Citrix Secure Private Access™ Hybrid Deployment

Contents

Solution overview

November 26, 2025

Citrix Secure Private Access™ for hybrid deployments provides a Zero Trust Network Access (ZTNA) solution that divides functions between your on-premises environment and Citrix Cloud. This architecture allows you to leverage existing investments while gaining cloud-based management. The responsibilities are distributed as follows:

- **On-premises components (data plane):** Your existing NetScaler Gateway, StoreFront, and Windows Cloud Connector installations remain on-premises. These components are responsible for controlling and routing all user access traffic.
- **Citrix Cloud components (control plane):**
  - Centralized management: Use the Citrix Cloud UI for all configuration, administration, and policy management.
  - Monitoring and troubleshooting: Utilize the hosted Citrix Monitor service for all monitoring, analytics, and troubleshooting functions.

Why Use Secure Private Access

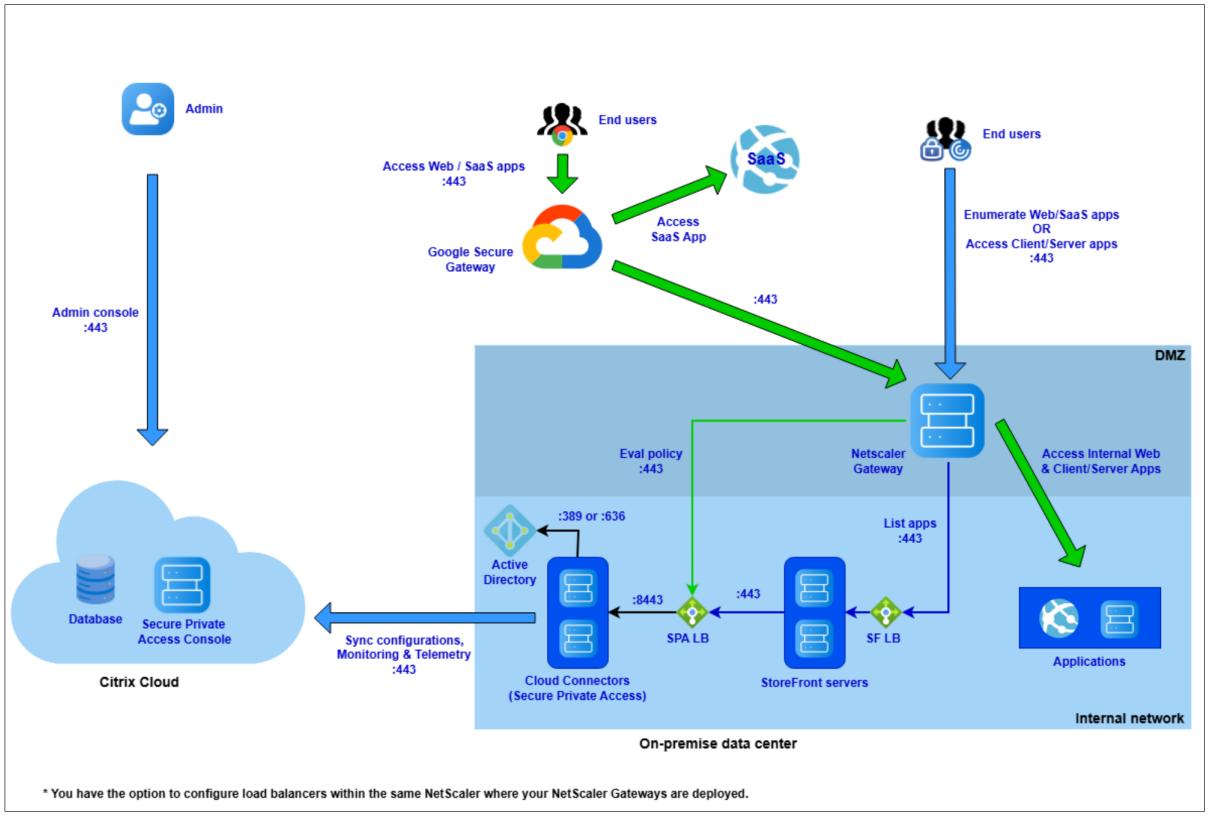
Citrix Secure Private Access solution provides end-to-end access control by integrating single sign-on (SSO), remote access, and content inspection into a unified platform.

- **Govern app access:** Enforce security policies and provide simplified SSO experience for all approved SaaS and internal applications.
- **Enhance security:** Protect the network and user devices from malware and data leaks by filtering access to specific websites and website categories.
- **Google Chrome Enterprise Premium integration:** Leverage Google Chrome Enterprise Premium, allowing users to natively access authorized corporate web apps with a familiar and secure experience.
- **Data loss prevention (DLP):** Enforce granular controls to restrict printing, downloads, and clipboard copy-paste actions.
- **Analyse user activity and protect enterprise network:** Gain deep visibility into user activities, such as malicious website visits or risky file transfers. Use these analytics to take corrective actions and protect the enterprise network.
- **Seamless user experience:** Provide secure, seamless access to critical business applications from any device, location, or network.

Key components

Network diagram

The following figure illustrates the network diagram of the Secure Private Access hybrid solution.



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

- **Secure Private Access admin console:** Click the Secure Private Access tile in Citrix Cloud to access the admin console. Use the admin console to onboard, configure apps, and set policies. Site management is centralized and streamlined. No on-premises infrastructure required.
- **Google Chrome and Chrome Enterprise Premium Secure Gateway:** End users access corporate internal and SaaS applications using the Google Chrome browser.

  The Chrome Enterprise Premium Secure Gateway functions as a forward proxy to enforce a zero-trust access framework. It provides granular, context-aware control over application access. All traffic from the user's Chrome browser connects to the NetScaler Gateway through the Chrome Enterprise Premium Secure Gateway, ensuring policies are applied before access is granted.

  > **Note:**
  >
  > The Google components are required only when using Secure Private Access to provide secure access to SaaS and internal Web applications. They are not required if you plan to

> use Secure Private Access only for TCP/UDP (client/server) applications.

- **NetScaler Gateway:** The NetScaler Gateway component provides secure remote access to applications and desktops. It acts as the secure entry point for external users, allowing them to connect to corporate resources from outside the network. For details, see NetScaler.
- **Cloud Connector:** The Cloud Connector is an on-premises component, installed on a Windows server, that acts as a secure communication bridge between your network and Citrix Cloud.

  Cloud Connector is responsible for synchronizing all configurations and policies from the Secure Private Access service in the cloud. These policies are then used to enforce access rules for applications. The connector also persistently caches this data, which allows users to continue accessing applications even if Citrix Cloud becomes unavailable. For details, see Cloud Connector.
- **StoreFront:** The on-premises StoreFront is the user facing component that aggregates, enumerates, and delivers all authorized applications and desktops to end-users. It functions as an enterprise app store. This hybrid architecture allows you to leverage your existing StoreFront setup without migrating to the cloud. For details, see StoreFront.

  > **Note:**
  >
  > StoreFront is optional if you plan to use Secure Private Access only for TCP/UDP (client/server) applications. If you do configure StoreFront, it only enumerates applications that are configured as a web application type. Standard TCP/UDP apps are not displayed in the store.

End user access methods

End users can access the Secure Private Access apps using any of the following methods:

- **Citrix Workspace App (CWA) and Workspace UI:** These are the two clients end users can use to connect and view Citrix Store.
  - **Citrix Workspace App (native client):** This is the full, native application installed on the user's endpoint (for example, Windows and macOS). It provides the richest user experience and is required for certain advanced features.
  - **Citrix Workspace UI (web client):** This is the browser-based version of the store. Users access it by navigating to the StoreFront URL in a web browser. It allows users to access their applications without installing any client software.
- **Google Chrome:** All web and SaaS applications are launched exclusively through the Google Chrome browser using a managed enterprise profile. When a user launches an application from their Citrix Store, it automatically opens in this managed Chrome Enterprise profile to enforce all security controls.

> **Note:**
>
> Google Chrome is not mandatory if you plan to use Secure Private Access only for TCP/UDP (client/server) applications. Users can use any browser (such as a non-managed Chrome, Edge, or Firefox) to access TCP/UDP applications.

- **Citrix Secure Access (CSA) client:** This is the client-side agent, installed on the user's endpoint, that is required for ZTNA access to all TCP/UDP (client/server) applications.

  CSA provides secure, per-application connectivity to internal corporate resources without requiring a traditional, full-tunnel VPN.

Citrix Endpoint Analysis (EPA) client

The Citrix EPA client is a lightweight plug-in that runs on the user's endpoint to perform device posture scans (also known as EPA scans). This client is required only if you have configured access policies that check the endpoint's security posture (for example, up-to-date OS, specific antivirus software, or registry keys) before granting access.

Limitations

- EPA as a factor is not supported. Instead, you can use the Device Posture service. For more information about the Device Posture service, see Device Posture.
- Enabling device posture checks at virtual server level is not supported with Always On.
- Policy modeling supports only user conditions. Device posture and network location conditions are not supported.
- StoreFront analyzer supports only one Secure Private Access type Store in StoreFront.
- The simplified Secure Private Access user interface for hybrid deployments supports only one data center (one gateway and one StoreFront) in the current release.
- IPv6 is not supported for Network Locations in the Citrix Secure Access client.

What's new

December 18, 2025

18 December 2025

- **Secure access to SSH and RDP applications within the browser**

  Citrix Secure Private Access is integrated with Chrome Enterprise Premium to enable secure SSH and RDP sessions directly within the browser. For details, see the following topics:

  - Secure access to SSH apps within the browser
  - Secure access to RDP apps within the browser

November 2025

- **Simplified onboarding journey**

  The Secure Private Access for hybrid deployments onboarding interface is now significantly simplified to streamline the configuration process for all components. The enhanced user interface now features an intuitive topology view that displays step-by-step configuration status for each component. This visual approach enables administrators to quickly understand the deployment state, identify the configuration steps are complete, and determine actions that are still pending, thereby reducing setup time and minimizing configuration errors.

  Also, the SecurePrivateAccessProfile is supported in NetScaler to simplify the NetScaler Gateway configuration for the hybrid deployment.

  For details, see Get Started with Secure Private Access hybrid deployment.

- **Google Chrome Enterprise Premium support**

  With the integration of Citrix Secure Private Access service with Google Chrome Enterprise Premium, end users can now securely access private Web/SaaS applications using the Google Chrome browser as their enterprise browser, and achieve per-application access with data loss prevention (DLP) controls, web filtering, and ZTNA policy enforcement.

  For details, see Integration with Google Chrome Enterprise Premium

- **Analyzer to verify and identify configuration issues in components**

  Component Analyzer is a web-based tool that performs the configuration checks required for a Secure Private Access hybrid setup. After uploading the necessary reports, the Analyzer identifies issues with detailed error messages and explanations, including examples of detected StoreFront configuration errors. The tool also lists potential remediations to resolve the identified problems.

  For details, see Component Analyzer.

- **Support for launching apps from StoreFront UI using NetScaler Gateway URL**

End users can now seamlessly launch applications directly from the StoreFront user interface by accessing the NetScaler Gateway URL.

For details, see Accessing Web and SaaS applications.

- **Network Location Service condition support in access policies**

  The Network Location Service (NLS) is a policy condition that allows you to restrict access based on the user's network location. An admin can configure the access policy based on the location from where the user is accessing the application. The location can be the country from where the user is accessing the application or the user's network location. The network location is defined using an IP address range or subnet addresses.

  For details, see Network Location.

- **Configuration reports**

  Customer administrators can now generate configuration reports to gain insights into the Secure Private Access setup.

  For details, see Configuration report.

September 2025

- **Secure Private Access hybrid deployments support for iOS devices**

  Secure Private Access hybrid deployments are now supported for mobile devices starting with Secure Access Client version 25.08.1 for iOS. Mobile users can access corporate applications from their iOS devices.

  > **Important:**
  >
  > For Secure Private Access support with Citrix Secure Access for the iOS platform, you must also add the string "NSGiOSplugin"in the HTTP "User-Agent"header.
  >
  > Example: `add vpn sessionPolicy PL_OSspahybrid "HTTP.REQ.HEADER (\"User-Agent\").CONTAINS(\"CitrixReceiver\")&& (HTTP.REQ. HEADER(\"User-Agent\").CONTAINS(\"NSGiOSplugin\")|| HTTP.REQ .HEADER(\"User-Agent\").CONTAINS(\"CitrixSecureAccess\"))" AC_OSspahybrid`

  For details, see the following topics:

  - Update existing NetScaler Gateway configuration
  - Citrix Secure Private Access for mobile device.

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

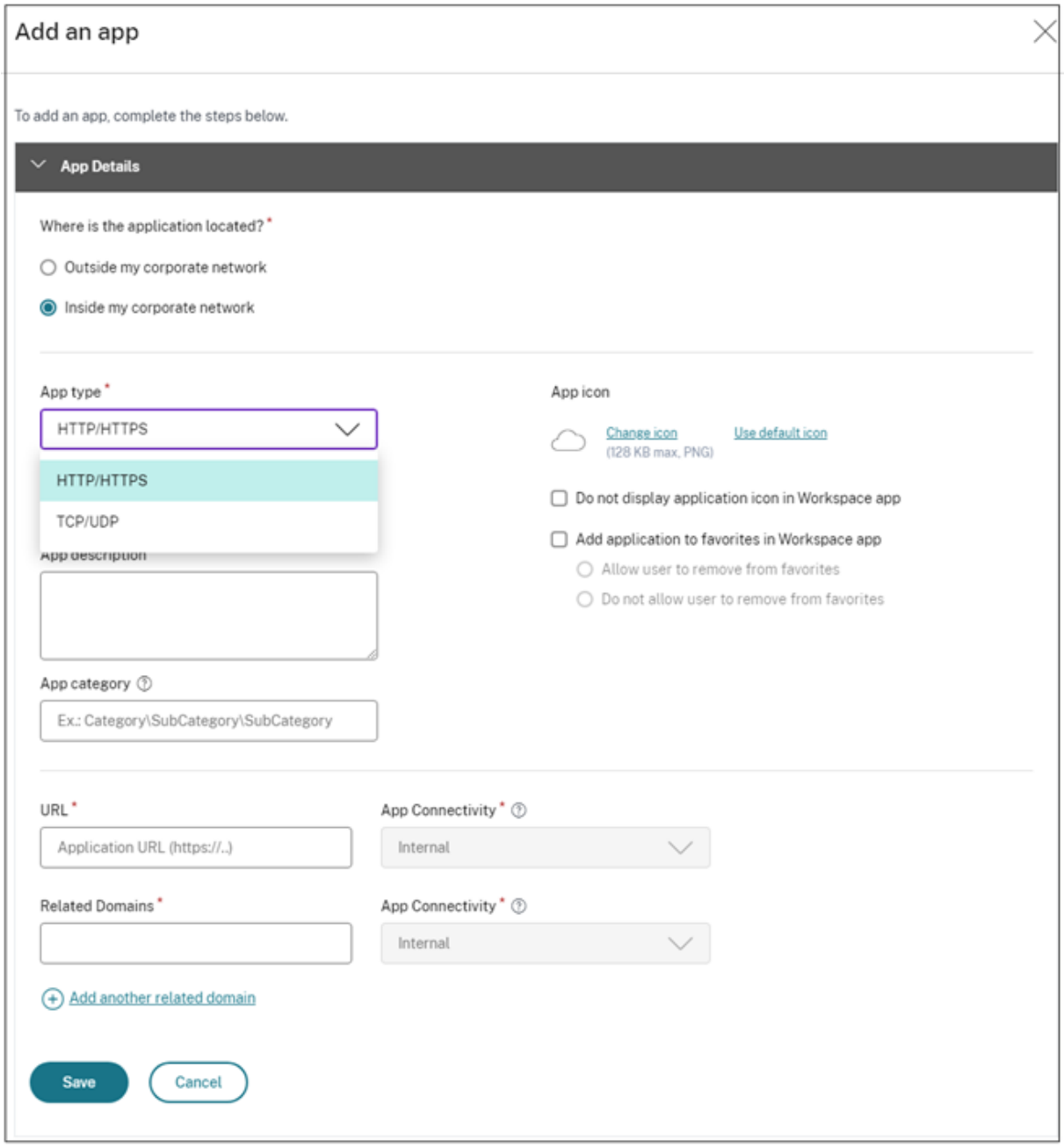
Citrix Secure Private Access for hybrid deployment allows customers to implement a Zero Trust Network Access (ZTNA) solution using on-premises StoreFront and NetScaler Gateway components and use Citrix Cloud™ for managing the configuration, administration, and monitoring functions.

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

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

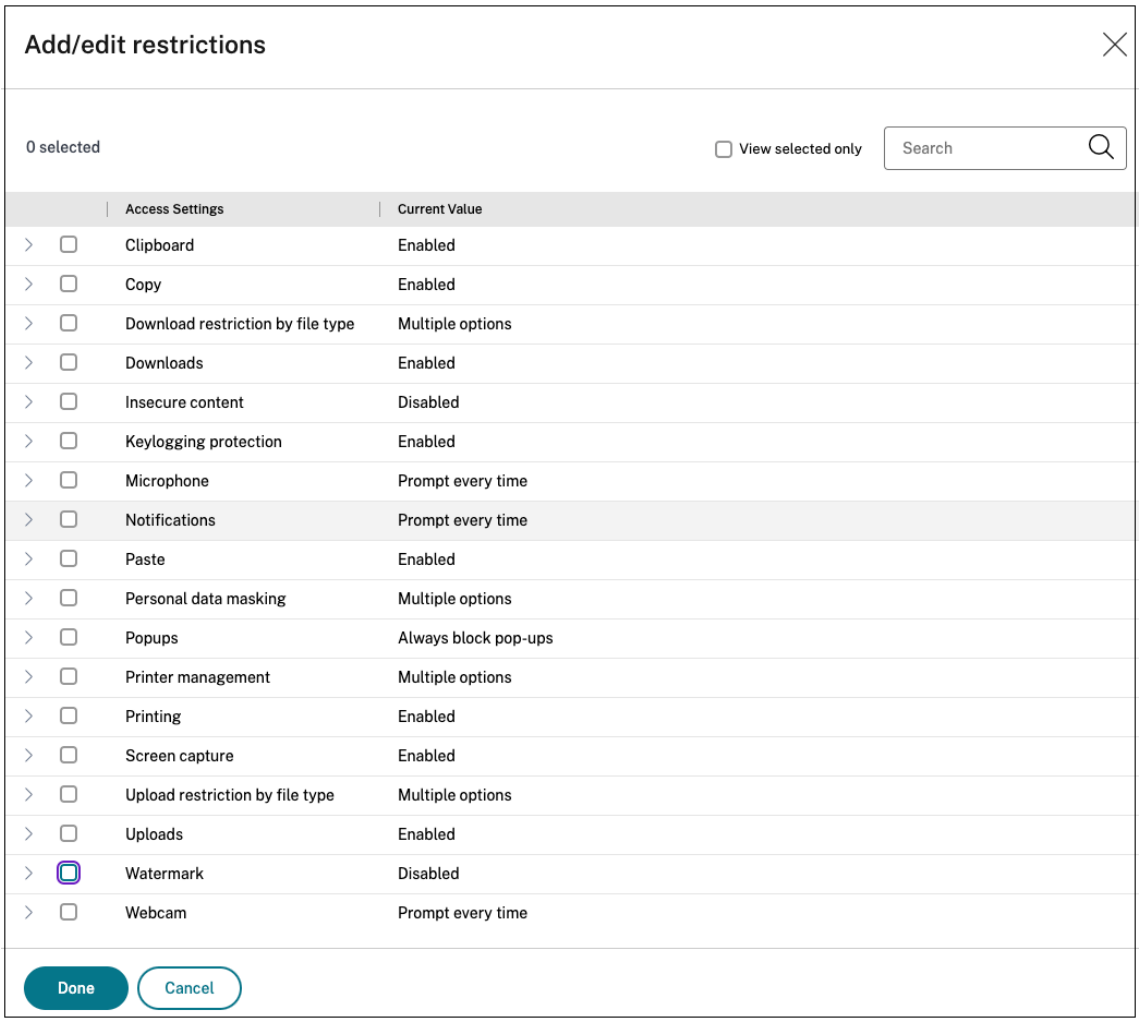
  Citrix Secure Private Access for hybrid deployment supports Web/SaaS and TCP/UDP apps. For details, see the following topics:

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



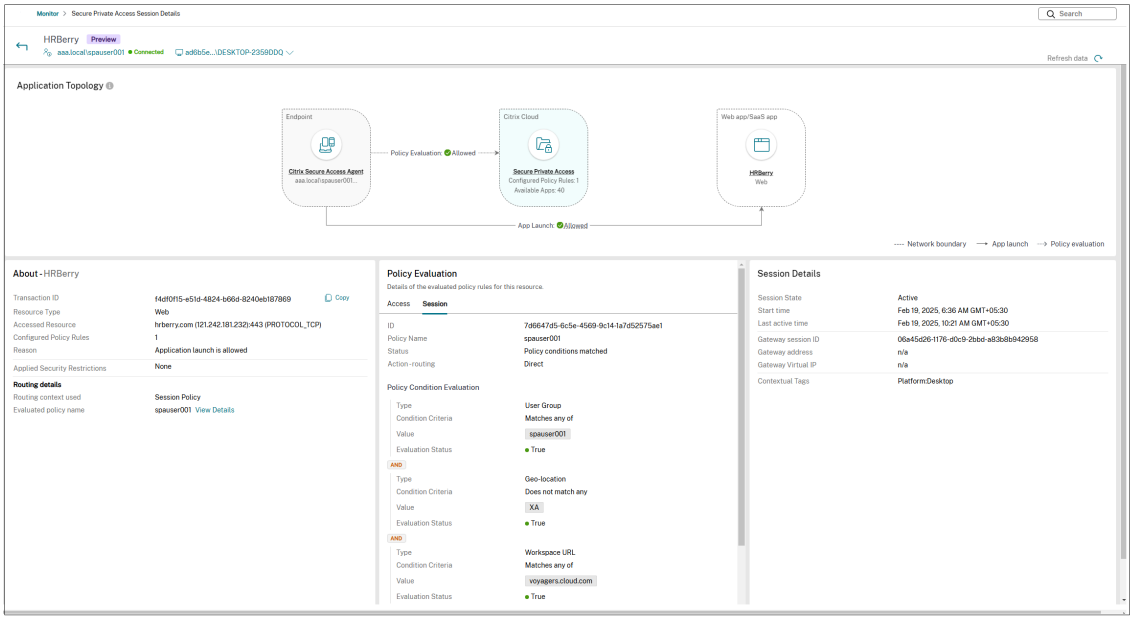
- **Enhanced access restriction options:**

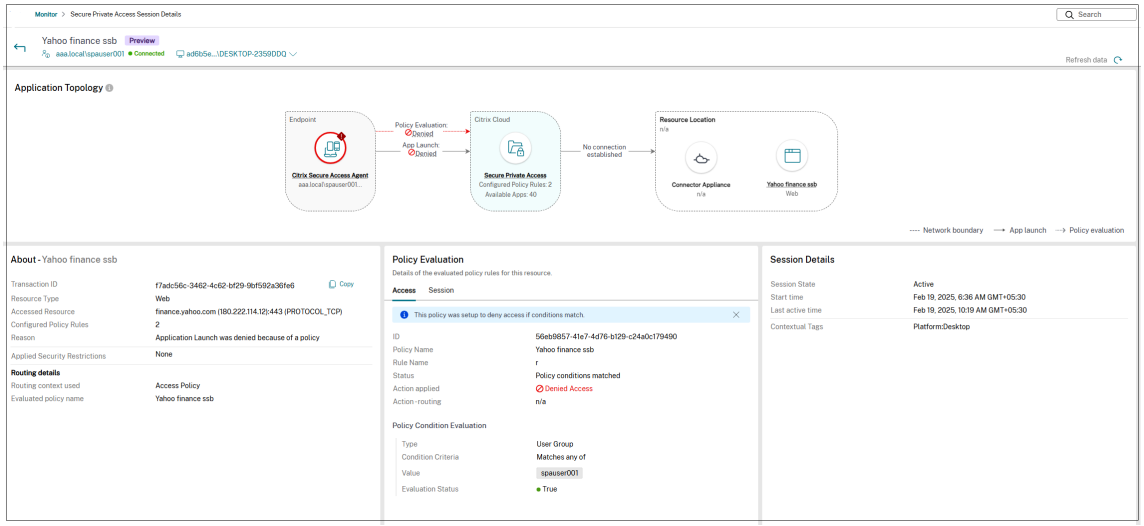
  While creating access policies for applications, you can select access restrictions that must be enforced on the applications. These security restrictions are predefined in the system. Admins cannot modify or add other combinations. For details, see Access restriction options.



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

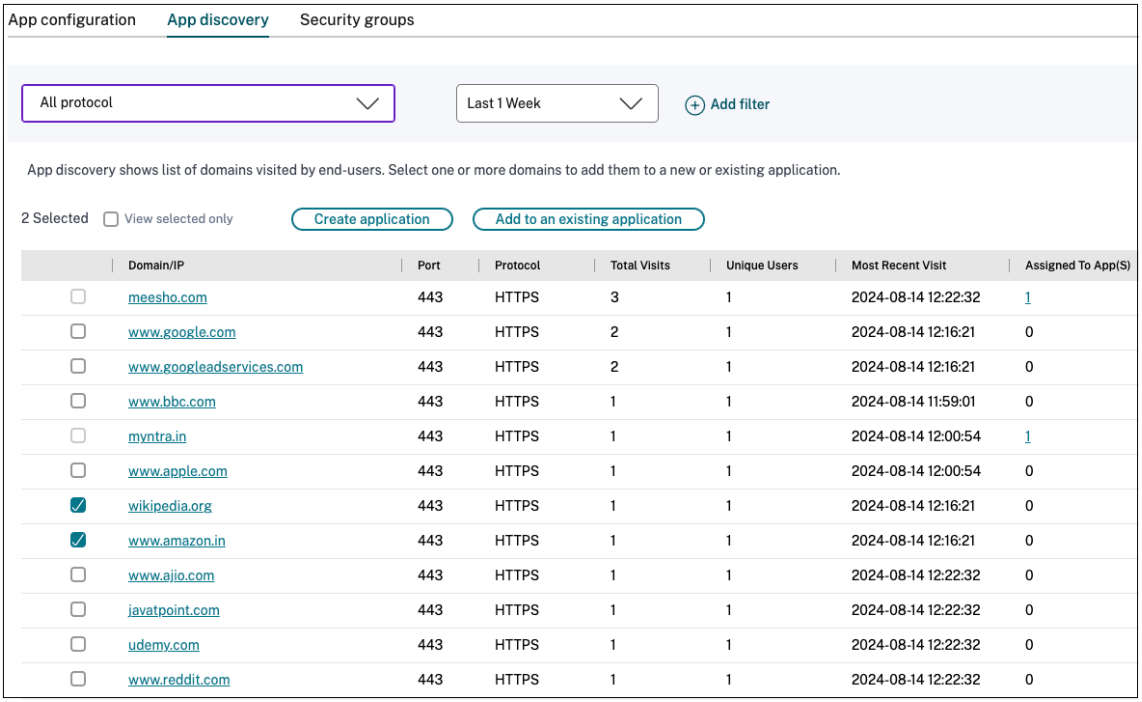
  Secure Private Access is integrated with Monitor, the monitoring and troubleshooting console for Citrix DaaS. Administrators and help-desk personnel can monitor and troubleshoot Web/SaaS and TCP/UDP app sessions and events from the DaaS Monitor. For details, see Secure Private Access integration with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





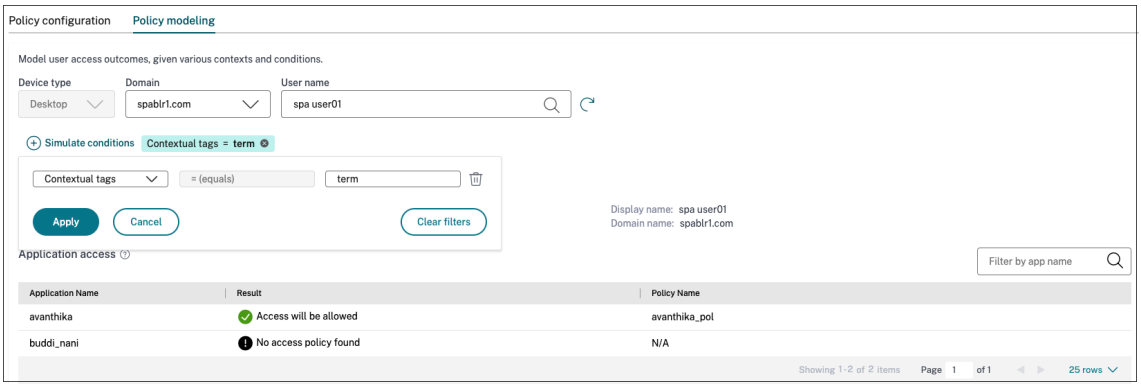
- **Application Discovery:**

  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.



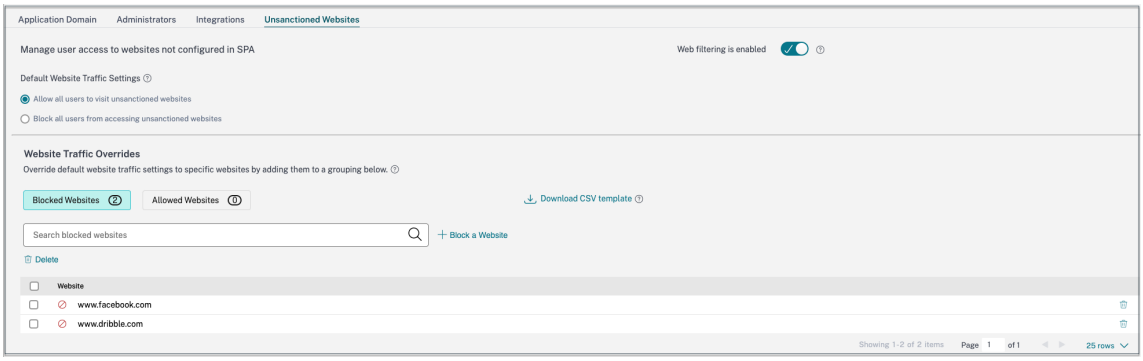
- **Policy modeling tool:**

  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.



Known issues

November 25, 2025

The following known issues exist in the Secure Private Access for hybrid deployments in the 2511 release.

- App launches from Citrix Workspace app or web-based user interface prompts for proxy login.

  Workaround: Cancel the prompt to continue with app launch.

  [SPAOP-8997]

- On the first app launch from Citrix Workspace app or the web-based user interface without a Chrome profile, the app does not open in the Chrome browser after the profile is added.

  [SPAOP-10480]

- If NetScaler is added as an IdP for OIDC under Third Party SSO in Google Cloud Identity, users are unable to sign in to the Chrome profile after signing out either explicitly or due to a session timeout.

  Workaround: The managed profile must be removed and re-added.

  [SPAOP-10479]

- In Secure Private Access hybrid CEP deployment, the mTLS handshake between the CEP proxy and Secure Private Access proxy fails when SSL default profile or cipher group is enabled.

  [SPAOP-10478]

- Policy changes on Network Location service condition (adding or removing a location tag) fail on update.

  [SPAOP-10446]

- When configuring Citrix Enterprise Premium, if the Google customer changes, incorrect validation and unclear error message is displayed.

  [SPAOP-10441]

- The Policy modeling tool does not display the apps from a disabled policy.

  [SPAOP-10451]

- The Application Launch count chart in the Secure Private Access dashboard does not display the SaaS apps launch count.

  [SPAOP-10398]

- The Application Launch count chart in the Secure Private Access dashboard does not display all launched apps for a given time frame.

  [SPAOP-10175]

- Web app launches from Citrix Receiver for Linux display an AM_ERROR_UNEXPECTED prompt.

  [RFLNX-12726]

- You cannot add conditions for a machine-based policy from the access policy user interface (**Secure Private Access > Access Policies)**.

  [SPAOP-10492]

- Device Posture with SAML is not supported in an nFactor authentication flow.

  [SPAOP-8529]

- Special characters (#, @, !, ^, &, %) are not allowed in the Client Secret field while configuring the OAuth IdP profile on NetScaler.

  [NSAUTH-17351]

- The Citrix Secure Access client for Linux doesn't work if the client certificate authentication is configured in the NetScaler Gateway.
- The Citrix Secure Access client for Linux cannot tunnel the applications if the app FQDN ends with ".local".
- First-time app launches intermittently show the error message 'Service Unavailable…'in a managed profile.
- If data loss prevention (DLP) is configured, app access is allowed by the Citrix Secure Access client.

System requirements and prerequisites

March 5, 2026

Software version requirements

The following software versions are required for the Secure Private Access hybrid configuration:

- **NetScaler:** 14.1–66.54 and later
- **StoreFront:** 2507 LTSR CU1 or 2511 CR and later
- **Cloud Connector:** 6.141.0 / 4.420.200 and later

The following minimum software versions are required on the end user devices:

- **For web/SaaS applications:**
  - Google Chrome: 142
  - Citrix Workspace app for Windows: 2507.1 LTSR or 2508
  - Citrix Workspace app for Mac: 2508.10
- **For TCP/UDP applications:**
  - Citrix Secure Access for Windows: 25.5.1.15
  - Citrix Secure Access for Mac: 25.11.1.1
- **For endpoint analysis (EPA):**
  - EPA client for Windows: 25.10.1.7
  - EPA client for Mac: 25.10.3

Firewall requirements

The following firewall requirements assume that the standard HTTPS port 443 is used for StoreFront servers and the StoreFront load balancer. If a non-standard port is used, adjust the port settings accordingly.

Source	Source IP	Destination	Protocol	Port	Description
Internet	Any	NetScaler Gateway	TCP	443	-

Source	Source IP	Destination	Protocol	Port	Description
StoreFront servers	StoreFront server machine IP address	Secure Private Access load balancer	TCP	443	-
Cloud Connector	Cloud Connector machine IP address	Active Directory	TCP	389 or 636	-

If same NetScaler contains gateway and load balancers for StoreFront and Secure Private Access configurations:

Source	Source IP	Destination	Protocol	Port	Description
NetScaler	NetScaler Subnet IP (SNIP) address	StoreFront servers	TCP	443	-
NetScaler	NetScaler Subnet IP (SNIP) address	Cloud Connector	TCP	8443	Assuming the default port is used for Secure Private Access
NetScaler	NetScaler Subnet IP (SNIP) address	NetScaler outbound proxy	TCP	Depends on the outbound proxy port	-
NetScaler	NetScaler Subnet IP (SNIP) address	Backend applications (Web app or client/server apps)	Depends on the back-end application protocol	Depends on the back-end application port	-

If different NetScalers are used for gateway and load balancers for StoreFront and Secure Private Access configurations:

Source	Source IP	Destination	Protocol	Port	Description
NetScaler Gateway	NetScaler Subnet IP (SNIP) address	StoreFront Load balancer	TCP	443	-
StoreFront load balancer	StoreFront load balancer IP address	StoreFront servers	TCP	443	-
NetScaler Gateway	NetScaler Subnet IP (SNIP) address	Secure Private Access load balancer	TCP	443	-
Secure Private Access load balancer	Secure Private Access load balancer IP	Cloud Connectors	TCP	8443	Assuming the default port is used for Secure Private Access
NetScaler Gateway	NetScaler Subnet IP (SNIP) address	NetScaler outbound proxy	TCP	Depends on the outbound proxy port	-
NetScaler Gateway	NetScaler Subnet IP (SNIP) address	Backend applications (Web app or client/server apps)	Depends on the backend application protocol	Depends on the back-end application port	-

Prerequisites

March 5, 2026

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

NetScaler prerequisites

Chrome Enterprise Premium + Citrix Secure Access deployment

- Ensure that a NetScaler Gateway exists with the required settings for Citrix Desktop as a Service (DaaS). This NetScaler Gateway is used to enumerate Secure Private Access apps and DaaS apps in Citrix Workspace App/Citrix Receiver for Web.
  - To create Gateway using the wizard, see Setting up NetScaler for Citrix Virtual Apps and Desktops.
  - To set up NetScaler Gateway, see How to configure NetScaler.
- Ensure that a new public IP address and the corresponding private IP address exist for the new fully qualified domain name (FQDN). The public IP must be NATed to the private IP. This information is used to configure a new NetScaler Gateway for Secure Private Access apps. This Gateway FQDN is used to access private web apps using a managed Chrome profile. End users can also connect to the gateway using this FQDN from Citrix Secure Access client to access internal apps. This private IP address must be used in the **Internal IP address** field in the UI. For more information, see Get started with Secure Private Access hybrid deployment.
- Ensure that you have an SSL server certificate for the NetScaler Gateway. The certificate must include the necessary Fully Qualified Domain Names (FQDNs), including the FQDN for the new Secure Private Access NetScaler Gateway. See NetScaler configuration for the relevant configuration details.
- Ensure that an authentication profile is configured on NetScaler. You can use an existing authentication profile and the corresponding authentication virtual server as well. See Configure authentication for details.

> **Note:**
>
> For using NetScaler Gateway as an IdP for Google OIDC, see Open ID Connect profile to use NetScaler Gateway as the IdP.

Citrix Secure Access only deployment

- A new public IP address and the corresponding private IP address must exist for the new fully qualified domain name (FQDN). The public IP must be NATed to the private IP address. This information is used to configure a new NetScaler Gateway for Secure Private Access apps. This gateway FQDN is used to access private web apps using a managed Chrome profile. End users can also connect to the gateway using this FQDN from Citrix Secure Access client to access internal apps. This private IP address must be used in the **Internal IP address** field in the UI. For more information, see Get started with Secure Private Access hybrid deployment.

- You must have an SSL server certificate for the NetScaler Gateway. The certificate must include the necessary Fully Qualified Domain Names (FQDNs), including the FQDN for the new Secure Private Access NetScaler Gateway. See NetScaler configuration for the relevant configuration details.
- Ensure that an authentication profile is configured on NetScaler.

  Existing authentication profile and the corresponding authentication virtual server can also be used.
  See Configure authentication to create a new authentication profile.

Cloud Connector prerequisites

- Ensure that the Secure Private Access service is enabled on the Cloud Connector. Reach out to Citrix Support if you need help.
- Ensure that the outbound calls to Connector Common and Secure Private Access FQDNs are allowed from Cloud Connectors on port 443. For more details, see System and Connectivity Requirements for Cloud Connectors.

See Cloud Connector configuration for details.

StoreFront prerequisites

- Ensure that a Store is created on StoreFront with enabled remote access (NetScaler Gateway is configured). See StoreFront documentation.
- Add Secure Private Access as a site in your StoreFront store:
  - Open your store and select **Manage Sites**.
  - Click **Add Site**, choose **Secure Private Access** as the type, and enter the display name and the Secure Private Access load balancer FQDN.

> **Note:**
>
> StoreFront is optional if you are using Secure Private Access only for TCP/UDP (client/server) applications.

See StoreFront Configuration for details.

Secure Private Access prerequisites

- Ensure that a Windows Cloud Connector inbound rule allows port 8443 from the data center network. Citrix Secure Private Access exposes a plain HTTP service at port 8443.

- Ensure that the internal load balancer for Citrix Secure Private Access targets the Cloud Connector backend on port 8443.
- Ensure that an SSL Bridge or SSL Offload is configured on the internal load balancer for Citrix Secure Private Access.

See Secure Private Access service for details.

Google prerequisites

Chrome Enterprise Premium license

Ensure that you have an active Chrome Enterprise Premium license, available through the Citrix Cloud Platform License (CPL) program.

Google Workspace Admin console

- **Google customer ID:** Obtain your Google Customer ID from the Google Admin console. This ID is required to configure Google services and integrations. Your customer ID can be retrieved through **Account > Account Settings** in the Google Admin console.
- **Create a custom role in the Google Admin console:** To onboard customers to Chrome Enterprise Premium (CEP) and enable Google Chrome integration, admins must create a custom role and assign the appropriate privileges in the Google Admin console. For details, see Admin roles and privileges.
- **Proxy mode configuration:** Set the proxy mode to Allow user to configure proxy. Avoid restrictive options such as No proxy, OS proxy, or Use this proxy only.

  > **Note:**
  >
  > If the Google Admin console is set to use system proxy settings, the managed profile cannot apply the required proxy configuration for Citrix Secure Private Access, and the integration with Chrome Enterprise Premium fails.

- **Restrict DevTools extensions:** Chrome DevTools for force-installed extensions must be disabled to prevent exposure of sensitive data. This is the default option in the Google Admin console.
- **Access restrictions are now configured in Google Admin console for Chrome Enterprise Premium:** Access restrictions that were previously configured in the Secure Private Access console only apply to Citrix Enterprise Browser. When Google Chrome is the enterprise browser, access restrictions 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.

For details on creating policies and rules in the Google Workspace Admin console, see the following topics:

- Set Chrome Enterprise connector policies for Chrome Enterprise
- Data protection rules

- **License:** Ensure that you have an active Chrome Enterprise Premium license, available through the Citrix Cloud Platform License (CPL) program.

Google Chrome

Managed Chrome profiles

All end users must access Chrome using a managed profile. Managed profiles ensure that Chrome policies, extensions, and security settings are enforced on user devices.

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

You must synchronize the user directory configured in Citrix Workspace or StoreFront with the Google Cloud user directory. Specifically, the following user directories are supported:

- Active Directory
- Microsoft Entra ID (previously known as Azure Active Directory)

> **Note:**
>
> Synchronize the user directory periodically to ensure that application access is appropriately enforced.

Populate Email Address fields (mandatory) The Google Cloud user directory requires the email address field to be populated. To be synchronized with the Google Cloud user directory, a user or group object in Secure Private Access must have an email address. Otherwise, the synchronization fails.

Ensure that all users that require access to the integrated Chrome Enterprise Premium and Secure Private Access offering, as well as all groups involved in access security policies, have the email address field populated. The email address domain part must be a domain that is configured and verified in your Google Admin console.

Active Directory sync You must synchronize your AD with the Google Cloud user directory to ensure seamless integration and consistent user management across your enterprise using the Google Cloud Directory Sync.

For details on how to sync your AD with Google Cloud to include custom AD fields under the custom schema "Citrix-schema", see Connect Google Cloud Identity as an identity provider to Citrix Cloud.

Microsoft Entra ID You must synchronize your Microsoft Entra ID with the Google Cloud user directory for user and group management across both Google and Microsoft cloud platforms. For details, see Get started with Directory Sync.

For more information, see Google Directory sync.

Bypass TLS inspection

To ensure that Chrome Enterprise Premium endpoints function correctly on networks employing TLS inspection (or SSL inspection), you must exclude the following hostnames from inspection.

- `ingress.cloudproxy.app`
- `securegateway.goog`
- `*.securegateway.goog`

This exclusion is essential because many TLS inspection solutions (such as SSE vendors or proxy servers) do not fully support the HTTP CONNECT method used by Chrome Enterprise Premium, which can result in traffic being abruptly dropped.

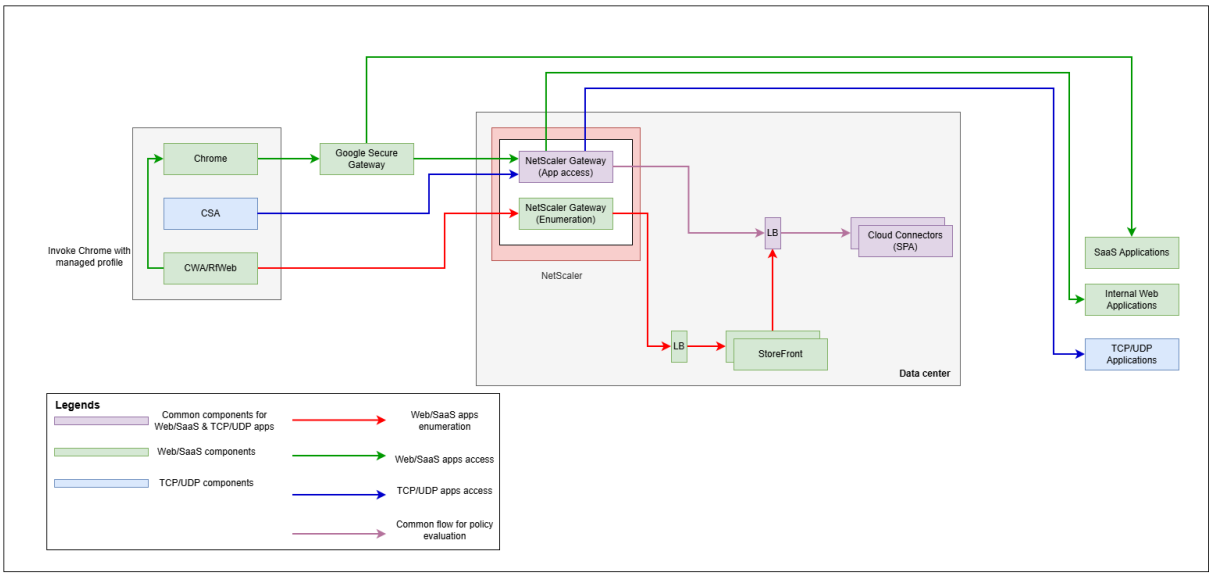
Furthermore, it is recommended to exclude the following hostnames from TLS inspection to avoid potential end-user performance issues and connection delays.

- `safebrowsingrealtime.googleapis.com`
- `secureconnect-pa.clients6.google.com`
- `secureconnect-pa.mtls.clients6.google.com`
- `secureconnect-pa.googleapis.com`
- `chromereporting-pa.googleapis.com`

Get Started with Secure Private Access hybrid deployment

December 2, 2025

This topic provides step-by-step instructions for setting up the Secure Private Access hybrid environment.



Before you begin

Verify your Secure Private Access entitlement

You must be entitled to the Secure Private Access service in your Citrix Cloud account.

- Log in to the Citrix Cloud console.
- On the dashboard, verify that the **Secure Private Access** service tile is visible and available.
- If the service is not visible, you cannot proceed. Contact your Citrix representative to resolve the entitlement issue.

Verify prerequisites

Ensure that all prerequisites are met. For details, see Prerequisites.

Verify that all networking prerequisites are met. Refer to the network diagram for complete details of all required ports and communication paths.

Choose the deployment mode

On the welcome screen, select **Set up Hybrid** to begin the configuration.

Next steps

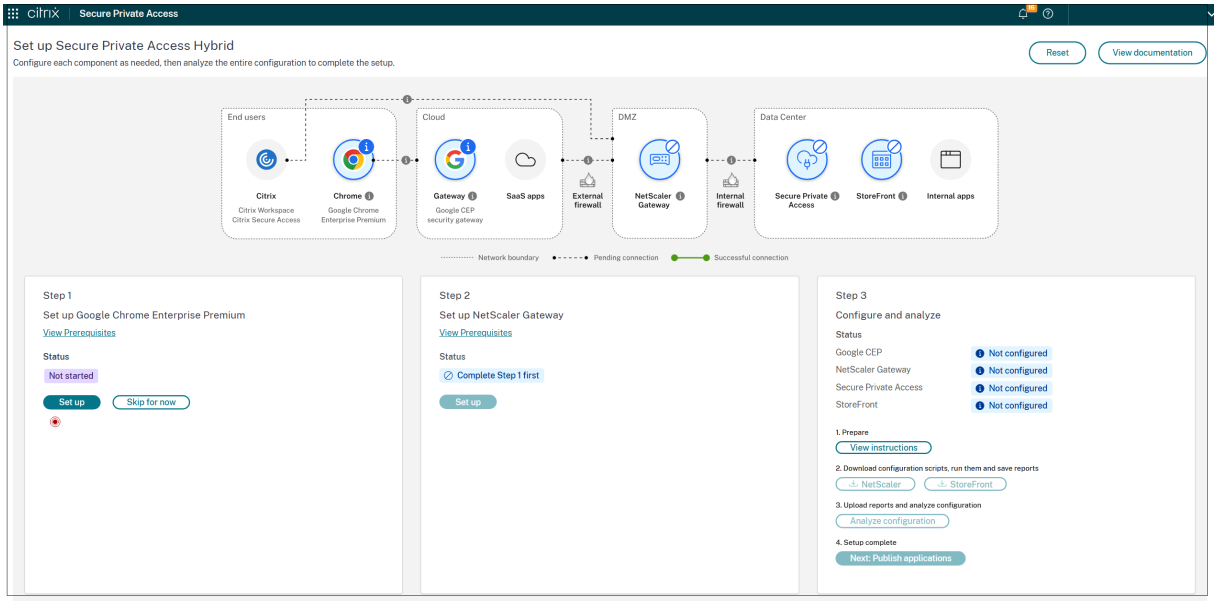
- Step 1: Set up Google Chrome Enterprise Premium
- Step 2: Set up NetScaler Gateway
- Step 3: Configure and analyze

Step 1: Set up Google Chrome Enterprise Premium

March 13, 2026

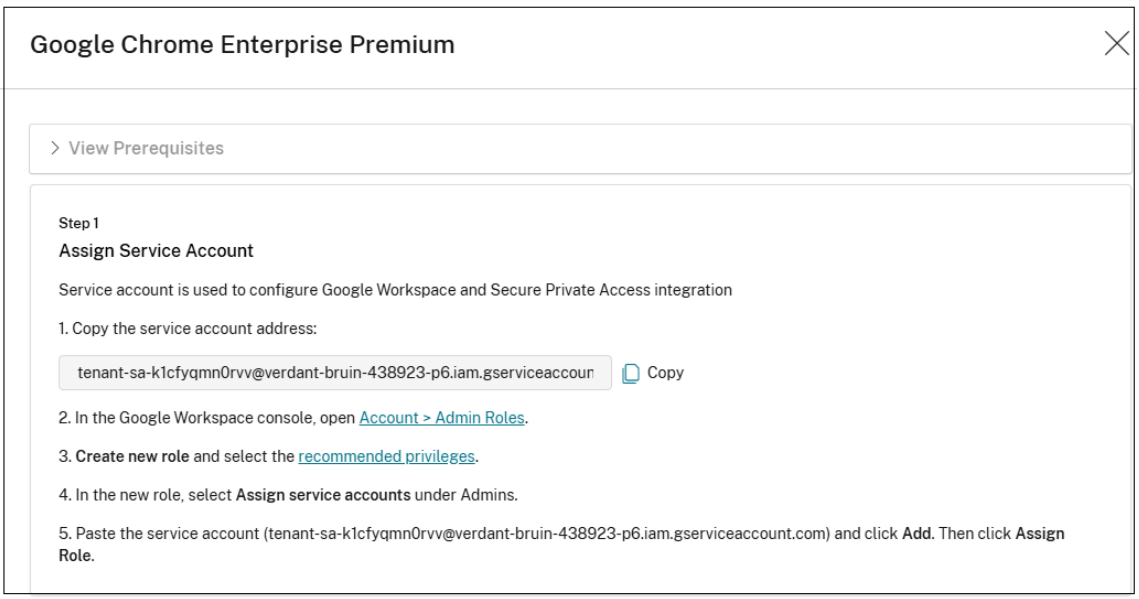
At this step, you are prompted to configure Google Chrome Enterprise Premium.

> **Note:**
>
> Before setting up Google Chrome Enterprise Premium, consider the following points:
>
> - If you are using Secure Private Access only for TCP/UDP (client/server) applications, click **Skip for now**. Otherwise, click **Set up** to begin the configuration for securing web and SaaS applications.
> - If you click **Skip for now**, you cannot enable Chrome Enterprise Premium later without a full reset.
> - If you choose to **Set up** Chrome Enterprise Premium, you are enabling support for Web/SaaS applications. This path also allows you to configure TCP/UDP (client/server) applications. If you plan to use Secure Private Access for Web or SaaS applications in the future, you must click **Set up** now.
>
> The only way to enable Web/SaaS features after skipping this step is to reset your entire Secure Private Access configuration. To do this, contact Citrix Support.

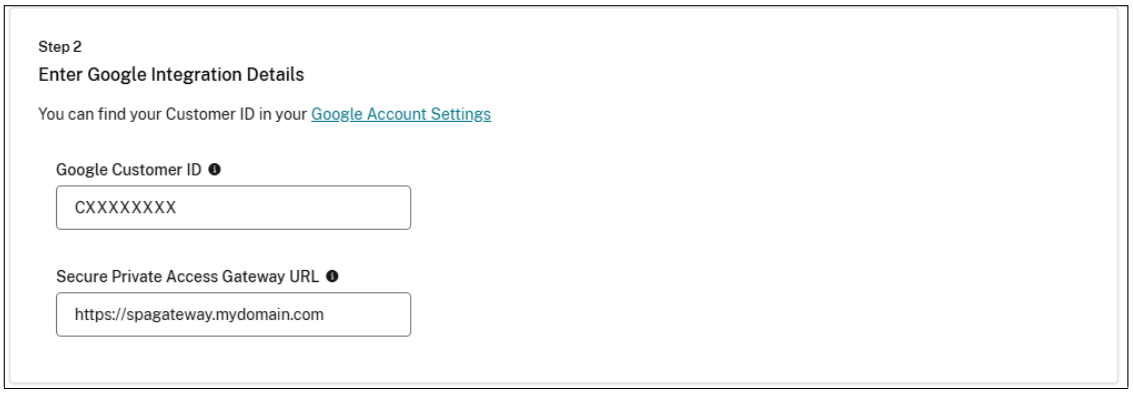


Google Chrome Enterprise Premium configuration

1. Follow the on-screen instructions to create a **Google Admin Role**.
2. Assign the new role created for Secure Private Access role to the **Citrix service account** as shown in the instructions. This account is used by Citrix to perform the necessary integration configuration in your Google Workspace Admin console.



3. Follow the on-screen instructions to find your **Google Customer ID** within the Google Workspace Admin console.



4. Copy the Google customer ID and paste it into the **Google Customer ID** input field.
5. Ensure that you have already reserved a public IP address and DNS record for your NetScaler Gateway.

   “Enter this public URL in the **Secure Private Access Gateway URL** field. This URL will be the public address for the NetScaler Gateway you will configure in the Step 2 - Set up NetScaler Gateway.

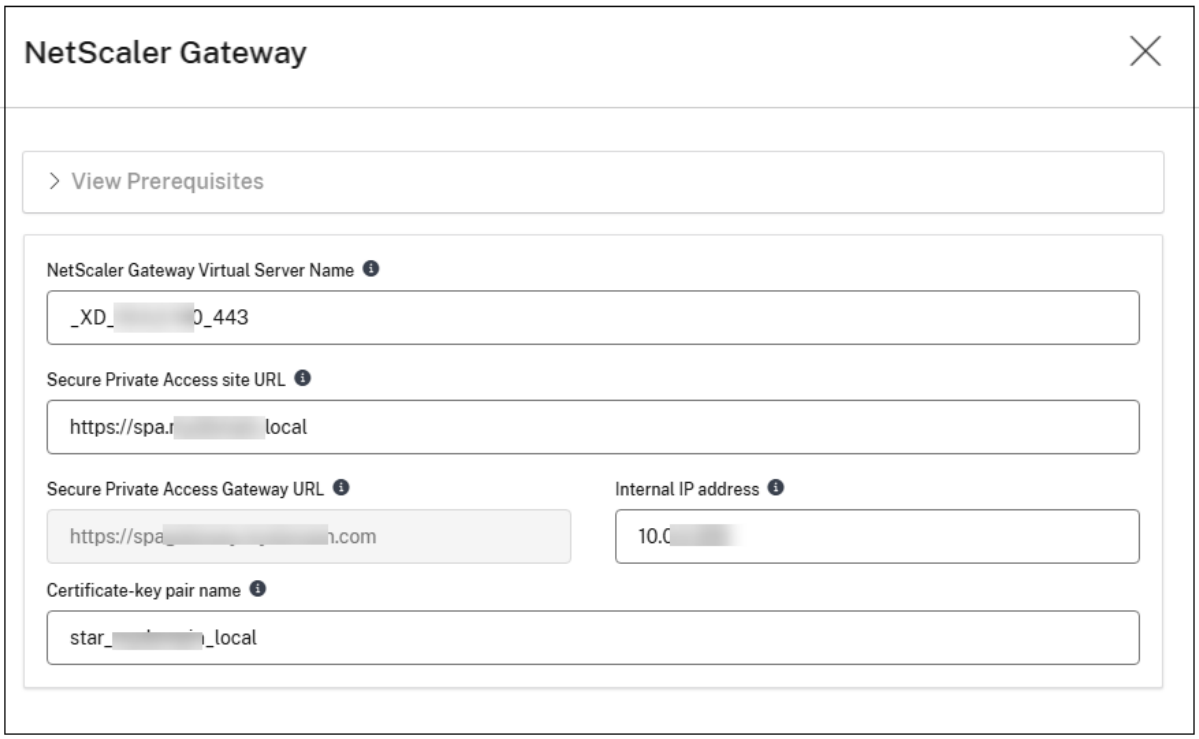
   Saving this setting automatically configures the **Google Secure Gateway** to use this address, which enables it to connect to your NetScaler Gateway for internal app access.
6. Click **Verify** to ensure that all configurations are correct, and that Secure Private Access is ready for Chrome Enterprise Premium integration.
7. Click **Save**.

Step 2: Set up NetScaler Gateway

December 2, 2025

In this step, you are prompted to enter the details required to configure Secure Private Access on your NetScaler.

> **Note:**
>
> Ensure NetScaler meets all prerequisites.



- **NetScaler Gateway virtual server name:** Enter the name of the NetScaler Gateway virtual server that is already configured with your StoreFront deployment. This virtual server is used to enumerate applications configured in Secure Private Access within the Citrix Store.

  > **Note:**
  >
  > This input is not required if you skipped the Chrome Enterprise Premium configuration.

- **Secure Private Access site URL:** Enter the load balancer URL that directs traffic to the Secure Private Access services running on your Cloud Connectors.

  This load balancer must be configured to use **HTTPS on port 443**. If you have not yet created this load balancer, see Secure Private Access load balancer for instructions before proceeding.

- **Secure Private Access Gateway URL:** This URL is the public address for the NetScaler Gateway that is shared with the users. It is utilized to connect to internal applications.

- **Internal IP address:** Enter the **private IPv4 address** that is used for your Secure Private Access gateway. This IP address is assigned to the NetScaler Gateway virtual server during the configuration in Step 3 - Configure and Analyze.

- **Certificate-key pair name:** Enter the name of the **SSL certificate-key pair** that is already configured on your NetScaler.

- Click **Save**. Once saved, a **Shared Secret** is displayed. You need this shared secret value for configuration in Step 3 - Configure and Analyze.

Step 3: Configure and analyze

December 2, 2025

Configuration can now be applied to the on-premises StoreFront and NetScaler components.

Before proceeding, ensure that all prerequisites for both StoreFront and NetScaler are met.

Download and run NetScaler and StoreFront scripts

NetScaler script

> **Note:**
>
> All Secure Private Access configurations on the **NetScaler** must be performed using the **Command Line Interface (CLI)**.

1. Click **NetScaler** to download the setup script. This script is a diagnostic tool designed to configure and analyze your NetScaler Gateway for the Secure Private Access deployment, and collect the required information. For more information, see NetScaler Gateway Analyzer.

   The script file name has the following format:

   `gateway_analyzer_<tenant-id>_<timestamp>.tar.gz`

2. Use an **SCP client** (like `scp` or WinSCP) to copy the downloaded `*.tar.gz` file to your **NetScaler**.
3. Place the file in the `/var/tmp/` directory.
4. Log in to your NetScaler's command-line interface (CLI) using **SSH** (for example with PuTTY) with administrative (`nsroot`) privileges.
5. Type "shell"on the CLI prompt to access the NetScaler shell. Navigate to the temporary directory: `cd /var/tmp/`
6. Extract the archive.

   > **Note:**
   >
   > Your file name is specific to your download.
   >
   > `tar -xzf gateway_analyzer_<tenant-id>_<timestamp>.tar.gz`

7. The `tar` command creates a directory. Use `ls` to see the new folder's name, then navigate into it.
8. Run the analyzer script using python3: `python3 analyzer.py`

9. When the script prompts for the **Shared Secret**:
    a) Return to the Secure Private Access setup page in your browser.
    b) Copy the **Shared Secret** from the **Set up NetScaler Gateway** section (the one you saved in the earlier step).
    c) Paste the secret into the CLI and press **Enter**.

> **Note:**
>
> The **Shared Secret** is a password field. Characters are not visible on the screen as you paste or type. This is expected.

10. After the script is successfully run, it generates an analysis report in the current folder.
11. Download and save this report using scp/winscp. You need it for the Analyzer later.

StoreFront script

> **Note:**
>
> This step is optional for CSA-only mode, that is, if CEP configuration is skipped in Step 1 - Set up Google Chrome Enterprise Premium.

1. Click **StoreFront** to download the PowerShell script.
2. This script is a diagnostic tool designed to:
    a) **Analyze** your on-premises StoreFront configuration.
    b) **Collect** the information needed for your deployment.

> **Warning:**
>
> **Administrator and execution policy required:** You must run this PowerShell script with administrator privileges (example, right-click and "Run as Administrator").

    Additionally, you might need to adjust the PowerShell execution policy to allow the script to run. If necessary, you can do so by running `Set-ExecutionPolicy Bypass` (or an appropriate policy for your organization) from an elevated PowerShell prompt.

    The script file name has the following format:

    `storefront_analyzer_<tenant-id>_<timestamp>.zip`.

3. Copy the downloaded .zip file to your **StoreFront server**.
4. On the StoreFront server, **extract** the contents of the .zip file (for example, to a folder like C:\temp\spa-sf-script).

5. Open a **PowerShell** window with **Administrator privileges** (right-click, "Run as Administrator").
6. In the PowerShell window, navigate (using cd) to the directory where you extracted the script.
7. Execute the script by running the following command:

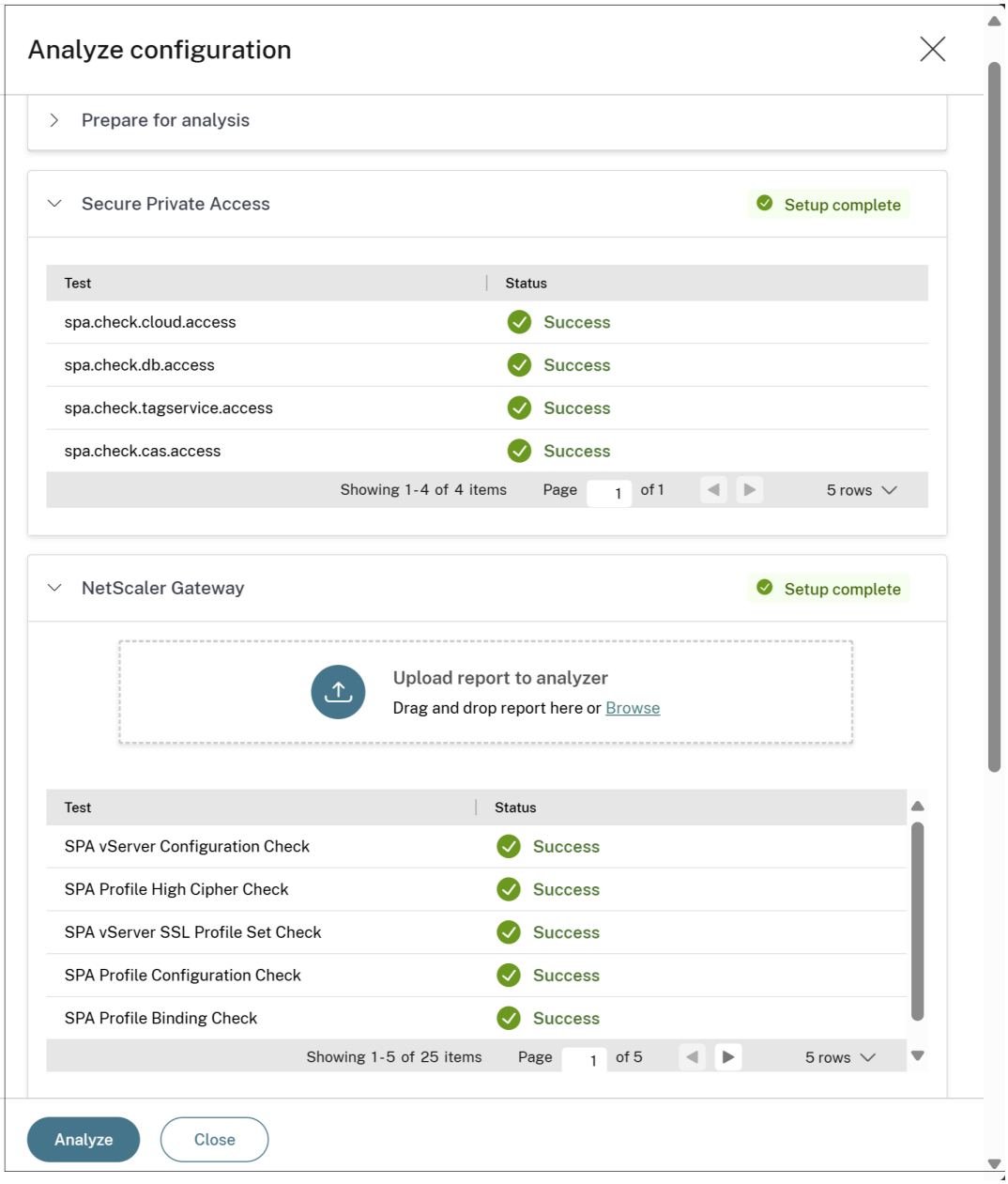
   ```
   .\CollectAnalyzerStorefrontInfo.ps1
   ```

Once the script is successfully run, it generates an analysis report. Download and save it for the next step.

Upload reports and analyze configuration

You can now upload the reports generated by the on-premises scripts to validate your configuration.

1. Click **Analyze**.
2. You are prompted to upload your analysis reports. Upload the two files that you generated:
   - The **NetScaler** analysis report.
   - The **StoreFront** analysis report.
3. Once both files are successfully uploaded, click **Analyze**.
4. Wait for the analysis to complete. The system displays the **Success/Failed** results for all checks.
5. **Review the analysis results:**
   a) **If all analyzer steps have passed:** You have successfully validated your configuration and can proceed to the next step.



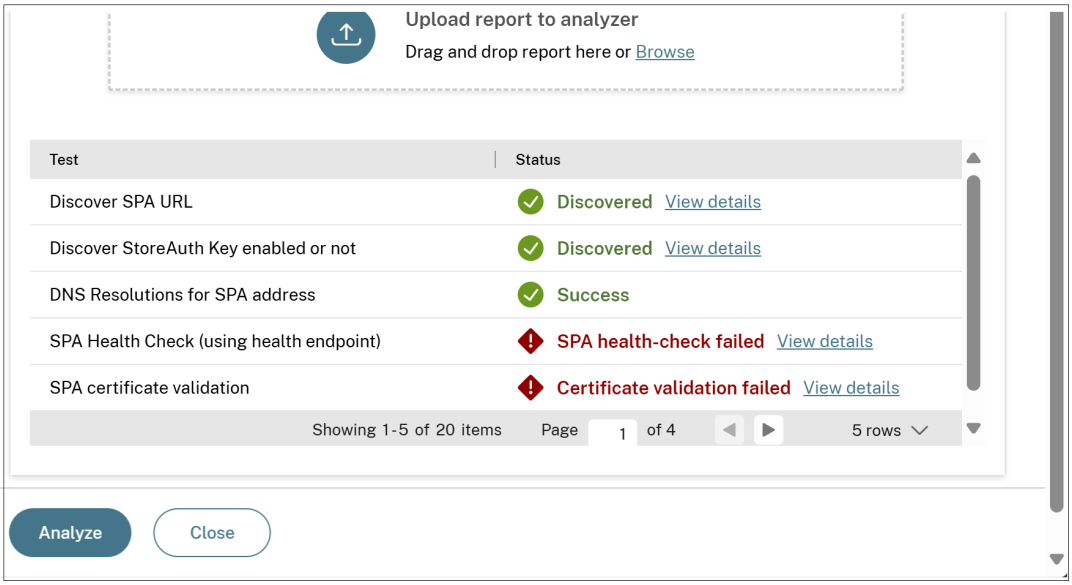
b) **If any of the steps failed:**

i. The report suggests **remediation steps**.

ii. Follow the suggested instructions to fix the error on the failed component (NetScaler or StoreFront).

iii. After fixing the issues, **re-run the diagnostic script** on that component to generate a new report.

iv. Return to this step and **re-upload the new analysis report**.



Complete onboarding and publish applications

Click **Next: Publish applications** to complete and exit the setup wizard.

This completes your initial hybrid onboarding.

Post-onboarding tasks

December 2, 2025

Configure applications

Your next immediate task is to publish your first application. It is recommended that you test your setup by publishing at least one internal web application or one TCP/UDP application. Follow the detailed instructions in the Apps Configuration and Management.

Configure access policies

- In the Secure Private Access admin console, navigate to **Policies > Access Policies**.
- Create an access policy for your application, making sure to define the **User conditions**.
- See the Access policies configuration and management for complete details.

Synchronize the configuration

After saving the changes (new applications or policies), the Secure Private Access component inside your on-premises Cloud Connectors must synchronize this new configuration from Citrix Cloud.

This process typically takes up to **10 minutes** to complete.

How to verify: It is recommended to check if the new configuration has been applied by using the **Policy Modeling tool** (under **Policies > Policy Modeling**) to see if your new policies are active.

Access your applications (end users)

This section captures information about how end users access published applications on their devices.

Supported Devices:

- **Web/SaaS applications** (via Google Chrome managed profile) are accessible from any desktop OS.

  On Linux, iOS, and Android devices, Web/SaaS applications are accessible via the Citrix Secure Access client.

- **TCP/UDP applications** (via the Citrix Secure Access client) are supported on **Windows, macOS, Linux, iOS, and Android**.

Accessing Web and SaaS applications

There are three primary ways for users to access their web applications on desktop devices. All these methods will automatically launch the app in the Google Chrome managed profile.

Method A: Using Chrome browser with managed profile (recommended) This is the most seamless experience for the user.

1. Launch the **Google Chrome** browser.
2. If this is your first time, add a new browser profile using the corporate email address that is configured on the access policy. This creates a managed profile.
3. In the managed profile, navigate to your **NetScaler Gateway URL** (the one configured in Step 2 - Set up NetScaler Gateway).
4. Log in to your store.
5. Click a Web or SaaS application icon to launch it.

The app launches in a new tab in the managed profile.

Method B: Using a non-managed web browser

> **Note:**
>
> This method requires a supported version of the Citrix Workspace app to be installed on the desktop device.

1. Launch any browser of your preference (for example, non-managed Chrome, Edge, Firefox).
2. Navigate to your **NetScaler Gateway URL** (the one configured for StoreFront in Step 2 - Set up NetScaler Gateway).
3. Log in to your store.
4. Click a Web or SaaS application icon to launch it.
5. The browser displays a dialogue prompting you to open the **Citrix Workspace App**.
6. Click **Continue** or **Open**.
7. Citrix Workspace app takes over and launches the application in the **Google Chrome managed profile**. If a profile is not already created, a setup screen with your email address pre-populated appears for you to complete the profile.

Method C: Using Citrix Workspace app

1. Launch the **Citrix Workspace App** on your device.
2. If not already configured, add your store using the **NetScaler Gateway URL** (the one configured for StoreFront in Step 2 - Set up NetScaler Gateway).
3. Log in to your store.
4. You can see your list of enumerated applications.
5. Click a Web or SaaS application icon to launch it. The application automatically opens in the managed Google Chrome profile.

Accessing TCP/UDP (client/server) applications

Accessing TCP/UDP applications requires the Citrix Secure Access client.

You must install Citrix Secure Access with the supported version on the endpoint device.

Connect the Secure Access Client

1. Launch the **Citrix Secure Access client**.
2. When prompted for a URL, enter the **Secure Private Access Gateway URL** (the FQDN configured in Step 2 - Set up NetScaler Gateway).

3. Complete the login and authentication prompts.
4. The client connects and then runs securely in the background.

Launch your published applications You can now use your native client software directly if allowed by Secure Private Access policies. For example:

- Open **Microsoft Remote Desktop** and connect to the internal host name of your RDP server.
- Open an **SSH client** and connect to the internal IP of your Linux server.

Cloud Connector Configuration

November 25, 2025

Secure Private Access service runs in Cloud Connectors as Windows service. Ensure that Cloud Connectors are installed in your resource location. Set them up if necessary.

For details, see Cloud Connector installation.

Ensure that your Cloud Connectors (or their configured proxy) can send outbound traffic on port 443 to all FQDNs listed in the Connector Common and SPA FQDNs of the `allowlist.json` file.

Secure Private Access service

November 25, 2025

The Secure Private Access™ service provider for 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.

Port Configuration for Citrix Secure Private Access service

- Citrix Secure Private Access uses port 8443 as a plain HTTP service.
- Ensure that the inbound rule for port 8443 is added to allow access from the data center network. The port 8443 can be opened by manually configuring the firewall rules or by running the Citrix Secure Private Access config tool.
    - Navigate to the Citrix Secure Private Access installation folder (default path - C:\Program Files\Citrix\AccessSecurityService).
    - Run the command .\Citrix.AccessSecurityService.exe /ENABLE_SPA_PORTS 8443.

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

- The internal load balancer for Citrix Secure Private Access adds the Cloud Connector back-end service using port 8443.

Secure Private Access load balancer

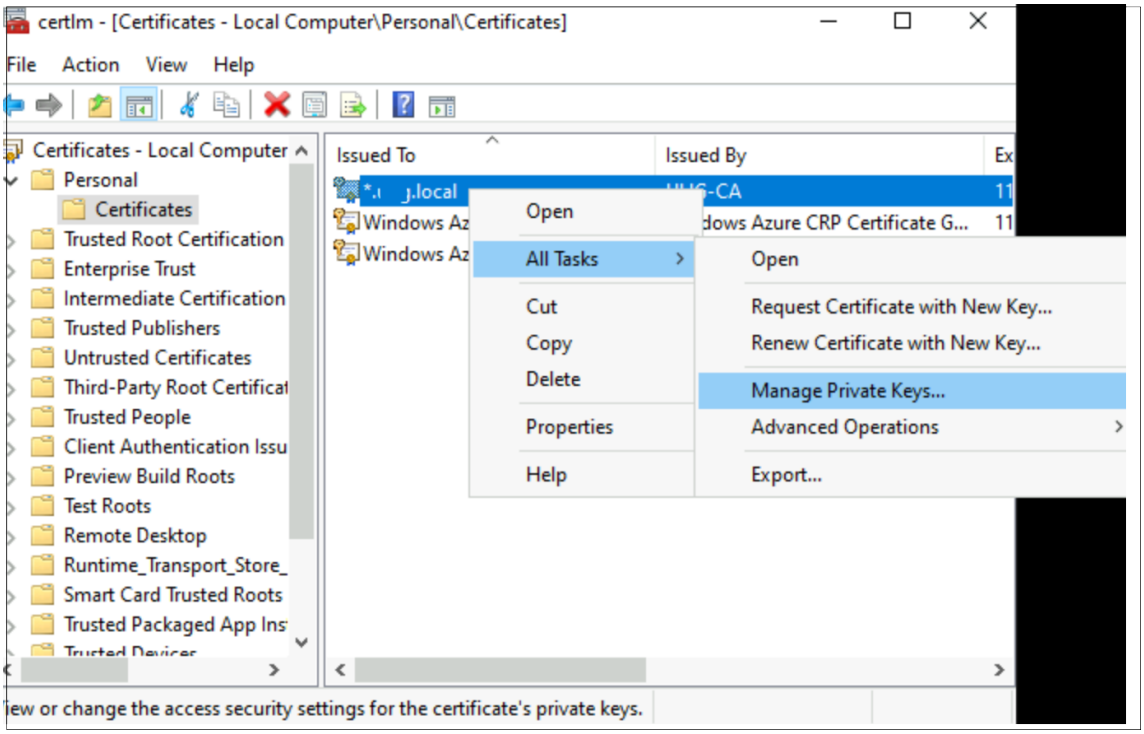
The load balancer for the Secure Private Access service must be configured with TLS enabled using one of two approaches:

- **SSL offload on the load balancer:** The Secure Private Access load balancer communicates with the Secure Private Access service on Cloud Connector over HTTP on port 8443, and the TLS/SSL certificate is installed on the load balancer. Traffic between the load balancer and the Secure Private Access service is plain HTTP and not encrypted. For details, see Configure SSL offloading.
- **SSL bridge:** The load balancer forwards encrypted traffic to the Secure Private Access service on Cloud Connector. TLS/SSL certificate must be installed for the Secure Private Access service on each Cloud Connector host. For details, see See Configure SSL bridging.

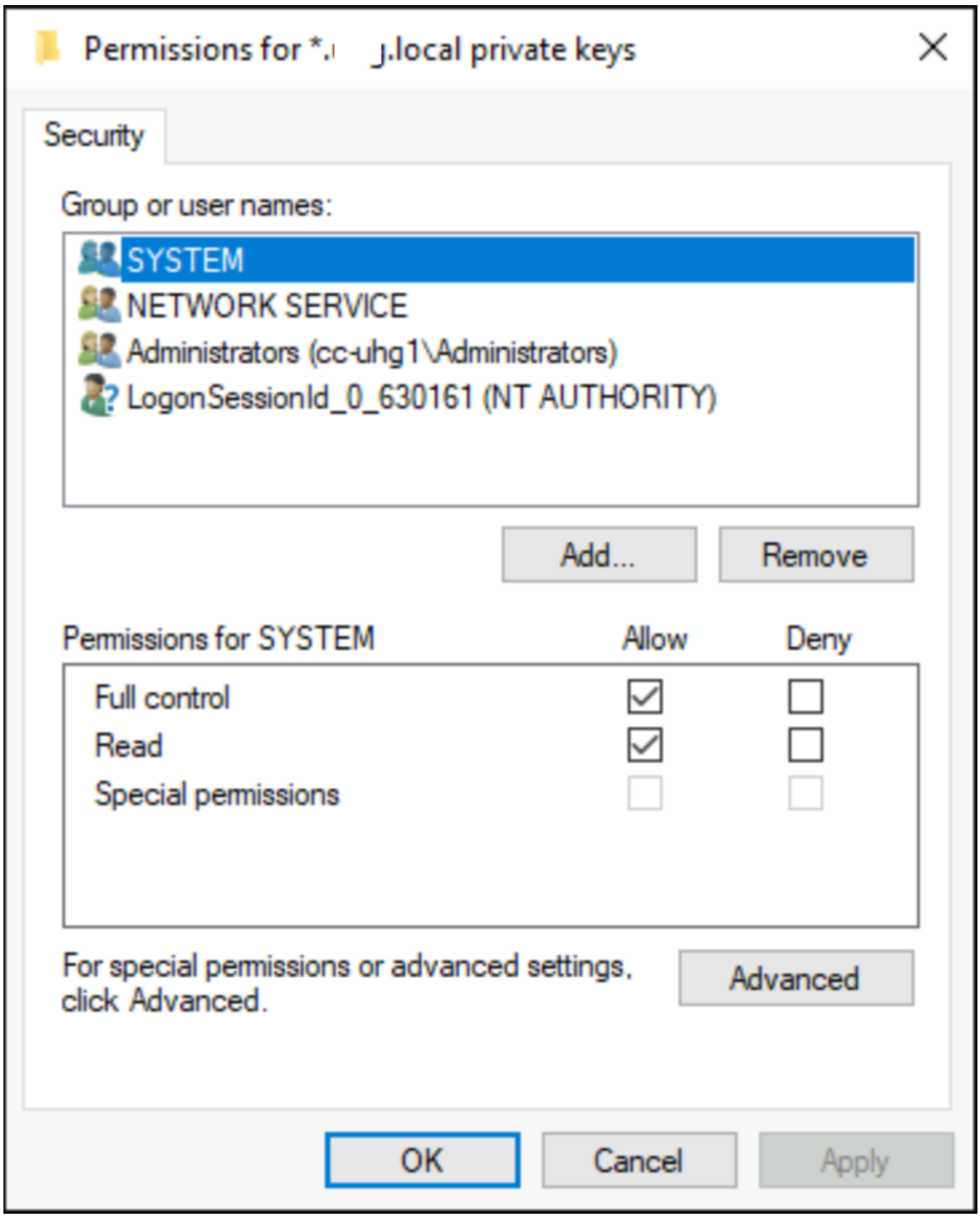
Configure TLS/SSL certificates for the Secure Private Access service on Cloud Connector

1. Install a valid TLS/SSL certificate on the Cloud Connector's local machine Personal certificate store. Ensure that the certificate is trusted. Add the issuing CA certificates if necessary.
2. Grant Network Service account permission to access the installed certificate.
    a) Open the Microsoft Management console and add certificate snap-in to your local computer account, follow the wizard, and click **OK**.
    b) In the Microsoft Management Console, go to **Console Root > Certificates > Personal > Certificates**.

c) Right-click the certificate that is required to configure Secure Private Access and select **All Tasks > Manage Private Keys**.



a) In the **Permissions** window, click **Add** and then search for the Network Service account, and select **Read only permission**.



3. Configure the Secure Private Access service with TLS/SSL certificate thumbprint.

   a) Copy the thumbprint from **TLS/SSL Certificate Details**.

   b) Navigate to the Citrix Secure Private Access installation folder (default path - C:\Program Files\Citrix\AccessSecurityService) and run .\Citrix.AccessSecurityService.exe /CERTIFICATE_THUMBPRINT <ThumbprintValue>.

c) Restart the Citrix Secure Private Access service.

4. Ensure that the Secure Private Access service is running as a TLS service (use browser or cURL): `https://<Cloud connector address>:<port>/secureAccess/health`.

   Expected result: `response 200 OK with status "Ok"`.

NetScaler

November 26, 2025

The topic helps you ensure that all prerequisites for NetScaler configuration are met.

- Set up NetScaler Gateway for Citrix Virtual Apps and Desktops by using one of the following methods:
  - Create a NetScaler Gateway virtual server for remotely accessing StoreFront, for users who are using Citrix Workspace app or a web browser. For details, see Integrate NetScaler Gateway with StoreFront.
  - Configure the settings on NetScaler Gateway. For details, see ConfigureNetScaler Gateway appliance by using wizards.

  > **Note:**
  >
  > The XenApp and XenDesktop wizard configures the basic authentication. Secure Private Access requires advanced authentication. Therefore, you can skip the **Authentication step** in XenApp and XenDesktop wizard. You can configure the authentication profile later once NetScaler Gateway is created using the wizard.

- Add SSL certificates to NetScaler. For details, see Install SSL certificates on a NetScaler instance.

Configuring a load balancer for StoreFront. For details, see Load balancing with NetScaler.

Configure authentication

Perform the following steps to configure authentication:

- Configure an authentication virtual server. For details, see Authentication virtual server.
- Configure an authentication profile. For details, see Configuring Authentication Profiles.
- Configure nFactor authentication. For details, see nFactor authentication.

  Commonly used nFactor authentication methods:

- LDAP authentication
- RADIUS authentication
- Microsoft Entra ID

Sample authentication configurations

Multifactor authentication with conditional authentication

- Dual factor authentication with LDAP and RADIUS using dual factor schema (taking user input only once)
- Authentication log on method according to user's departments (Employee, Partner, Vendor) in organization with drop-down menu to select the department
- Authentication log on method according to user domains with drop-down menu
- Configure email ID (or user name) input as first factor with conditional access based on group extraction with email ID at first factor and provide different logon type for each group
- Multifactor authentication using Certificate authentication for users with user certificates and Native OTP registration for non-cert users
- Different authentication type with conditional authentication according to user host name inputs
- Dual factor authentication with Native OTP authentication
- Google Re-CAPTCHA

Third-party integration with multifactor authentication

- Configure Azure AD as SAML IdP (Configure next factor as LDAP policy - NO_AUTH to complete OAuth trust)
- Conditional authentication with First factor as SAML and then custom login to certificate or LDAP based on SAML attributes
- First factor as webauth login followed by LDAP

Device posture scans (EPA)

- Device posture check for version check followed by customized login for compliant (RADIUS) and non-compliant users(LDAP)
- LDAP authentication followed by mandatory device posture scan
- Device posture check before and after AD authentication - Pre and Post-EPA as a factor
- Device Certificate as an EPA factor

Miscellaneous scenarios

- Add EULA with authentication
- Customize nFactor policy labels, login schema

StoreFront

November 25, 2025

To display Secure Private Access web applications in your on-premises Citrix Store, you must configure the Secure Private Access service as a new Delivery Controller on StoreFront.

Follow this procedure, especially if you are integrating with an existing Citrix DaaS environment (as it allows you to use your existing StoreFront).

1. On the StoreFront server, open the StoreFront admin console.
2. Navigate to the section for managing Delivery Controllers (for example, select **Store** and click **Manage sites**).
3. Click **Add** to create a new controller.
4. When prompted for the controller type, select the **Secure Private Access** option.
5. In the **Server** field, enter the FQDN of your Secure Private Access load balancer.
6. Select Transport type **HTTPS** and Port **443**.
7. Save your changes.

Configuring a new Store

If the Store doesn't already exist, install the supported version of StoreFront, and then follow the **Create Store** wizard. Ensure that the Store is configured with:

- **Remote access:** Remote access configuration requires NetScaler Gateway virtual server address that is used to enumerate web/SaaS applications published in Secure Private Access.
- **Authentication methods:** Ensure Pass-through from Citrix Gateway is enabled.

For details, see Create store.

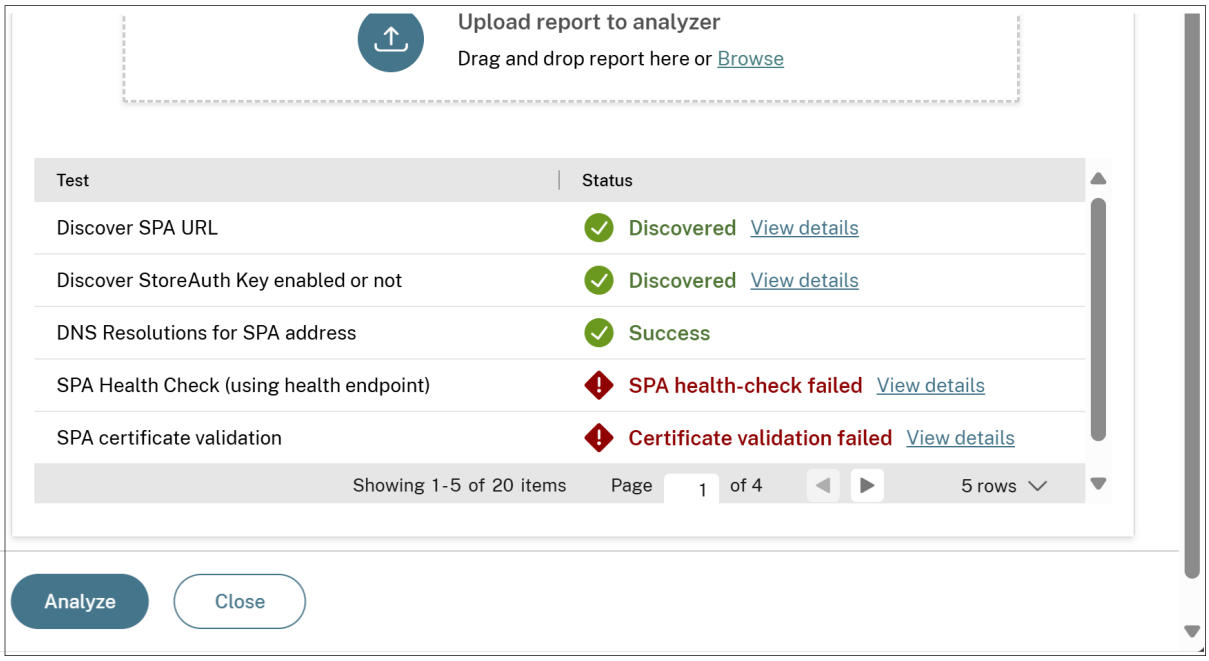
Component Analyzer

November 25, 2025

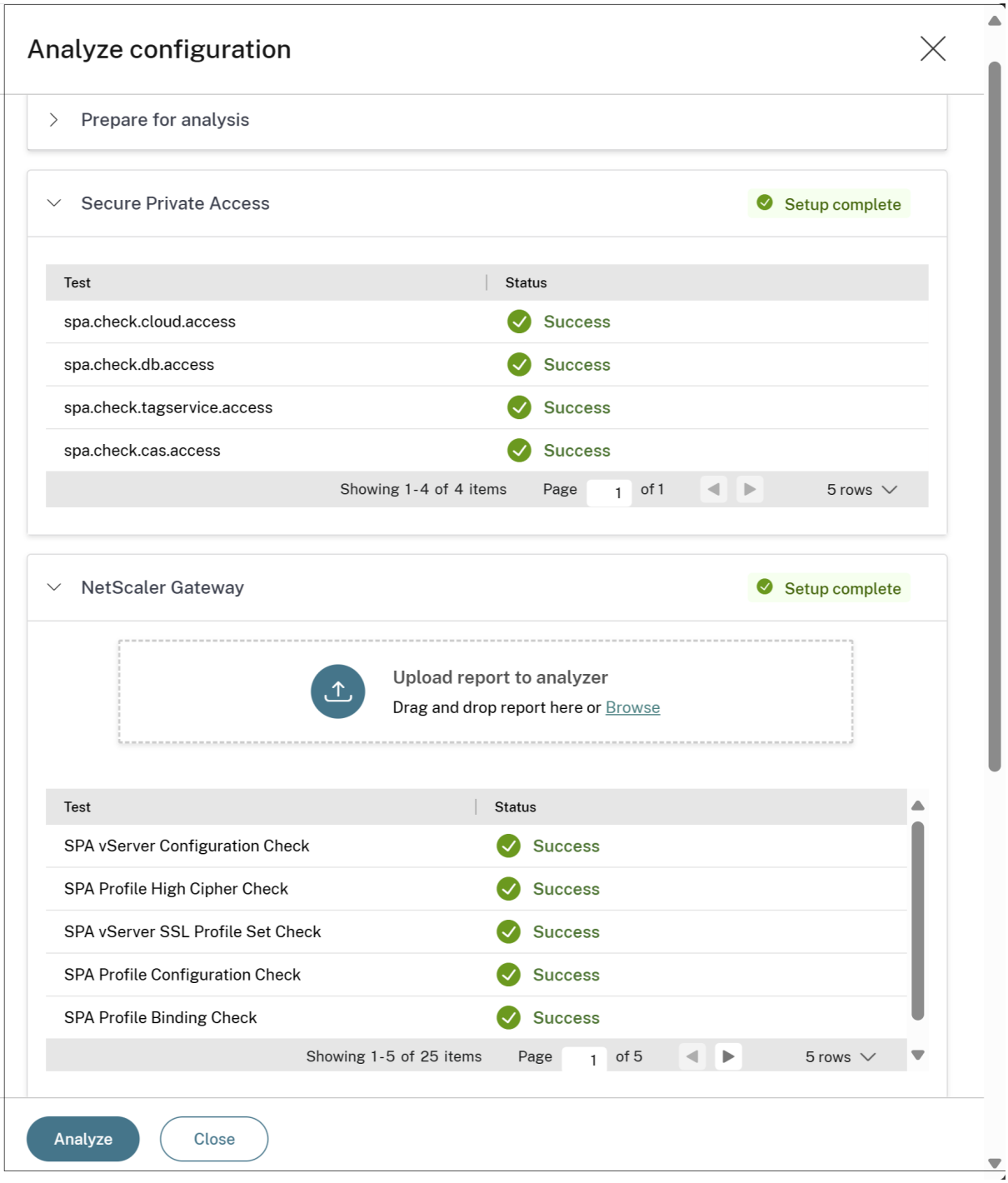
Component Analyzer is a web-based tool that performs the configuration checks required for a Secure Private Access hybrid setup. After uploading the necessary reports, the Analyzer identifies issues with detailed error messages and explanations, including examples of detected StoreFront configuration errors. The tool also lists potential remediations to resolve the identified problems.

You must re-run the Analyzer after applying remediations to confirm that all configuration checks pass.

Example of a detected StoreFront configuration error.



If there are no errors, the Analyzer displays successful results for all checks.



Secure Private Access Analyzer

The Secure Private Access Analyzer evaluates the readiness and reachability of key Citrix Cloud components required for Secure Private Access deployment. Without the need for report uploads, it automatically checks connectivity to essential services such as Cloud Access, database services, and other

required internal services.

By verifying each component's accessibility and operational status, the tool helps administrators quickly identify network or configuration issues, ensuring that all Citrix Cloud dependencies are available and properly functioning for Secure Private Access integration.

NetScaler Gateway Analyzer

NetScaler Gateway Analyzer streamlines Secure Private Access deployments by automating key tasks and highlighting configuration issues. It performs targeted checks and validations, producing actionable diagnostics that enhance reliability and performance while reducing manual effort and configuration risk.

The NetScaler Gateway Analyzer capabilities include:

- **Configuration:** Automatic or interactive setup of the NetScaler Gateway component.
- **Analysis:** Assessment of connectivity, compliance, and operational health across Secure Private Access components.
- **Cleanup:** Removal of Secure Private Access configurations when required.

Each capability is invoked via dedicated command line options (see README.txt), supporting flexible lifecycle management from initial rollout through maintenance to controlled teardown.

The execution generates timestamped artifacts containing structured logs and analysis summaries. Outputs cover configuration state, connectivity test results, discovered component metadata, and identified issues. Cleanup operations provide confirmation of entity removal to ensure a clean state. All results are delivered in a structured JSON format suitable for automation, integration, and audit.

See Step 3: Configure and analyze to download and run the script on NetScaler.

StoreFront Analyzer

StoreFront Analyzer streamlines Secure Private Access readiness checks for Citrix StoreFront by automating discovery and validation tasks. It performs targeted assessments of configuration, connectivity, authentication, and certificates, producing actionable diagnostics that improve reliability while reducing manual effort and configuration risk.

The StoreFront Analyzer capabilities include:

- **Analysis:** Read-only evaluation of StoreFront configuration, network reachability, authentication settings, remote access parameters, and certificate validity relevant to Secure Private Access compatibility.

The execution produces timestamped artifacts with structured logs and analysis summaries. Outputs include Secure Private Access URL discovery, StoreAuth key status, DNS resolution results, health endpoint accessibility, SSL certificate validation, and discovered component metadata. All results are delivered in a structured JSON format suitable for automation, integration, and audit.

No configuration changes are made. The analyzer operates in read-only mode.

See Step 3: Configure and analyze to download and run the script on NetScaler.

Integration with Google Chrome Enterprise Premium

March 5, 2026

Citrix customers can leverage the world's most popular and secure web browser, Chrome with a familiar experience to natively access authorized corporate web applications. Citrix Secure Private Access enforces per application least privilege access based on admin-defined policies that are centrally managed through the Secure Private Access console. Administrators can easily configure enterprise application domains and zero trust access policies on the Secure Private Access console. They can model policies to validate and test security outcomes and deliver the right level of user access and end-user experience.

The integrated solution includes the following components:

- Google Chrome Enterprise Premium (CEP), which includes features such as data loss 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 secure browser with per user level policy enforcement via Chrome managed profiles.
    - 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 access to the cloud infrastructure, ZTNA policy engine, and Connector Appliances deployed in the customer environment.
- 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 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**: Use advanced scanning techniques 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**: Restrict access to websites based on their content category, preventing users from accessing inappropriate or malicious content.
- **Web usage insights and analytics**: Provide 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 successful integration

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

The prerequisites are broadly classified into the following categories.

- NetScaler prerequisites
- Cloud Connector prerequisites
- StoreFront prerequisites
- Secure Private Access prerequisites
- Google prerequisites
- Synchronize user directory configured in Citrix Workspace with the Google Cloud user directory
- Bypass TLS inspection

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**: In this deployment mode, all components, including the control plane and gateway infrastructure, are hosted in Citrix Cloud. 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 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 and also use Citrix Monitor hosted in the Citrix Cloud for monitoring and troubleshooting functions. For more information, see Citrix Secure Private Access hybrid deployment.

Legal

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

Admin roles and privileges

December 9, 2025

To onboard customers to Chrome Enterprise Premium (CEP) and enable Google Chrome integration, you must assign the appropriate roles and privileges in the Google Admin console.

Types of admin roles

Two types of roles are available in the Google Admin console:

- **System Role:** These are default roles provided by Google. They typically do not include all the necessary privileges required for Google Chrome integration.
- **Custom Role:** These are roles you create, allowing you to include all necessary privileges specifically for Chrome integration. We recommended to create a custom admin role with all the required privileges for Google Chrome integration.

Note: Super admin roles cannot be assigned to service accounts.

Create and assign roles and privileges

Perform the following steps to create a custom admin role and assign privileges:

1. In the Google Admin console, go to **Accounts** > **Admin roles**.
2. Click **Create new role** and enter a name and description for the role.
3. Add all the privileges required for Google Chrome integration to this custom role. For the list of required privileges, see Required privileges for Google Chrome integration.

   For more information related to roles and privileges, see the Google documentation.
4. Save the custom role.
5. After creating the custom role, open the role and click **Assign members**.
6. Select the users who need these permissions.

Required privileges for Google Chrome integration

The following privileges must be enabled in the admin role that is assigned to the service account.

- **Admin Console privileges:**
  - Manage User Settings (Services > Chrome Management > Settings > Manage User Settings)

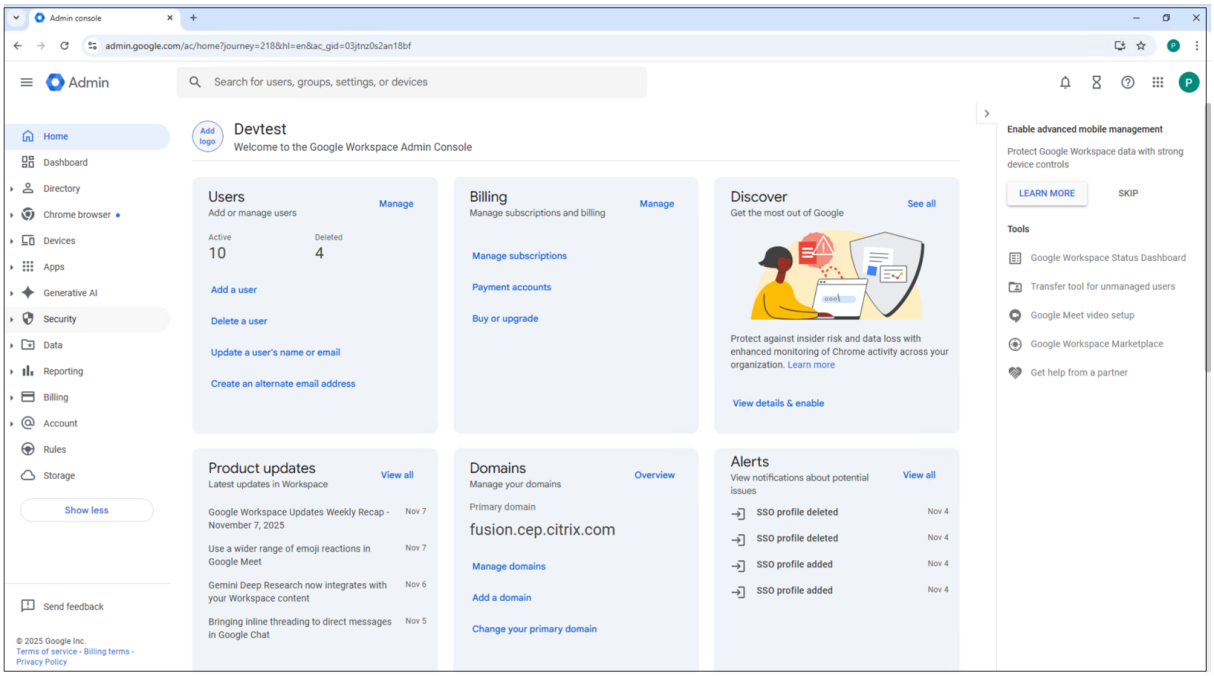
    > **Note:**
    >
    > Ensure that you select the top-level privilege **Manage User Settings** and the sub-privileges (**Manage Application Settings** and **Manage Web Settings**). Selecting only the sub-privileges is not sufficient.

- **Admin API privileges:**
  - Domain Management
  - Groups > Read
  - Organization Units > Read

Open ID Connect profile to use NetScaler Gateway as the IdP

November 25, 2025

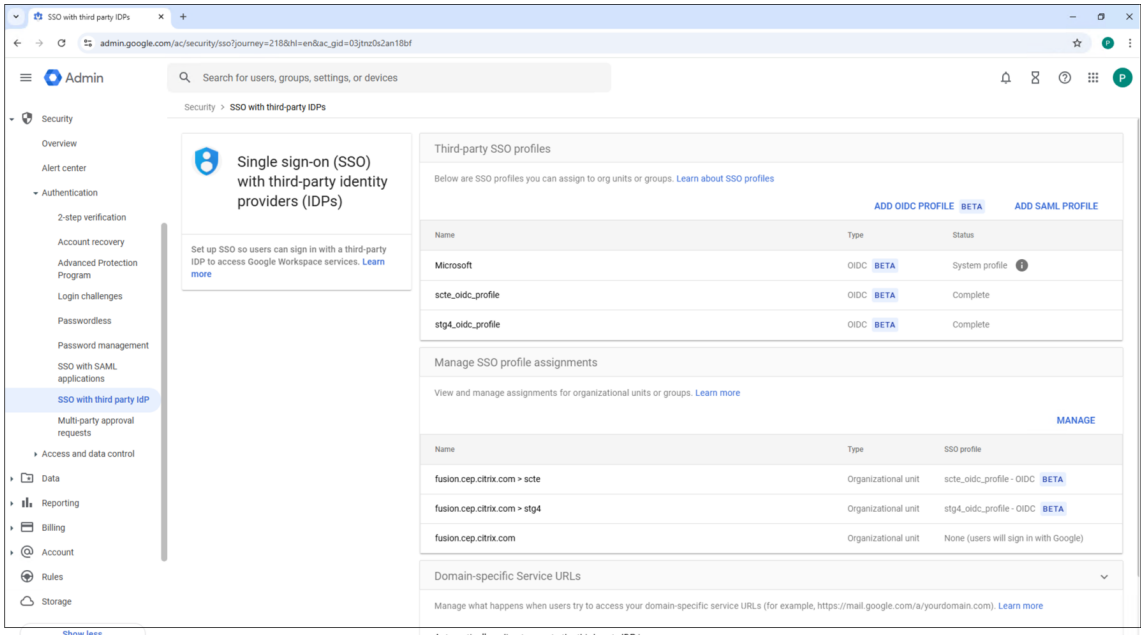
You must create an OIDC profile on the Google Admin console for using NetScaler Gateway as an IdP.



Create a Google OIDC SSO profile

Perform the following steps in the Google Admin console.

1. Go to **Security > Authentication > SSO with third party IdP** and then select **Add OIDC Profile**.



2. Enter a name for the profile.
3. Enter the OIDC details.

- **Client ID:** Use a random client ID (usually a 22 characters numeric string)
- **Client Secret:** Generate a random string of a minimum of 32 characters. The string must include alphanumeric and special characters.

  Some special characters such as, - #, @, !, ^, &, %, are not allowed in the **Client secret** field while configuring OAuth IdP profile on NetScaler. Therefore, you must not use these special characters in the **Client Secret** field here.

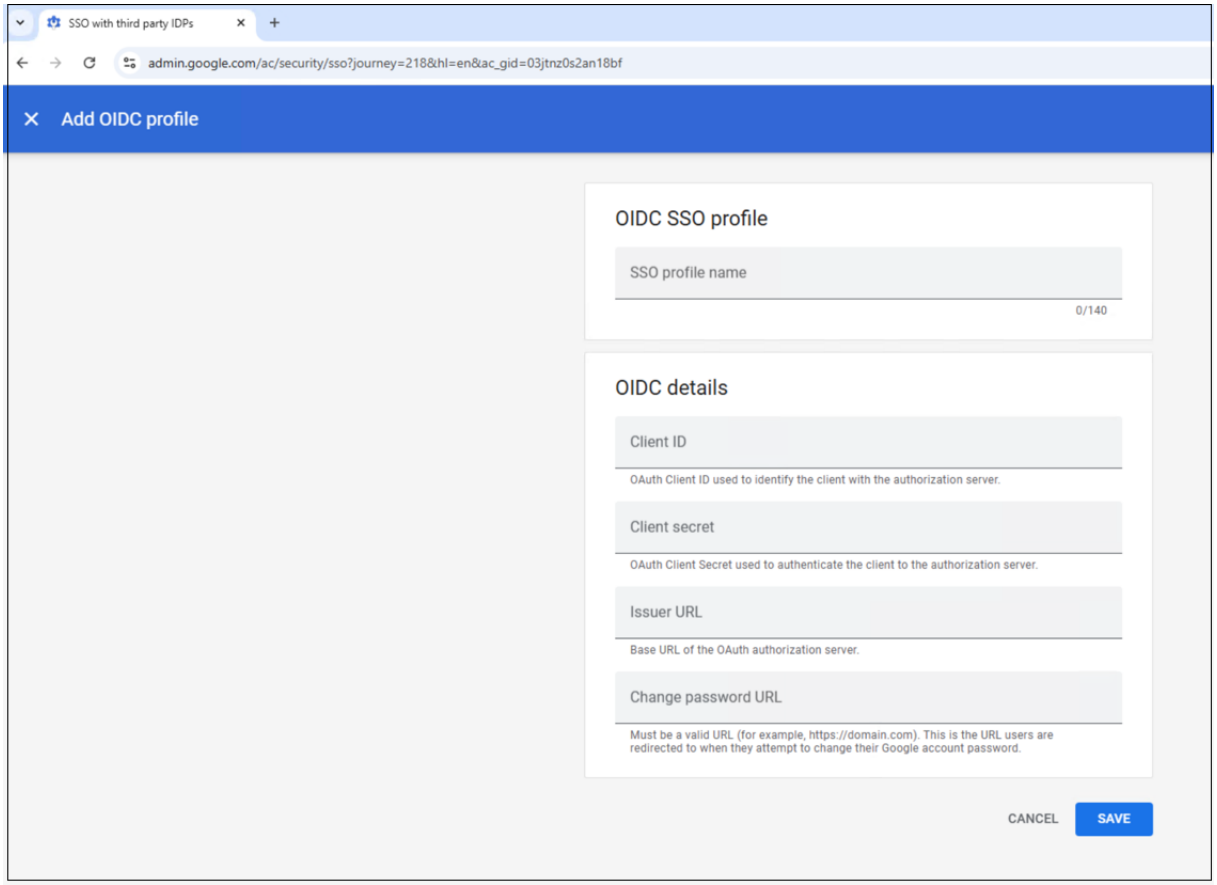
> **Note:**
>
> You must manually generate the client ID and client secret in NetScaler Gateway.

- **Issuer URL:** Set this field to `https://<SPAGatewayFQDN>/oauth/idp/<OAuthIdpProfileName>`, where `SPAGatewayFQDN` is the FQDN corresponding to the Secure Private Access Gateway URL and `OAuthIdpProfileName` is the name of the OAuth IdP profile, which is created on the NetScaler Gateway.

> **Note:**
>
> Do not use spaces in the IdP profile name.

- **Change password URL:** Leave it blank (not needed at this point)

4. Click **Save**.

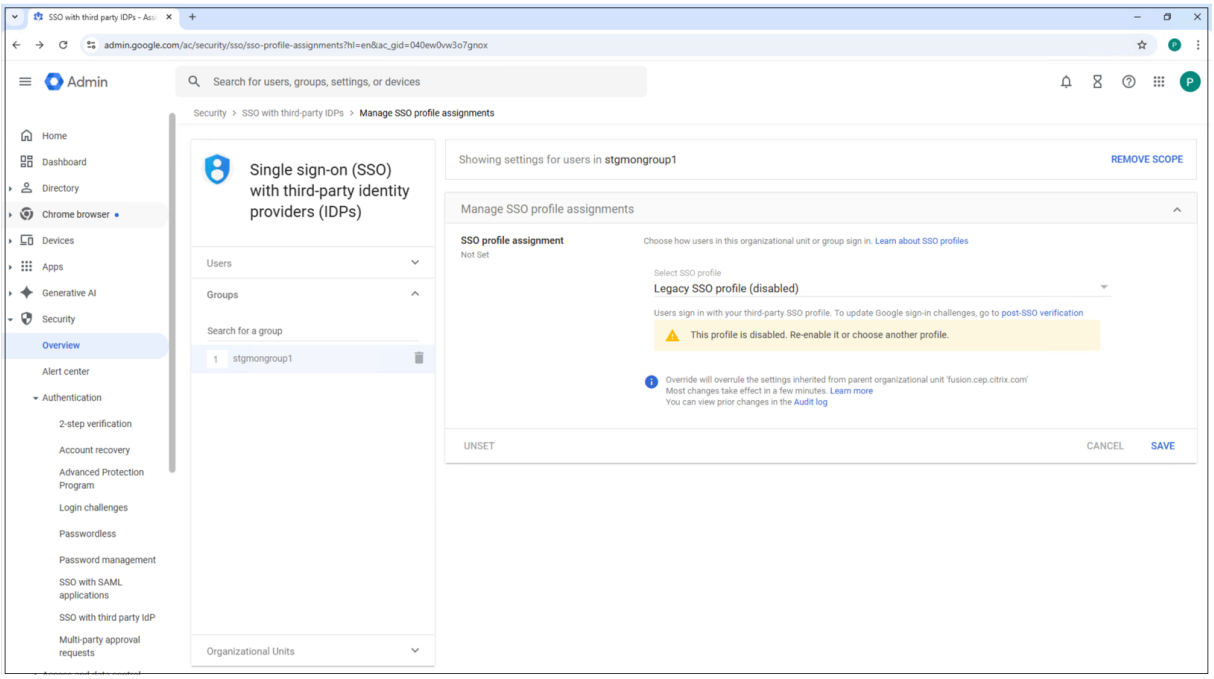


> **Important:**
>
> Note down the Client ID, Client secret, and the Redirect URL. These values are required while configuring the OAuth IdP profile on NetScaler Gateway.

Bind the OIDC Profile (To either an OU or group)

To complete the OIDC profile configuration, you must bind it to specific organizational units (OUs) or groups in your Google Workspace. This binding determines which users can authenticate using this OIDC profile with NetScaler Gateway as the IdP.

1. Navigate to **Security > Authentication > SSO with 3rd Party IDPs**.
2. In **Manage SSO profile assignments**, click **Manage**
3. From the left navigation pane, select the root organizational unit (OU) and your SSO profile to enable SSO for all users of your organization. Alternatively, you can assign the SSO profile to specific groups or OUs.
4. Select the SSO profile that you created and click **Save**.



Configure NetScaler as an OAuth IdP

See NetScaler as an OAuth IdP for configuring NetScaler as an OAuth IdP.

> **Note:**
>
> - The **Audience** field value in the OAuth IdP profile must be same as the client ID value.
> - The **Issuer URL** must match with the one configured in the Google Admin console.
> - The **Client ID**, **Client Secret** and **Redirect URL** values must be taken from the Google Admin console.

Google Cloud Directory Sync (GCDS)

December 16, 2025

Microsoft Entra ID using G Suite connector

You must synchronize your Microsoft Entra ID with the Google Cloud user directory for user and group management across both Google and Microsoft cloud platforms. For details, see the following topics:

- Microsoft Entra ID (formerly Azure AD) user provisioning and single sign-on

- Configure Google Cloud / G Suite Connector by Microsoft for Single sign-on with Microsoft Entra ID

The email address field must be populated for all users and groups. The email domain must match the one configured in Google Directory. Implicitly, this means that Security Groups without an email address or groups with an @onmicrosoft.com email domain are currently not supported.

Single sign-on: Single sign-on (SSO) configuration is optional. You might configure a separate password in the Google directory. See To configure SSO with Open ID Connect profile to use NetScaler Gateway as the IdP.

Google Cloud Directory Sync tool

With Google Cloud Directory Sync (GCDS), you can synchronize the data in your Google Account with your Microsoft Active Directory or LDAP server. GCDS doesn't migrate any content (such as email messages, calendar events, or files) to your Google Account. You use GCDS to synchronize your Google users, groups, and shared contacts to match the information in your LDAP server.

For details, see About Google Cloud Directory Sync.

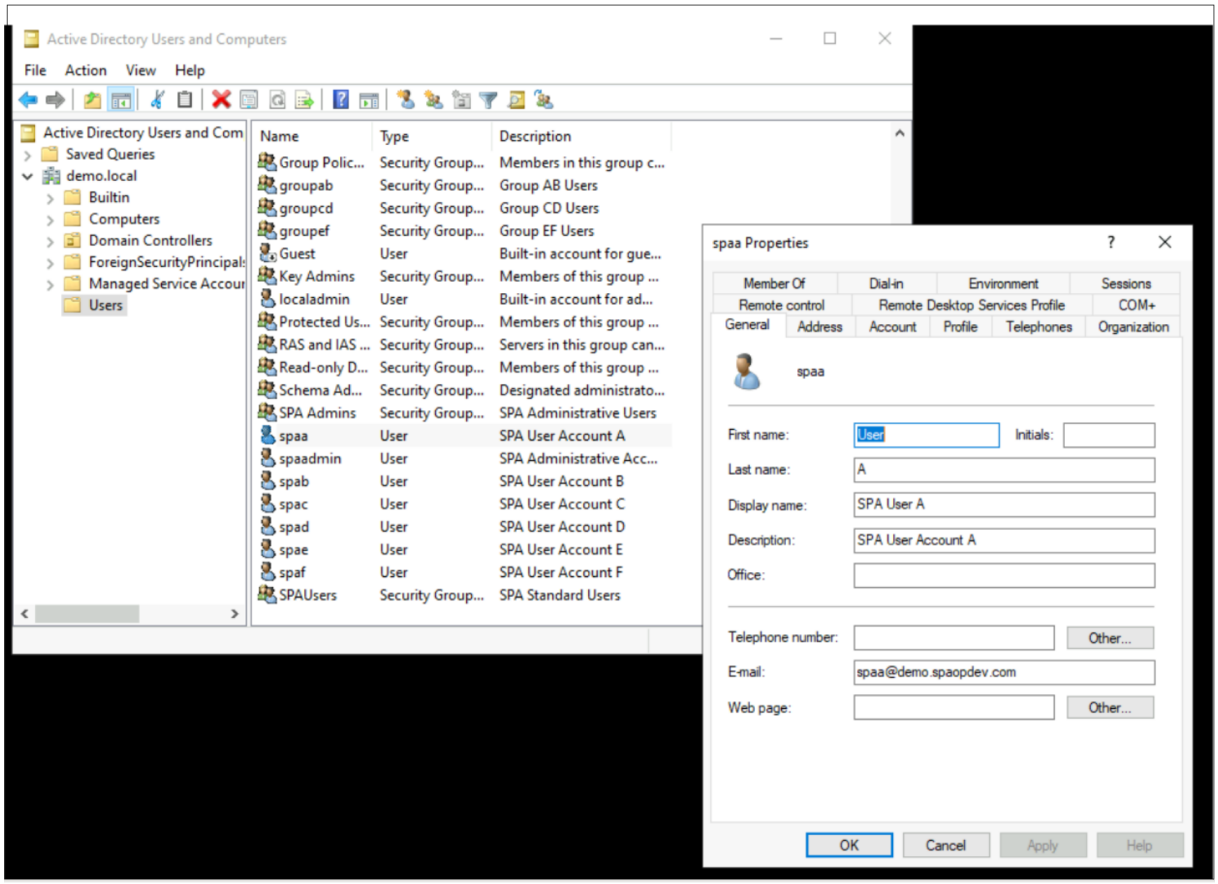
Install and prepare GCDS:

- Download
- Installation

> **Notes:**
>
> - For POC purposes, the GCDS tool can be installed on an AD machine.
> - Run the installer with Administrator permissions.
> - Configuration can be saved in a file (File\Save As) and opened next time when you want to synchronize.

Active Directory

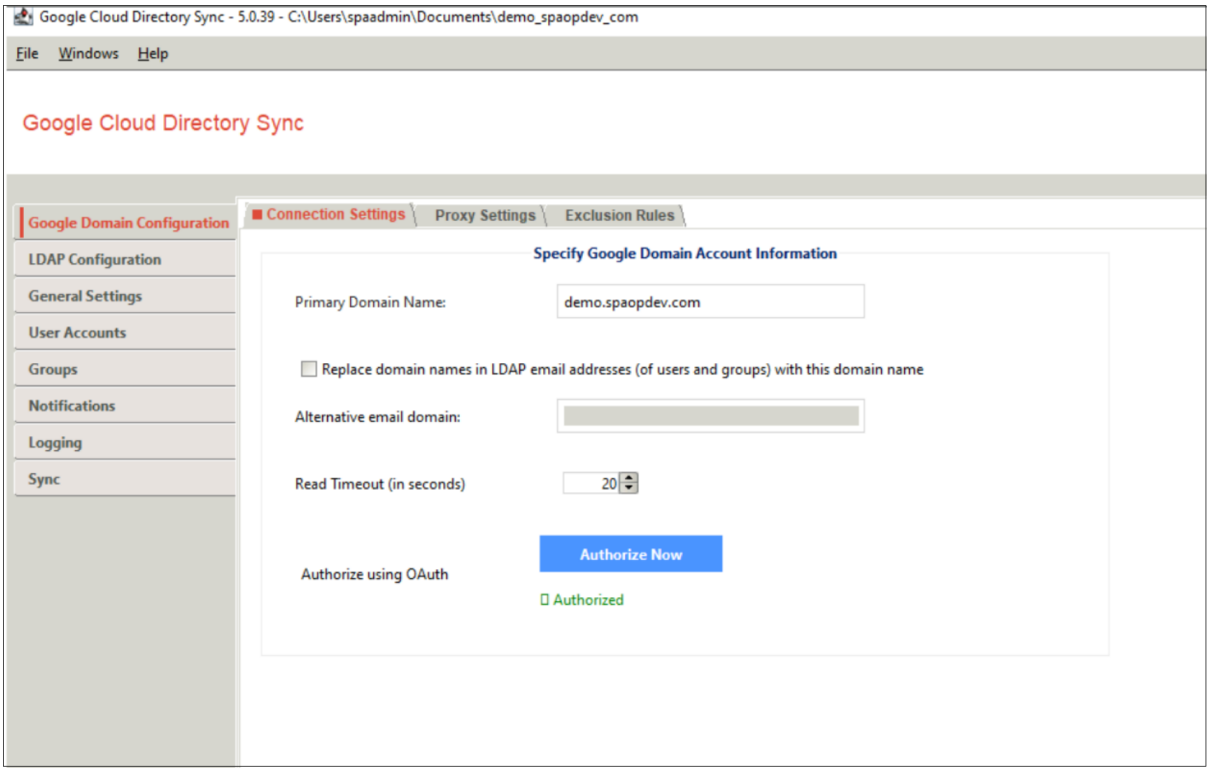
As a prerequisite, ensure that you have users and groups created on Active Directory. Users and groups must have the email attribute.



Google Cloud Directory Sync configuration

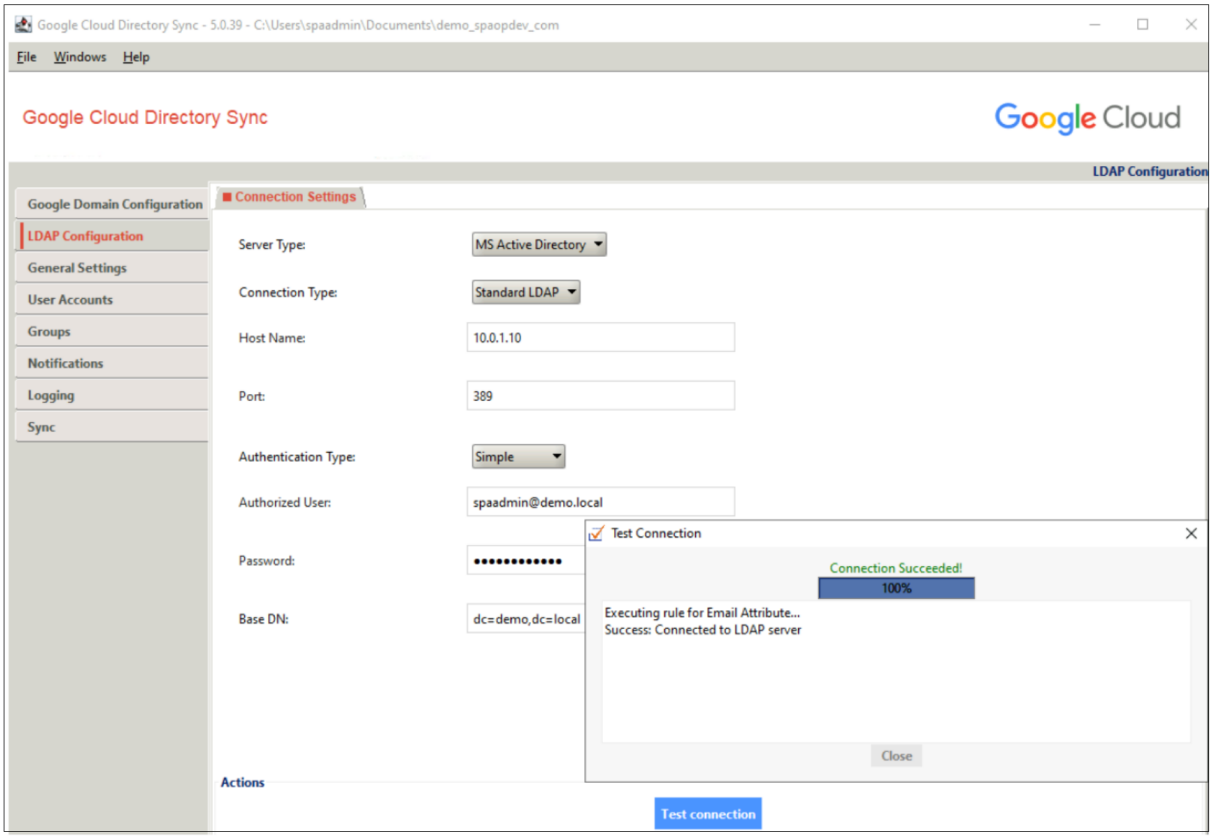
Google domain configuration:

1. Enter the primary domain name.
2. Authorize using OAuth. Click **Authorize Now**. You are prompted to enter your Google Workspace admin credentials and asked to allow access to Google Workspace Directory.



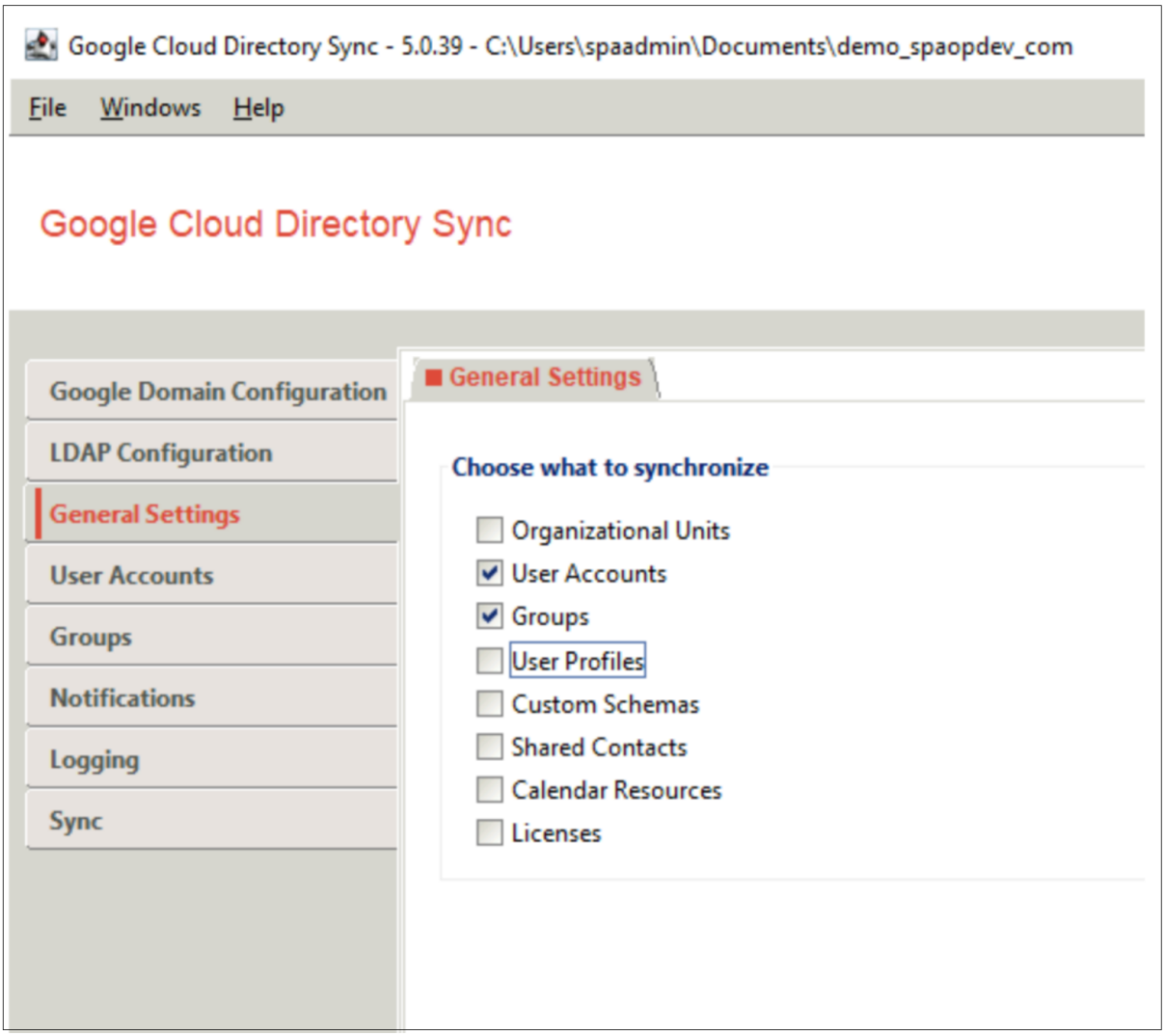
LDAP configuration:

1. Enter the host name, port, authorized user, and password.



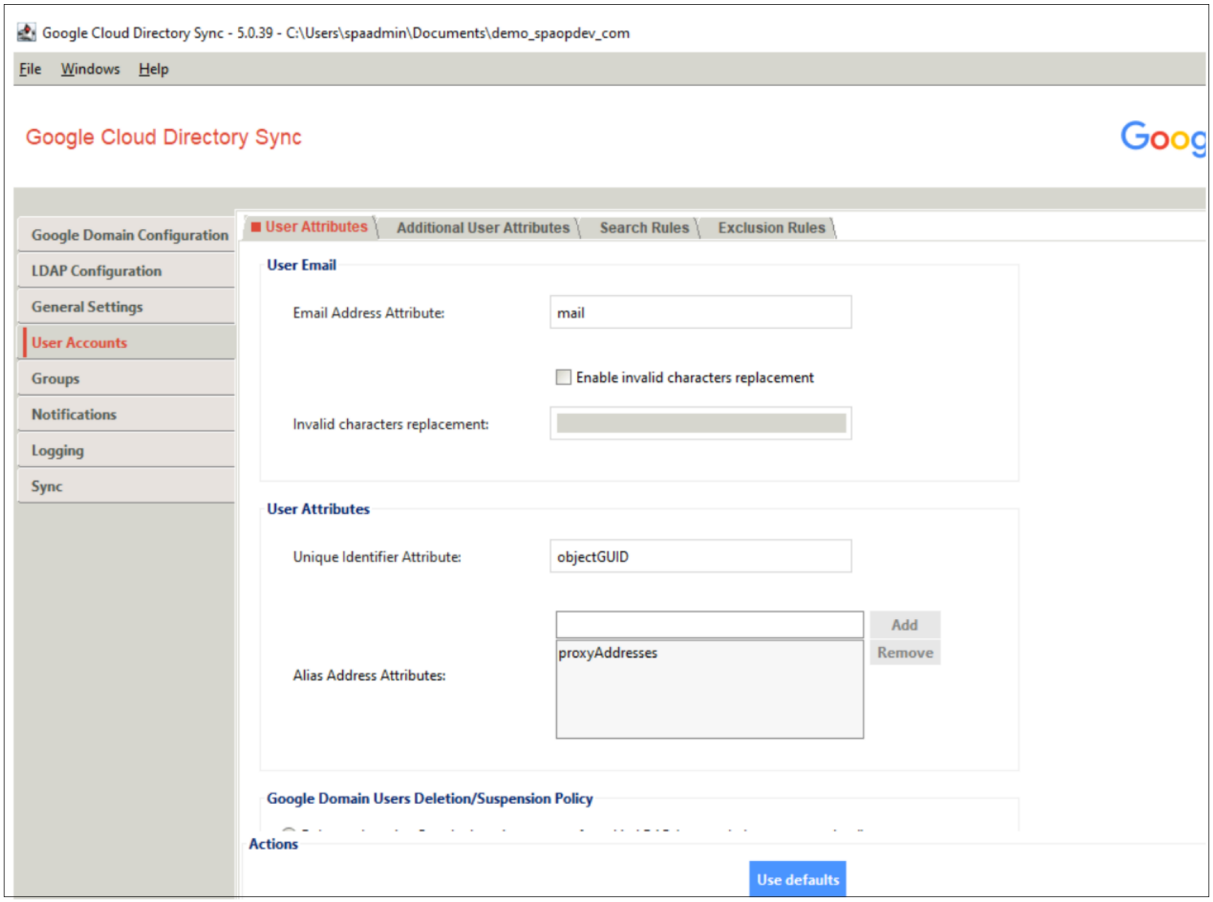
General settings:

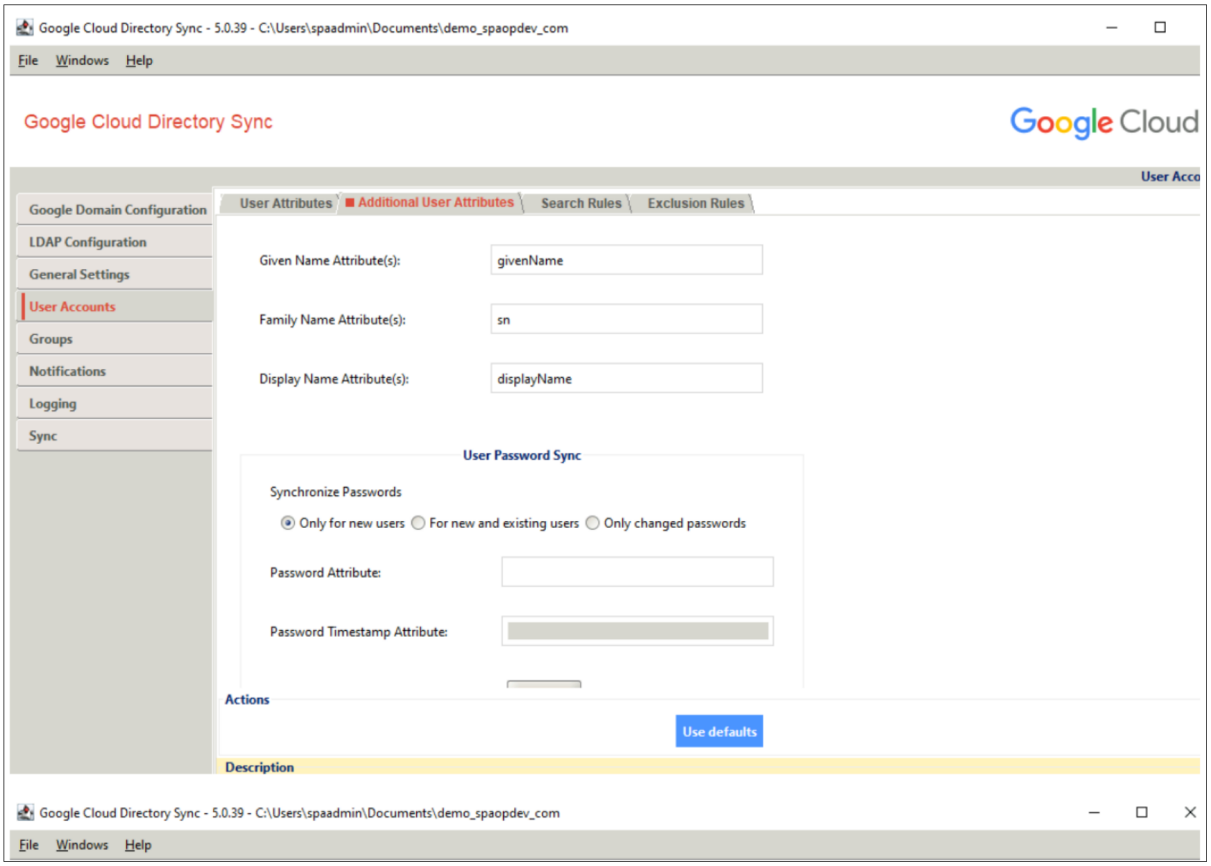
Select the items for the synchronization.

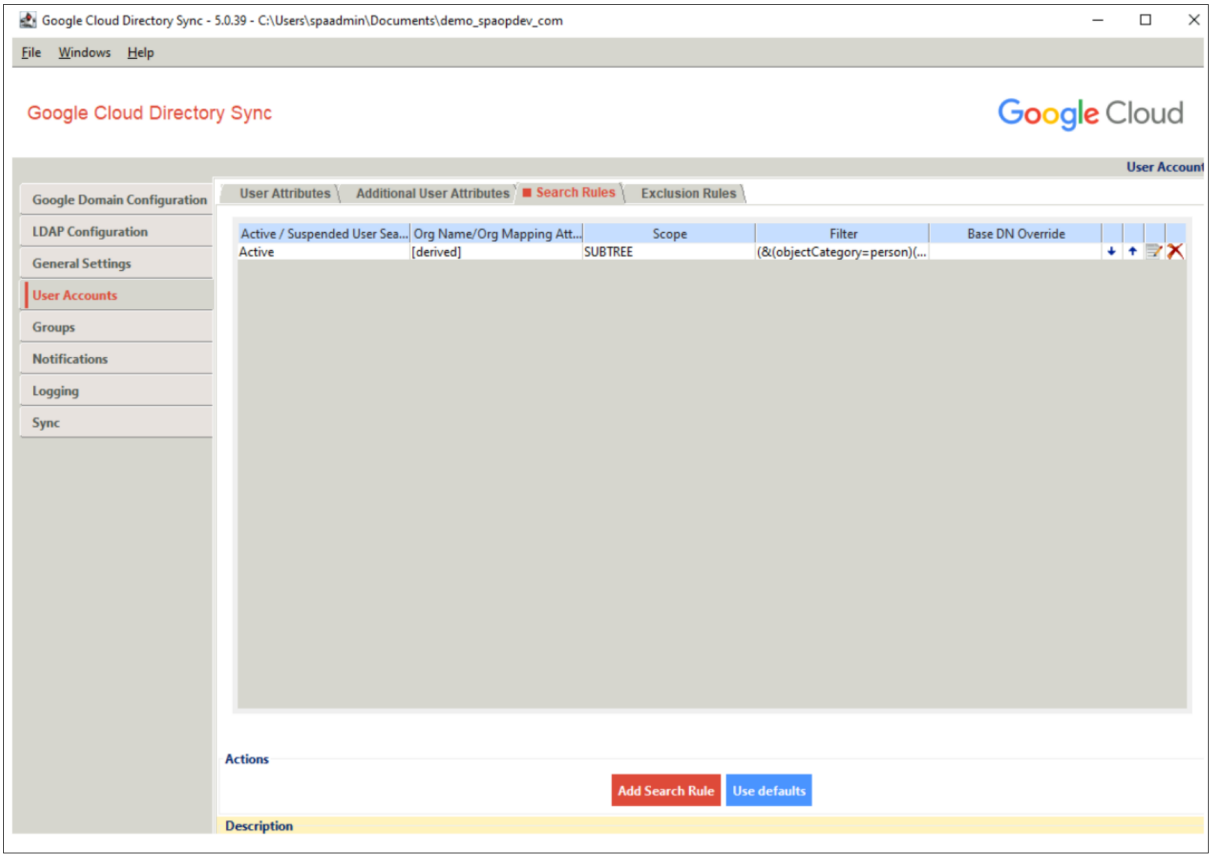


User Accounts:

1. Specify which users to import and synchronize.
2. Click **Use defaults** for **User Attributes**, **Additional User Attributes**, and **Search Rules**.

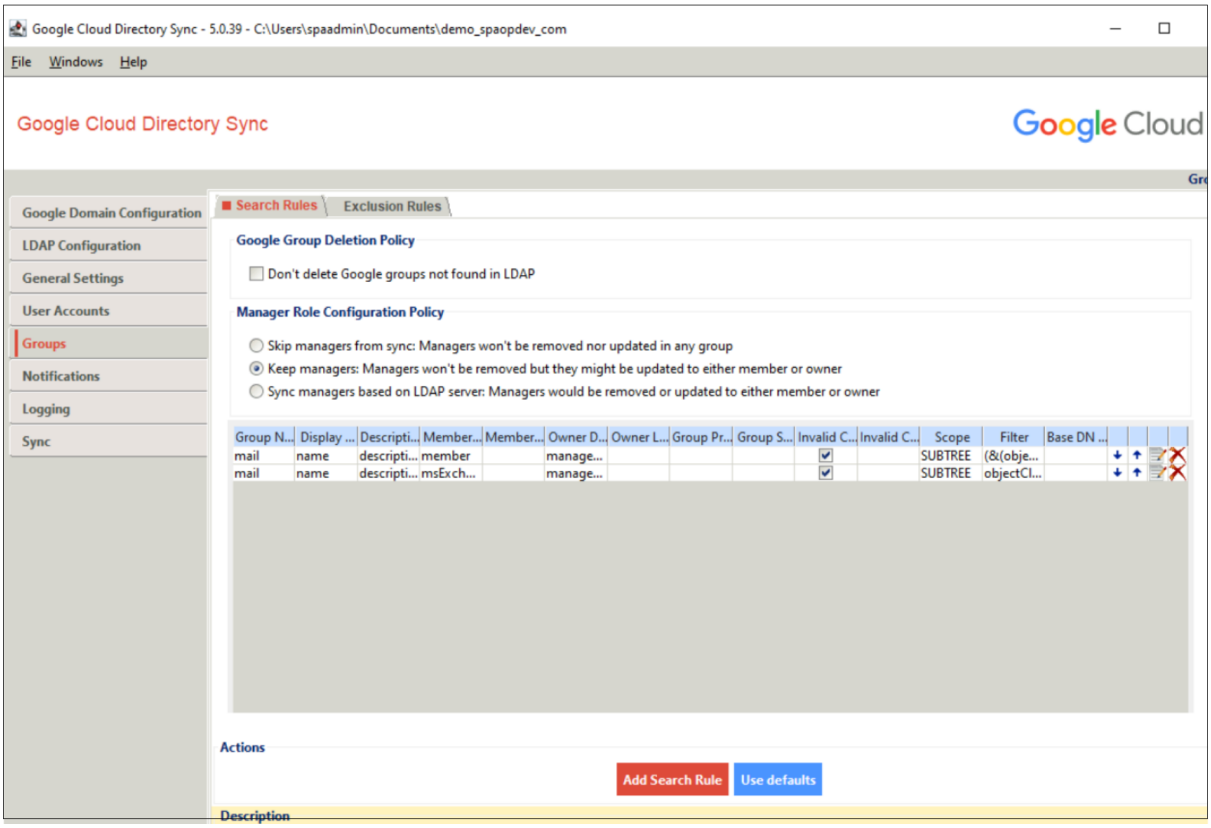






Groups:

1. Specify which groups to import and synchronize.
2. Click **Use defaults** for groups **Search Rules**.



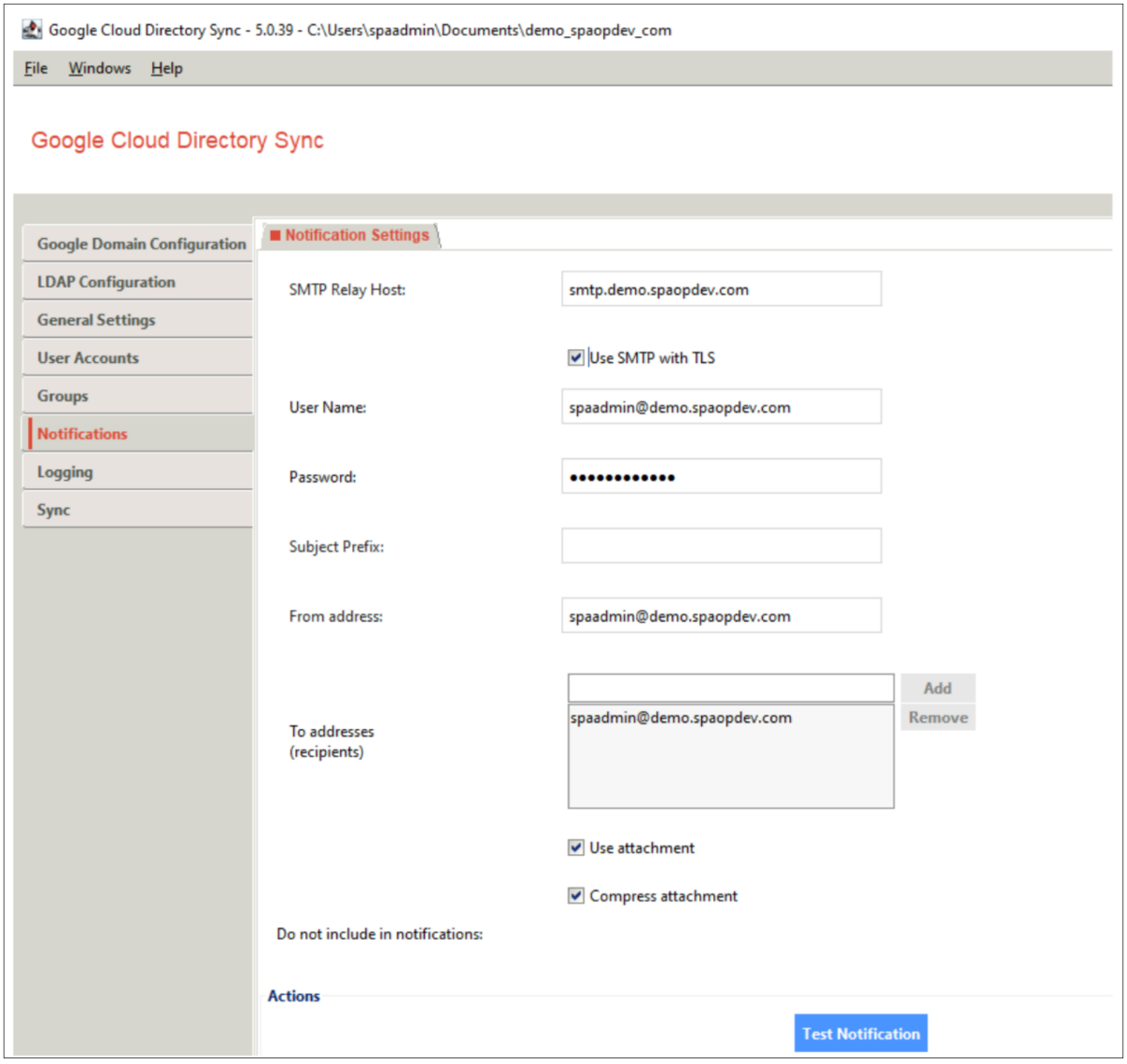
Notifications:

This step is optional.

After synchronization, Google Cloud Directory Sync connects to your SMTP relay host and sends a notification with synchronization details.

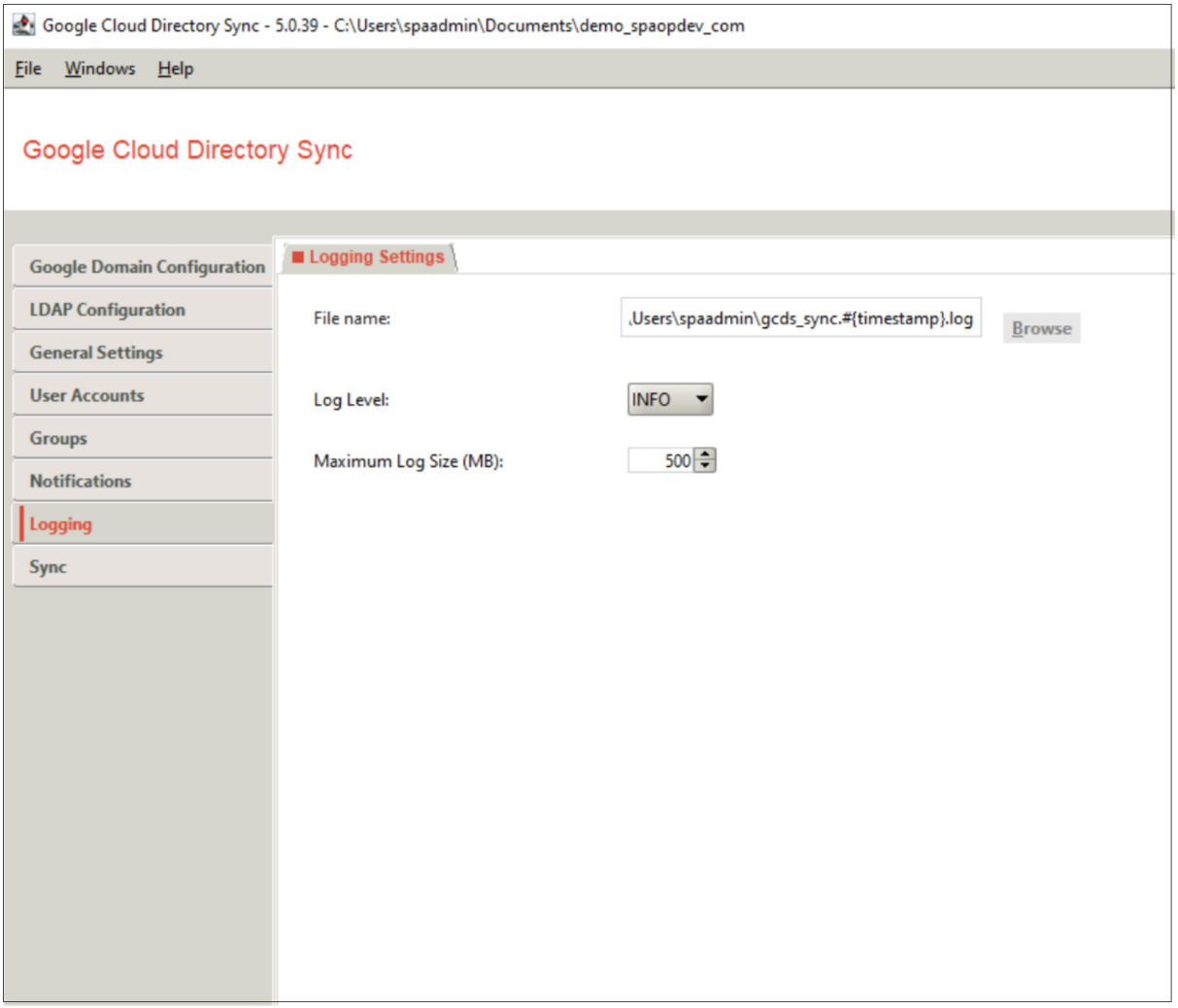
- Specify the senders address that you want to appear in the notification header.
- Enter the recipient email addresses one at a time and click the **Add** button for each address.

If the synchronization report exceeds 24 MB, it is compressed and sent as a ZIP attachment.



Logging:

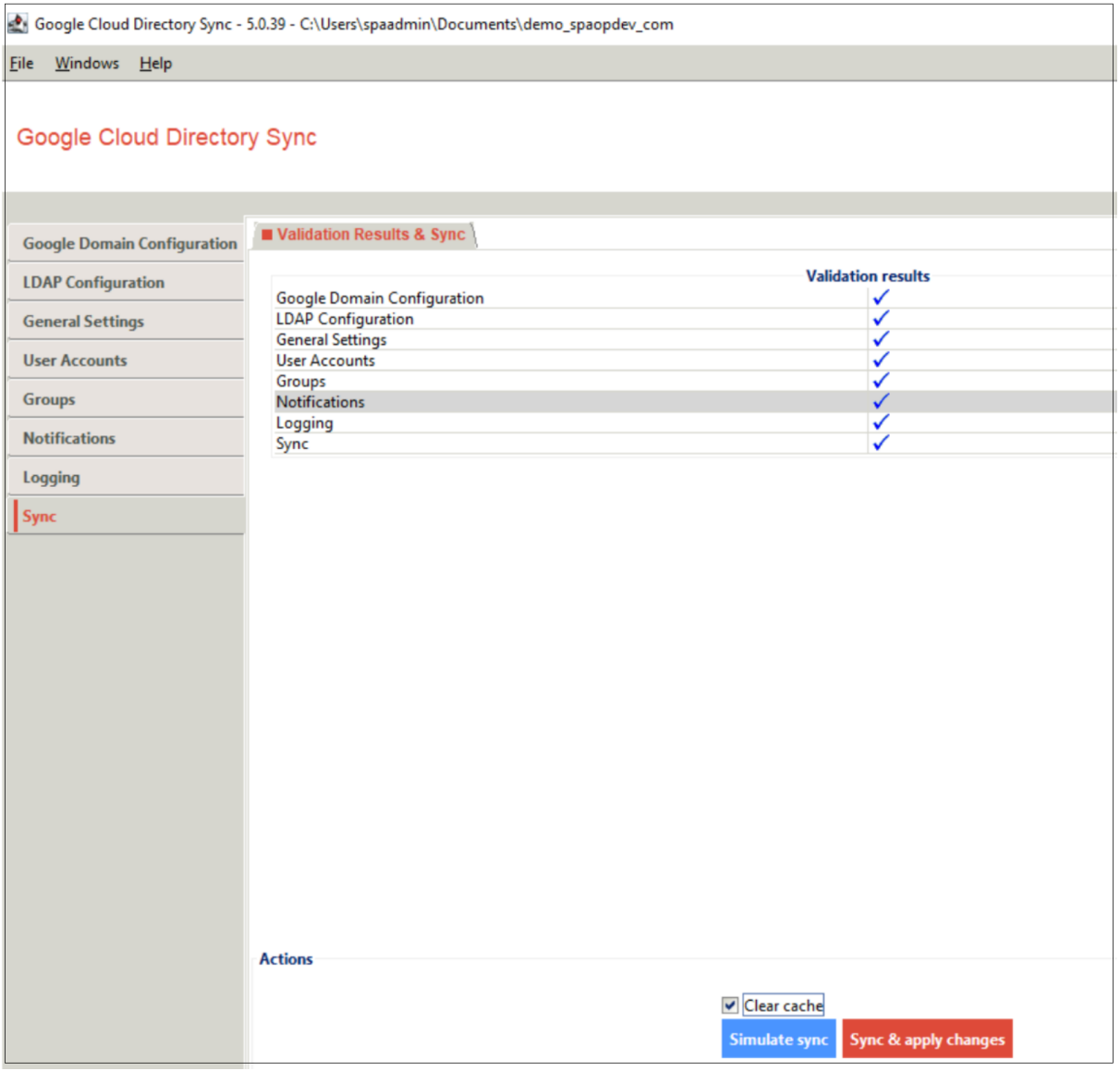
Specify where to write the log file information, the level of detail, and the maximum log file size.



Synchronization:

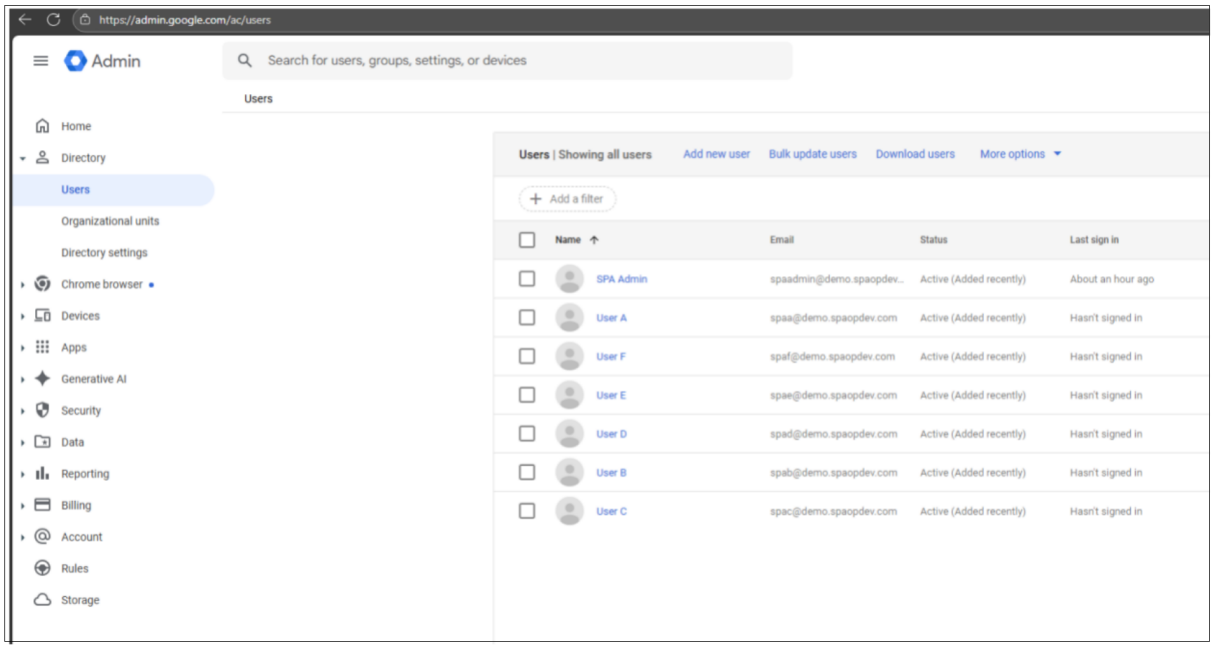
Review your settings and correct any problems before you synchronize.

- Once your settings are correct, click **Simulate sync** to connect to both servers and generate a list of changes for the simulated synchronization.
- To commit changes, save the configuration file and click **Sync** and apply changes or run `sync -cmd` from the command line.



Google Workspace Directory:

New users are created during the synchronization.



Synchronize using CLI:

See Synchronize using the command line.

End user experience

February 4, 2026

Users can access applications through Secure Private Access using the following methods. Each access method provides a different user experience allowing organizations to choose the most appropriate approach based on their desired user experience and deployment strategy.

- **Citrix Workspace App (CWA)** - The native desktop application that provides the most secure and feature-rich access experience with full policy enforcement and single sign-on capabilities.
- **Workspace user interface (WSUI)** - A web-based interface that can be accessed through different browser environments:
  - Non-Chrome browsers (such as Firefox, Safari, or Edge)
  - Chrome with non-managed profile (personal Chrome browser without enterprise policies)
  - Chrome with managed profile (enterprise-managed Chrome browser with Chrome Enterprise Premium policies)
- **Chrome managed profile** - Users access applications directly by using bookmarks or manually typing the application URL in the address bar of a Chrome managed profile.

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

		Direct	WSUI	CWA Workspace / StoreFront portal
	Non-chrome browser	Access denied for SaaS apps (assuming that the SaaS apps have been configured with the appropriate IP address allow list). Private apps are unreachable.	Apps are enumerated in the Workspace / StoreFront portal. The applications are launched in the appropriate Chrome managed profile. A profile creation wizard is launched if the respective managed profile has not been created already.	Not-applicable
	Chrome (non-managed profile)	Access denied for SaaS apps (assuming that the SaaS apps have been configured with the appropriate IP address allow list).	The applications are launched in the appropriate Chrome managed profile.	Not-applicable

		Direct	WSUI	CWA Workspace / StoreFront portal
		Private apps are unreachable.	A profile creation wizard is launched if the respective managed profile has not been created already.	
	Chrome (managed profile)	Apps are allowed or denied depending on the Secure Private Access configuration.	The enumerated app is launched in a new tab.	Not-applicable
	CWA	Not-applicable	Not-applicable	Apps are enumerated in the Workspace / StoreFront portal. The applications are launched in the appropriate Chrome managed profile. A profile creation wizard is launched if the respective managed profile has not been created already.

Citrix Secure Access browser extension for Chrome Enterprise Premium

February 4, 2026

The Citrix Secure Access browser extension for Chrome Enterprise Premium (CEP) enables secure, clientless access to internal and external applications directly from the Chrome browser. It combines Citrix Secure Private Access and Chrome Enterprise capabilities to deliver enterprise-grade security, Zero Trust access, contextual controls, and a modern user experience.

Organizations can use this extension to provide secure access to SaaS applications, internal web apps, SSH servers, and RDP systems, all without requiring VPNs or native client installations.

The Secure Access browser extension is automatically installed when you integrate Secure Private Access with Chrome Enterprise Premium. For setup instructions, see Setup Google Chrome integration. Once installed, you can access the extension from the icon in the upper-right corner of your Chrome browser.

The Secure Access browser extension supports SSH and remote desktop (RDP) applications. For details, see the following topics:

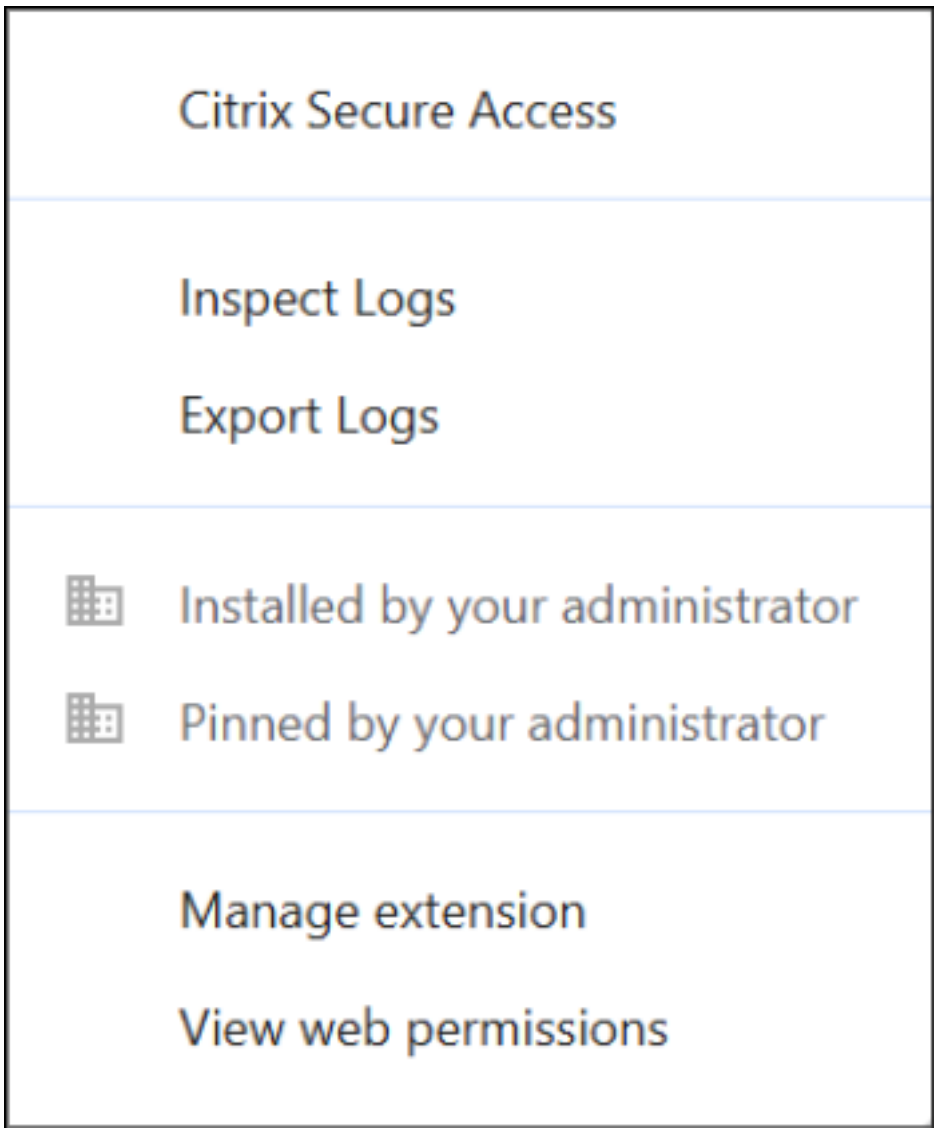
- Secure access to SSH apps within the browser
- Secure access to RDP apps within the browser

Browser extension logs

The Secure Access browser extension logs are essential for monitoring and troubleshooting. End users can review and download logs to share with administrators or support teams when issues occur.

To review or download logs:

1. Right-click the browser extension icon.
    - Click **Inspect Logs** to review logs.
    - Click **Export Logs** to download logs.



Secure access to SSH apps within the browser

January 23, 2026

Citrix Secure Private Access is integrated with Chrome Enterprise Premium to enable secure SSH sessions directly within the browser. This integration enhances security and streamlines access for administrators and users.

Organizations require secure remote administration of SSH-based systems. Traditional methods using standalone SSH clients pose risks by exposing endpoints to unmanaged environments and lacking robust Data Loss Prevention (DLP) enforcement, making compliance challenging.

The SSH sessions are now launched within the Chrome browser instead of standalone SSH clients, reducing dependency on local installations and improving compliance.

> **Note:**
>
> - This feature is applicable for Chrome Enterprise Premium integrated Secure Private Access setup for hybrid and cloud deployments. For details, see the following topics:
> - You must have admin rights to configure Secure Private Access and Chrome Enterprise Premium policies.
> - Connections to FreeBSD servers are not supported.

Benefits of this integration

This integration offers the following key benefits:

- **Enhanced security:** Eliminates reliance on unmanaged SSH clients, reducing exposure to security risks.
- **Simplified access:** Provides browser-native access, removing the need for additional software installations.
- **Compliance:** Enforces corporate DLP policies directly within the browser, helping meet regulatory requirements.
- **Operational efficiency:** Reduces IT overhead associated with endpoint management and client deployment.

Use cases

This feature supports various use cases such as:

- **Healthcare kiosks:** Enables secure SSH access for device troubleshooting without installing native clients.
- **IT administration:** Allows administrators to securely access Linux servers from managed Chrome browsers with enforced DLP policies.
- **Contractor access:** Provides temporary SSH access for third-party vendors without compromising the organization's security posture.

System requirements

Ensure that your environment meets the following requirements:

- Latest version of Chrome Enterprise Premium.

- Citrix Secure Private Access is configured for the integration.
- Access policies to allow SSH traffic must be created in the Secure Private Access admin console.

Prerequisites

Ensure that the following prerequisites are met for enabling secure access to SSH applications:

- Citrix Secure Private Access is configured with Google Chrome Enterprise Premium integration. For details, see Integration with Google Chrome Enterprise Premium.
- The end user has installed the latest Google Chrome browser with the Citrix Secure Access browser extension.
- For the deployment specific prerequisites, see the following topics:
  - Cloud deployment - Get started with Citrix Secure Private Access
  - Hybrid deployment –System requirements and prerequisites

Configure Secure Private Access for SSH access

1. Log in to Citrix Cloud and then click **Secure Private Access**.
2. In the admin console, Click **Applications > App Configuration**, and then click **Add an app**.
3. Configure the SSH app as a TCP/UDP app within Secure Private Access.
   - The app can have an exact IP address or a range, FQDN, or host name of the server.
   - SSH is supported over default and non-default ports.
4. Assign access to relevant user groups.

For detailed information on creating a TCP/UDP app, see the following topics.

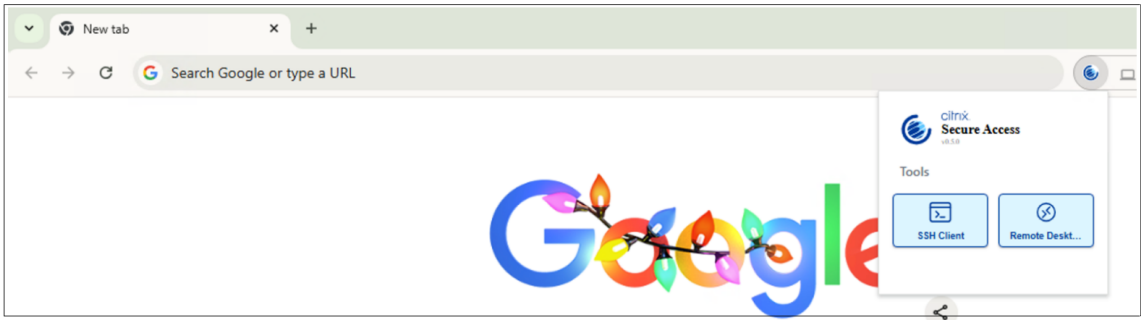
- Cloud deployment - Support for TCP/UDP apps
- Hybrid deployment –Support for TCP/UDP apps

Access the SSH app

The SSH app access button is visible to the end-user in the extension UI irrespective of whether it is configured or not. If not configured, the user cannot access the SSH-based application.

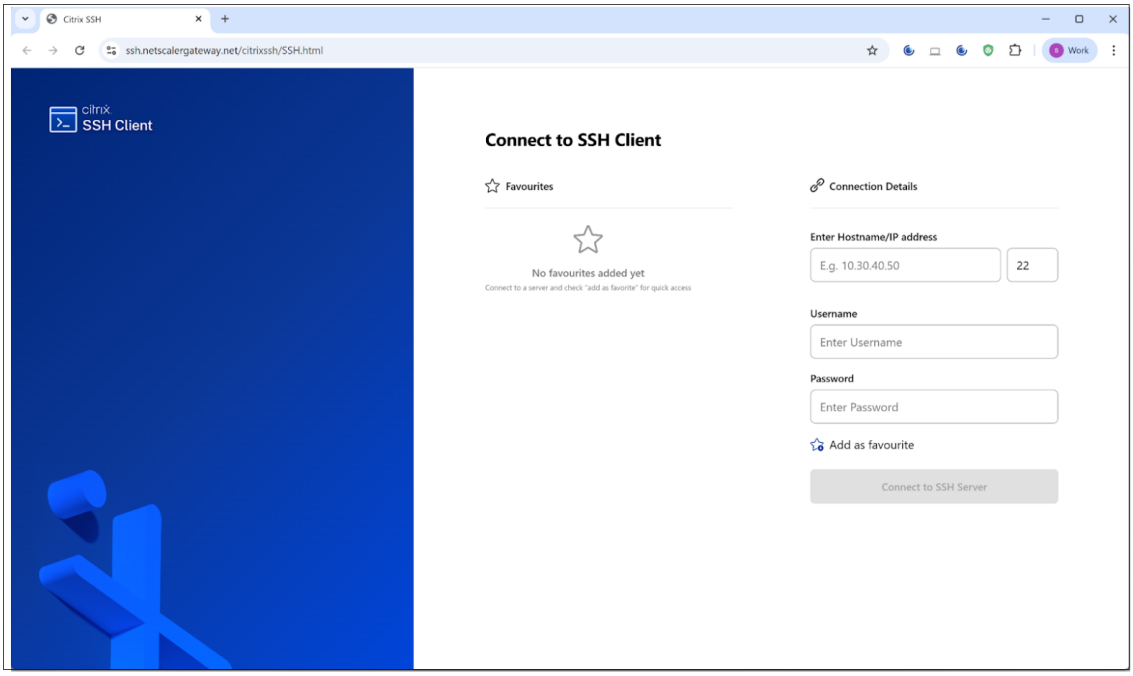
- Type `CitrixSSH` and hit **tab** in the URL bar, then enter the IP address and hit **enter** to start an SSH session.

- Alternatively, you can click the extension icon and click **SSH** from the menu.

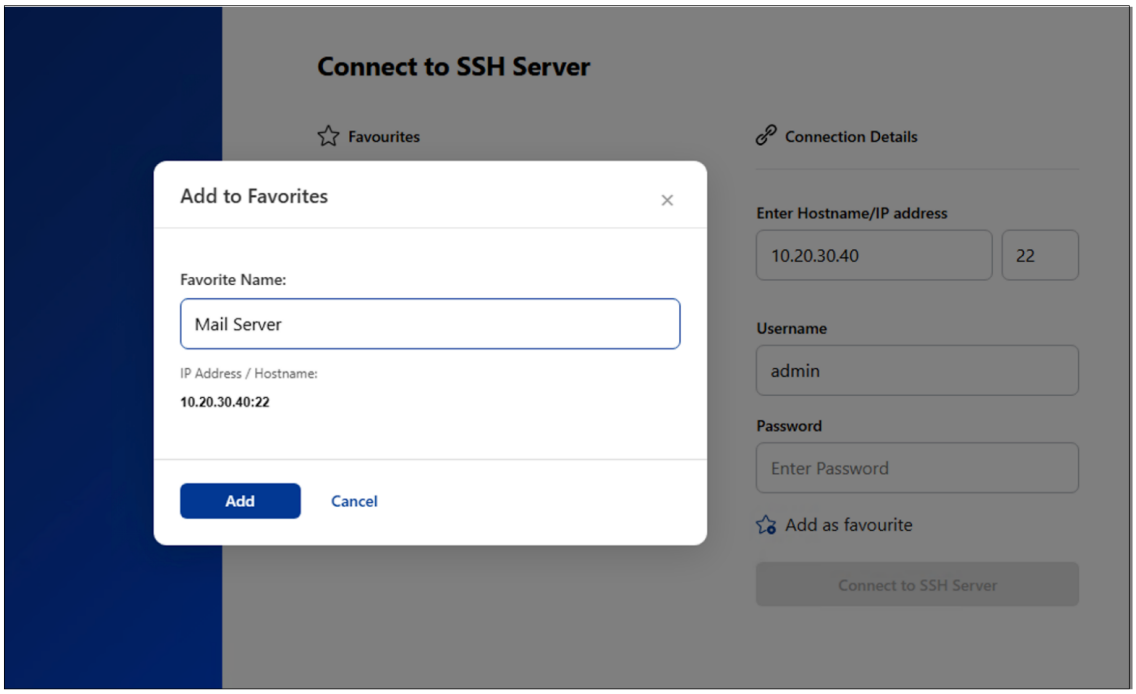


- Port 22 is filled in by default. You can choose to change the port number as required.

> **Note:**
>
> Enter your user name and password. Only the user name and password-based authentication is supported.



- You can also save sessions as favorites.



Secure access to RDP apps within the browser

January 23, 2026

Citrix Secure Private Access is integrated with Chrome Enterprise Premium to enable secure RDP sessions directly within the browser. This integration enhances security and streamlines access for administrators and users.

Traditional remote desktop access often relies on native RDP clients, which typically lack browser-based DLP enforcement. This deficiency can increase security risks, especially in unmanaged environments, and make compliance challenging. Organizations require a secure, compliant, and simplified solution for remote access that addresses these concerns.

This integration enables admins to enforce enterprise-grade DLP controls such as clipboard control and screenshot prevention.

> **Note:**
>
> - This feature is applicable for Chrome Enterprise Premium integrated Secure Private Access setup for hybrid and cloud deployments. For details, see the following topics:
> - You must have admin rights to configure Secure Private Access and Chrome Enterprise Premium policies.

Unsupported features:

The following features are not supported:

- Clipboard sharing
- Audio/WebCam/SmartCard/USB redirection
- Two-factor and biometric authentication

Benefits of this integration

This integration offers the following key benefits:

- **Security:** Prevents data leakage during remote sessions by enforcing granular DLP policies.
- **Compliance:** Helps meet regulatory requirements for sensitive environments through robust security controls.
- **Ease of use:** Eliminates the need for installing separate RDP clients, simplifying user access and deployment.
- **Flexibility:** Supports secure RDP access from managed Chrome browsers, providing a consistent and secure experience.

Use cases

This feature supports various use cases such as:

- **Enterprise contractors:** Provides secure remote desktop access for third-party vendors without compromising internal security.
- **Healthcare staff:** Enables secure access to Windows systems from kiosks or shared workstations in healthcare settings.
- **IT support:** Allows IT personnel to troubleshoot remote desktops without requiring additional software installations.

System requirements

Ensure that your environment meets the following requirements:

- Latest version of Chrome Enterprise Premium.
- Citrix Secure Private Access is configured for the integration.
- Access policies to allow RDP traffic must be created in the Secure Private Access admin console.

Prerequisites

Ensure that the following prerequisites are met for enabling secure access to RDP applications:

- Citrix Secure Private Access is configured with Google Chrome Enterprise Premium integration. For details, see Integration with Google Chrome Enterprise Premium.
- The end user has installed the latest Google Chrome browser with the Citrix Secure Access browser extension.
- For the deployment specific prerequisites, see the following topics:
  - Cloud deployment - Get started with Citrix Secure Private Access
  - Hybrid deployment –System requirements and prerequisites

Configure Secure Private Access for RDP access

1. Log in to Citrix Cloud and then click **Secure Private Access**.
2. In the admin console, Click **Applications > App Configuration**, and then click **Add an app**.
3. Configure the RDP app as a TCP/UDP app within Secure Private Access.
   - The app can have an exact IP address or a range, FQDN, or host name of the server.
   - RDP is supported over default and non-default ports.
4. Assign access to relevant user groups.

For detailed information on creating a TCP/UDP app, see the following topics.

- Cloud deployment - Support for TCP/UDP apps
- Hybrid deployment –Support for TCP/UDP apps

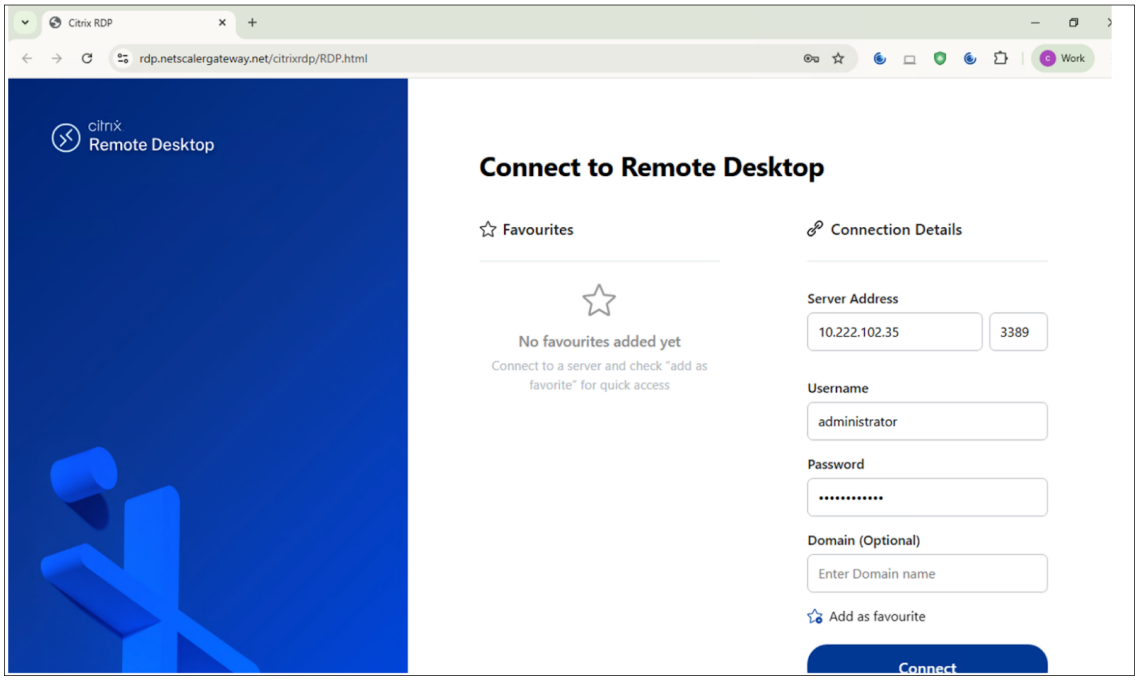
Access the RDP app

The RDP app access button is visible to the end-user in the extension UI irrespective of whether it is configured or not. If not configured, the user cannot access the RDP-based application.

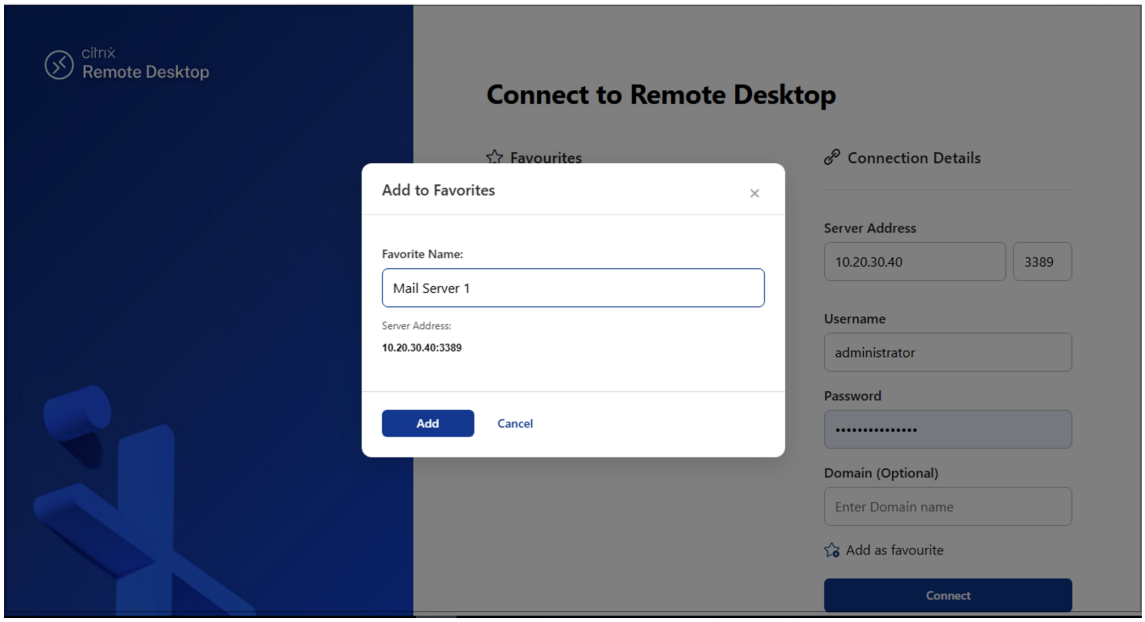
- Users can access the Remote Desktop app directly from the extension UI.

- Users are presented with a login screen to authenticate.

> **Note:**
>
> Only the user name and password-based authentication is supported. You can also enter the domain name for the authentication.



- Users can save the frequently used Remote Desktop connections as favorites for quick access.

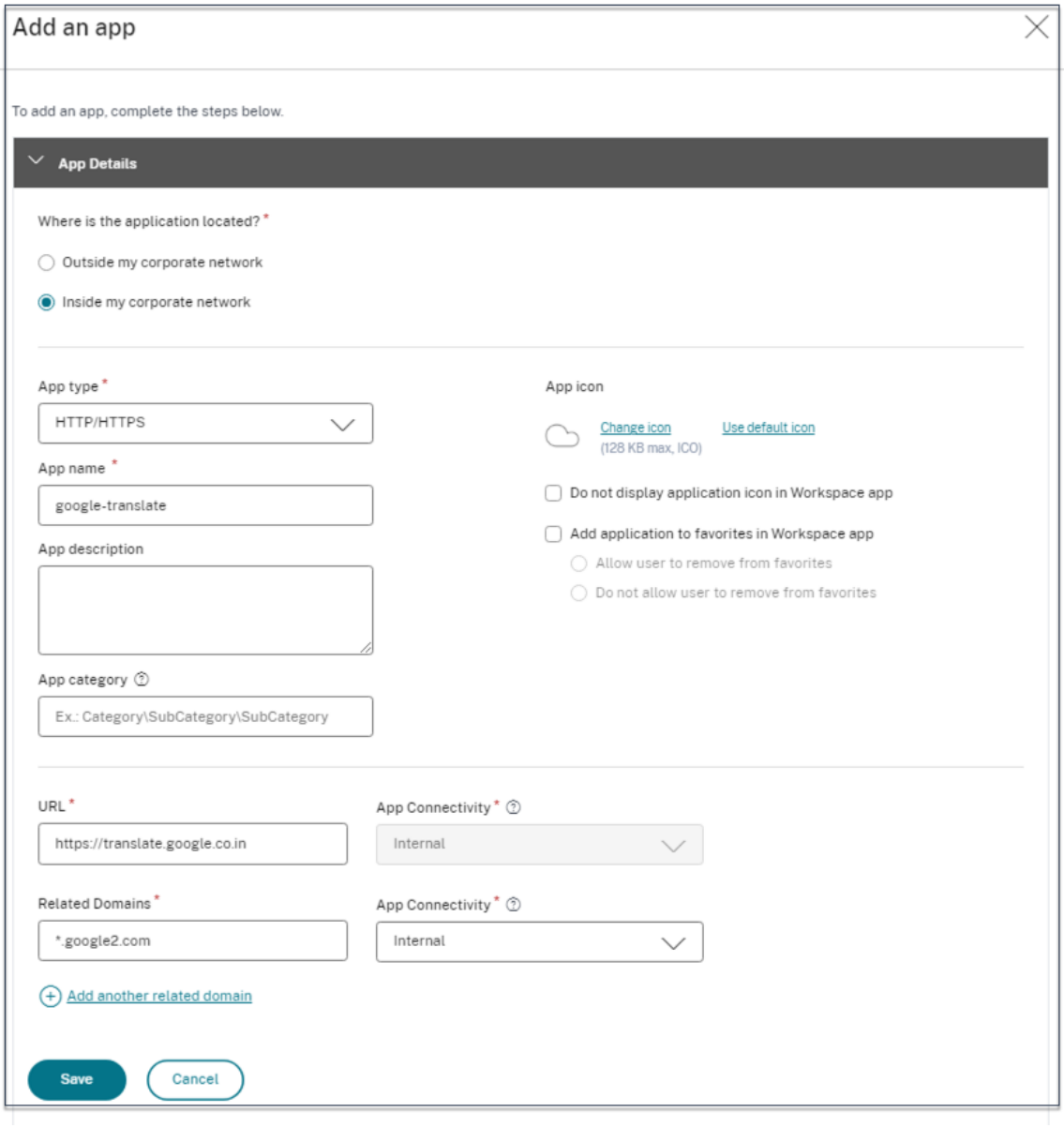


Configure Web/SaaS applications

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.

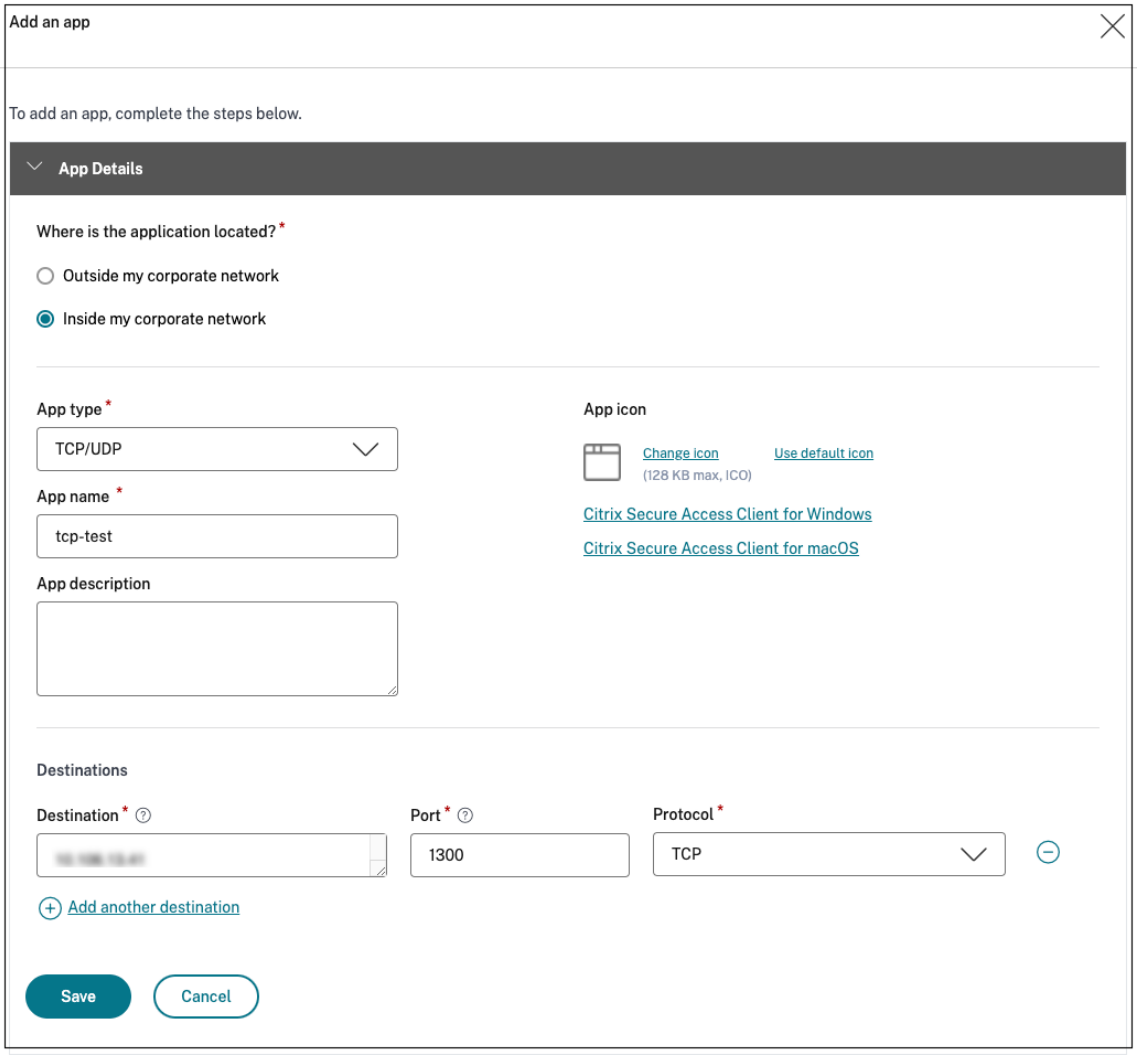
Configure TCP/UDP apps

November 25, 2025

Before configuring TCP/UDP apps, see System requirements.

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:

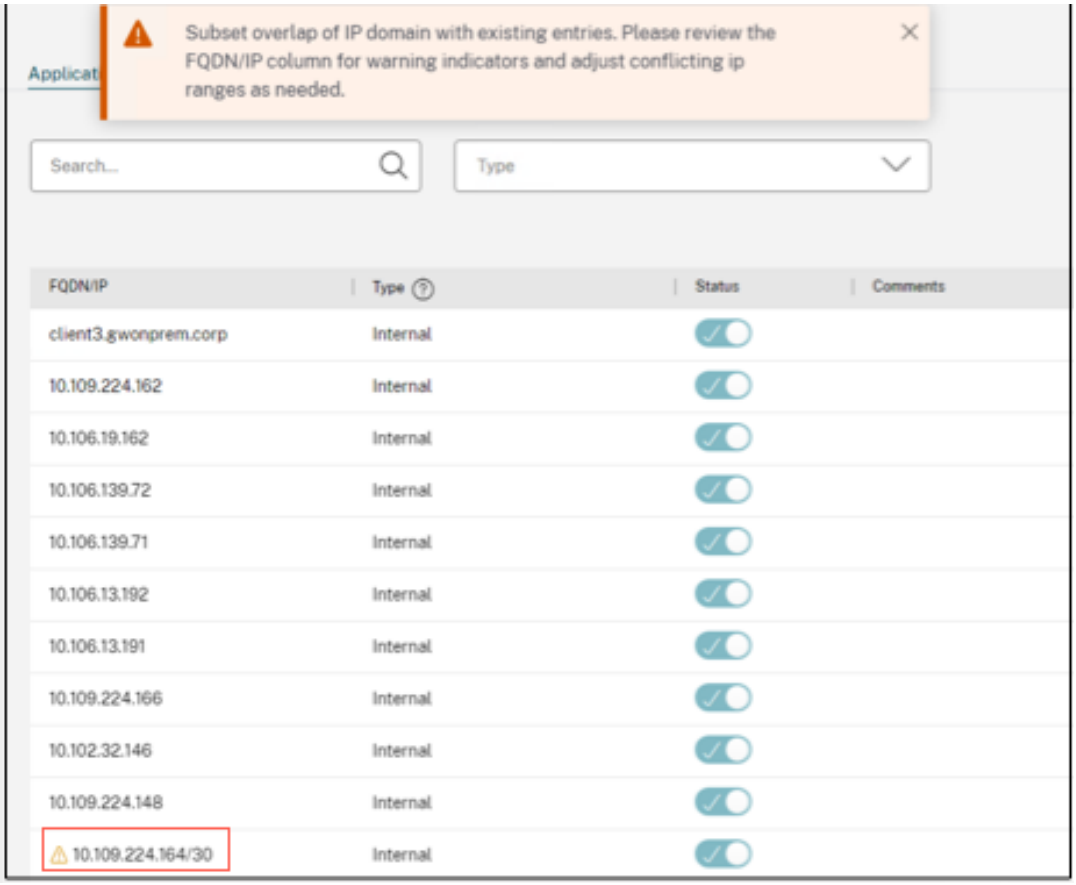
   - **App type** –Select **TCP/UDP** for initiating connections with the back-end servers residing in the data center.
   - **App name**–Name of the application.
   - **App description** –Description of the app you are adding. This field is optional.
   - **Destinations** –IP Addresses or FQDNs of the 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

November 26, 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:

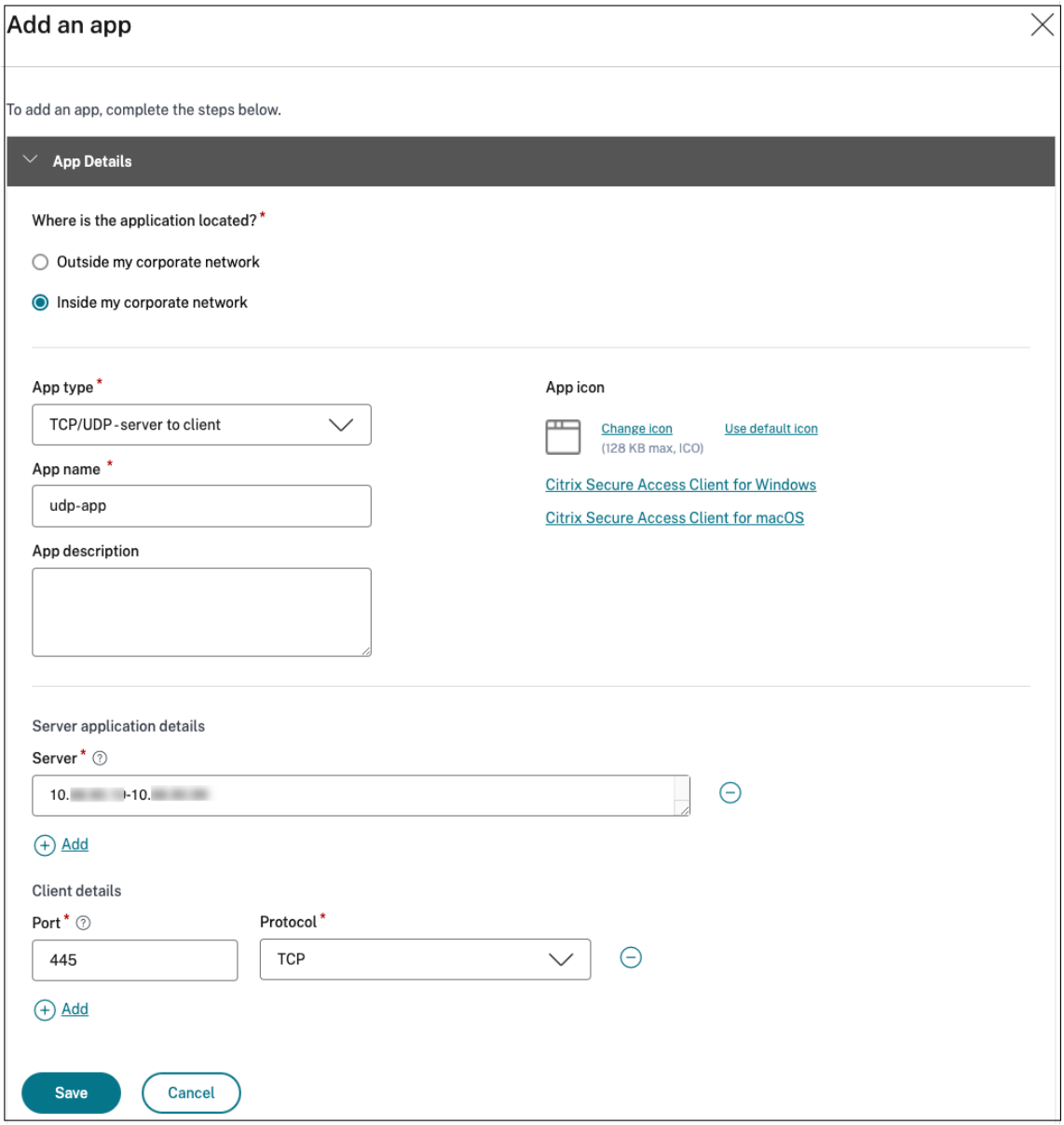
  ```
  set vpn sessionAction ns_default_vpn_session_profile_spa_tcp_udp_apps
   -useMIP NS -useIIP NOSPILLOVER
  ```

  (Optionally users can create a VPN session profile and a session action with `-useMIP NS -useIIP NOSPILLOVER`)

  bind vpn vserver <`spa vserver name`> -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.

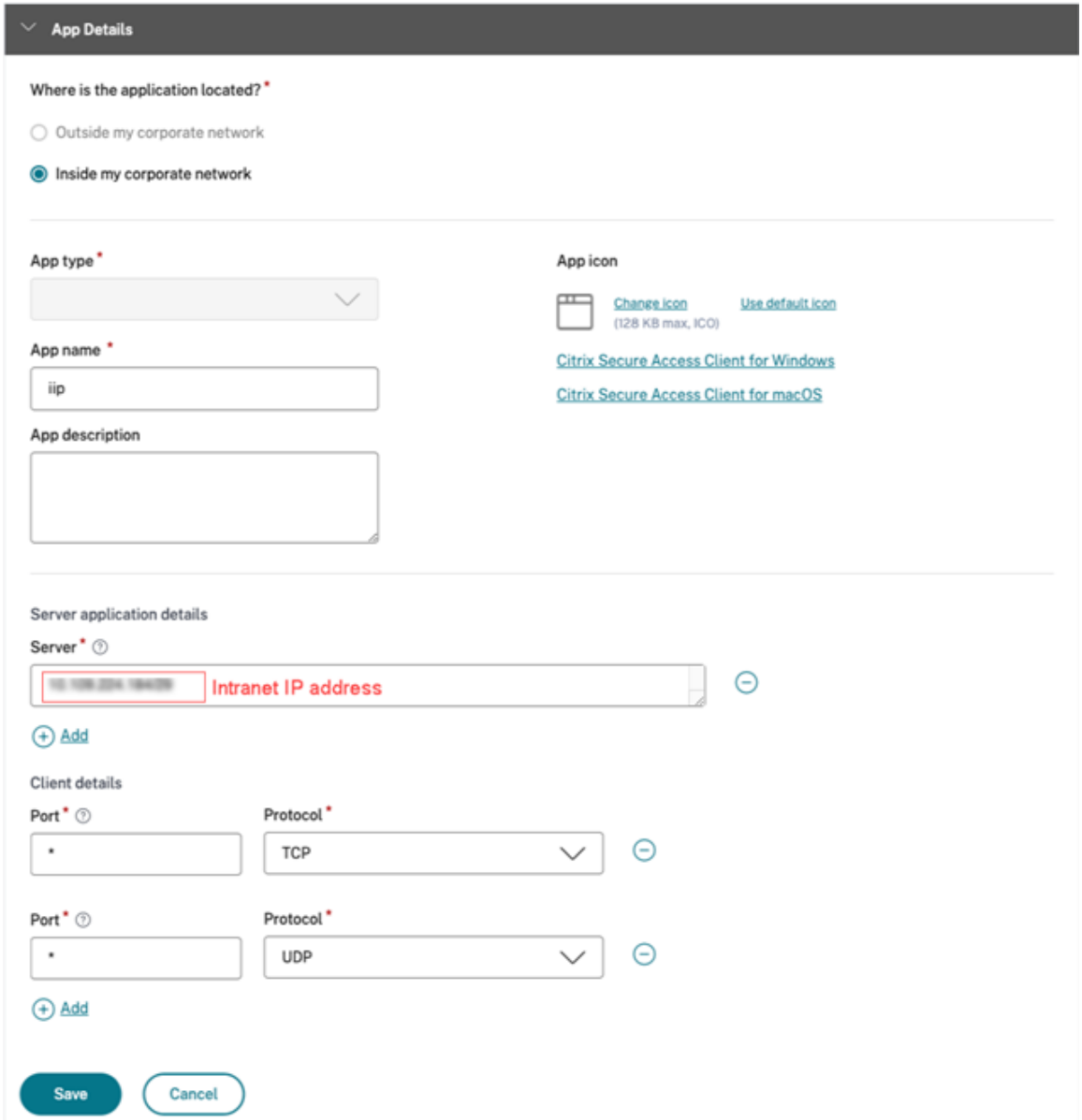
5. Click **Save**. The app is added to the **App Configuration** page. You can edit or delete an app

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.



Edit an application

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

Next steps

Configure access policies for the applications.

Configure access policies for the applications

November 25, 2025

Access policies within Secure Private Access allow you to enable or disable access to the apps based on the context of the user or user's device.

Access restrictions must be configured through the Google Admin console rather than within the Secure Private Access interface.

Rules are configured in the **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.

For details on creating policies and rules for Google Chrome in the Google Admin console, see the following topics:

- Set Chrome Enterprise connector policies for Chrome Enterprise
- Data protection rules

Configure access policies

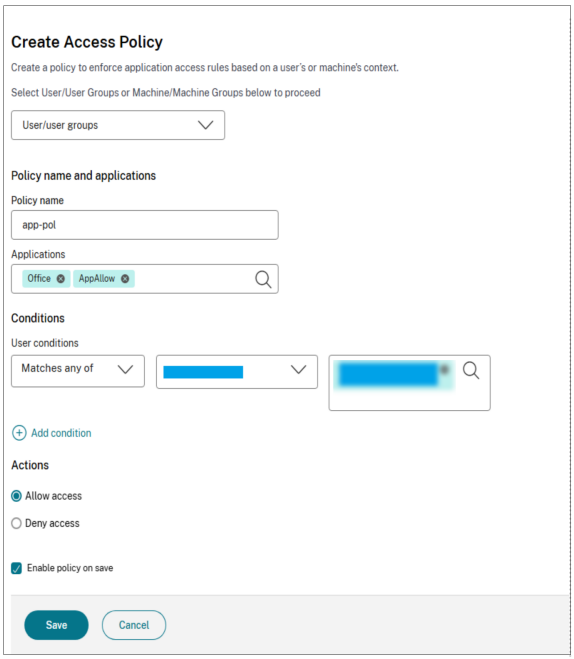
1. In the admin console, click **Access Policies**.
2. Click **Create Policy**.
3. In the **Create Access Policy** page, select one of the following:
    - **Users/User groups**
    - **Machines/Machine groups**

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

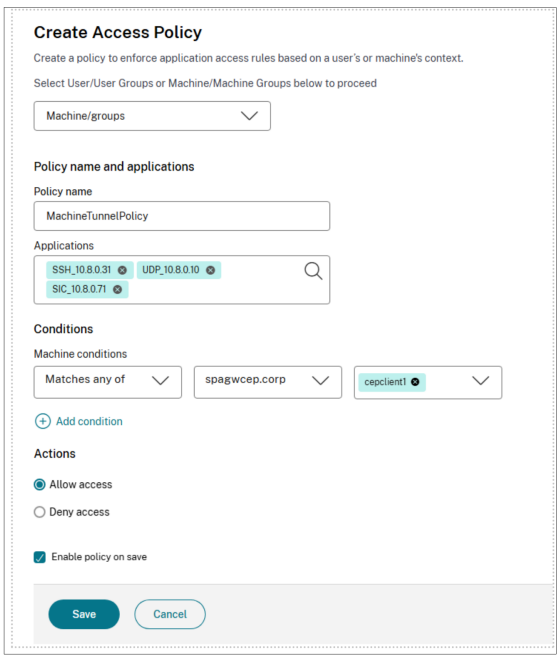
You can select **Machine/Machine groups** to enable Always On connectivity. For Always On connectivity, you must have the device certificates enrolled. For details see Device certificate enrollment configuration.

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

Access policy for Web/SaaS apps



Access policy for TCP/UDP apps



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

   - **Matches any of**: Only the users 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. For details, see Policy conditions.

7. (Optional) Click **+** to add multiple conditions based on the context.

   When you add conditions based on a context, an AND operation is applied on the conditions, and the policy is evaluated only if the Users and the optional contextual based conditions are met. You can apply the following conditions based on context.

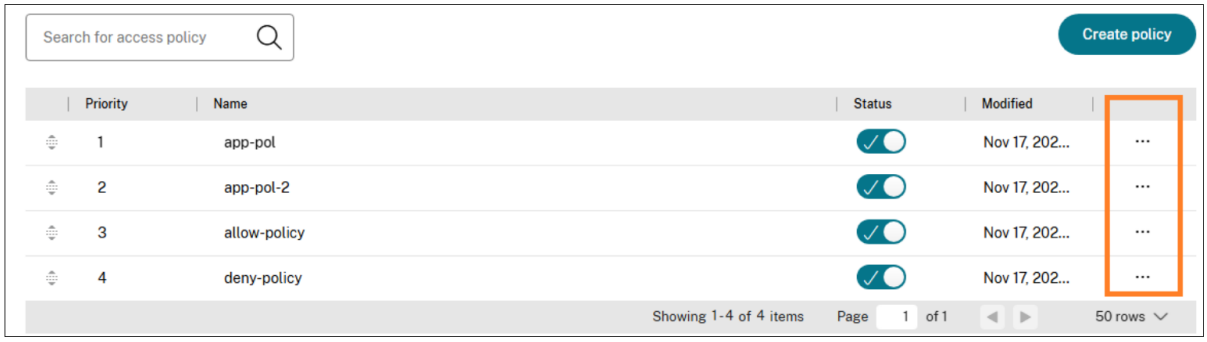
- **Network Location** - Select the condition and the network using which the users access the apps.
  - **Matches any of:** Only users or user groups accessing the apps from any of the network locations listed are enabled for access to the apps.
  - **Does not match any:** All users or user groups other than those from the listed network locations are enabled for access.
- **Device Posture** - Select the conditions that the user device must fulfill to access the apps.

For details, see Policy conditions.

8. In **Actions**, select one of the following actions that must be enforced on the app based on the condition evaluation.
   - **Allow access**
   - **Deny access**
9. Select **Enable policy on save**. If you do not select this option, the policy is only created and not enforced on the applications. Alternatively, you can also enable the policy from the Access Policies page by using the toggle switch.

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**.



Change 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

Configure access policies for the applications

November 25, 2025

Access policies within Secure Private Access allow you to enable or disable access to the apps based on the context of the user or user's device.

Access restrictions must be configured through the Google Admin console rather than within the Secure Private Access interface.

Rules are configured in the **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.

For details on creating policies and rules for Google Chrome in the Google Admin console, see the following topics:

- Set Chrome Enterprise connector policies for Chrome Enterprise
- Data protection rules

Configure access policies

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

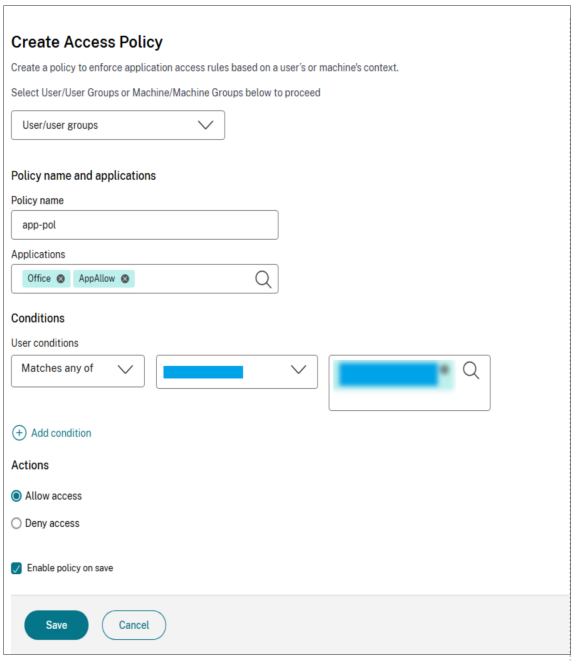
   - **Users/User groups**
   - **Machines/Machine groups**

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

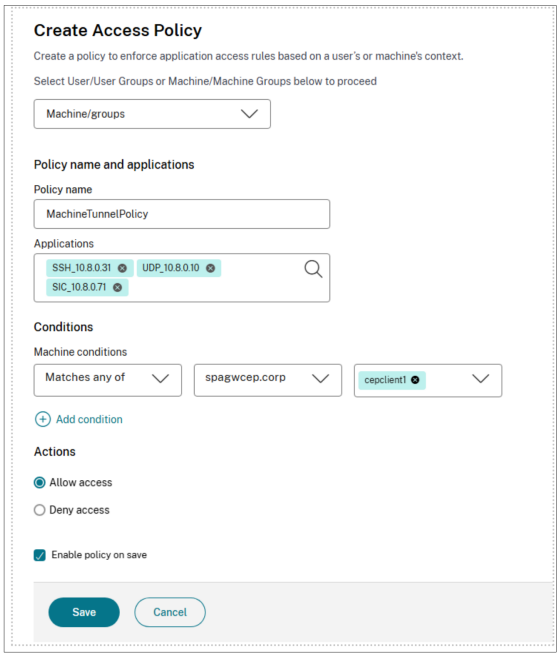
   You can select **Machine/Machine groups** to enable Always On connectivity. For Always On connectivity, you must have the device certificates enrolled. For details see Device certificate enrollment configuration.

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

Access policy for Web/SaaS apps



Access policy for TCP/UDP apps



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

   - **Matches any of**: Only the users 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. For details, see Policy conditions.

7. (Optional) Click **+** to add multiple conditions based on the context.

   When you add conditions based on a context, an AND operation is applied on the conditions, and the policy is evaluated only if the Users and the optional contextual based conditions are met. You can apply the following conditions based on context.

   - **Network Location** - Select the condition and the network using which the users access the apps.
     - **Matches any of:** Only users or user groups accessing the apps from any of the network locations listed are enabled for access to the apps.
     - **Does not match any:** All users or user groups other than those from the listed network locations are enabled for access.
   - **Device Posture** - Select the conditions that the user device must fulfill to access the apps.

   For details, see Policy conditions.

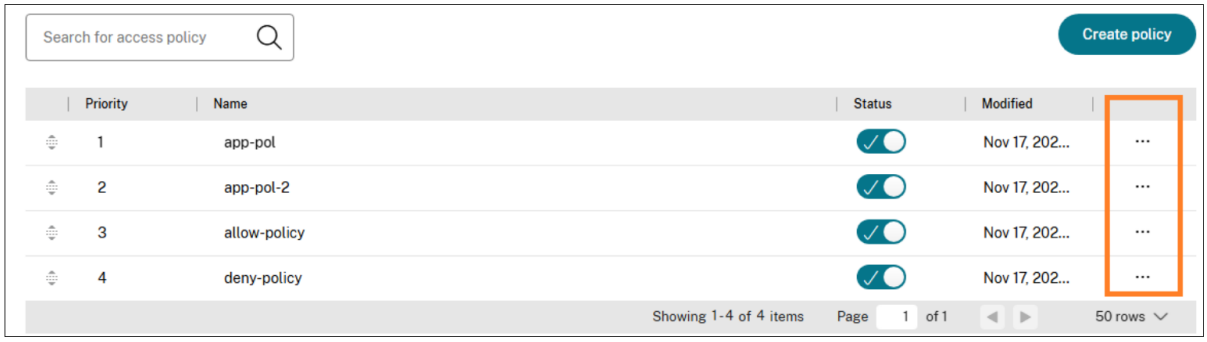
8. In **Actions**, select one of the following actions that must be enforced on the app based on the condition evaluation.

   - **Allow access**
   - **Deny access**

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

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**.



Change 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

Policy conditions

November 25, 2025

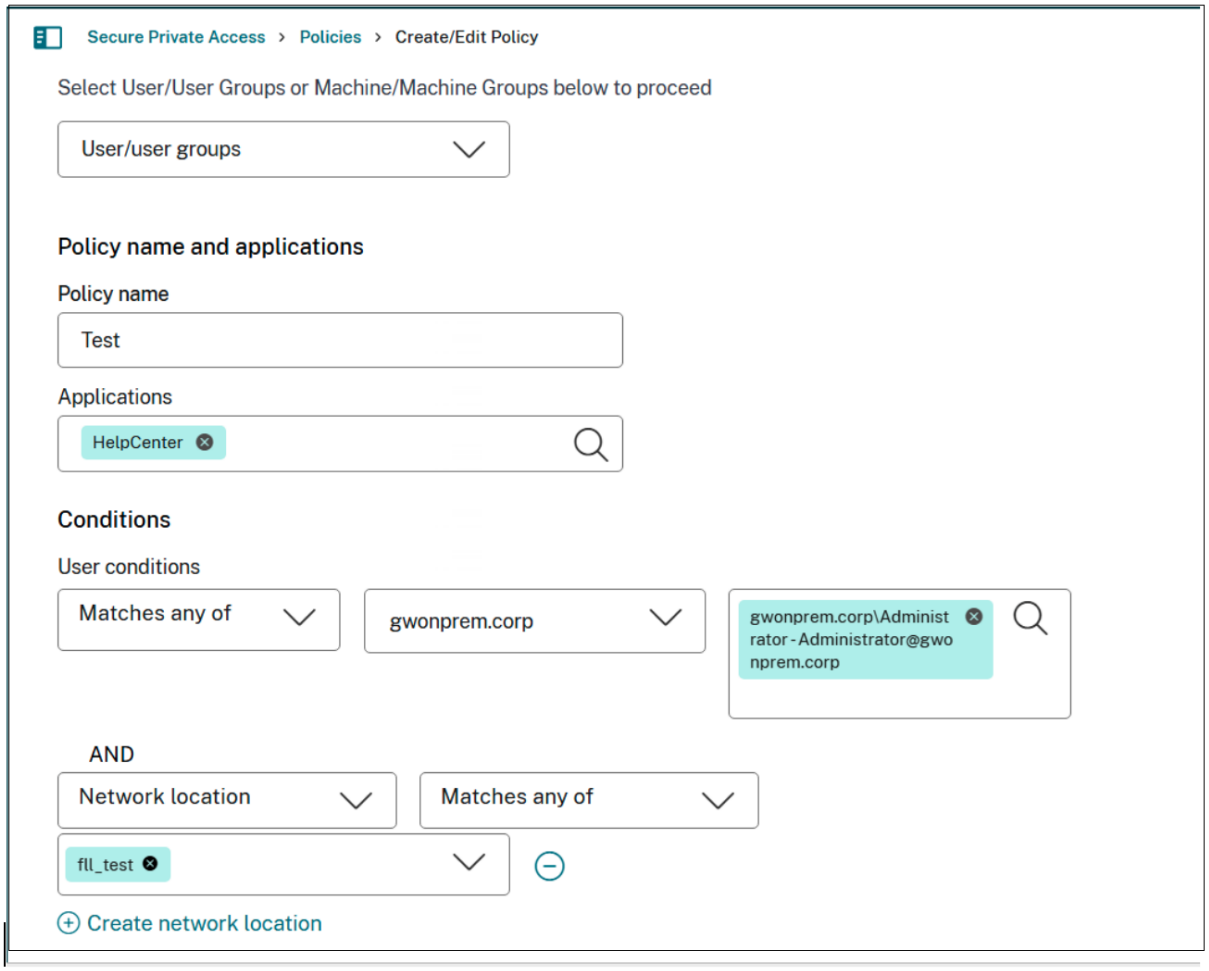
User and user groups

User conditions define which users, groups, or identity attributes the access policy applies to. These rules let administrators include or exclude specific identities when determining access to an application.

User conditions consist of three primary components:

Match Type:
This drop-down list controls how the list of selected identities is evaluated.

- **Matches any of:**
  - Use this when the policy must apply only to the selected users or groups.
  - The condition is satisfied if at least one identity in your list matches.
  - Works like an IN filter.
- **Does not match any**
  - Use this to apply the policy to everyone except the selected users or groups.
  - The condition is satisfied only if none of your selected identities match.
  - Works like a NOT IN filter.



Domain Selector:

The **Domain** drop-down list filters identities by directory or identity source.

- **Identity Selector (user emails, group emails)** - This field allows selecting one or more identities, including user emails and group emails.

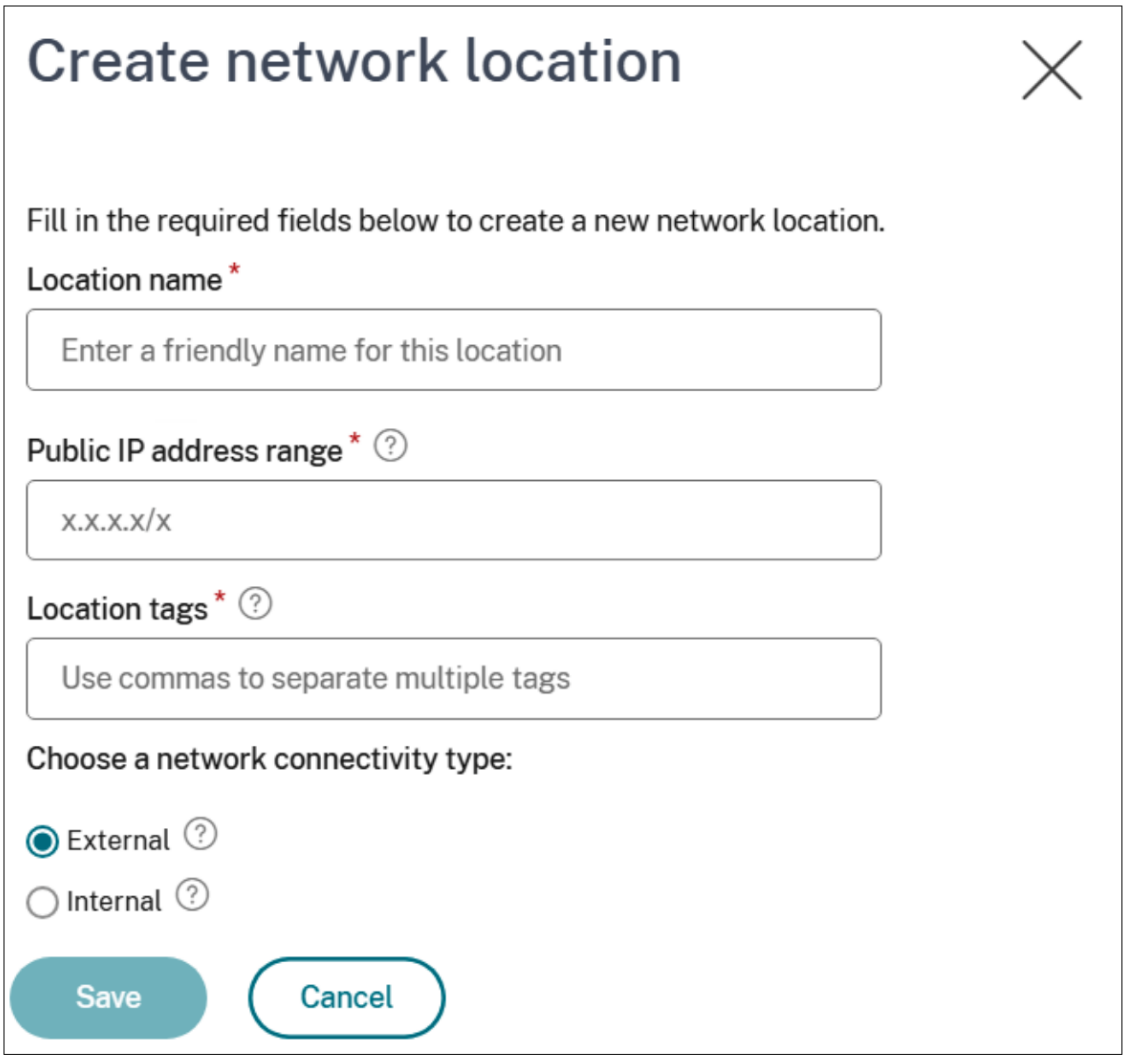
Network Location

The Network Location Service (NLS) is a policy condition that allows you to restrict access based on the user's network location. An admin can configure the access policy based on the location from where the user is accessing the application. The location can be the country from where the user is accessing the application or the user's network location. The network location is defined using an IP address range or subnet addresses.

To configure an access policy based on the location, do the following:

1. Under **Conditions** section, click **Add condition**.

2. Select **Network location**.



If you have configured multiple network locations, then select one of the following as per your requirement.

- **Matches any of** –The network locations match any of the network locations configured in the database.
- **Does not match any** –The network locations do not match with the network locations configured in the database.

> **Note:**
>
> For **Network location**, you can select an existing network location or create a network location. To create a new network location, click **Create network location**.

- Ensure that you have enabled Adaptive Access from **Citrix Cloud > Citrix Workspace > Access > Adaptive Access**. If not, you cannot add the location tags. For details, see Enable

Adaptive Access.

You can also create a network location from the Citrix Cloud console. For details, see Citrix Cloud network location configuration.

3. Complete the policy configuration.

Device Posture service

November 25, 2025

Citrix Device Posture service is a cloud-based solution that helps admins to enforce certain requirements that the end devices must meet to gain access to Citrix DaaS (virtual apps and desktops) or Citrix Secure Private Access resources (SaaS, Web apps, TCP, and UDP apps). Establishing device trust by checking the device's posture is critical to implement 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 more information about device posture, see Device Posture.

Configure the device posture checks on NetScaler Gateway

The Citrix Device Posture service is integrated with NetScaler Gateway. You can configure the device posture checks on NetScaler Gateway.

For more information, see Device Posture checks on NetScaler® Gateway.

> **Note:**
>
> - It is recommended to enable device posture checks at the virtual server level.
> - Ensure that the customer ID is set up using the `set dps parameter` that is `set dps parameter -CustomerID <CCID>`. The rest of the parameters are auto populated.

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.

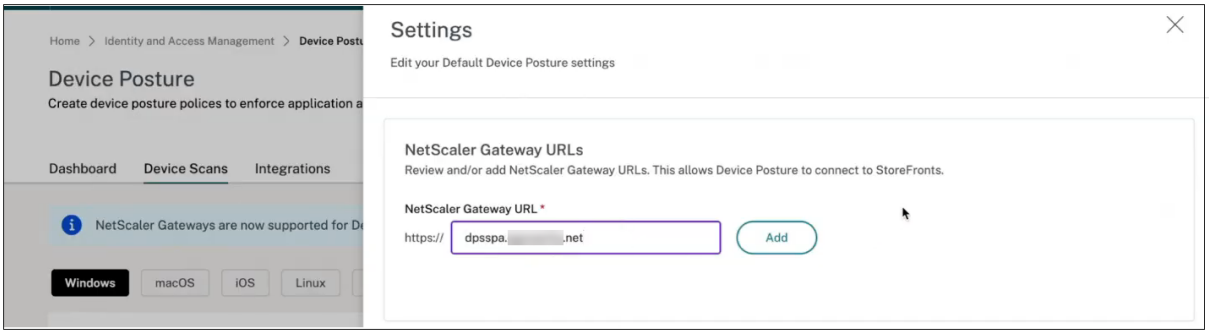
Enable Device Posture for Secure Private Access hybrid solutions

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`.



Manage settings

November 25, 2025

Application domains

Secure Private Access admins can view the list of application domains added to 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. Click the edit icon and change the routing type, if necessary.

Configuration report

Customer administrators can generate configuration reports to gain insights into the Secure Private Access 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.
- Security Groups.
- Cloud connectors.
- Site configurations.
- Browser settings.

You can also include additional configuration reports in the bundle:

- Details from the connector plug-in database.
- Details from the proxy service.
- Details from the analyzer configuration.

Generate a configuration report

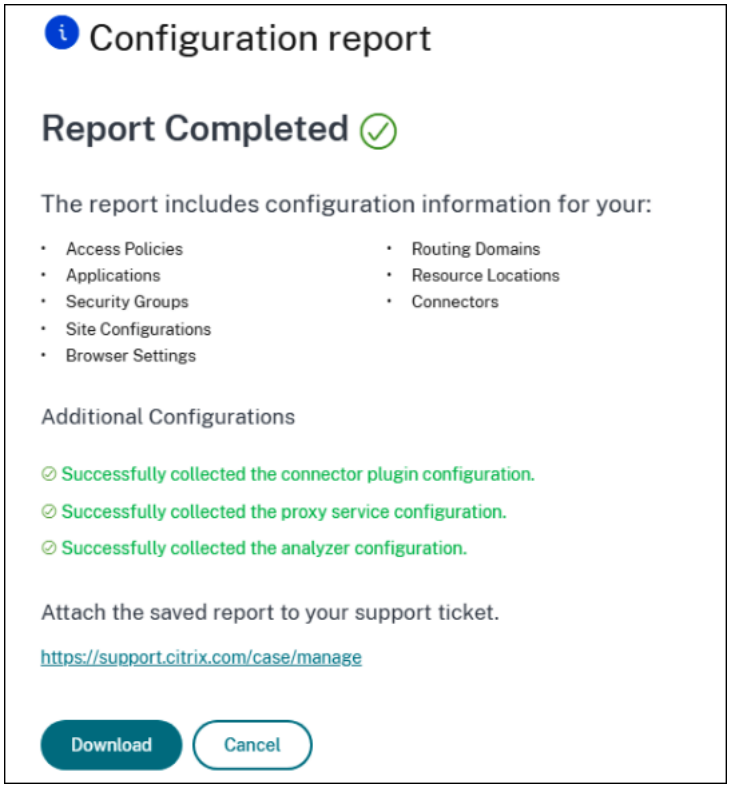
Perform the following steps to generate a configuration report:

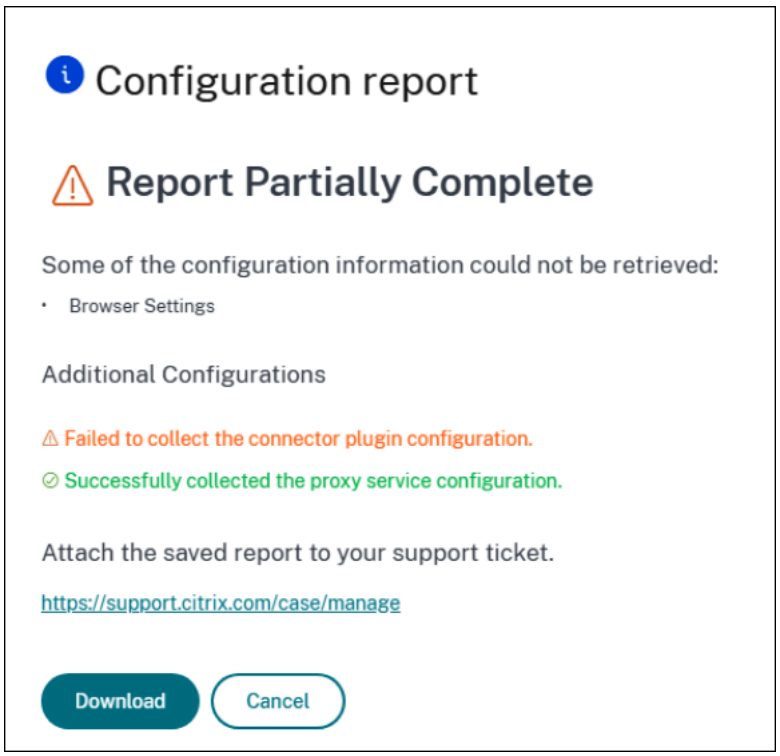
1. In the Secure Private Access admin console, go to **Settings > Configuration Report**.
2. To include the additional reports in the bundle by collecting the configuration details stored in the connector plug-in database, the proxy service, or the analyzer configuration, check the appropriate checkboxes under the **Additional Configurations** section.
3. Click **Create report** to initiate the report generation process.

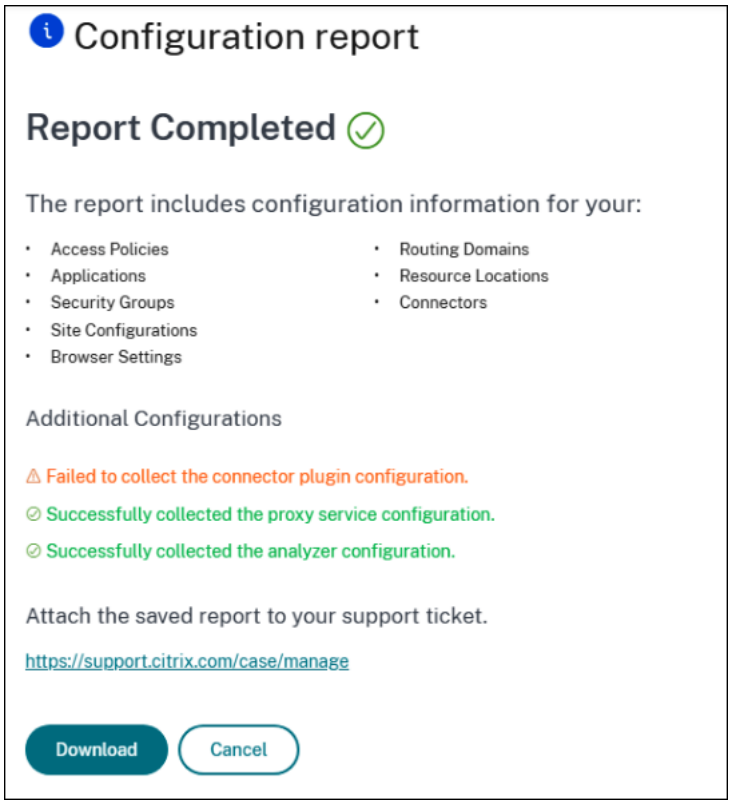
   Once the report is generated, the **Configuration Report** dialog displays the following status:

   - **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 displays a sample **Configuration Report** dialog with complete and partially complete status.







4. Click **Download** to manually export the reports 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.

Note:

Reports can contain sensitive data.

Manage setup configuration after installation

November 25, 2025

The **Setup configuration** menu option can be used to manage various configuration inputs provided during the onboarding.

> **Warning:**
>
> Changing the configuration values can be disruptive. Since this configuration is referenced by multiple components, changes may necessitate re-configuration in dependent components to avoid service interruptions.

The following table summarizes the additional actions needed if any configuration is changed.

Config name	Action needed	Description
Step1		
Google Customer ID	Reconfigure and re-analyze NetScaler by downloading the script again.	Google services are automatically reconfigured.
Secure Private Access Gateway URL	Reconfigure and re-analyze NetScaler by downloading the script again.	Google services are automatically reconfigured. **Note** If CEP config is skipped, this setting is part of Step2.

Config name	Action needed	Description
Google Workspace user groups	No manual action needed	New user groups are auto configured on required Google services when settings are saved.
Step2		
NetScaler Gateway virtual server name	Rerun the NetScaler Analyzer only	Use the analyze option when running the NetScaler script.
Secure Private Access site URL	Reconfigure StoreFront with the new Secure Private Access address. Re-analyze StoreFront by downloading scripts again Reconfigure and re-analyze NetScaler by downloading the script again.	
Internal IP address (for Secure Private Access Gateway URL)	Reconfigure and analyze NetScaler by downloading the script again.	
Certificate-key pair name	Reconfigure and re-analyze NetScaler by downloading the script again.	

Reset Secure Private Access configuration

November 25, 2025

If you have a Citrix Secure Private Access hybrid deployment with Citrix Enterprise Browser integration and you want to switch to Chrome Enterprise Premium, you can reset the Secure Private Access configuration. This action deletes the entire configuration, including applications and access policies. The StoreFront and NetScaler configurations require manual cleanup. After configuration reset, you can onboard a Secure Private Access hybrid deployment again and select Chrome Enterprise Premium.

Reach out to Citrix Support if you need to reset the configuration.

Upgrade

November 25, 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.

> **Note:**
>
> NetScaler upgrade through the GUI sometimes does not install Python. It is recommended that you upgrade NetScaler through the CLI.

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

- StoreFront
- NetScaler Gateway

Discover domains or IP addresses accessed by end users

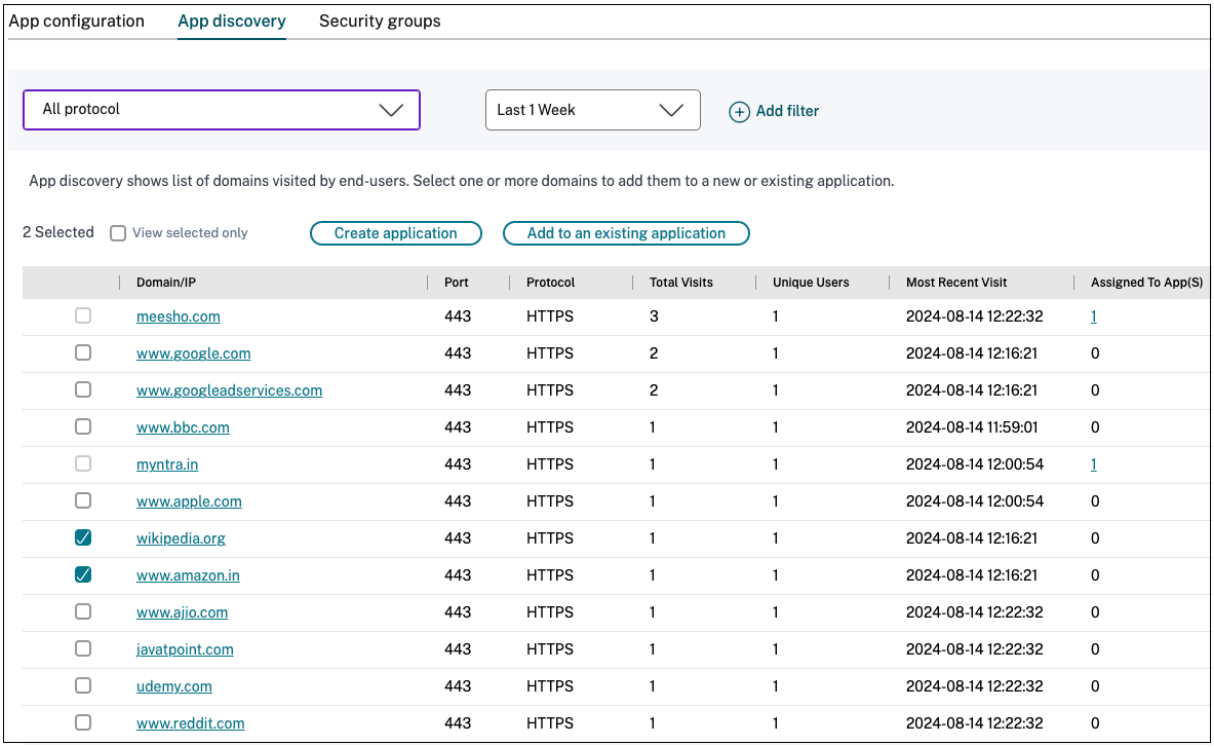
September 6, 2025

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

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

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

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

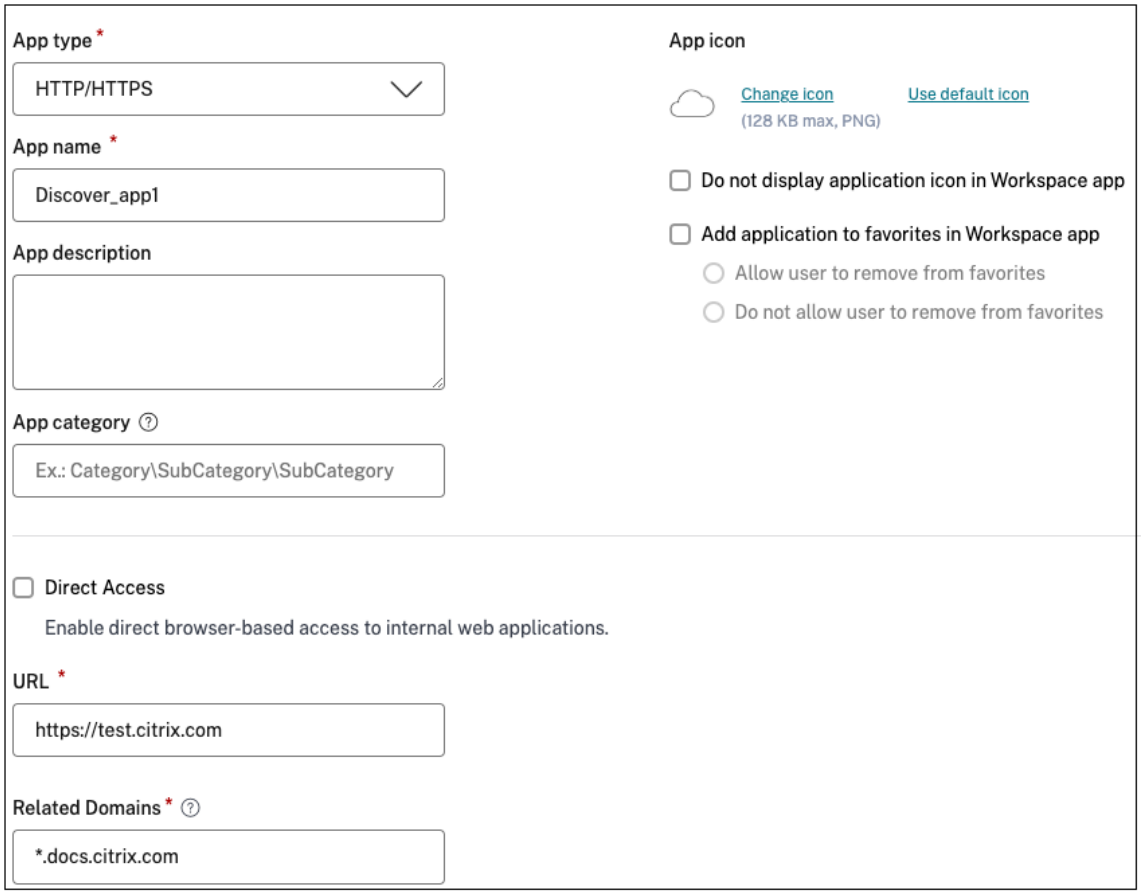


Application Discovery for internal domains in a new environment

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

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

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

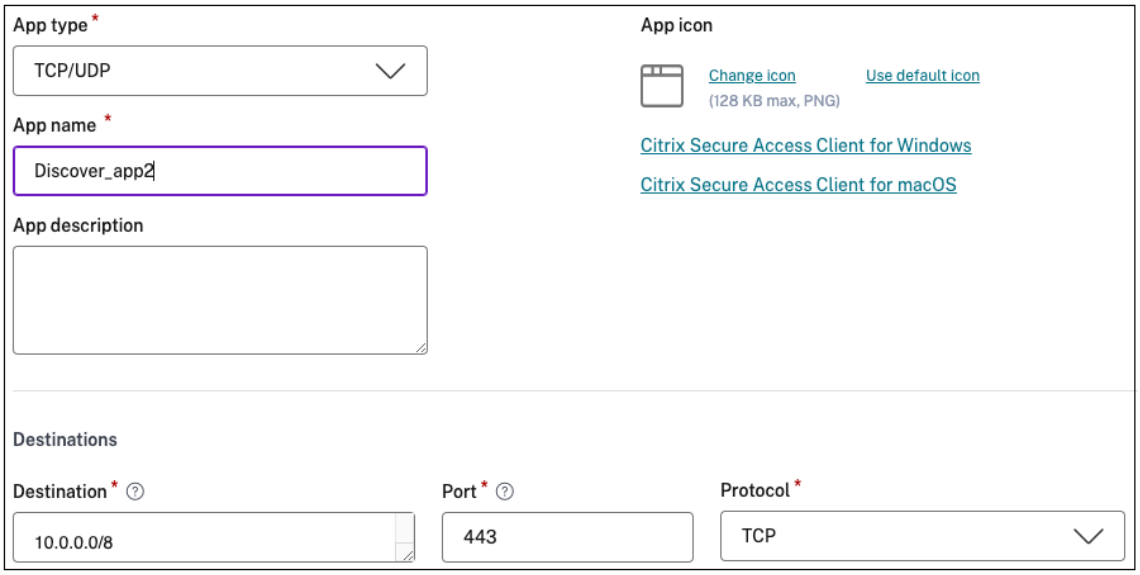


Web app URL: `https://test.citrix.com/`
Related domain: `*.citrix.com`

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

  Port: (*)

  Protocol: TCP



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

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

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

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

Create an application from the App discovery page

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

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

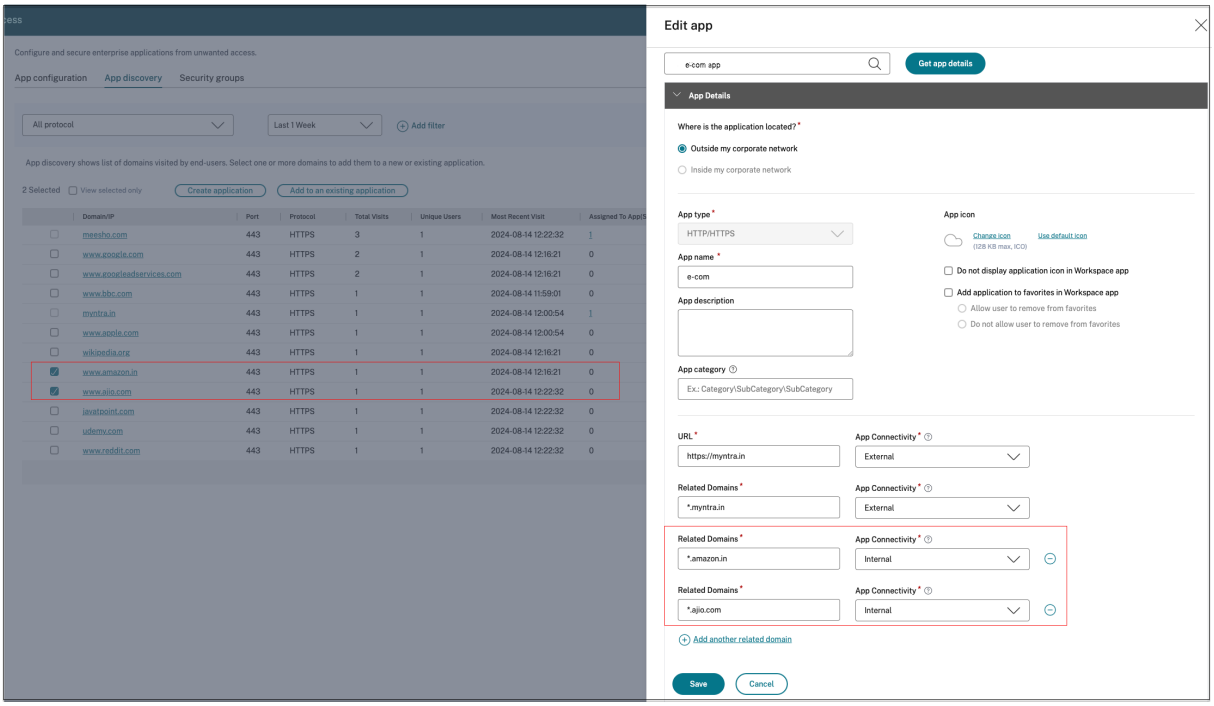
   > **Note:**
   >
   > - You cannot select domains belonging to different protocols to create an application. An error message is displayed when you select domains belonging to different protocols.
   > - If a domain is already associated with an application, you cannot select that domain again to create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

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

Update an existing application

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

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



Note:

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

Policy modeling tool

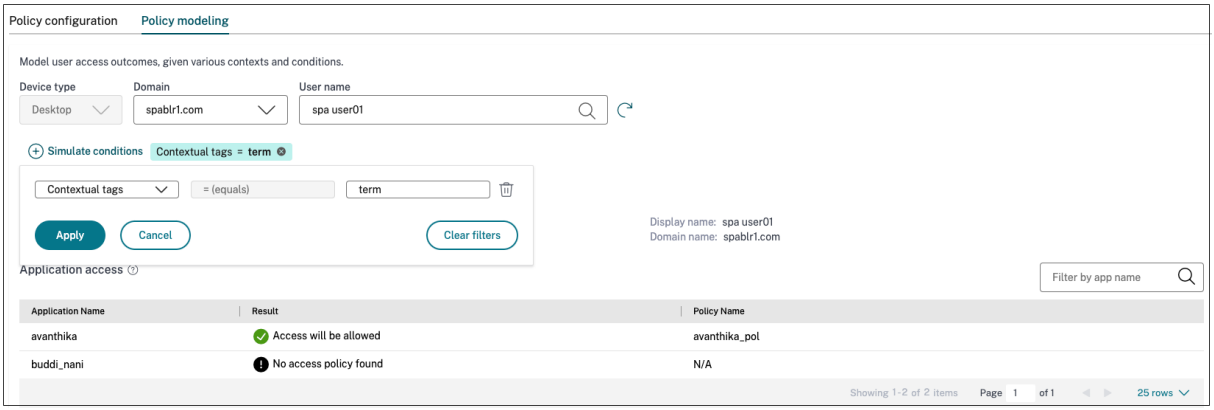
September 6, 2025

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.



Configure Data Loss Prevention (DLP) policies

November 25, 2025

Access restrictions are configured in the Google Admin console for CEP. Access restrictions that were previously configured in the Secure Private Access console only apply to Citrix Enterprise Browser. When Google Chrome is the enterprise browser, access restrictions 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.

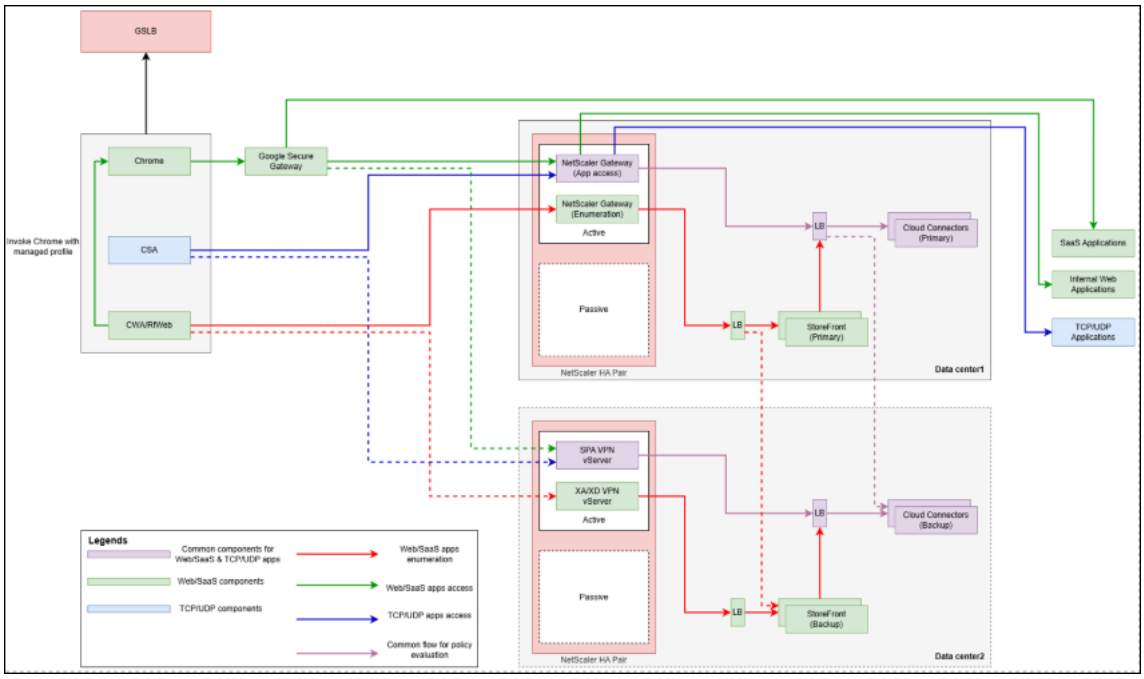
For details on creating policies and rules in the Google Workspace Admin console, see the following topics:

- Set Chrome Enterprise connector policies for Chrome Enterprise
- Data protection rules

High availability deployments

January 2, 2026

You can configure high availability for Secure Private Access in just a few straightforward steps.



High availability within the data center

NetScaler

For high availability, it is recommended to Create NetScaler high-availability Pair. This is an active-passive NetScaler pair.

If the active NetScaler is down, the passive NetScaler is automatically promoted as active, and all user traffic is routed to the new active NetScaler. Users are not required to re-authenticate as the sessions are also synchronized across the NetScaler high availability pair.

For more details on NetScaler HA pair, see High Availability.

Cloud Connectors (Secure Private Access servers)

Configure a NetScaler load balancer for Secure Private Access with service group configuration.

1. **Create a new service group on NetScaler:** Navigate to **Configuration > Traffic Management > Load Balancing > Service Groups**.
2. Click **Add**.
3. Enter a **Name** for the service group, for example, `primary_spa_servers`.
4. Depending upon the type of load balancer (**SSL** or **SSL_BRIDGE**), choose the appropriate **Protocol** for the service group.
5. Leave other fields with default values and click **OK** to save the service group.
6. Click **No Service Group Member** to add Cloud Connectors from the current data center.
7. Use the **IP Based** option and add the current data center's Cloud Connectors **IP address** and **Port**. By default, Secure Private Access uses port **8443**. Other fields can be retained with default values.
8. Repeat this step if additional Cloud Connectors must be added.
9. Click **Create** to create the load balancer service.
10. Click **OK** to add the service to the service group.

    > **Note:**
    >
    > Optionally you can add an HTTP Monitor for the Secure Private Access service. The following URL path can be used to do so.
    >
    > `/secureAccess/health`
    >
    > It returns **200 OK** if Secure Private Access is up and running.

11. Click **Done**.
12. Now create a load balancer. Navigate to **Configuration > Traffic Management > Load Balancing > Virtual Servers**.
13. Click **Add**.
14. Enter a load balancer name.

15. Choose the appropriate **Protocol**, for example, **SSL** or **SSL_BRIDGE**.
16. Set **IP Address Type** as **IP Address** and **Port** as 443.

    > **Note:**
    >
    > The protocol must be SSL or SSL_BRIDGE. HTTP type is not supported for Secure Private Access load balancer. The port must be 443. Custom HTTPS ports are not supported.

17. Click **OK**.
18. Click **No Load Balancing Virtual Server ServiceGroup Binding**.
19. Click to select the service group created earlier, then click **Select**.
20. Set **Order** value as **10**. Click **Bind**, then **Continue**.
21. If using **SSL** type **Protocol**, click **No Server Certificate** to bind the appropriate server certificate. For SSL_BRIDGE type load balancer, no server certificate is required in the load balancer, but the server certificate must be configured in the Cloud Connector for Secure Private Access service. For details, see Configure TLS/SSL certificates for the Secure Private Access service on Cloud Connector.

This concludes the load balancer configuration with the service group for Secure Private Access.

All the Secure Private Access servers in the load balancer are active. If one Secure Private Access server goes down, users are not impacted as the other Secure Private Access servers continue to serve the traffic. The Secure Private Access servers are stateless, so there is no persistency requirement.

StoreFront servers

StoreFront servers also behave the same as Secure Private Access servers during failover within the same data center.

Reset Secure Private Access configuration

November 25, 2025

If you have a Citrix Secure Private Access hybrid deployment with Citrix Enterprise Browser integration and you want to switch to Chrome Enterprise Premium, you can reset the Secure Private Access configuration. This action deletes the entire configuration, including applications and access policies. The StoreFront and NetScaler configurations require manual cleanup. After configuration reset, you can onboard a Secure Private Access hybrid deployment again and select Chrome Enterprise Premium.

Reach out to Citrix Support if you need to reset the configuration.

Visibility and monitoring

November 25, 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:

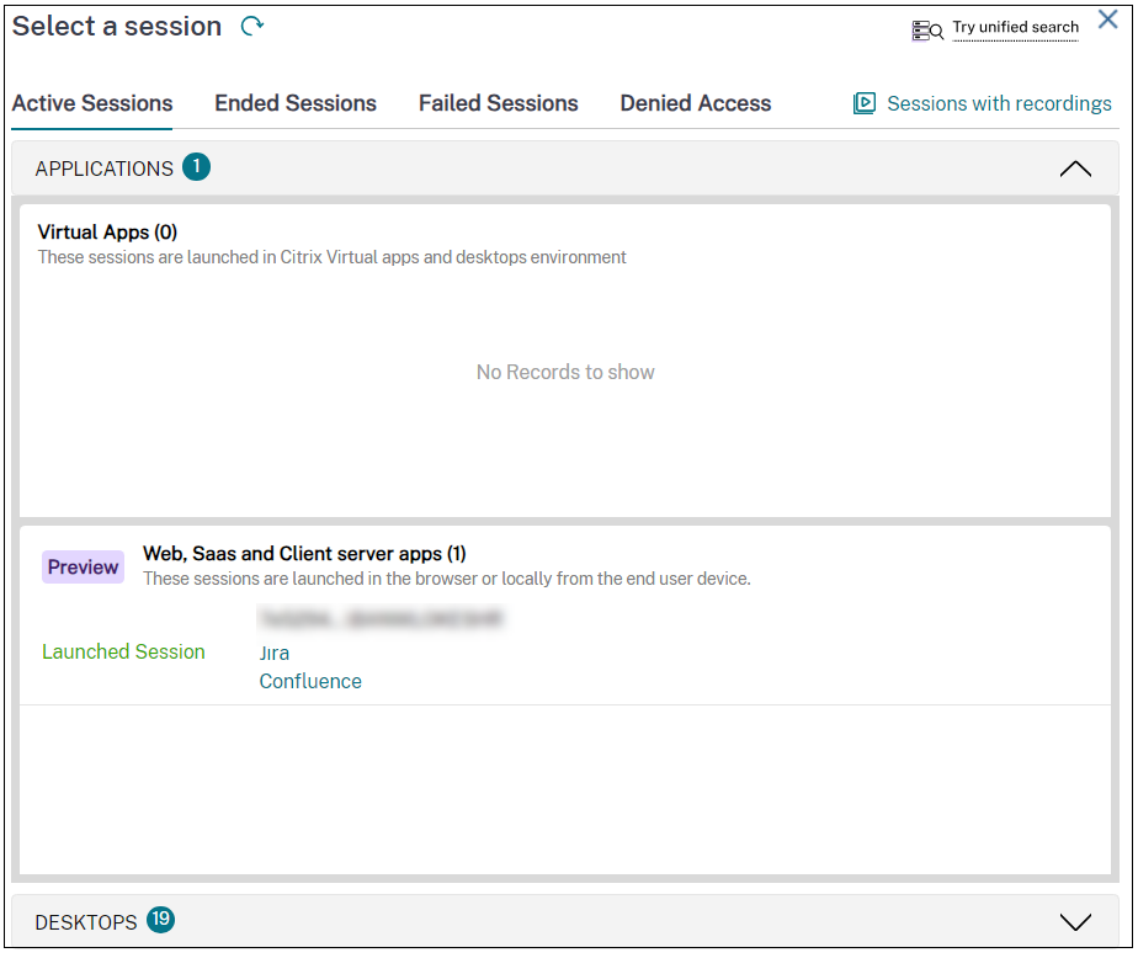
- Start: You log in to the Citrix Secure Access™ client and access the apps.

- 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.

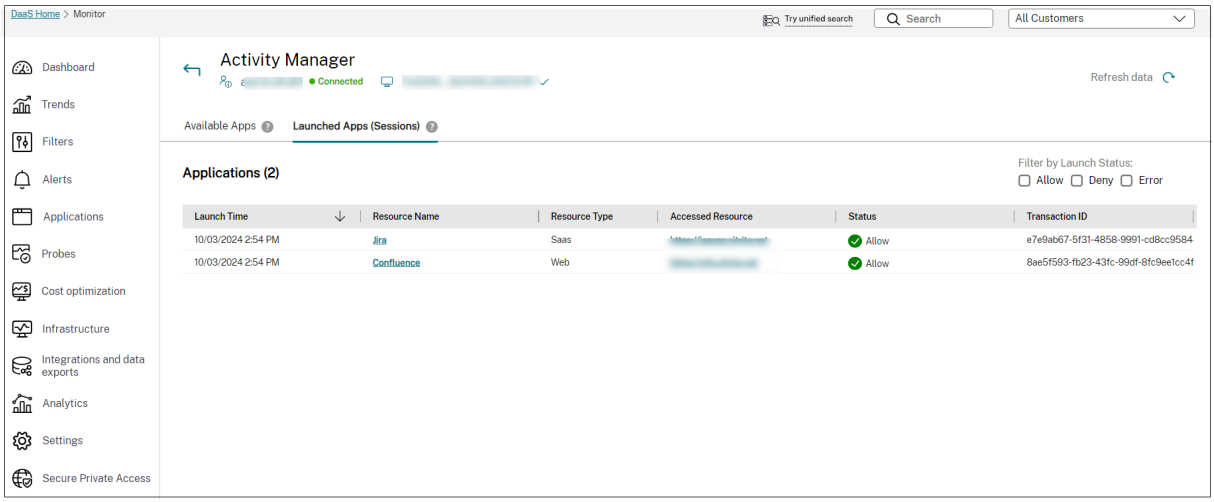
3. Click one of the following tabs:

- **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.

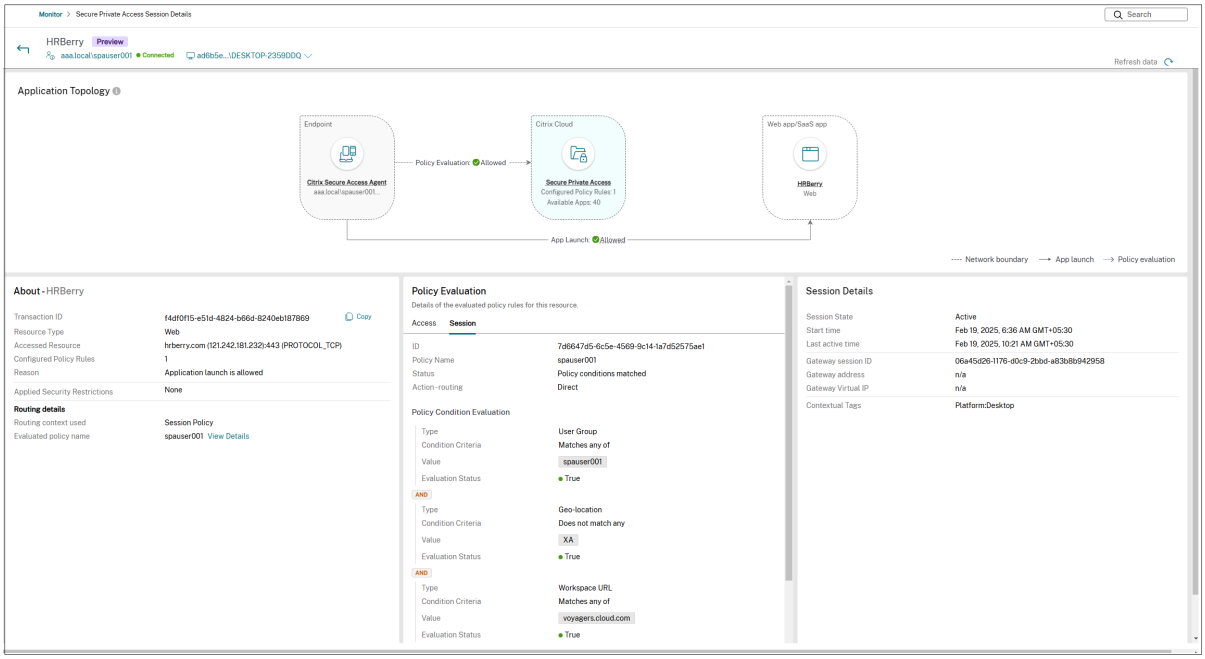
- **Session Topology:** Displays the app launch flow.
- **About:** Displays app-related information such as app type, number of policy rules, security restrictions, and accessed resources. The data that appears in the **Accessed Resources** section varies depending on the app type.

  - SaaS apps - URL or the app FQDN
  - TCP/UDP –IP address/FQDN, port, and protocol

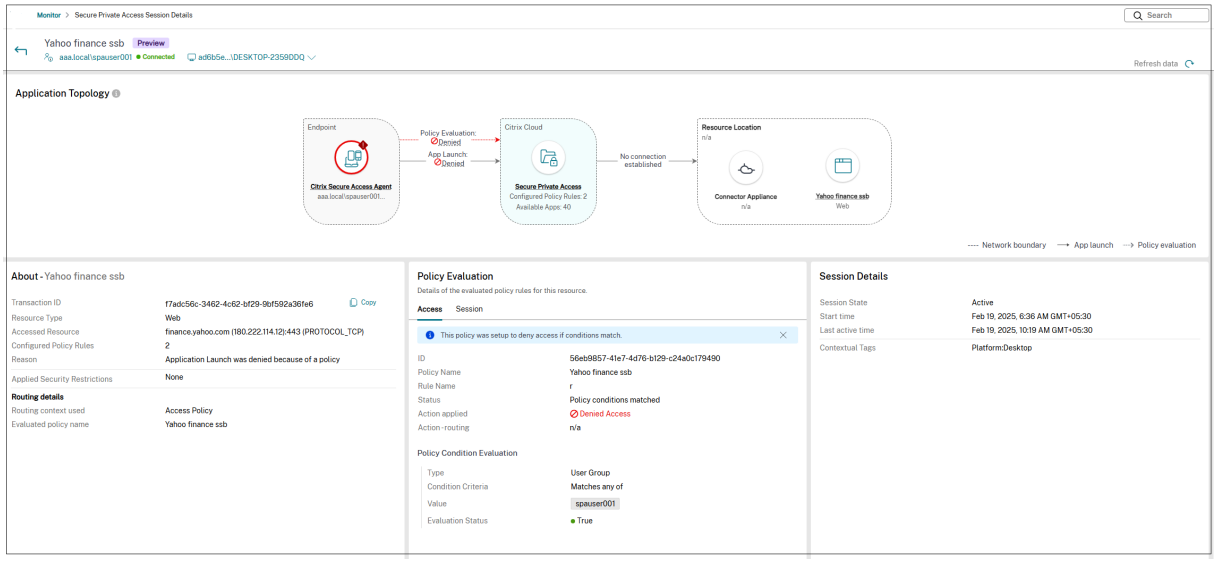
- Web app (launched via Citrix Secure Access client) - FQDN, port, and protocol
- Web app (launched via Citrix Workspace) - URL

- **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.



Triage and troubleshoot

November 25, 2025

This topic outlines the essential considerations and procedures for effectively troubleshooting and triaging issues related to Citrix Secure Private Access. Admins can use this document as a guide for identifying, diagnosing, and resolving problems, ensuring seamless and secure access for users.

User/client issues in Citrix Secure Access mode

User unable to log in

Things to check:

- Check if the VPN virtual server and authentication virtual server is UP.

```
> show vpn vserver _spa_cep_csa_vpn_vs_10.8.0.35
        _spa_cep_csa_vpn_vs_10.8.0.35 (10.8.0.35:443) - SSL      Type: CONTENT
        State: UP


 > show authentication vserver authvs
         authvs (0.0.0.0:0) - SSL         IPSet: ???       Type: CONTENT
         State: UP  ARP:DISABLED
```

- Check if the Secure Private Access profile URL status is UP.


```
> show vpn securePrivateAccessProfile _spa_cep_csa_profile
1)      Name: _spa_cep_csa_profile
                URL: https://stg4spalb.spagwcep.corp  [Status: UP]
```

- Ensure that the apps and access policies are correctly configured for the user in the Secure Private Access admin console. See Apps configuration and management and Configure access policies for the applications.
- Check the load balancer virtual server status to ensure that all connector servers are added and are UP.
- To troubleshoot any nFactor authentication issues, see Troubleshoot authentication, authorization, and auditing issues.

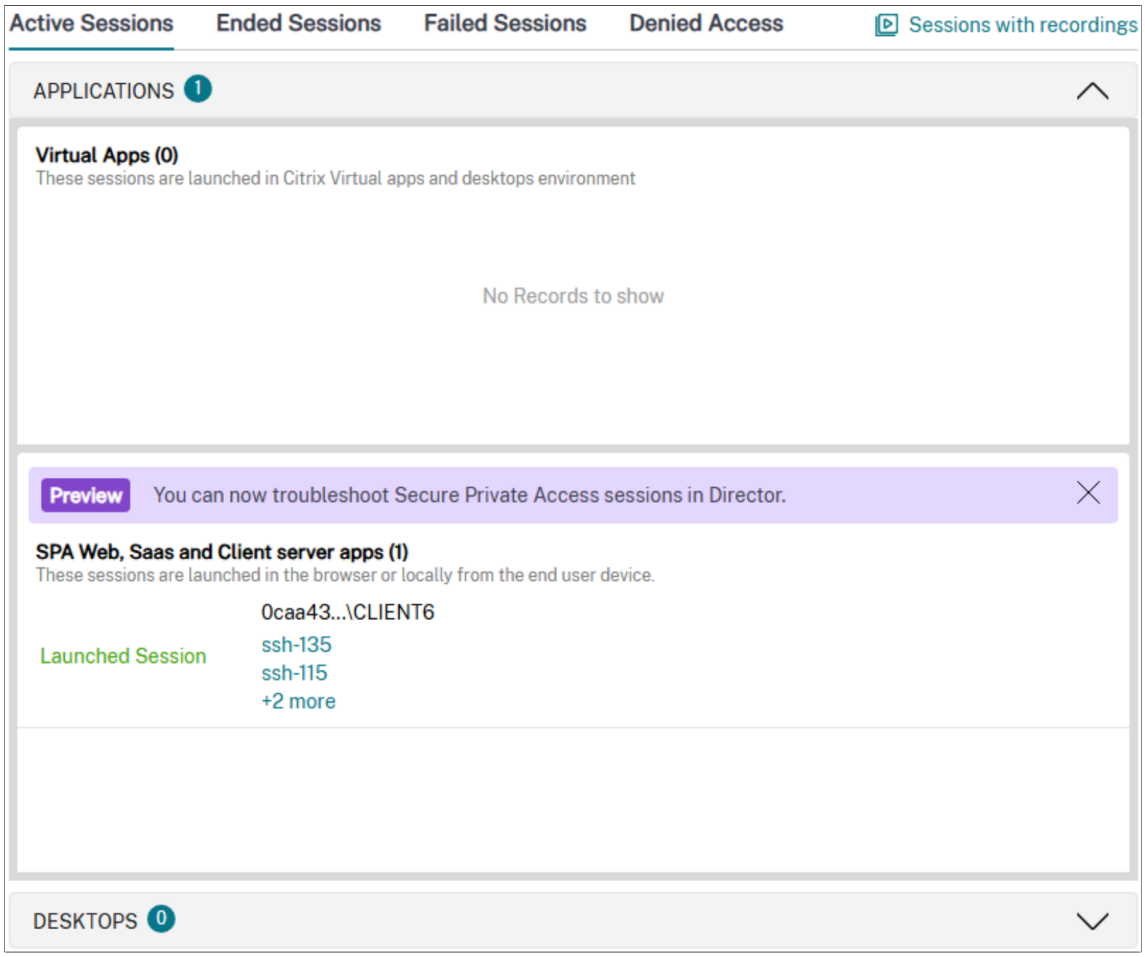
After confirming what was mentioned earlier, do the following:

1. Enable debug level logging and collect a support bundle from NetScaler.
2. Enable verbose logging on the CSA client and collect client logs.
3. Contact Citrix Support and provide the collected diagnostics.

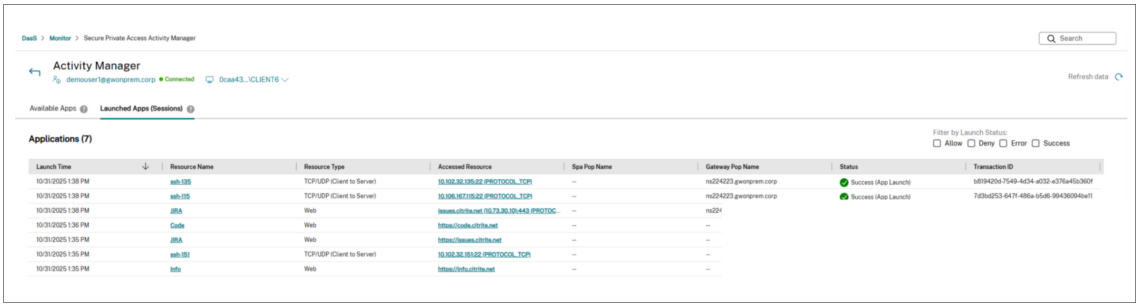
User unable to launch an app

Things to check:

- In Citrix Monitor, search for the user UPN and verify that an active Secure Private Access session exists.

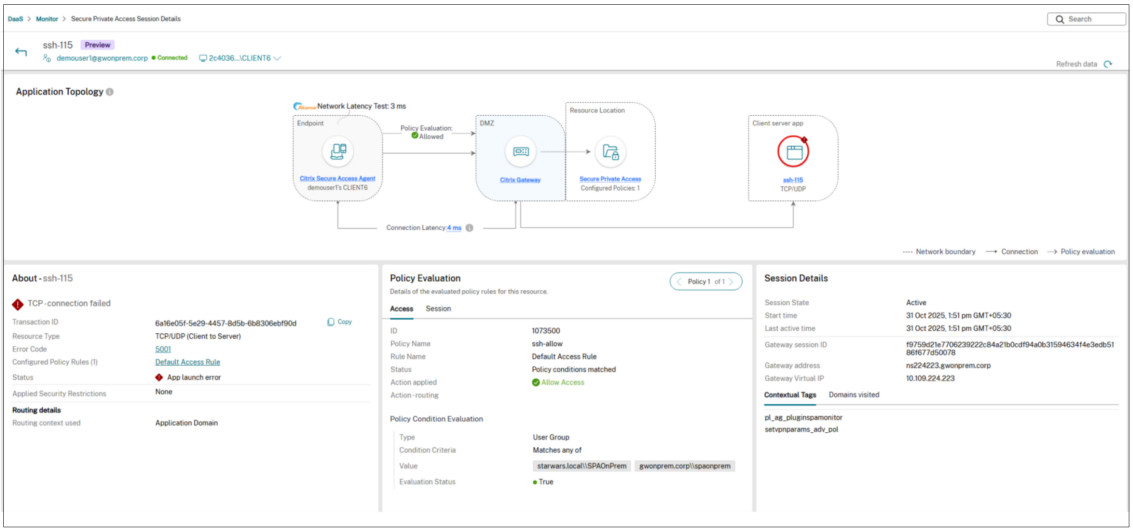


- The launched app must appear under **Available apps**.
- An **App Launch Allow** event for the app must be visible under **Launched apps**.



- If not present, check that the app and access policies are correctly configured for the user in the Secure Private Access admin console.

- In Citrix Monitor, look for any app launch error event for the app under **Launched apps**.



- Common errors: DNS resolution failure/TCP connection failure.
- From the NetScaler CLI, verify connectivity to the app from the appropriate SNIP.

Steps to collect a NetScaler support bundle with debug-level logging

1. Set debug-level syslog from the CLI.

   ```
   set syslogparams loglevel ALL DEBUG
   ```

2. Enable Secure Private Access specific verbose logging from Shell.

   ```
   nsapimgr_wr.sh -ys ns_vpn_enable_spa_verbose_logging=1
   ```

3. Collect the support bundle (and optional traces)
4. Use your standard method to collect the NetScaler support bundle.
5. Optionally capture additional traces if requested by support.

> **Important:**
>
> Revert verbose logging after collecting the bundle. Leaving verbose logging enabled can generate excessive logs and impact performance. Always revert verbose logging once the collection is complete.

Revert verbose logging

1. Restore syslog level from the CLI.

   ```
   set syslogparams loglevel ALL
   ```


2. Disable Secure Private Access specific verbose logging from Shell.

```
nsapimgr_wr.sh -ys ns_vpn_enable_spa_verbose_logging=0
```

Additional References:

- How to generate a technical support bundle for a NetScaler® instance Logs
- How to record a packet trace on NetScaler

Tools that help to troubleshoot

- Configuration reports
- Component Analyzer
- Policy modeling

Collect client logs

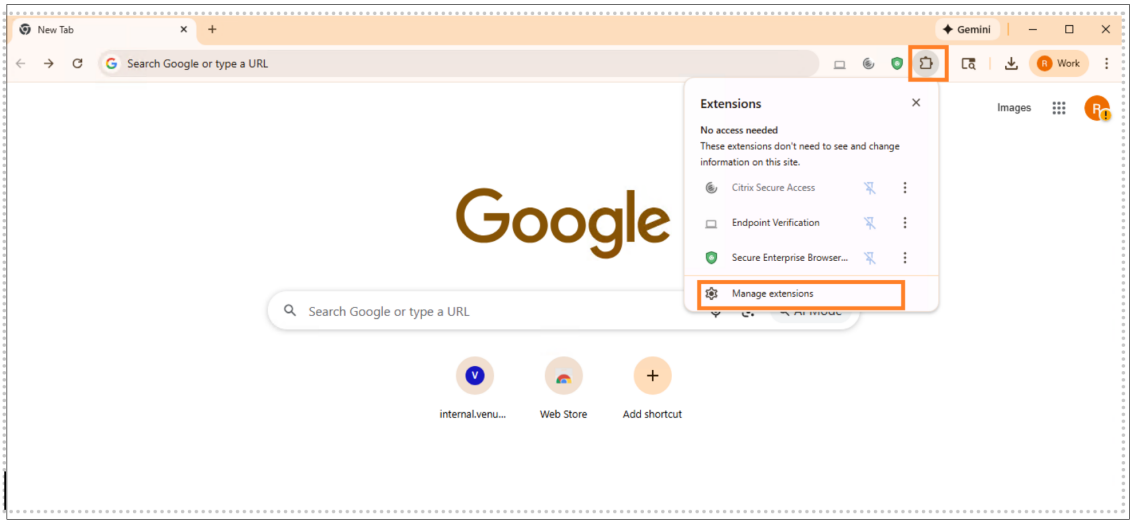
November 25, 2025

Chrome Enterprise Premium logs

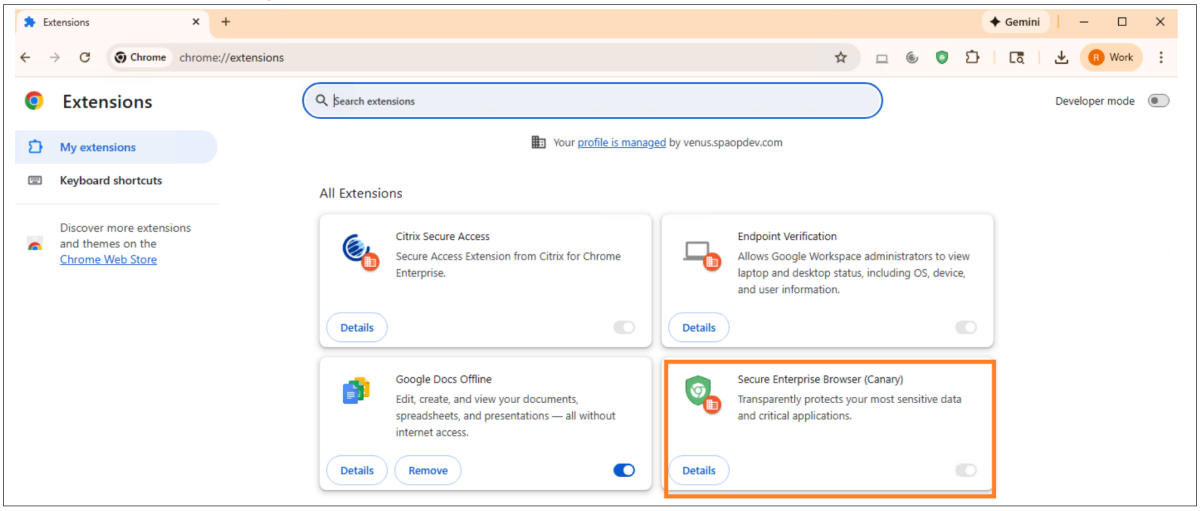
If you experience issues on the client side with Chrome Enterprise Premium, collect the extension logs for both Secure Enterprise Browser and Citrix Secure Access.

Steps to capture logs for the Secure Enterprise Browser extension

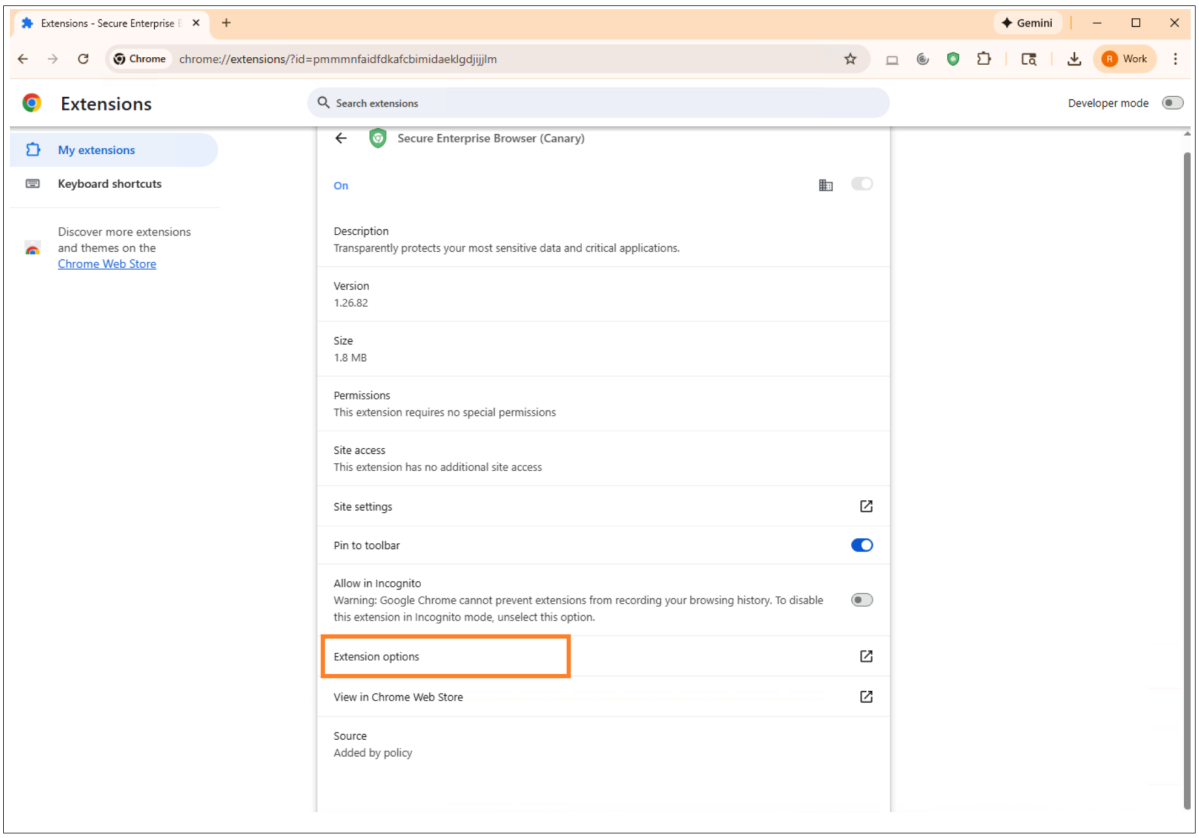
1. Open the Chrome browser.
2. Switch to your managed Chrome profile.
3. Click the **Extensions** icon and select **Manage extensions**.



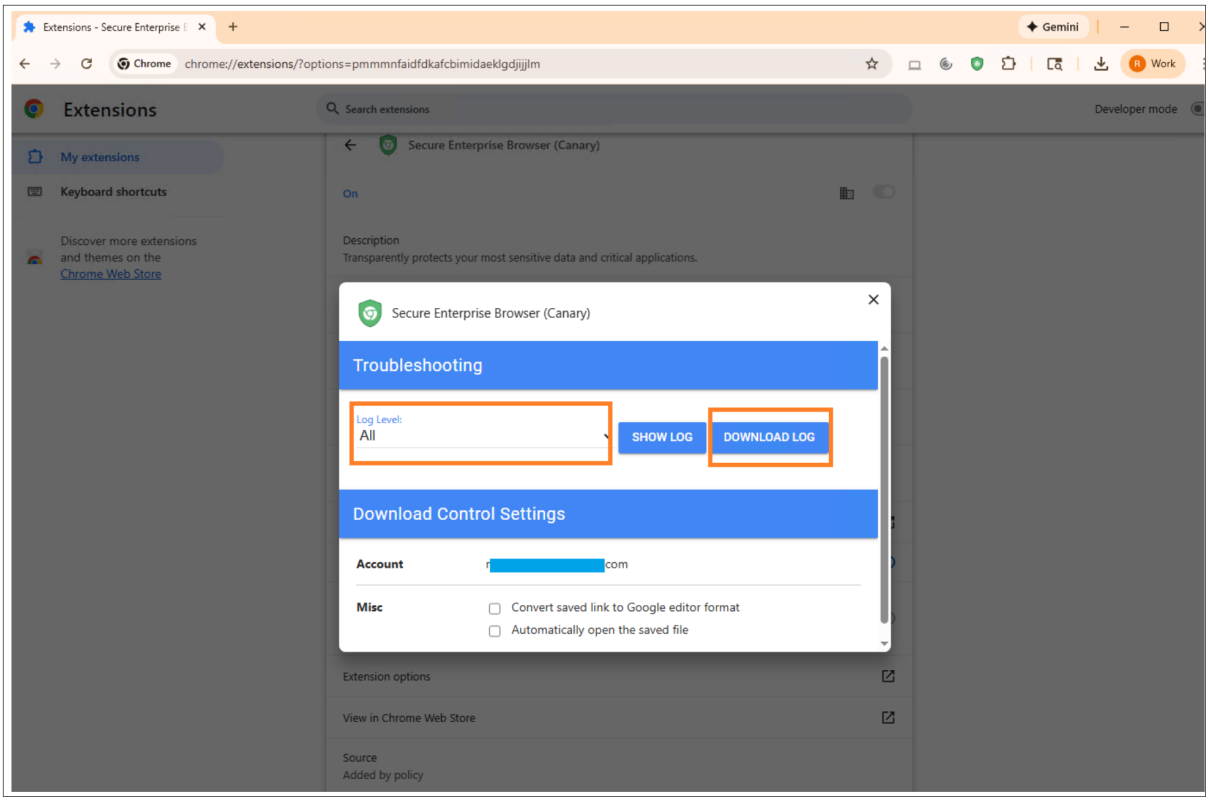
4. Under Secure Enterprise Browser, click **Details**.



1. Select **Extension options**.



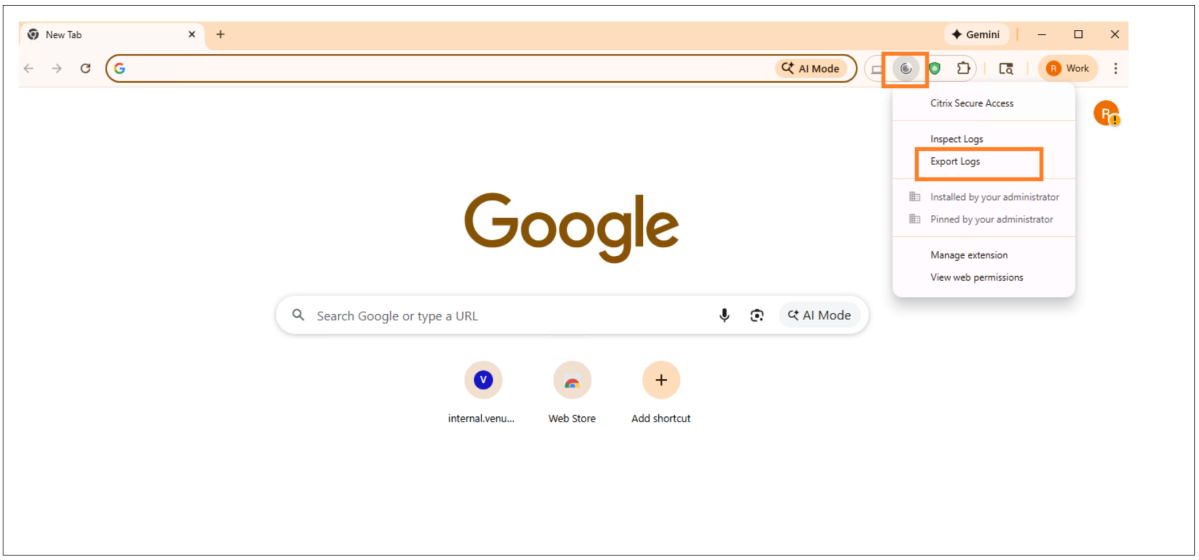
1. Click **DOWNLOAD LOG**.



1. Save the downloaded log files to your computer.

Steps to capture logs for Citrix Secure Access Extension

1. Open the Chrome browser.
2. Switch to your managed Chrome profile.
3. Click the **Citrix Secure Access extension** icon next to the address bar.
4. Select **Export Logs**.



1. Save the exported log files to your computer.

Real-time session troubleshooting using Monitor

February 25, 2026

Administrators can monitor and troubleshoot Secure Private Access sessions in real-time using the Monitor console.

For related information, see the following topics:

- For information on integrating Secure Private Access with Monitor, see Integration with DaaS monitor.
- You can search for Secure Private Access user sessions in Monitor to quickly locate specific sessions for troubleshooting and reporting purposes. For details, see View a Secure Private Access session by user.
- For more information on Monitor, see DaaS Monitor.

The following error codes are captured for Secure Private Access hybrid deployments:

- Session codes
- App enumeration message codes
- App launch message codes
- App launch error codes

Session codes

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

App enumeration message codes

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

Code	Status	Description
1103	failure	No applications were enumerated and at least one app evaluation failed
3000	Allow	Application enumeration is allowed
3001	Deny	Application enumeration is denied by policy
3002	Deny	Application was not enumerated because no policies matched
3003	Unknown	Application enumeration status is unknown
3004	Application launch from CEB	Application launch attempt from Citrix Enterprise Browser™
3101	Failure	Application enumeration - An internal error occurred (currently unused)
3102	Failure	Application was not enumerated because there was an exception during policy evaluation
3103	Failure	Application enumeration status is null - An internal error occurred during policy evaluation
3104	Allow/deny/failure	Error retrieving policy details for the app

App launch message codes

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

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

App launch error codes

Code	Description	Resolution/Workaroud
5001	TCP - connection failed	Verify network reachability to the destination (ping `-S <SNIP>` from NetScaler Gateway).
5003	TCP - probe failed	
5002	TCP - proxy server down	Ensure that the proxy host is UP.
5004	TCP - memory allocation in gateway failed	Enable debug level logging and collect support bundle from NetScaler.
5005	TCP - server down	Verify network reachability to the destination (ping `-S <SNIP>` from NetScaler Gateway) and check if the server is DOWN.
5006	TCP - proxy connection failed	Ensure that the proxy host is UP and accepting connections.

Code	Description	Resolution/Workaroud
5007	TCP - proxy probe failed	Verify network reachability to the destination (ping `-S <SNIP>` from NetScaler Gateway). Enable debug level logging and collect support bundle from NetScaler.
5008	SPA - server down	Verify that the Secure Private Access site URL is UP. (Use the `show vpn securePrivateAccessProfile` CLI command on NetScaler CLI to check the URL status).
5009	SPA - callout request error	Verify that the Secure Private Access site URL is UP. Enable debug level logging and collect support bundle from NetScaler.
5010	SPA - callout response error	
5011	TCP - session expired	This indicates that the app was accessed when the user session was no longer active. Start a new active user session.
5013	TCP - gateway internal error	Enable debug level logging and collect support bundle from NetScaler.
5014	TCP - DNS server down	Ensure that the DNS server is UP.
5015	TCP - gateway DNS internal error	Ensure that the DNS Server is UP. Enable debug level logging and collect support bundle from NetScaler.
0x1300000C	DNS resolution failed for application domain	Ensure that the host name your application uses is resolved by the intended DNS servers (internal vs public).

End user experience

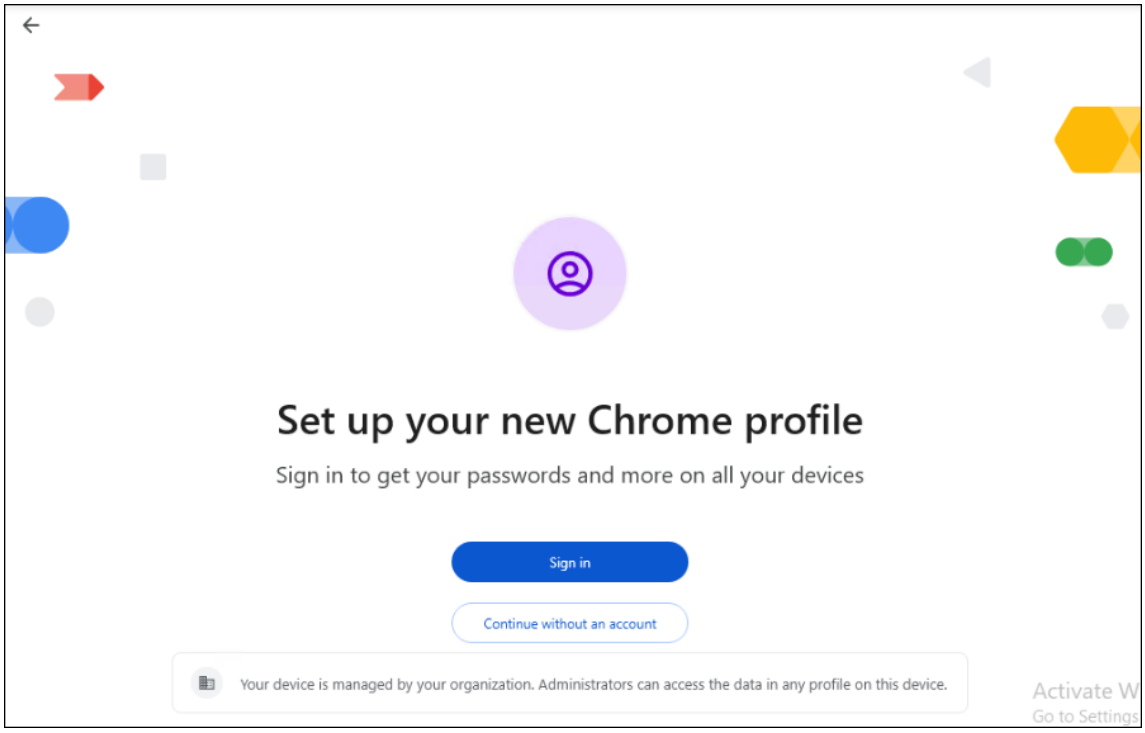
November 25, 2025

Accessing web and SaaS applications with Chrome Enterprise Premium

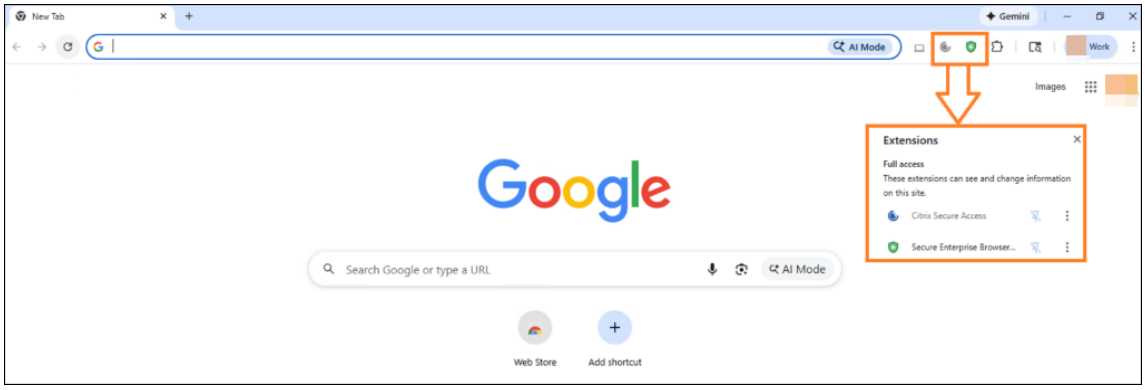
You can access published internal web applications and external SaaS applications using Chrome Enterprise Premium in four different ways. Choose the option that applies to your environment.

Option 1: Create a managed Chrome profile and access apps directly (recommended)

- Open the Chrome browser.
- Add a new Chrome profile using your company's credentials (that is, create a managed Chrome profile).

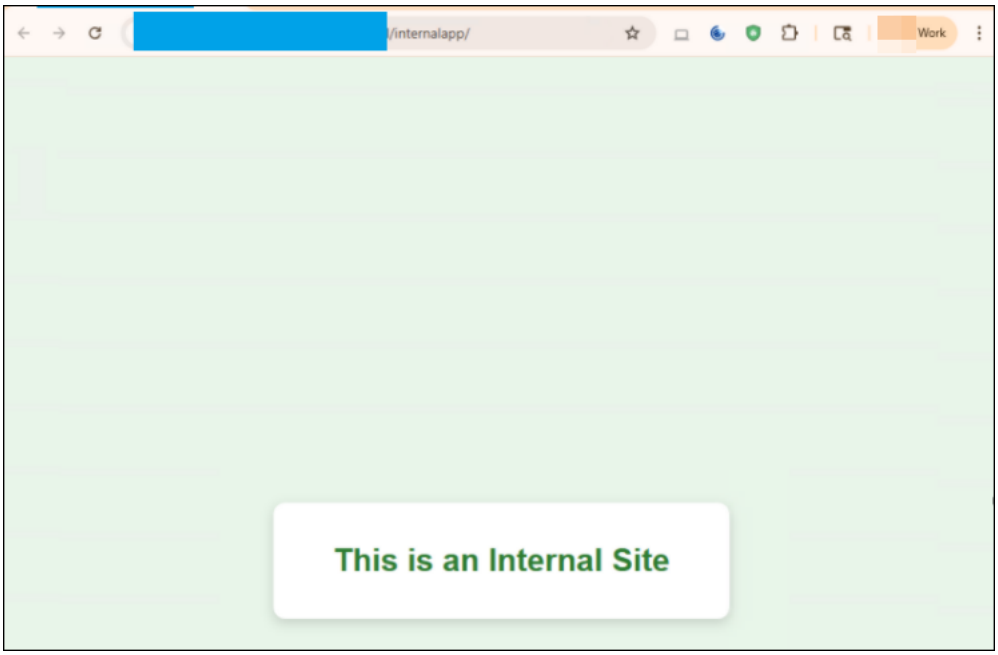


- After the profile is created, two extensions are automatically installed:
  - Citrix Secure Access
  - Secure Enterprise Browser



- Access internal and external applications by entering the URL in the address bar or by navigating to the published sites.
- Behavior when the URL is entered manually:
  - **Internal web app (allowed):**

    The request is securely tunneled through Secure Private Access and the site loads.



  - **Internal web app (denied):**

    Secure Private Access blocks the request, and an **Access Restricted** page appears.

- **External SaaS app (allowed):**

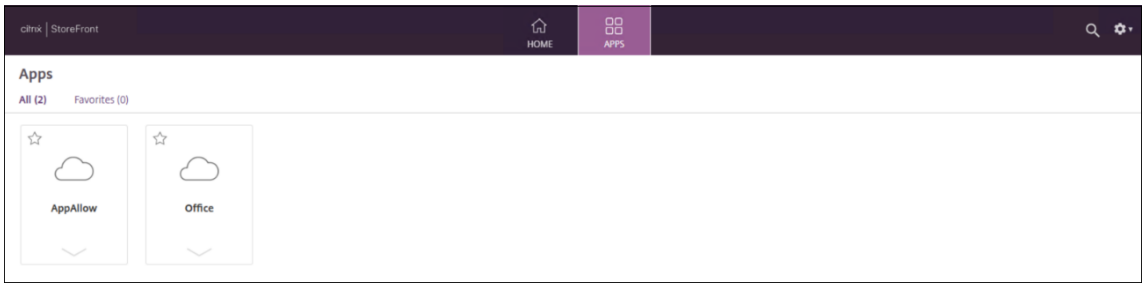
  The request is allowed directly without tunneling.

- **External SaaS app (denied):**

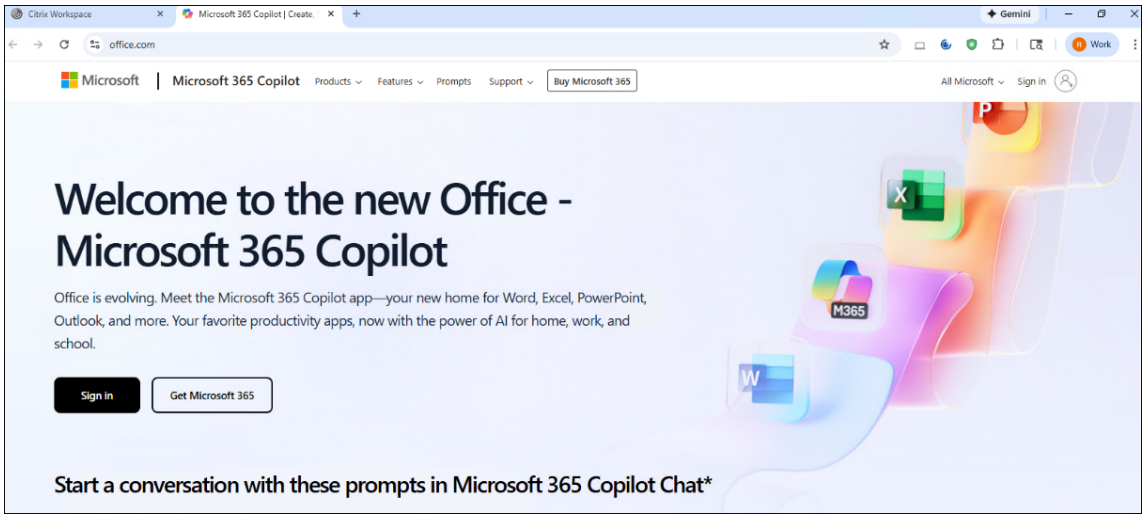
  Secure Private Access blocks the request, and an **Access Restricted** page appears.

Option 2: Managed Chrome profile already exists —access through StoreFront (Citrix Workspace Web UI)

- Ensure the managed Chrome profile with company credentials already exists.
- Launch Chrome with the correct company-managed profile.
- Open the StoreFront™ store from the Citrix Workspace™ Web UI (RFWeb).
- Log in to the store.
- Go to the **Apps** tab and select the web/saas app published by your company's admin.



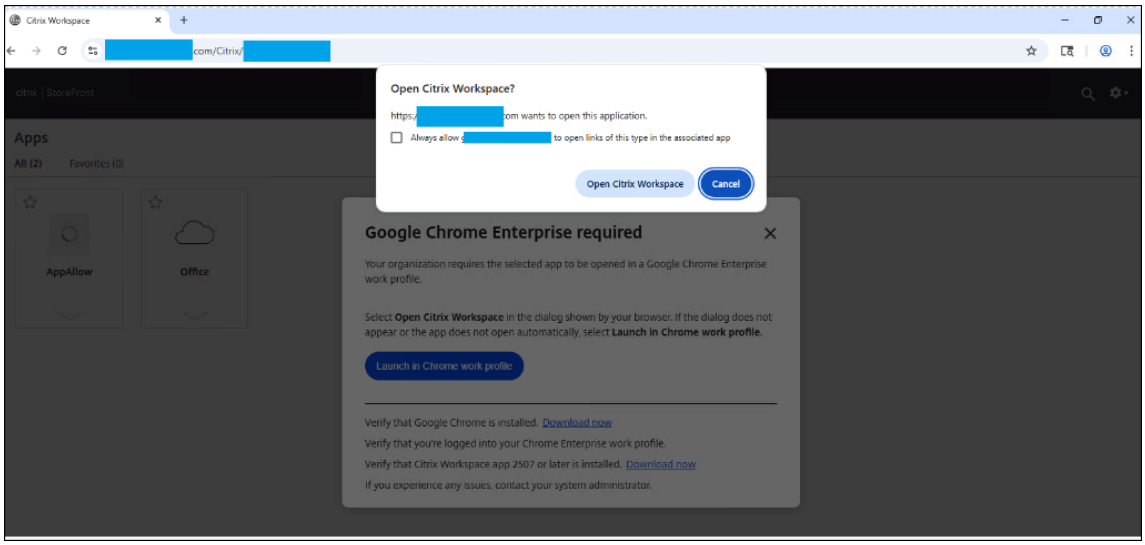
- The web/saas app launches seamlessly in a new tab within the same managed Chrome profile.



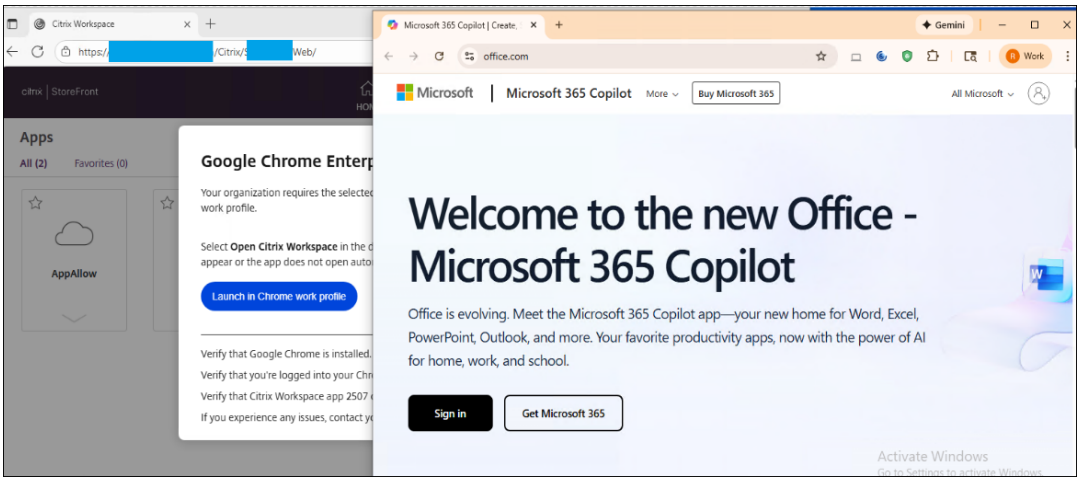
- Allow and deny logic remains the same as Option 1.

Option 3: Access StoreFront (Citrix Workspace Web UI) from a non-managed Chrome profile or a non-Chrome browser (Edge, Firefox)

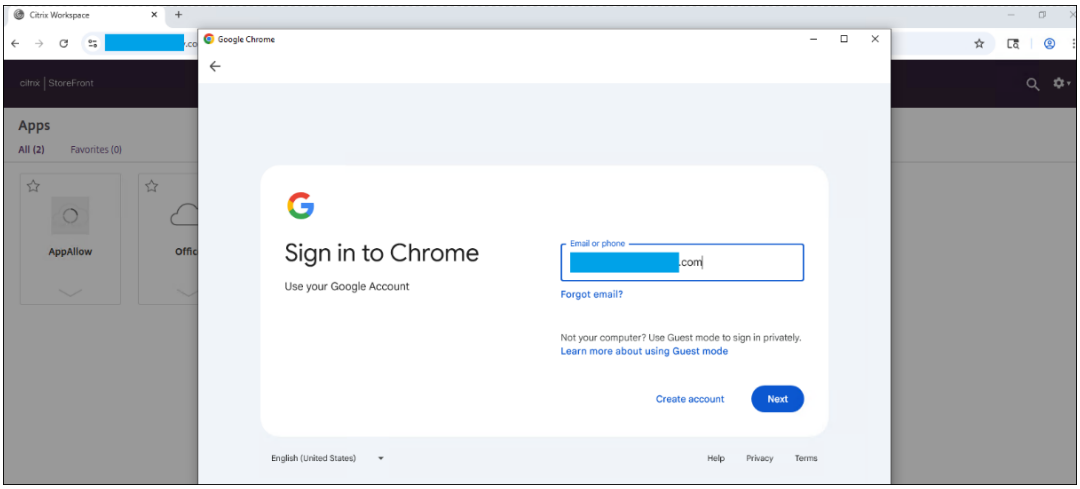
- Launch Edge, Firefox, or a non-managed Chrome profile.
- Open the StoreFront store from the Citrix Workspace™ Web UI (RFWeb).
- Log in to the store.
- Go to the **Apps** tab and select the published web app.
- A popup appears with a dialog showing the button **Open Citrix Workspace**. Click this button to proceed.



- After clicking the button, one of the following happens:
  - **Managed Chrome profile already exists:** The app launches directly in the managed profile.



  - **Managed Chrome profile does not exist:** You are prompted to create a managed Chrome profile before the app launches.

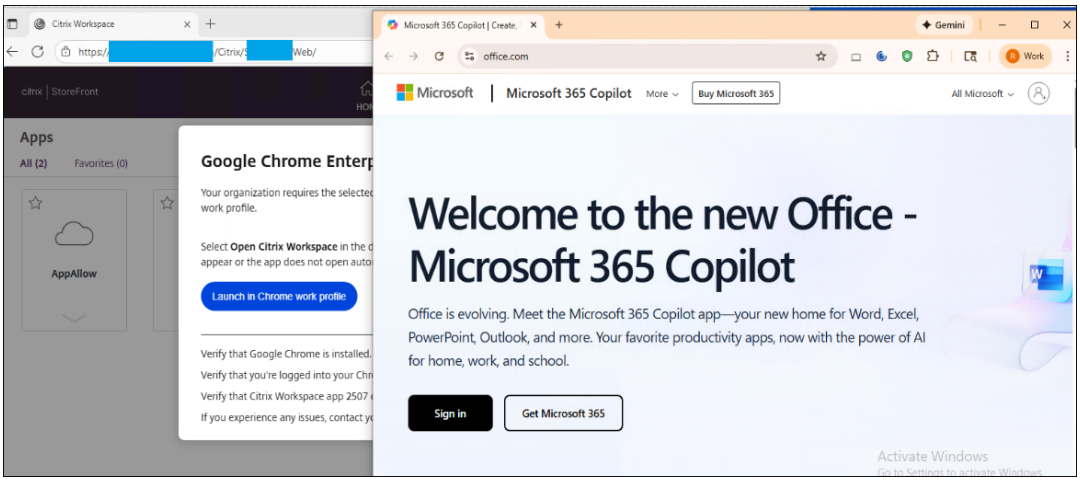


- Allow and deny logic remains the same as Option 1.

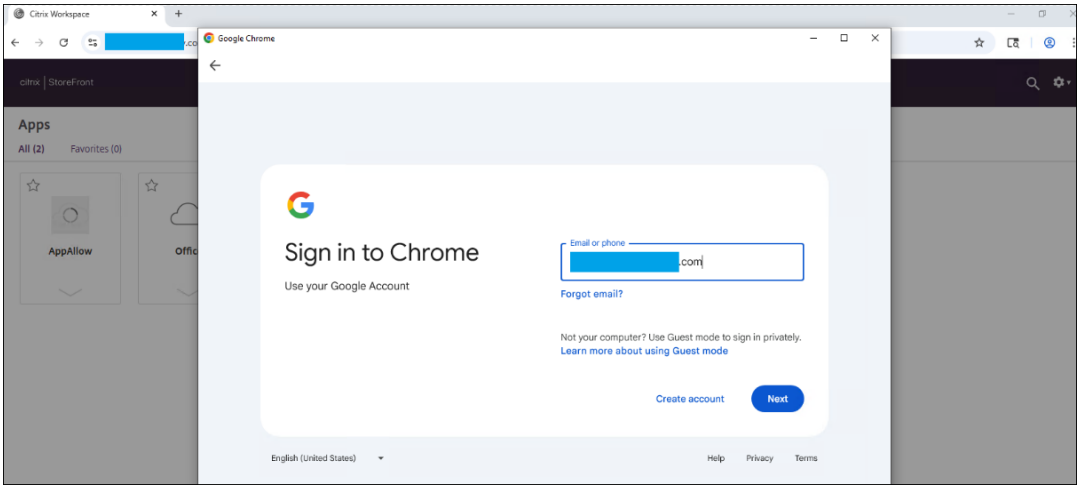
Option 4: Access apps through the Citrix Workspace app

- Open the StoreFront store using the Citrix Workspace app.
- Log in to the store.
- Go to the **Apps** tab and select the published web app.
- The Workspace app launches Chrome automatically. Based on your setup:

- **Managed Chrome profile exists:** The app opens directly in the managed profile.



- **Managed Chrome profile does not exist:** You are prompted to create one before the app opens.

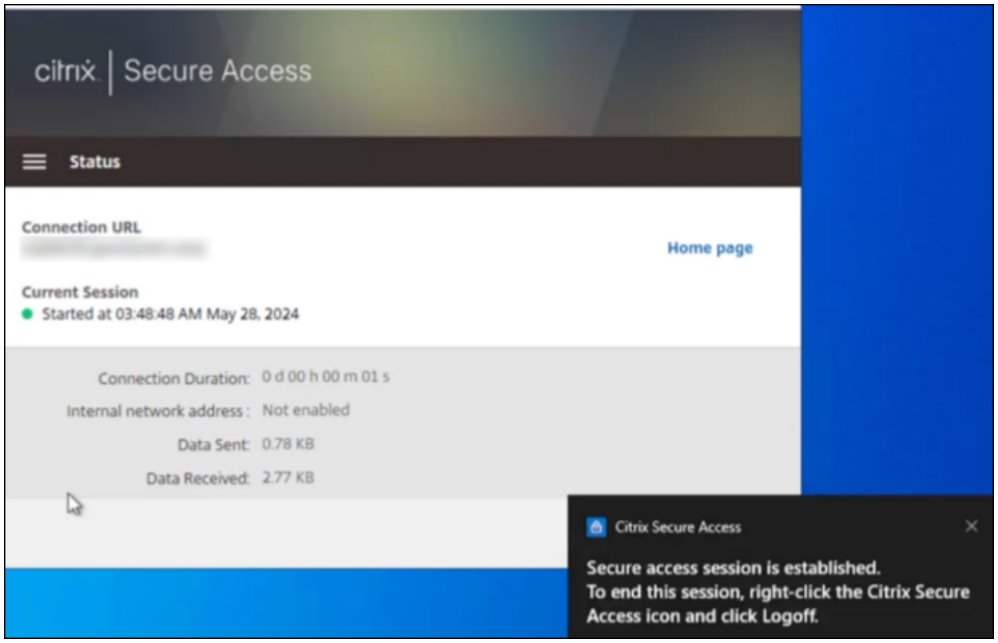


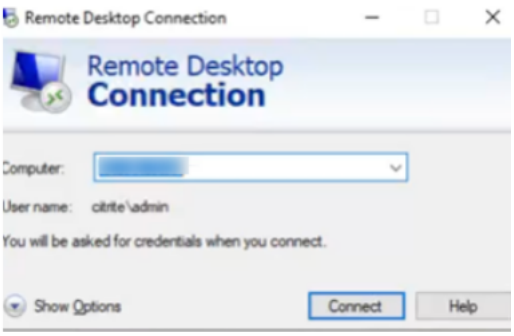
- Allow and deny logic remains the same as Option 1.

Accessing client/server (TCP/UDP) applications

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 are 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.