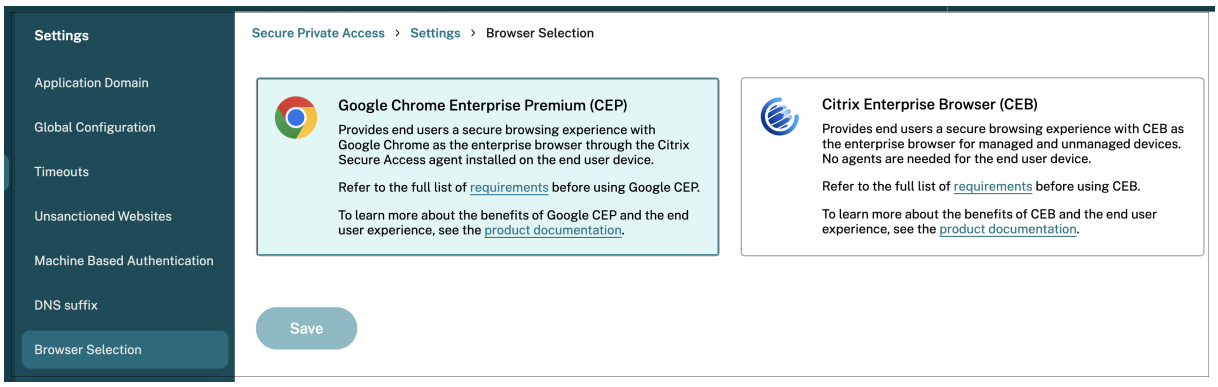
You can set Google Chrome as your default enterprise browser from the Secure Private Access admin console.

> **Note:**
>
> Citrix Enterprise Browser functions as the default enterprise browser unless the setting is changed to Google Chrome in the Secure Private Access administration console.

Perform the following steps:

1. Log on to Citrix Cloud™ and then click **Secure Private Access**.
2. Click **Settings** and then click **Browser Selection**.
3. Click **Google Chrome**.




**Note:**

- You can switch between Citrix Enterprise Browser and Google Chrome at any time.
- Global application configuration service (GACS): (Not applicable for hybrid deployments) When using Citrix Workspace with GACS, the **App Configuration > Citrix Enterprise Browser** setting in Workspace Configuration determines whether the target URL opens in Citrix Enterprise Browser or Google Chrome. Ensure that the **Open All SaaS Apps Through Citrix Enterprise Browser** setting is disabled. For details on disabling this setting, see Manage Citrix Enterprise Browser through Global App Configuration service. Also, Google Chrome must still be set as the default system browser as per the guidelines in Prerequisites for the integrated solution.
- Disabling the enterprise browser setting in Workspace Configuration prevents the enforcement of security controls, causing all applications to launch in the device's native browser. Hence, Google Chrome must be set as the default system browser as per the guidelines in Prerequisites for the integrated solution.

## Considerations prior to switching browser

Note the following prior to switching browsers:

- When you switch between Google Chrome and Citrix Enterprise Browser, you must log out of the Citrix Secure Access client and login again because switching between browsers does not terminate the Citrix Secure Access session. As a result, app launches might not work as intended.
- Chrome cannot enforce access to SaaS apps, because these apps are not tunneled through Citrix Secure Private access. To enable SaaS app access enforcement with Chrome and prevent the use of other browsers, route these apps through the Citrix Secure Private Access tunnel by changing the app routing type to **Internal.** For details, see Steps to change the routing type or resource location.
- When Google Chrome is used as the enterprise browser, DLP policies and security controls configured in Citrix Secure Private Access are not enforced. Therefore, all necessary security poli-

cies must be recreated in the Google Admin console to maintain consistent data protection. For details, see Prerequisites for the integrated solution.

- The URL filtering (Unsanctioned websites) feature is not supported when using Chrome as the enterprise browser. Any URL filtering policies must be recreated within the Google Admin console.

## Citrix Secure Private Access - Supported deployment modes

The integrated solution supports the following deployment modes from Citrix Secure Private Access:

- **Citrix Secure Private Access service:** This deployment mode utilizes the fully cloud-managed Citrix Secure Private Access service. All components, including the control plane and gateway infrastructure, are hosted and managed by Citrix. For more information, see Citrix Secure Private Access.
- **Citrix Secure Private Access hybrid deployment:** This deployment allows customers to implement a Zero Trust Network Access (ZTNA) solution using on-premises StoreFront and NetScaler Gateway components and use the Citrix Cloud for managing the configuration, administration, and monitoring functions. This means customers can leverage existing NetScaler Gateway on-premises to control user traffic routing while using Citrix Cloud hosted UI for management of configurations and policies. Also, use Citrix Monitor hosted in the Citrix Cloud for monitoring and troubleshooting functions. For more information, see Citrix Secure Private Access hybrid deployment.

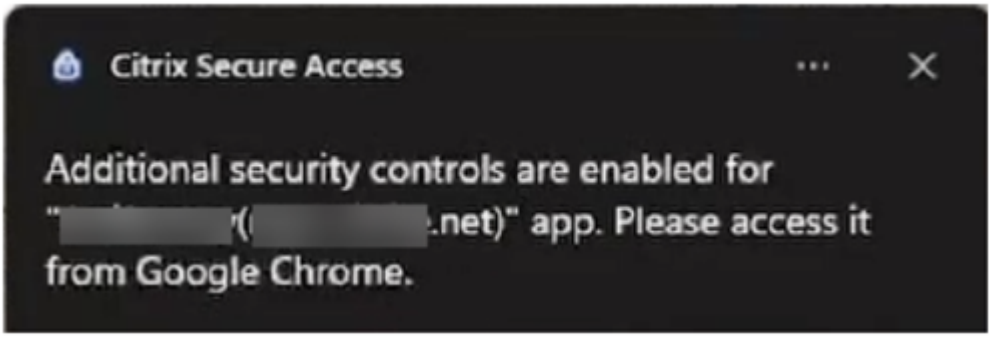
## End user experience

### Google Chrome as your enterprise browser

When Google Chrome is your enterprise browser, application launches and security control enforcement vary based on the application types.

- **Published apps:**
  - Citrix Workspace app: Applications launched from the Citrix Workspace app open in the default system browser. If the recommendations as suggested in Prerequisites for the integrated solution are followed, the default system browser is Chrome, with security controls being enforced within that browser environment.
  - Other browsers: Launching the same application from other browsers, such as Firefox or Microsoft Edge is blocked. A pop-up notification from Citrix Secure Access clients appears asking the user to use Google Chrome.




- **Internet apps:** The browser setting does not affect the general internet applications. These applications can be launched from any browser, including Google Chrome.

#### Citrix Enterprise Browser as your enterprise browser

When Citrix Enterprise Browser is your enterprise browser, application launches and security controls enforcement remain unaffected.

- **Launch apps from Citrix Workspace app:**
  - The application is launched using the Citrix Enterprise Browser.
  - Any security controls that have been enabled for the application are enforced accordingly.
- **Launch apps from Citrix Secure Access:**
  - After the connection is established, open Chrome and launch the same app.
  - Any security controls that have been enabled for the app are enforced accordingly.

> **Note:**
>
> If you attempt to access the same application using a different browser (for example Firefox or Edge), you can still access the application, but the security controls are not enforced.

### End-user application access methods

The following table summarizes the end user experience when the applications are accessed using various methods:

| User access mode | Workspace (StoreFront™ in cloud) | StoreFront in on-premises |
|---|---|---|
| Citrix Workspace app (CWA) | Apps are enumerated on the workspace portal | Apps are enumerated on the StoreFront portal |

| User access mode | Workspace (StoreFront™ in cloud) | StoreFront in on-premises |
|---|---|---|
| Chrome (system browser) | The applications are launched in Chrome<br>Citrix Secure Access tunnels the application access<br>Apps are enumerated on the workspace portal | The applications are launched in Chrome<br>Citrix Secure Access tunnels the application access<br>Apps are enumerated on the StoreFront portal |
| Browser other than Chrome | The applications are launched in Chrome<br>Citrix Secure Access tunnels the application access via Secure Private Access<br>Access denied for private apps<br>Windows client: Citrix Secure Access blocks app access<br>macOS client: Admins can use tools like Jamf to block use of other browsers besides Chrome | The applications are launched in Chrome<br>Citrix Secure Access tunnels the application access via Secure Private Access<br>Access denied for private apps<br>Windows client: Citrix Secure Access blocks app access<br>macOS client: Admins can use tools like Jamf to block use of other browsers besides Chrome |

### Legal

Chrome Enterprise Premium is provided by Google LLC and your use is subject to Google's Acceptable Use Policy and Service Specific Terms.

## End user flow

September 6, 2025

### SaaS app

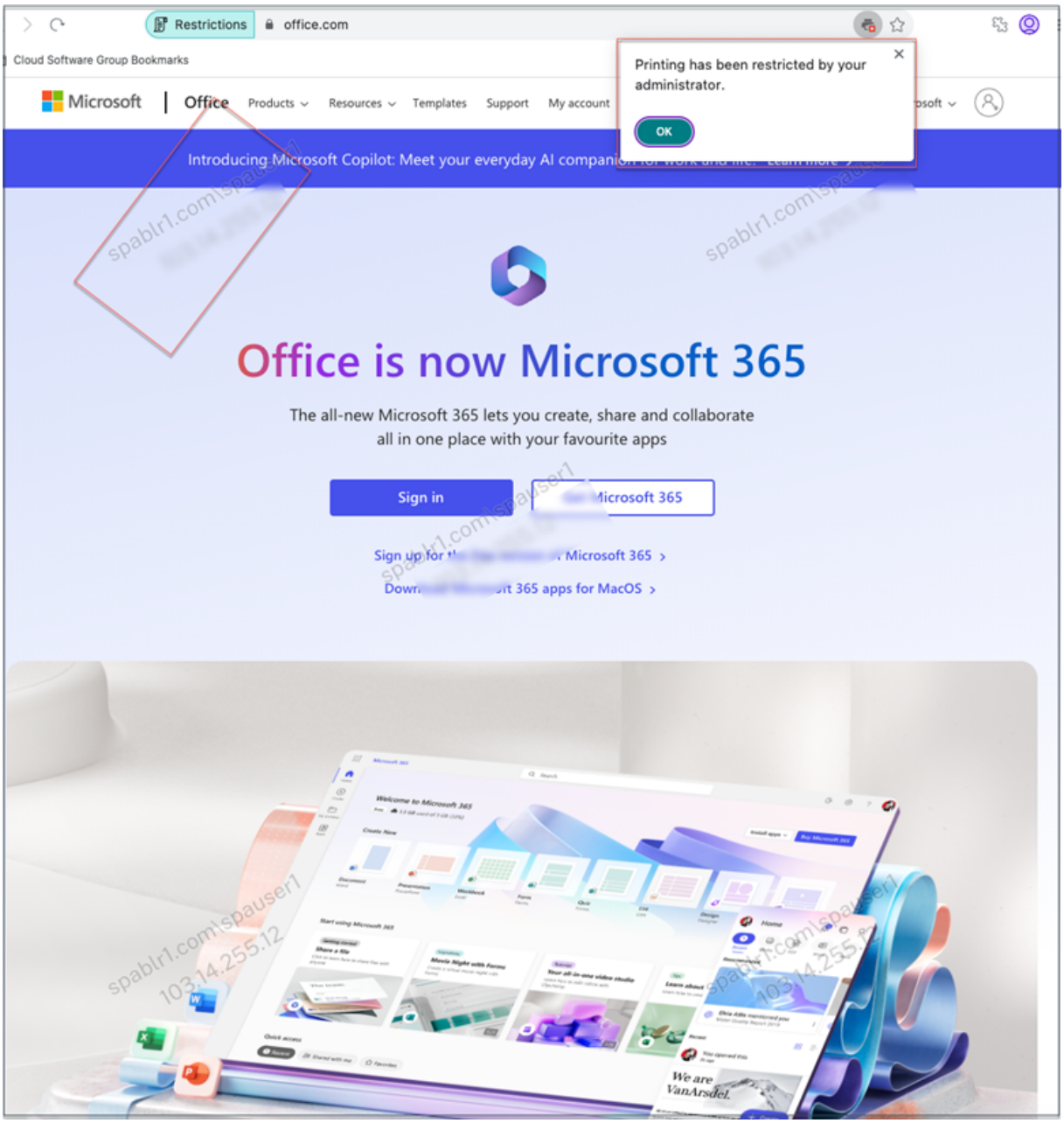
Assume that an admin has configured the Office 365 app with the watermark and print restriction for the end user. Now, when the end user accesses the Office 365 app, the watermark and print restrictions must be applied on the app.

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

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

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

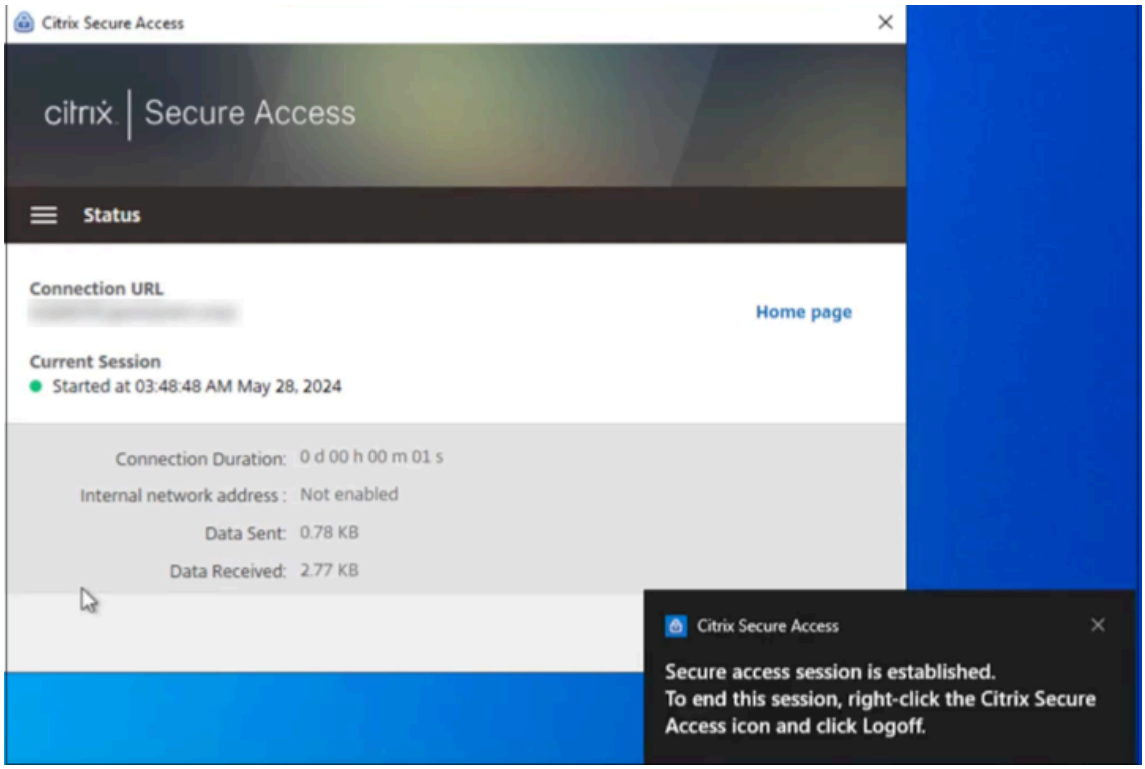


> **Note:**
>
> Administrators must provide users with the account information that they need to access virtual desktops and applications. For details, see Adding store URL to Citrix Workspace app.

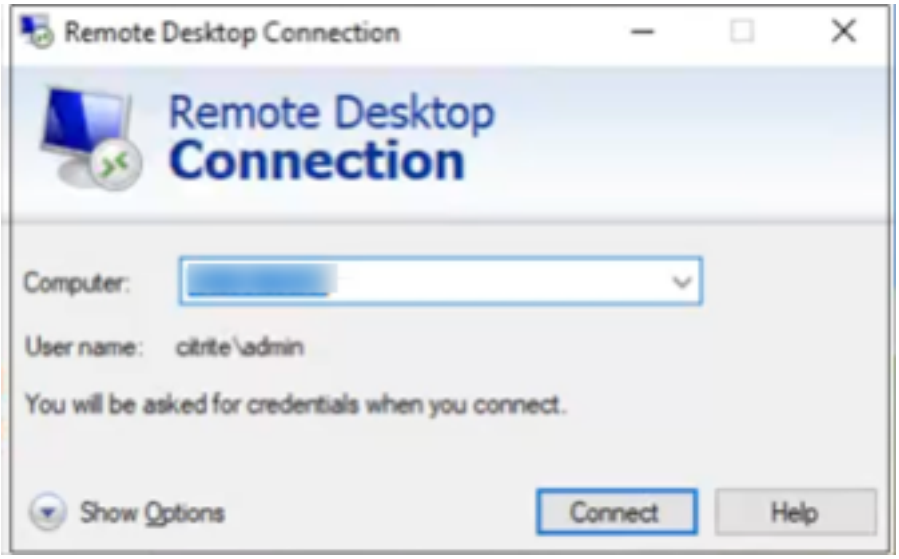
### TCP/UDP app

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

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






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

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

## Advanced features

September 6, 2025

Secure Private Access service supports the following advanced features.

**Policy modeling tool:** The policy modeling tool (**Access policies > Policy modeling**) provides the administrators full visibility into the expected application access result (allowed/allowed with restriction/denied). Admins can check the access results for specific users and add a user condition for contextual tags. For details, see Policy modeling tool.

### Application Discovery

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

as applications, providing access to those users. For details, see Discover domains or IP addresses accessed by end users.

### Policy modeling tool

The policy modeling tool (**Access policies > Policy modeling**) provides the administrators full visibility into the expected application access result (allowed/allowed with restriction/denied). Admins can check the access results for specific users and add a user condition for contextual tags. For details, see Policy modeling tool.

### Support for unsanctioned websites

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. For details, see Unsanctioned websites.

## Device Posture checks on on-premises NetScaler® Gateway

September 6, 2025

Citrix Device Posture service is a cloud-based solution that helps admins enforce certain requirements that the end devices must meet to gain access to Citrix Secure Private Access resources, such as SaaS/Web and TCP/UDP apps. Establishing device trust by checking the device's posture is critical for implementing zero-trust-based access. Device Posture service enforces zero trust principles in your network by checking the end devices for compliance (managed/BYOD and security posture) before allowing an end user to log in. For details on the Device Posture service, see Device Posture.

### Entitlements

The Device Posture service is available as part of the Universal Hybrid Multi Cloud (UHMC) license and Citrix Platform License (CPL). For more information, see https://www.citrix.com/buy/licensing/product.html.

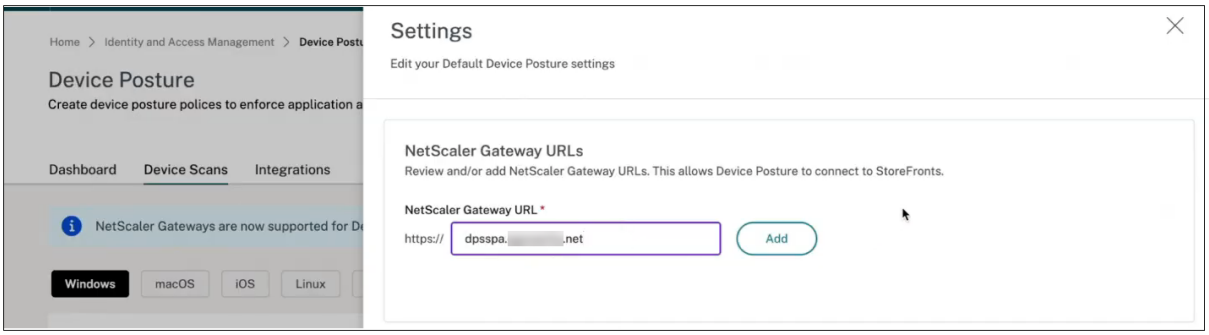
### Enable Device Posture for Secure Private Access hybrid solutions

Integration of the Device Posture service with Secure Private Access for hybrid solutions is supported only from NetScaler Gateway release 14.1 build 43.x. The Device Posture feature must be enabled on NetScaler Gateway for the Device Posture scans to function in the Secure Private Access hybrid deployment.

For details on enabling Device Posture checks on NetScaler Gateway, see Device Posture checks on NetScaler Gateway.

In addition to enabling the Device Posture feature on NetScaler Gateway, you must add the URL of NetScaler Gateway accessing StoreFront™ in the Device Posture **Settings** page.

1. In the Secure Private Access admin console navigation pane, click **Device Posture**.
2. In the **Device Scans** page, click **Settings**.
3. In **NetScaler Gateway URL**, enter the FQDN of the virtual server for which the Device Posture checks must be enabled. For example, `https://gw.example.net`.




## Discover domains or IP addresses accessed by end users

September 6, 2025

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

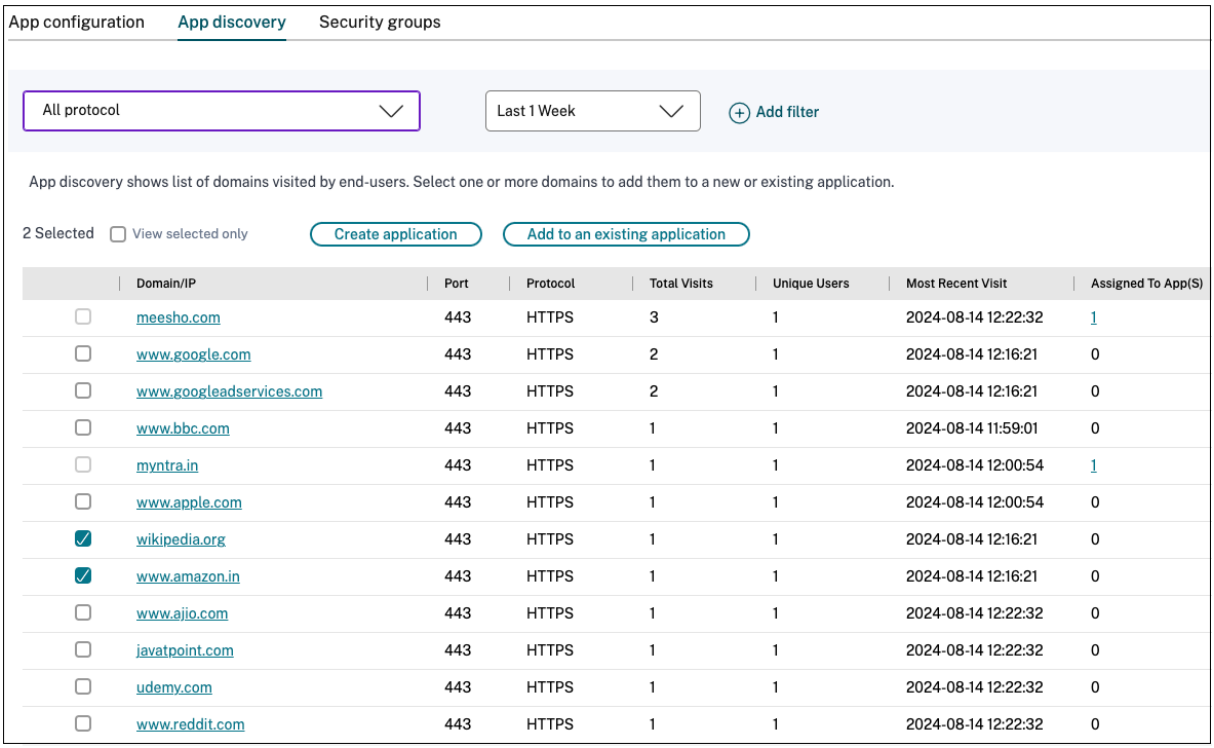
The Application Discovery feature provides the following capabilities to the admins:

- Provides visibility into both internal or external domains/IPs addresses accessed by the end users.

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

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




| Domain/IP | Port | Protocol | Total Visits | Unique Users | Most Recent Visit | Assigned To App(S) |
|---|---|---|---|---|---|---|
| meesho.com | 443 | HTTPS | 3 | 1 | 2024-08-14 12:22:32 | 1 |
| www.google.com | 443 | HTTPS | 2 | 1 | 2024-08-14 12:16:21 | 0 |
| www.googleadservices.com | 443 | HTTPS | 2 | 1 | 2024-08-14 12:16:21 | 0 |
| www.bbc.com | 443 | HTTPS | 1 | 1 | 2024-08-14 11:59:01 | 0 |
| myntra.in | 443 | HTTPS | 1 | 1 | 2024-08-14 12:00:54 | 1 |
| www.apple.com | 443 | HTTPS | 1 | 1 | 2024-08-14 12:00:54 | 0 |
| wikipedia.org | 443 | HTTPS | 1 | 1 | 2024-08-14 12:16:21 | 0 |
| www.amazon.in | 443 | HTTPS | 1 | 1 | 2024-08-14 12:16:21 | 0 |
| www.ajio.com | 443 | HTTPS | 1 | 1 | 2024-08-14 12:22:32 | 0 |
| javatpoint.com | 443 | HTTPS | 1 | 1 | 2024-08-14 12:22:32 | 0 |
| udemy.com | 443 | HTTPS | 1 | 1 | 2024-08-14 12:22:32 | 0 |
| www.reddit.com | 443 | HTTPS | 1 | 1 | 2024-08-14 12:22:32 | 0 |

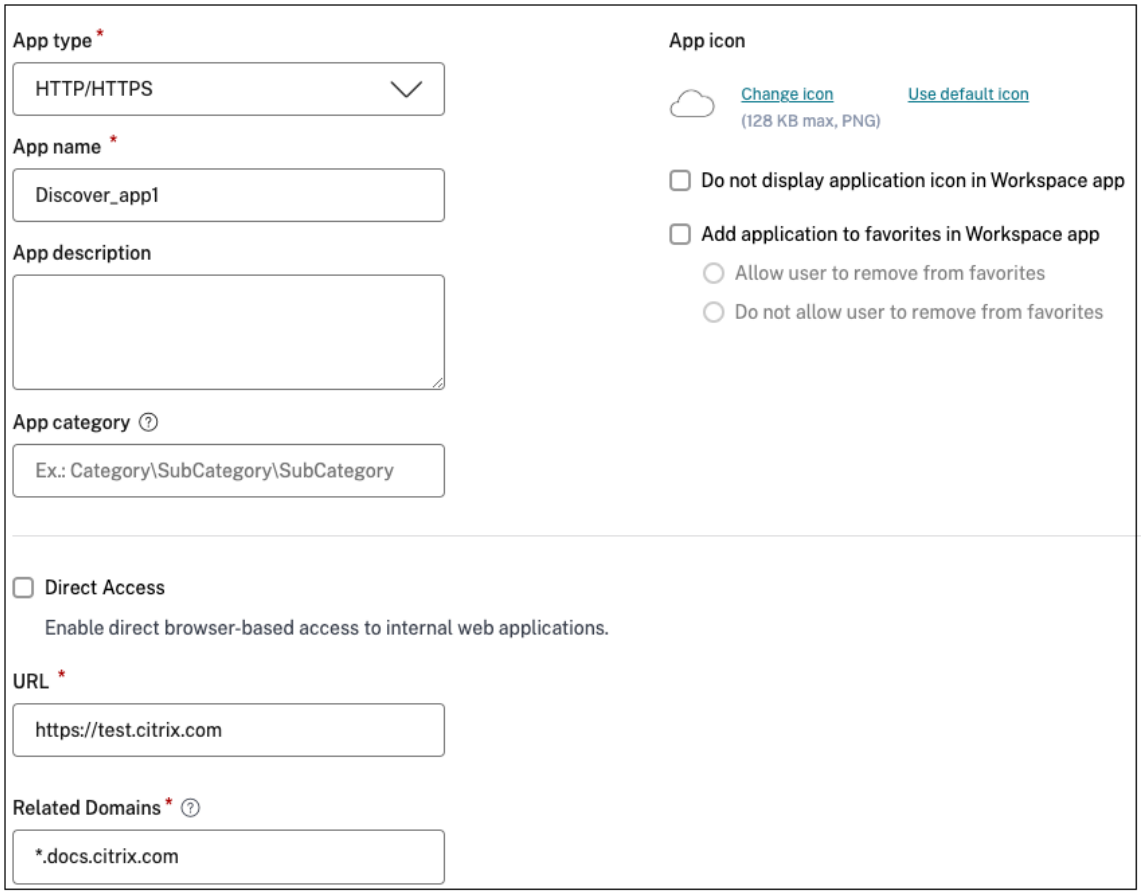
## Application Discovery for internal domains in a new environment

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

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

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



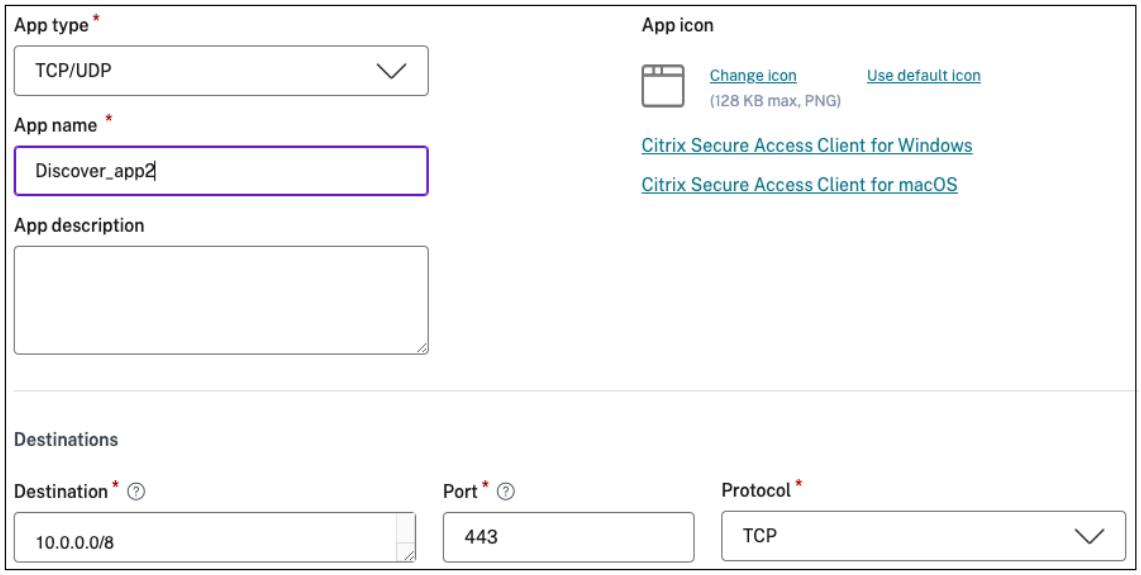

Web app URL: `https://test.citrix.com/`
Related domain: `*.citrix.com`

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

  Port: (*)

  Protocol: TCP




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

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

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

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

### Create an application from the App discovery page

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

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

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

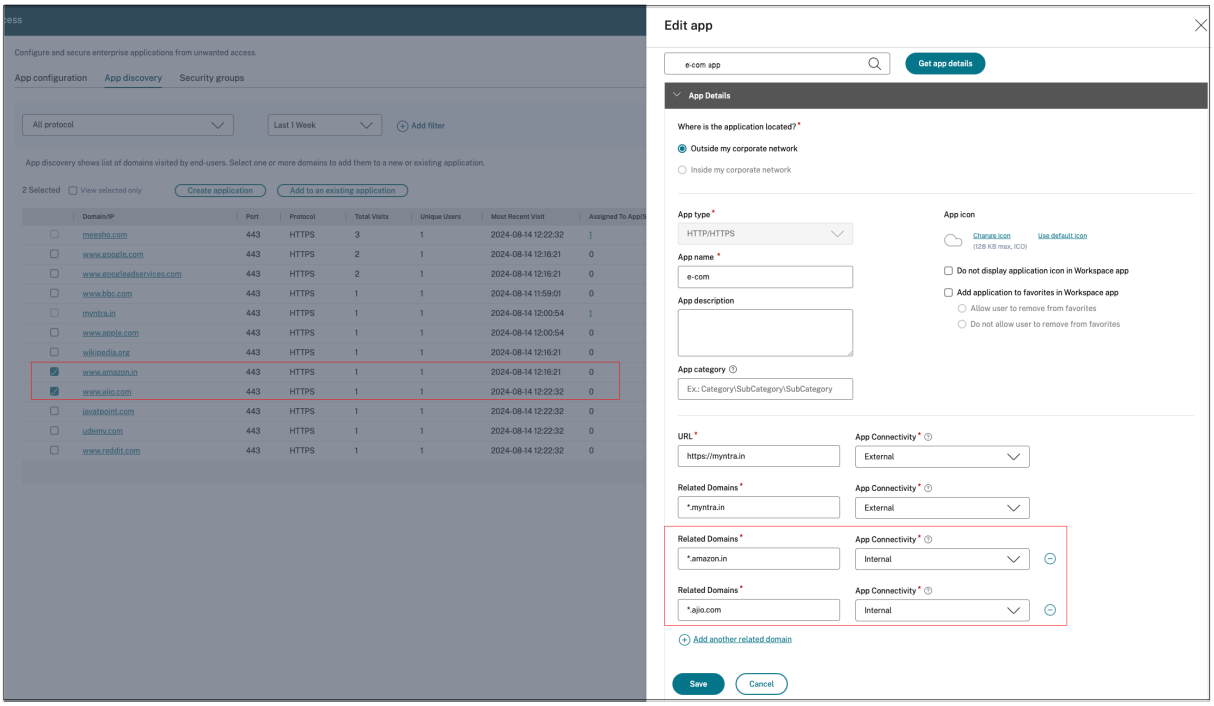
3. Click **Create application**. For details on creating an application, Configure HTTP/HTTPS applications and Configure TCP/UDP apps.

### Update an existing application

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

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




**Note:**

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

## Policy modeling tool

September 6, 2025

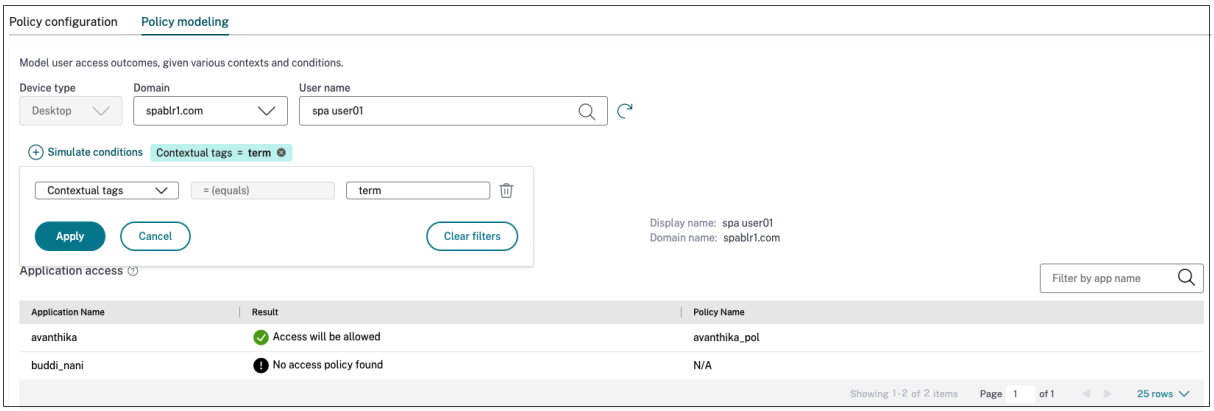
Admins can create multiple policies and assign these policies to multiple applications. As a result, it might become difficult for admins to understand the application access results for their end-users. That is, if the end-user is allowed or denied access based on the application and access policy configurations.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

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

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

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




## Configuration reports

September 6, 2025

Customer administrators can generate configuration reports to gain insights into the Secure Private Access site's setup. The configuration report includes information for the following categories:

- Access policies governing access to applications and resources.
- Applications configured within Secure Private Access.
- Routing domains set up for the applications.
- Resource locations associated with the customer.

- Secure Private Access site configuration details such as the following:
  - Secure Private Access site address
  - StoreFront™ store URLs
  - Gateway URLs
  - License Server URL
  - Director URL

The configuration reports can be used in the following scenarios:

- Identify and resolve configuration issues.
- Share with the Citrix Support team for investigation and troubleshooting purposes.
- Use the report as a reference to set up new sites or modify existing site details.

## Generate a configuration report

Perform the following steps to generate a configuration report:

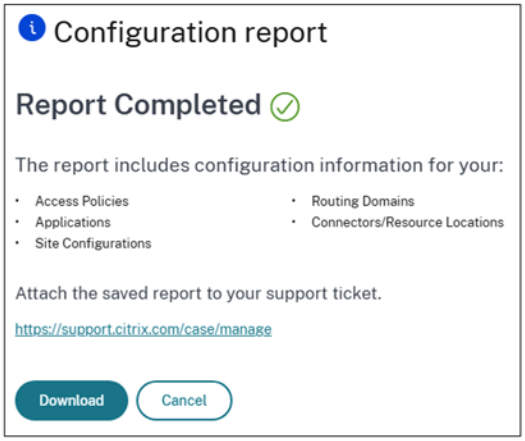
1. In the Secure Private Access admin console, go to **Settings > Configuration Report**.
2. Click **Create report** to initiate the report generation process.

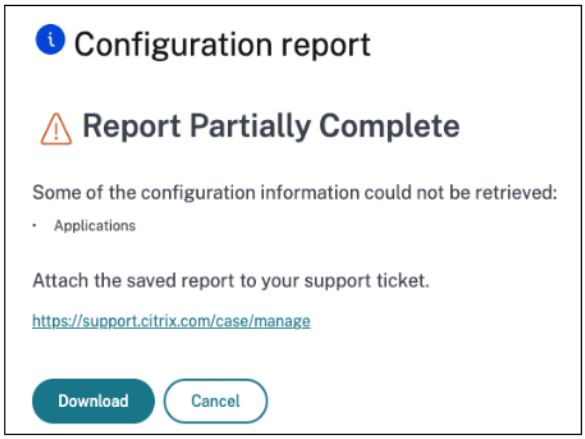
   Once the report is generated, the **Configuration Report** dialog displays the following status:

   - **Report Completed:** Indicates that all required details are successfully included in the report.
   - **Report Partially Complete:** Indicates that some details are missing or not generated.

   The dialog also lists the categories for which the report generation was incomplete.

   The following figure shows a sample configuration report dialog with complete and partially complete status.




3. Click **Download** to manually export the report to your local drive.

> **Important:**
>
> Generating configuration reports is limited to administrators with the following Secure Private Access roles:
>
> - Full Access Administrator
> - Read Only Administrator
> - Full Monitor Administrator
> - Administrators with the Help Desk Administrator role cannot generate configuration reports.

## Unsanctioned websites

September 6, 2025

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

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

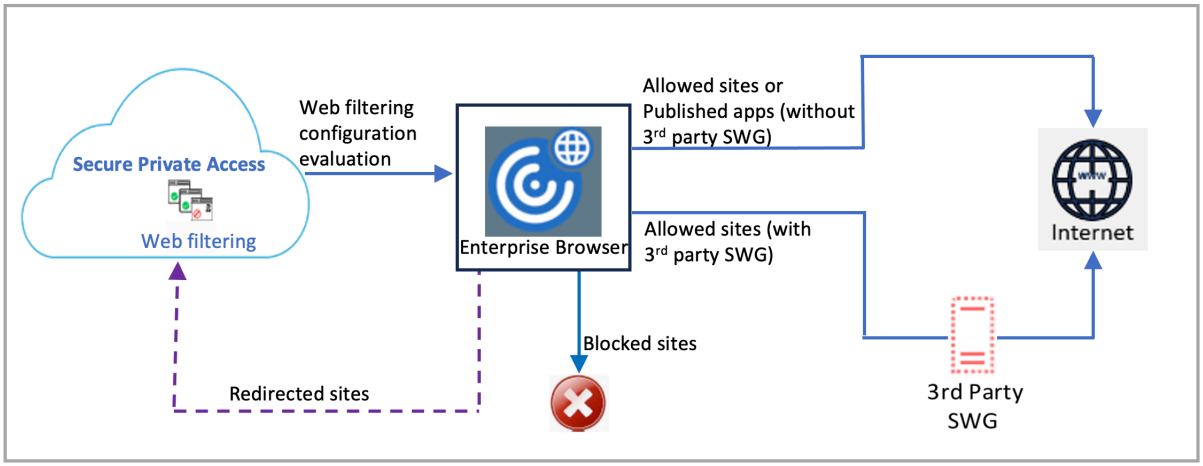
> **Note:**
>
> By default, settings are configured to ALLOW access to all internet URLs or SaaS apps via Citrix Enterprise Browser.

### How unsanctioned websites work

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

The following illustration explains the end user traffic flow.




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

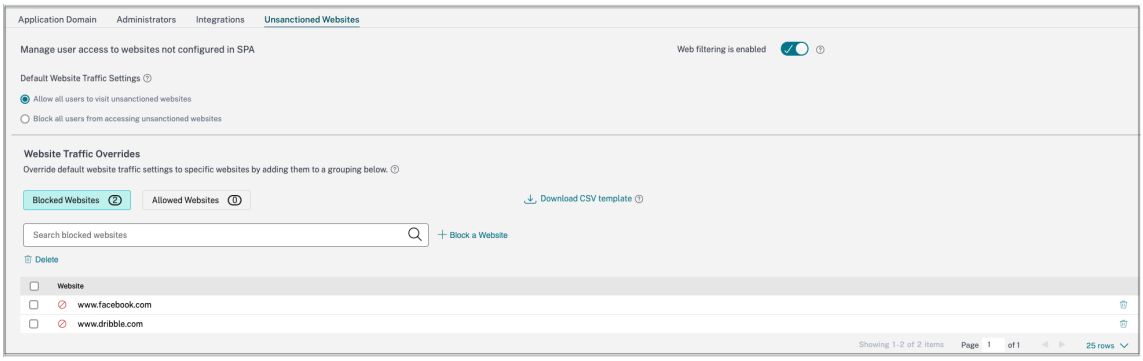
1. Does the request match the global allow list?
   a) If it matches, the user can access the requested website.
   b) If it does not match, website lists are checked.
2. Does the request match the configured website list?
   a) If it matches, the following sequence determines the action.
      i. Block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

## Configure rules for unsanctioned websites

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

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




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

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

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

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

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

   The URL is added to the list of allowed websites.

## Upgrade

September 6, 2025

Periodically, Citrix releases updates to enhance the performance, security, and reliability of the Cloud Connector. By default, Citrix Cloud™ installs these updates on each connector, one at a time, when they become available. Secure Private Access is upgraded as part of the Cloud Connector upgrade by default.

For details on Cloud Connector upgrade, see, Connector updates.

Refer to the following topics for details about the other components upgrade:

- StoreFront
- NetScaler Gateway

# Manage configurations

September 6, 2025

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

# Manage settings after installation

September 6, 2025

## Manage routing of application domains

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

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

## Manage administrators

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

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

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

### Modify integration settings

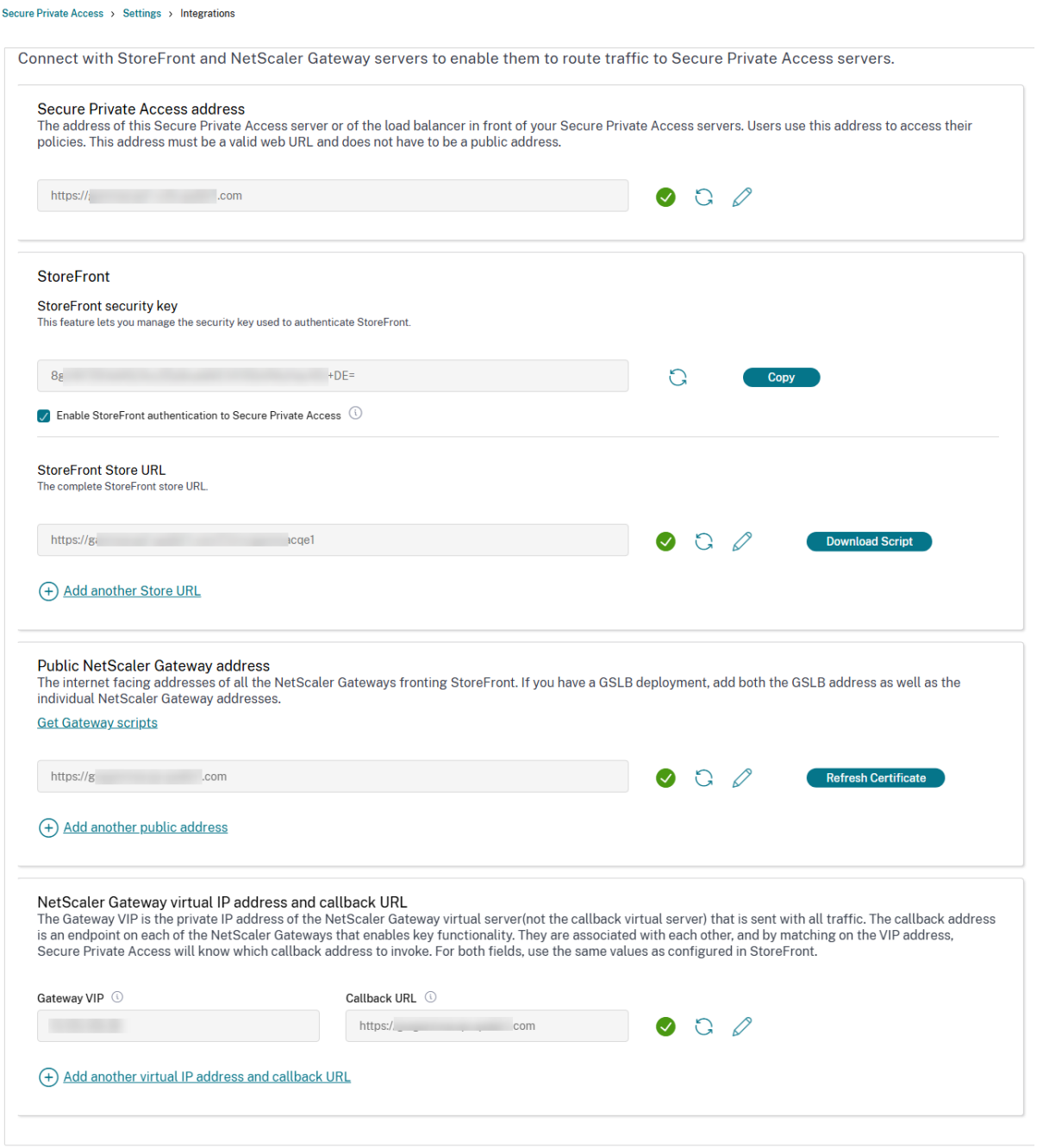
After you have set up Secure Private Access, you can modify or update the StoreFront™ and NetScaler Gateway entries from the **Integrations** tab.

1. Click **Settings > Integrations**.
2. Click the edit icon in line with the setting that you want to modify and update the entry.
3. Click the refresh icon to ensure that the settings are valid.
4. Select **Enable StoreFront authentication to Secure Private Access**. Starting from version 2502, a security key-based authentication method is introduced for StoreFront to Secure Private Access communication and is enabled by default.

   For existing customers, key-based authentication is disabled by default and a warning message prompting to enable key-based authentication appears on the admin console. You must select **Enable StoreFront authentication to Secure Private Access** and run the StoreFront script again.

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




## Manage applications and policies

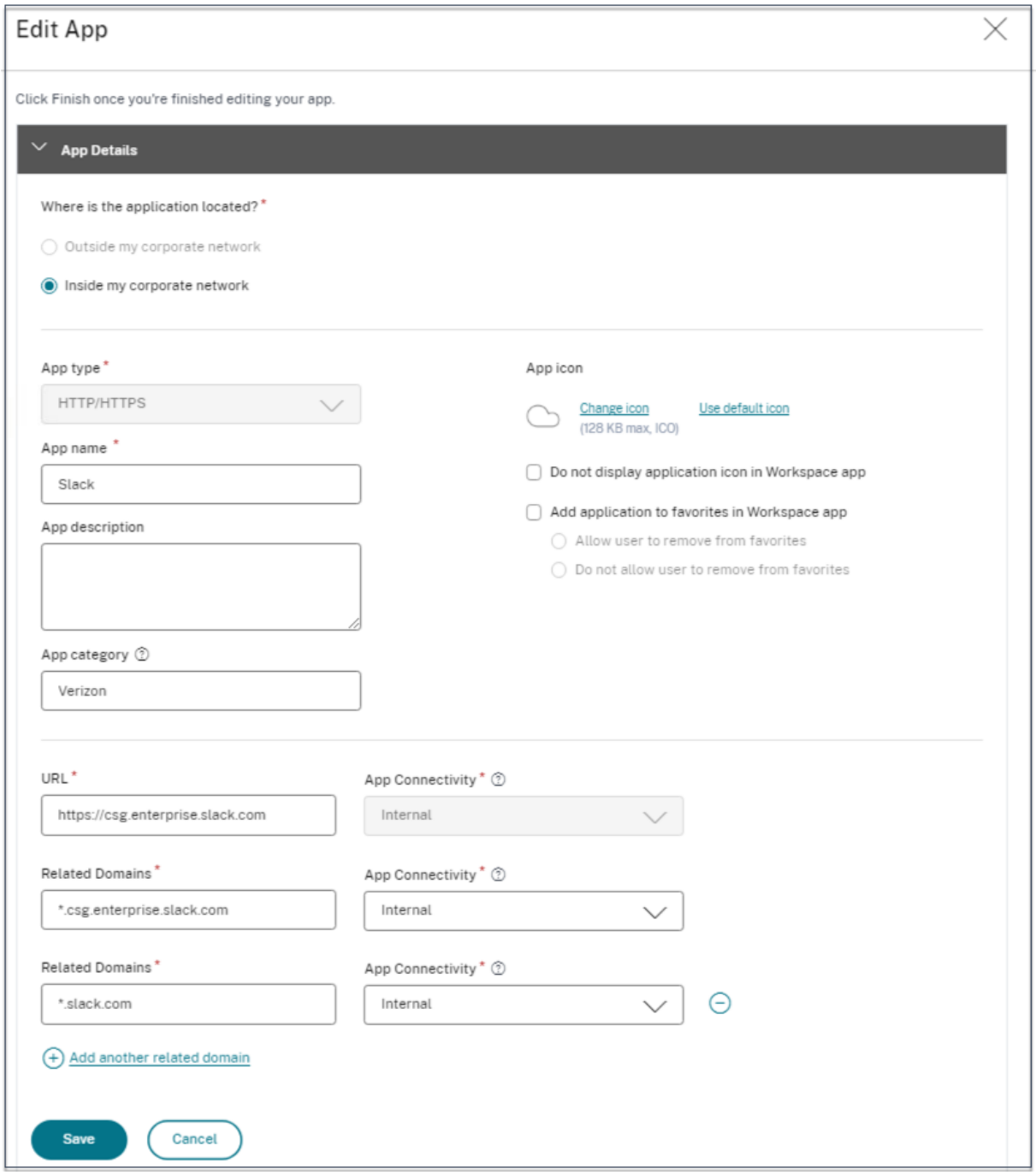
September 6, 2025

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

## Edit an application

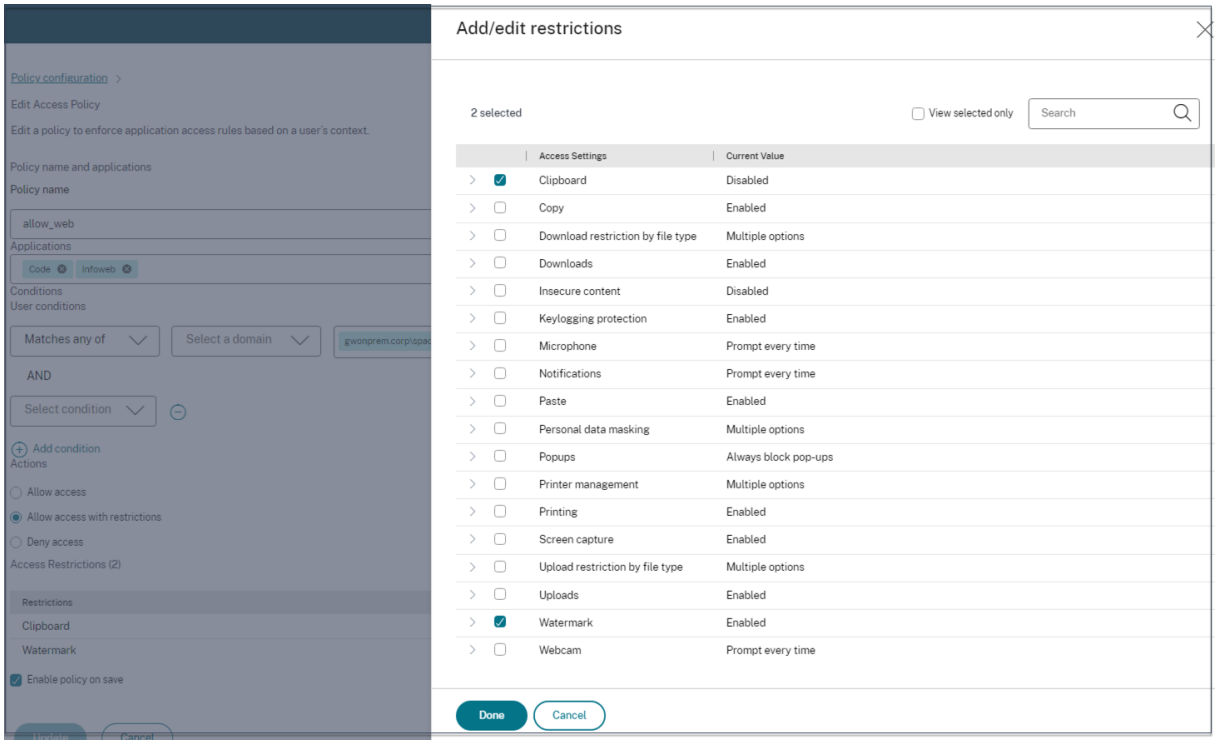
1. In the Secure Private Access admin console, click **Applciations**.
2. Click the ellipsis button in line with the application that you want to modify and then click **Edit Application**.
3. Edit the app details.
4. Click **Save**.



### Edit an access policy

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




## Role-based access control

September 6, 2025

Secure Private Access uses a role-based access control model to manage user permissions and access levels. This means that each user is assigned a specific role, and that role determines what they can and cannot do within the system. This model helps to ensure that users have the appropriate level of access to perform their tasks, while also preventing them from accessing sensitive data or functions that they must not have access to.

The following four main roles are available for Secure Private Access admins. Each of these roles has a different set of permissions, which are designed to match the needs of different types of users.

- Full Access Administrator

- Read Only Administrator
- Full Monitor Administrator
- Helpdesk Administrator

> **Note:**
>
> To monitor Secure Private Access using DaaS Monitor, administrators must be assigned the DaaS role in addition to one of the Secure Private Access roles.

The following table provides a brief description of each role:

| Role | Description |
| --- | --- |
| Full Access Administrator | Intended for individuals who need complete control over the configuration, management, and operation of the Secure Private Access environment. The Full Access Administrator has the following privileges.<br>Access to all Secure Private Access functionalities.<br>Permissions to create, edit, and modify apps, policies, and settings within the Secure Private Access console. |
| Read Only Administrator | Intended for individuals who need to monitor and analyze the Secure Private Access activities and system performance. The Read Only Administrator has the following privileges.<br>Access to the Secure Private Access dashboard.<br>Ability to view all Secure Private Access application configurations and settings.<br>The Read Only Administrator does not have the privileges to any of the create/update/delete functionality. |
| Full Monitor Administrator | Intended for users responsible for monitoring Secure Private Access activity and performance in the Monitor console. The Full Monitor Administrator has the following privileges.<br>Access to all monitoring dashboards and reporting tools within Secure Private Access.<br>Ability to view all Secure Private Access configurations and settings. |

| Role | Description |
| --- | --- |
| Helpdesk Administrator | The Full Monitor Administrator does not have permissions to create, edit, or modify Secure Private Access configurations, policies, or settings.<br>Intended for Helpdesk personnel responsible for troubleshooting and triaging user access issues.<br>The Helpdesk Administrator has the following privileges.<br>Limited visibility into Secure Private Access configurations and settings, focusing on information relevant to troubleshooting in the Monitor console.<br>Access to specific troubleshooting tools and diagnostic utilities within the Secure Private Access console.<br>View the troubleshooting and the Monitor dashboard.<br>The Helpdesk Administrator does not have permissions to create, edit, or modify Secure Private Access configurations or policies. |

## Roles and privileges

The following table summarizes the roles and privileges:

| | Full Access Administrator | Read Only Administrator | Full Monitor Administrator | Helpdesk Administrator |
| --- | --- | --- | --- | --- |
| Create/edit/delete apps | Yes | No | No | No |
| Create/edit/delete policies | Yes | No | No | No |
| Edit configurations/settings | Yes | No | No | No |
| View configurations/settings | Yes | Yes | Yes | Limited |

| | | Full Access Administrator | Read Only Administrator | Full Monitor Administrator | Helpdesk Administrator |
|---|---|---|---|---|---|
| | View the logging and troubleshooting widget in the Secure Private Access dashboard | Yes | Yes | Yes | Yes |
| | Search for users | Yes | Yes | Yes | No |
| | Retrieved configured domains | Yes | Yes | Yes | No |
| | View the Users, Applications, Access Policies widgets in the Secure Private Access dashboard | Yes | Yes | Yes | No |
| | View the sessions and applications in the Monitor dashboard | Yes | Yes | Yes | Limited |
| | Access reporting tools | Yes | No | Yes | Limited |

## Enable role-based access to admins

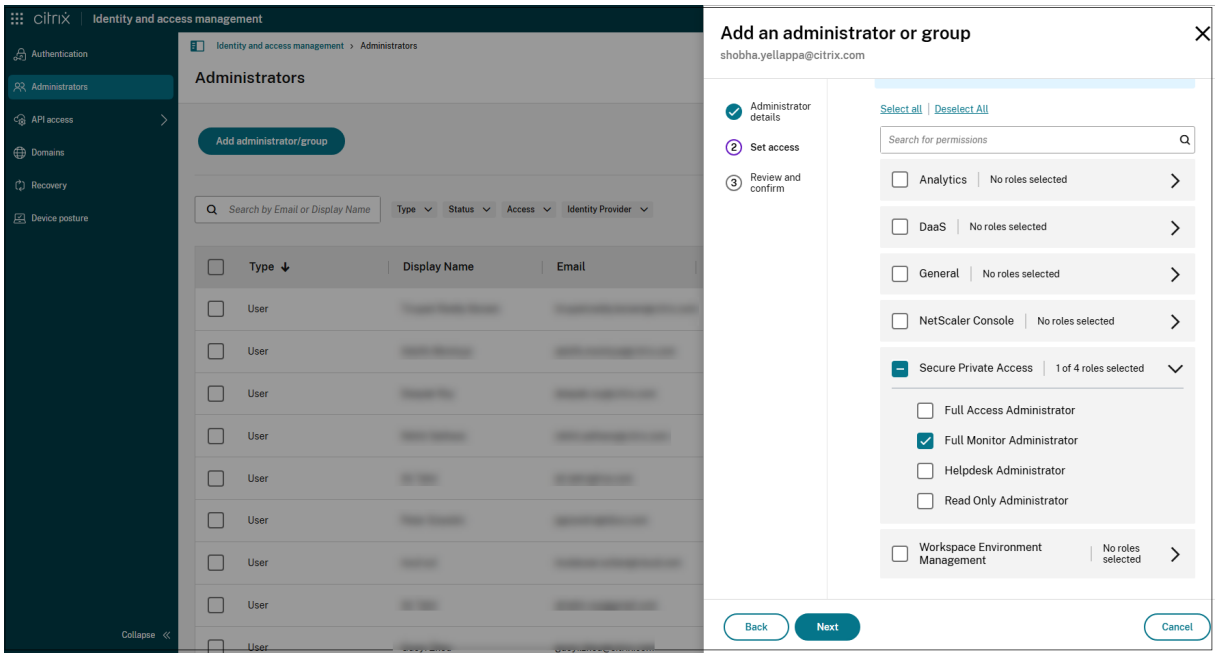
Perform the following steps to enable role-based access to admins:

1. After signing in to Citrix Cloud™, select **Identity and Access Management** from the menu.
2. On the **Identity and Access Management** page, click **Administrators**, and then click **Add administrator/group**. The console displays all the current administrators in the account.

3. In **Add an administrator or group**, select the identity provider from which you want to select the administrator. Sometimes, Citrix Cloud might prompt you to sign in to the identity provider first (for example, Azure Active Directory).
4. If **Citrix Identity** is selected, enter the user's email address, and then click **Next**.
5. Select **Custom access**, and then click the **>** icon in **Secure Private Access**.
6. Select one of the following roles and click Next.
   - Full Access Administrator
   - Read Only Administrator
   - Full Monitor Administrator
   - Helpdesk Administrator
7. Click **Send invitation**.

> **Note:**
>
> The **Analytics** and **General** services must be enabled for all Secure Private Access roles. The **Analytics** service is necessary for monitoring and reporting, while the **General** services are required for authentication, domains, authorization, traffic routing, and other functionalities.




## Dashboard overview

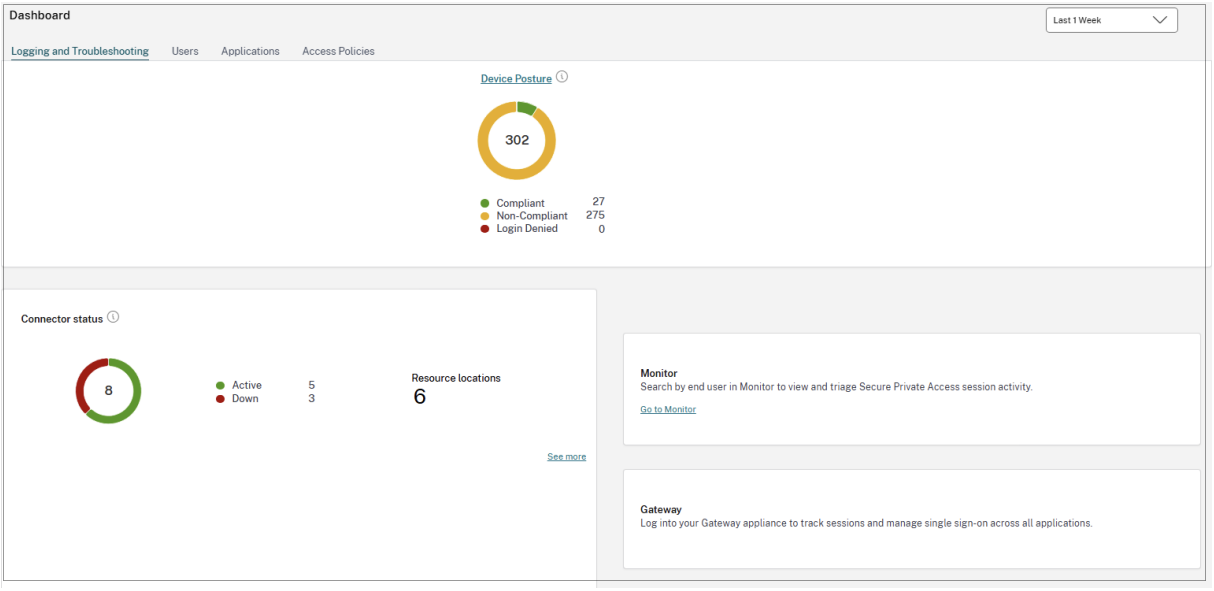
September 6, 2025

The dashboard provides admins full visibility into their apps, users, and access policies in a single place for consumption. This data is fetched from Citrix Analytics. The data for the various entities can be viewed for the preset time or for a custom timeline. For some of the entities, you can drill down to view further details. The data in the dashboard is broadly classified into the following categories.

## Logging and Troubleshooting

- **Device Posture:** Logs related to device posture that help administrators assess endpoint compliance. The device posture logs are categorized as Compliant, Non-Compliant, and Login Denied. For details on device posture logs, see Device posture logs and events.
- **Connector status:** Status of the Cloud Connector and the resource locations where the connectors are deployed. Click the **See more** link to view the details. In the **Connector insights** page, you can use the filters **Active** or **Inactive** to filter the connectors based on their status.
- **Monitor:** Secure Private Access is integrated with Monitor, which is the monitoring and troubleshooting console for Citrix DaaS. Administrators and help-desk personnel can monitor and troubleshoot Web/SaaS and TCP/UDP app sessions and events from the DaaS Monitor. For details about the integration and for viewing user sessions, see Integration with Monitor.




- **Gateway:** Admins can also log in to the NetScaler® Gateway to track sessions and manage single sign-on across all applications from the dashboard.

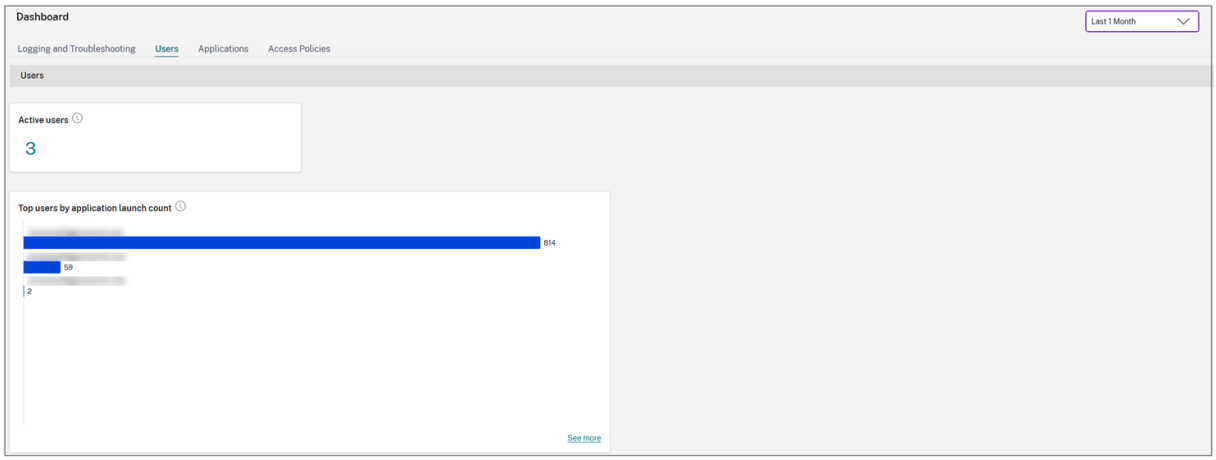
## Users

- **Active users:** Total number of unique users accessing the applications (SaaS/Web and TCP/UDP) for the selected time interval. Click the number to view the detailed information

about the users.

- **Top users by applications launch count:** Data per user. For example, the number of times a user has launched the app. You can filter the data for a pre-set timeline or for a custom timeline.

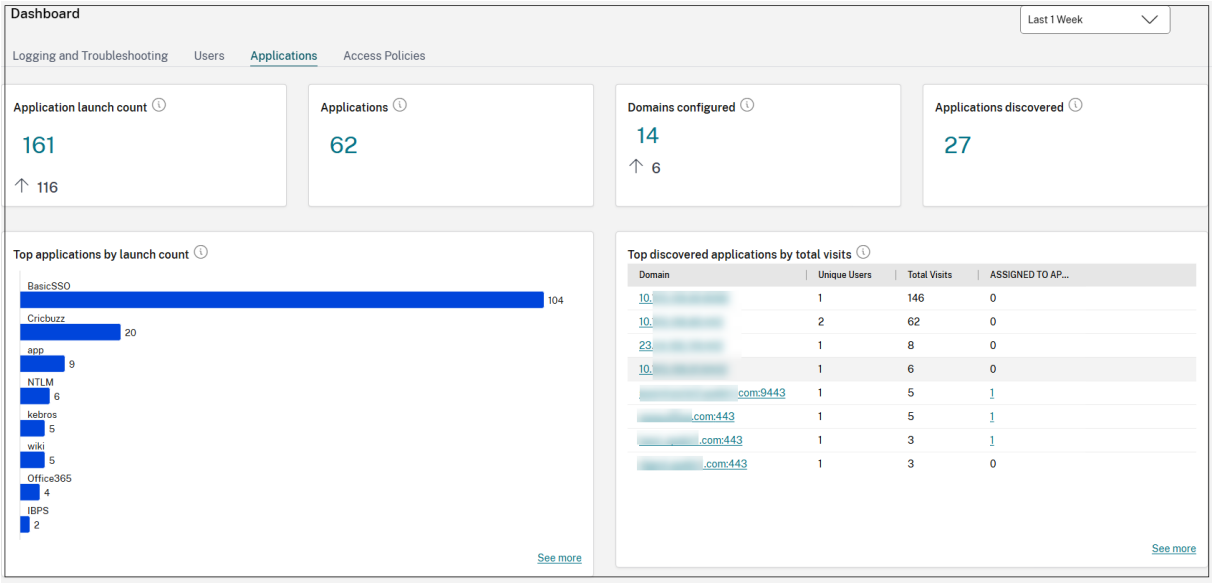



## Applications

- **Application launch count:** Total number of applications (app sessions) launched by each user for the selected time interval. Click the number to view the detailed information about the applications launch count.
- **Applications:** Total number of applications (independent of the time interval) configured currently.
- **Domains configured:** Total number of domains configured for the selected time interval.
- **Applications discovered:** Total number of unique, individual domains that have been accessed but are not associated with any apps. Click the number to view the detailed information about the applications discovered. For information on applications discovery, see Discover domains or IP addresses accessed by end users.
- **Top applications by launch count:** List of top applications based on the number of the times the app was launched. You can apply the filters SaaS Apps, Web Apps, or TCP/UDP Apps to narrow down your search to specific apps. You can filter the data for a pre-set timeline or for a custom timeline. Click the **See more** link to view the details.
- **Top discovered applications by total visits:** List of individual domains that have been accessed at some point but are not associated with any apps. These domains are listed based on the number of total visits to those domains. Admins can use this chart to see if any domain of particular interest is accessed by many users. In such cases, admins can create an app with that domain for easy accessibility. Click the **See more** link to view the list of domains visited

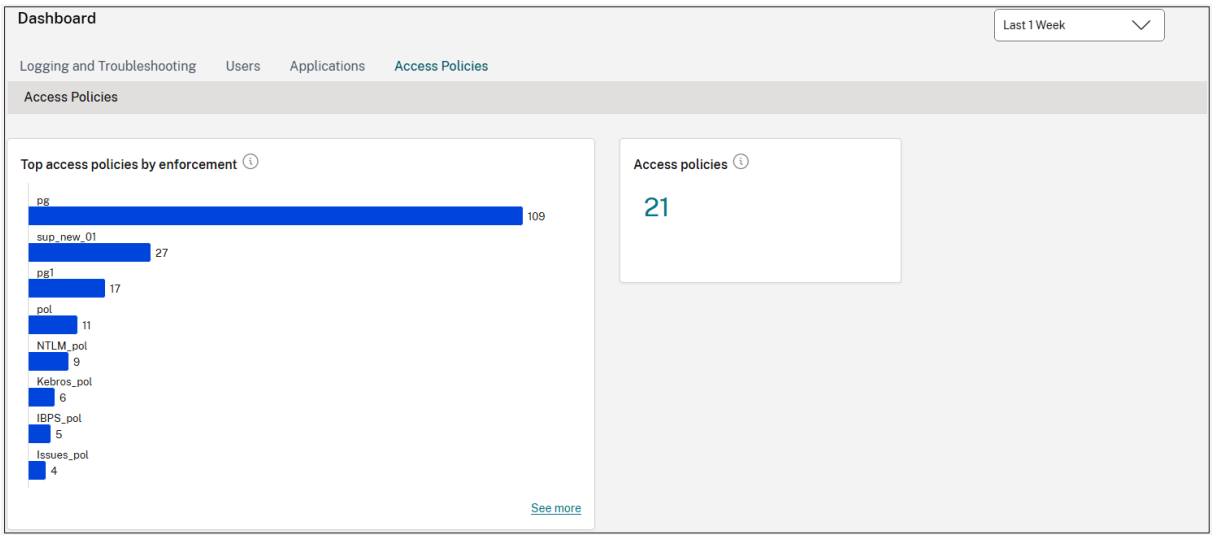
 

by end-users. For more information about application discovery, see Discover domains or IP addresses accessed by end users.




## Access policies

- **Access policies:** Total number of access policies (independent of the time interval) configured currently.
- **Top access policies by enforcement:** List of access policies that are enforced on the apps. Click the **See more** link to view the list of policies that are associated with the apps and the number of times the policies are enforced. You can also use the Search option in the Access policies page to filter the policies based on the policy name. You can also search for specific policies using the search operators to further refine your search. For details, see Search operators.



### Search operators

The following are the search operators that you can use to refine your search:

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

## Integration with DaaS monitor

September 6, 2025

Secure Private Access is integrated with Monitor, the monitoring and troubleshooting console for Citrix DaaS. Administrators and help-desk personnel can monitor and troubleshoot Web/SaaS and TCP/UDP app sessions and events from the DaaS Monitor, in addition to the Secure Private Access dashboard.

### Service entitlements

To use the DaaS Monitor feature with Secure Private Access, you must have both Secure Private Access and DaaS entitlements.

### Supported clients

- Citrix Workspace™ app - 2409 and later
- Citrix Secure Access for Windows - 24.8.1.19 and later
- Citrix Secure Access for macOS - 24.10.1 and later

### How to access Monitor

You can access Monitor from the Secure Private Access dashboard (**Go to Monitor**) or from the Citrix DaaS™ service tile.

In the **Monitor** page, search for the user to view the sessions.

## Session definitions

A Secure Private Access session offers a comprehensive summary of an end-user's session lifecycle, application activity, and user experience on a specific device. A session serves as a unified record for troubleshooting and analysis by providing visibility into the following aspects:

- Detailed insights into how applications are accessed, including launch hops, network topology, connections, and routing details. These details are crucial for resolving issues related to access policies.
- Tracks all session activity from:
  - Browsers accessing web or SaaS applications.
  - The Citrix Secure Access client for private applications using TCP/UDP protocols.

Some of the key characteristics of a Secure Private Access session are:

- Each session is assigned a unique ID for tracking and analysis.
- A single session can include multiple app launches and provides a comprehensive view of the user activity within that specific session.
- For each app, the session tracks:
  - The security controls that apply to the app.
  - The policy display name and ID that triggered the security controls.
  - The condition that resulted in the policy being enforced.
- The session tracks all the internal domains that a user has visited in Citrix Enterprise Browser™ providing insights into the user navigation within the secure environment.

### Web/SaaS app sessions

The session start and end for Web/SaaS apps is defined as follows:

- Start: Citrix Enterprise Browser is opened in the Citrix Workspace app and applications are accessed.
- End: A session ends in the following scenarios.
  - You close the Citrix Enterprise Browser.
  - After 30 minutes of inactivity, if no session activity is reported.

    The Citrix Enterprise Browser client sends a session activity to Monitor every 15 minutes to Monitor. If this session activity is not received for 30 minutes, which might occur due to reasons such as:

    * Network failure.
    * Internet connectivity issues.
    * Session is automatically closed after the 30-minute interval without session activity.

> **Note:**
>
> For apps launched through native browsers (agentless), the session ends after 120 minutes of inactivity.

#### TCP/UDP app sessions

The session start and end for TCP/UDP apps is defined as follows:

- Start: You log in to the Citrix Secure Access™ client and access the apps.
- End: A session ends in the following scenarios.
  - You log out of the Citrix Secure Access client.
  - After 30 minutes of inactivity, if no session activity is reported.

### View user sessions

Perform the following steps to view a user session:

1. Search for a user to view the sessions.
   - The **Select a session** page displays all active sessions. If you do not find your session in the **Active Sessions** tab, check in the **Denied Access** tab.
   - The **Ended Sessions** and **Failed Sessions** tabs are not applicable to Secure Private Access.
2. In the **Active Sessions** tab, click the session ID to view the details of the session.

   The **Activity Manager** page appears.
3. Click one of the following tabs:
   - **Launched apps:** View all applications launched by the user and the results (allow or deny) of the access policy evaluation.

     If an application was accessed multiple times in the same session, only the latest launch details are captured.
   - **Available Apps:** View app enumeration details of all the applications that were launched by this user.
     - If multiple enumeration requests were sent by Citrix Workspace app for a user, only the latest enumeration details are captured.

  - For TCP/UDP apps (web and ZTNA), although there is no concept of app enumeration, all apps configured and associated with the user are listed in the **Available Apps** list.
  - The **Available Apps** list does not contain external apps that are enumerated through the Citrix Secure Access client as they are not tunneled by Secure Private Access.
  - For the Citrix Secure Access agent, the **Available Apps** list only displays only the internal web and TCP/UDP apps.

### Application topology

When you click an app from the **Launched Apps** or **Available Apps** tabs, the application topology page appears, displaying complete information about the app.

- **Session Topology:** Displays the app launch flow.
- **About:** Displays app-related information such as app type, number of policy rules, security restrictions, and accessed resources. The data that appears in the **Accessed Resources** section varies depending on the app type.
  - SaaS apps - URL or the app FQDN
  - TCP/UDP –IP address/FQDN, port, and protocol
  - Web app (launched via Citrix Secure Access client) - FQDN, port, and protocol
  - Web app (launched via Citrix Workspace) - URL
- **Policy evaluation:** Displays information related to the access policy, such as rules, actions, and conditions.
- **Session Details:** Displays information related to the session, including session start and end time, session state, and contextual tags associated with the policy.
  - The **Domains Visited** field is applicable only for the Web/SaaS apps and is updated only after 15 minutes, as the Citrix Enterprise Browser clients on macOS and Windows send session activity every 15 minutes.
  - The **Session Details** column section remains empty for apps clicked from the **Available Apps** tab, as app enumeration is not associated with a session.

The following figure displays a sample topology diagram for a successfully launched app.

The following figure displays a sample topology diagram for an access denied app.

## Basic troubleshooting

September 6, 2025

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



## Certificate errors

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

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

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

## StoreFront™ failures

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

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

  **Resolution**:

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

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

  **Resolution**:

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

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

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

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

  **Resolution**:

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

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

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

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

## 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.