What's new

30 September 2026

- **Extended Secure Private Access data regionalization for new customers**

  Secure Private Access now routes management and data traffic to the correct regional data POPs and endpoints for new customers. For more information, see Data regionalization.

- **Access mode-based policy enforcement**

  Access mode-based policy enforcement lets administrators restrict how a user connects to an application. The connection can be through a browser-based client or the Citrix Secure Access client. For more information, see Access mode-based policy enforcement.

03 September 2026

- **User and group details in access policies displayed by domain, forest, and IdP type:**

  When you search for users or groups by display name, email ID, or user principal name, the users and groups that you select appear in a grid. Each row displays the identity details, such as name, email address, IdP type, OID, and domain. You can clearly distinguish between identically named users or groups across different domains, forests, or identity providers (IdPs). For details, see Create an access policy with multiple rules.

- **Discover related domains using a HAR File:**

  Secure Private Access now enables you to upload a HAR file to automatically discover the domains accessed by an application. You can review the discovered domains and select the ones you want to add to the application's related-domain configuration. This simplifies application onboarding by reducing the need to manually identify and configure related domains. For more information, see Discover related domains using a HAR file.

- **Apply Chrome Enterprise Premium (CEP) configurations to Google Directory organizational units:**

  In addition to all users and Google Directory user groups, you can now apply a CEP configuration to selected Google Directory organizational units. For more information, see Configure CEP for Google Directory organizational units.

- **Conditional Authentication support:**

  Single sign-on (SSO) for Chrome Enterprise Premium (CEP) that uses Citrix Cloud as the OpenID Connect (OIDC) authentication provider now supports conditional authentication. For more information, see Open ID Connect with Citrix Identity and access management.

- **Set up user attribute type:**

  You can now set up user attributes from the Managed profile identity page in the Secure Private Access admin console. For more information, see Managed profile identity.

- **Verify user and group synchronization:**

  When selecting users or groups, administrators can verify whether entries from the selected user directory are synchronized with and correctly configured in Google Directory. Secure Private Access policies evaluate correctly only when the users and groups are synchronized. For more information, see Verify user and group synchronization.

- **Automatic cleanup of routing entries on application deletion:**

  When you delete an application, Secure Private Access now cleans up the routing entries as well. For more information, see Automatic cleanup of routing entries on application deletion.

19 August 2026

- **Google Cloud Identity support for Chrome Enterprise Premium (CEP)**

  Google Cloud Identity can now be used as an identity provider with CEP. When Google Cloud Identity is your identity provider, users and groups reside natively in the Google Cloud directory, so no directory correlation is required. For details, see Prerequisites for the integrated solution.

05 August 2026

- **New routing method to access SaaS applications:**

  You can now set a SaaS app's routing type to either **External via Google Secure Gateway** to route traffic through Google Secure Gateway or **External** to route traffic directly from the client to the app. For details, see Configure a SaaS app.

31 July 2026

- **Citrix Secure Access controls for Chrome Enterprise:**

Citrix Secure Private Access supports security policies that are delivered to and enforced by the Citrix Secure Access extension for Google Chrome Enterprise Premium (CEP).

The following policies are supported by Secure Private Access.

- Anti-keylogging
- Clipboard container
- Domain suffix for web applications
- Session recording
- Browser session reauthentication

24 June 2026

- **Support for configuring egress hub regions:**

  Secure Private Access enables administrators to choose the egress regions that Chrome Enterprise Premium uses for SaaS application traffic. Each selected region provides a dedicated set of egress IP addresses, which administrators can add to their SaaS application allow lists to permit traffic routed through Google Secure Gateway. This feature is available for both cloud and hybrid deployments. For details, see Configure egress hub regions.

- **Removal of dependency on citrix-schema sync for Google Directory:**

  The dependency on Citrix schema sync for Google Directory in Chrome Enterprise Premium has been removed. Google Directory sync can now be performed using user email IDs. To enable this feature, contact Citrix Support.

- **SAML 2.0 authentication support for OIDC:**

  SAML 2.0 identity providers (IdPs) are now supported for OIDC. For more information about OIDC integration with Citrix Identity, see OpenID Connect with Citrix Identity.

18 June 2026

- **Define primary and secondary resource locations during CSV-based application import:**

The applications import using the CSV file now allows administrators to define both primary and secondary resource locations during bulk application creation. This enables efficient onboarding for enterprise deployments operating across different locations. For details, see Applications import tool.

09 June 2026

The following sections provide more information about the 09 June 2026 release.

Important notice

- **Citrix Secure Private Access™ Edge configuration update:**

  As part of the ongoing performance and infrastructure optimizations for Citrix Secure Private Access, certain Citrix Secure Private Access edge configuration updates will soon be deployed.

  > **Note:**
  >
  > This notification is intended **only** for customers who might have set up specific PoP-level FQDN allow lists at firewall or proxy level or custom entries outside of the documented recommendations.

  > **What is changing:**

  Citrix Secure Private Access edge FQDNs are being updated to a new format as shown below:

  Old FQDN: `<pop>-rdvz.g.nssvc.net`

  New FQDN: `<pop>-spa-rdvz.g.nssvc.net`

  Examples:

  `az-us-e-rdvz.g.nssvc.net` changes to `az-us-e-spa-rdvz.g.nssvc.net`

  `az-eu-w-rdvz.g.nssvc.net` changes to `az-eu-w-spa-rdvz.g.nssvc.net`

  Do I need to take action:

  - **No action required:** If you use the recommended wildcard domain (for example `*.nssvc.net`), both the old and new names are already covered and no action is needed. For details, see Connector Appliance for Secure Private Access.
  - **Action required:** If you use explicit, PoP-level FQDN allow lists, or custom entries outside of the documented recommendations, perform the required action.

  Required action:

Customers allowing outbound traffic to specific PoPs must update their firewall rules. For every currently permitted `<pop>-rdvz.g.nssvc.<suffix>` entry, add the corresponding `<pop>-spa-rdvz.g.nssvc.<suffix>` record to ensure uninterrupted service. For a list of PoPs, see Points of Presence (PoPs) locations for Citrix Secure Private Access service.

20 May 2026

- **Data regionalization**

  Data regionalization in Citrix Secure Private Access enables customers to control where their data is stored by selecting a preferred geographic region. Customers can choose the region where their data is stored, with options including Global, Europe (EU), APAC (Asia Pacific), and North America (NA). All configuration data at rest remains within the selected region, ensuring that it does not leave the designated geography. For details, see Data regionalization.

28 April 2026

- **Simplified Secure Private Access service configuration**

  The Secure Private Access service configuration has been streamlined into a single unified flow. The System Configuration page now includes a topology diagram that shows the components used in a Secure Private Access cloud deployment. Administrators can configure Connector Appliance and Google Chrome Enterprise Premium directly from this page. For details, see Secure Private Access onboarding and set up.

- **Mandatory Google admin permissions for telemetry purposes**

  A new set of privileges must be assigned to the service account in the Google Admin Console. These privileges are used primarily for telemetry purposes (for example, DLP activity events and security alerts). For details, see Setup Google Chrome integration.

- **Okta IdP support for CEP**

  Okta can now be used as an identity provider with Chrome Enterprise Premium (CEP). For details, see Create a Citrix OIDC client. For details, see Create a Citrix OIDC client.

07 April 2026

- **Listing the five most-used templates to simplify and accelerate app onboarding**

The **Choose a template** section in the application configuration page now lists the five most-used templates to simplify and accelerate app onboarding. For details, see Configure a SaaS app.

04 March 2026

- **Secure Private Access admin UI domain transition to secureaccess.cloud.com**

  The Secure Private Access admin UI domain has now been updated to `secureaccess.cloud.com`. Your current URL continues to function and is automatically redirected to the new domain. No action or configuration changes are required.

12 February 2026

- **Port-based routing using routing exceptions**

  The port-based routing feature allows admins to route traffic for different ports of the same destination differently for TCP/UDP apps using routing exceptions. For details, see Port-based routing using routing exceptions.

05 February 2026

- **Citrix Enterprise Browser to Chrome Enterprise Premium migration**

  The Citrix Enterprise Browser to Chrome Enterprise Premium phased migration approach allows organizations to maintain business continuity during the transition period by running both browser solutions in parallel. With the phased migration, customers can validate compatibility of existing applications and workflows with Chrome Enterprise Premium. For details, see Citrix Enterprise Browser to Chrome Enterprise Premium migration.

- **Domain mapping for user groups without email addresses**

  Google directory requires a verified email address for all user and group objects. However, this isn't always available for directories supported by Secure Private Access, specifically Active Directory (AD), and Microsoft Entra ID. AD and Microsoft Entra ID objects might lack an email address or have one pointing to an internal or special domain (for example, @fabrikam.onmicrosoft.com) that Google directory cannot verify.

  Because the email address normally serves as the common identifier between Secure Private Access and Google directory, groups from AD/Entra without a verified Google email address are typically unsupported for Secure Private Access policies. The Domain Mapping feature

resolves this by allowing administrators to configure policies against groups even if they lack an email address or have an email address with an unverified domain. For details, see Domain mapping for user groups without email addresses.

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

16 December 2025

- **Route DNS queries to application-specific resource locations**

  Administrators can route DNS queries for specific applications directly to their dedicated resource locations. This enables more accurate DNS resolution, intelligent traffic management, and a better user experience. For details, see Route DNS queries to application-specific resource locations.

11 December 2025

- **Citrix Enterprise Browser to Chrome Enterprise Premium migration**

  Existing Secure Private Access service customers can gradually transition from Citrix Enterprise Browser to Chrome Enterprise Premium (CEP). This phased migration approach allows organizations to maintain business continuity during the transition period by running both browser solutions in parallel. With the phased migration, customers can validate compatibility of existing applications and workflows with Chrome Enterprise Premium. For more information, see Citrix Enterprise Browser to Chrome Enterprise Premium migration.

30 October 2025

- **General availability of the agentless access release of Citrix Secure Private Access with Chrome Enterprise solution**

With the integration of Citrix Secure Private Access™ with Google Chrome Enterprise Premium, end users can now securely access private web and SaaS applications using the Google Chrome browser as their enterprise browser without needing a Zero Trust Network Access (ZTNA) agent, and achieve per-application access with data loss prevention (DLP) controls, web filtering, and ZTNA policy enforcement. For details, see Integration of Citrix Secure Private Access with Google Chrome Enterprise Premium.

Recommendations for current Secure Private Access / Citrix Enterprise Browser customers with a production tenant

We recommend that current production customers test the agentless access release in a separate tenant rather than their production tenant. A product update planned for late November 2025 will include enhancements to allow existing Secure Private Access customers to onboard the agentless access functionality while retaining their existing app configurations and access policies. The November 2025 release will also provide a user interface that allows existing Secure Private Access customers to migrate their app launches for current web and SaaS apps (currently launched via Citrix Enterprise Browser) to launch in the Chrome browser.

Customers who prefer to use this release prior to the November 2025 update must reset their existing Secure Private Access tenants to a clean state and then onboard the customers again to Secure Private Access service. Perform the following steps:

a. Delete all access policies, apps, and related domains in the Secure Private Access console.
b. Return to the Secure Private Access tile on the Citrix Cloud console.
c. Select **Fully Cloud-delivered Service architecture** and then click **Continue**. For details, see Secure Private Access onboarding and set up.

17 September 2025

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

  Secure Private Access is 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. For details, see Citrix Secure Private Access for mobile device.

13 August 2025

- **Custom store URLs for accessing apps via Citrix Enterprise Browser™**

The custom store URL feature allows organizations to provide users with access to SaaS and private web applications through a branded, organization-owned domain (for example, workspace.company.com) instead of the default *.cloud.com domain.

- **Enhancements to the policy modeling tool**

  The policy modeling tool now displays the routing type and specific policy type influencing an application's routing decisions. This enhancement helps administrators in troubleshooting routing issues and verifying that applications adhere to configured policies. For details, see Policy modeling tool.

14 July 2025

- **Monitor and troubleshoot Secure Private Access agentless apps in Monitor**

  Administrators and help-desk personnel can now monitor and troubleshoot Secure Private Access agentless apps sessions and events in Monitor. For details, see Secure Private Access integration with Monitor.

- **Server-to-client connections support for the UDP applications**

  Server-to-client connections are now supported for the UDP applications in addition to TCP applications. The servers in the customer’s resource location can establish a UDP connection with the remote client. For details, see Support for server-to-client connections.

- **New role-based access control roles for helpdesk personas**

  The following roles are available for Secure Private Access admins in addition to the Full Access Administrator and Read Only Administrator roles.

  - Full Monitor Administrator
  - Helpdesk Administrator

  For details, see Role-based access control.

- **Route UDP DNS queries to the application-specific resource location**

  The UDP DNS queries for specific host names can now be routed directly to the resource location where the corresponding application is hosted. This routing improves application performance by ensuring that DNS queries reach the most relevant resource location. Previously, all UDP DNS queries were, by default, routed to the geographically closest resource location, regardless of the application's actual location.

  How it works:

a. The routing of UDP DNS queries to the application-specific resource location is disabled by default. To enable this functionality, contact Citrix Support.

b. Once the feature is enabled, the DNS query is routed to Secure Private Access to identify the specific resource location associated with the application. Based on the response from Secure Private Access, the DNS query is then routed to the application's dedicated resource location.

c. In case an application-specific resource location is not identified, the query falls back to the nearest available resource location.

03 June 2025

- **Manage certificates within Secure Private Access console**

  The Secure Private Access certificate store now provides a centralized location for admins to efficiently manage both Certificate Authority (CA) and Secure Sockets Layer (SSL) certificates. This dedicated store simplifies certificate management by enabling administrators to seamlessly add new certificates, modify existing ones, and remove those that are no longer required. For details, see Manage certificates in the Secure Private Access console.

15 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.

24 April 2025

- **Hybrid data path support**

  The hybrid data path for Secure Private Access service leverages both on-premises and cloud infrastructures to provide secure access to applications. Organizations can use the hybrid data path to route all data traffic through an on-premises NetScaler Gateway. For details, see Hybrid data path for Secure Private Access service.

- **Display of contextual routing insights in Monitor**

Contextual routing can lead to dynamic changes in application routes. For instance, an application might be routed through the Secure Private Access service when the user is outside the corporate network, but directly to the app when the user is internal. Providing administrators with visibility into these routing decisions is crucial for troubleshooting routing issues. For details, see Contextual routing insights in Monitor.

- **Configure backup resource locations**

  Admins can ensure high availability of applications even during disruptions by configuring a secondary resource location or by using the First Available option. For details, see the following topics:

  - Support for Enterprise web apps
  - Agentless access to Enterprise web apps
  - Support for Software as a Service apps
  - Support for client-server apps

- **Delete IP address pools immediately or gradually over time**

  Support is added to delete IP address pools immediately deleted or over time by using one of the following options.

  - **Delete IP Pool by Force:** Stops allocating IP addresses to new users and releases unused IP addresses immediately. Active user sessions using the deleted IP addresses might be terminated, resulting in abrupt closures and forced logouts. Users with terminated sessions are allocated new IP addresses only after a different IP address pool is created.
  - **Delete IP Pool over time:** Stops allocating IP addresses to new users and releasing unused IP addresses immediately. The system waits for the active sessions to log out or expire before fully deleting the pool. Users with terminated sessions are allocated new IP addresses only after a different IP address pool is created.

  For details, see Delete an IP address pool.

22 April 2025

- **Import applications using the nsconfig file**

  The Secure Private Access admin console includes a file import tool that allows administrators to bulk import multiple applications into the system using the nsconfig file in addition to the CSV

file. This tool is especially useful for organizations shifting from a traditional VPN to a more advanced solution like Secure Private Access. For details, see Applications import tool.

Importing applications using the nsconfig file feature is under preview.

20 February 2025

- **Enhancements to the admin audit logging feature**

  The admin audit logging feature is enhanced to capture detailed logs of all admin actions within the Secure Private Access service. For details, see Audit logs.

- **Search and add users based on UPN and email address**

  You can now search and add users in Secure Private Access based on the UPN and email address in addition to the display 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 Configure an access policy.

08 January 2025

- **Dynamically route entire sessions using session policies**

  Admins can configure session policies to route internal corporate users directly to back-end apps without tunneling traffic through Secure Private Access. Session policies offer dynamic routing based on factors, such as network location and device posture. For details, see Route internal corporate users directly to back-end applications.

07 January 2025

- **Connector stickiness support**

  Secure Private Access supports connector stickiness. Connector stickiness ensures that after a client establishes a connection with the Connector Appliance, all subsequent requests from the same client are directed to the same source (Connector Appliance). For details, see Connector stickiness.

- **Client IP address stickiness support**

  Secure Private Access supports client IP address stickiness. Client IP address stickiness ensures that requests from a particular client IP address are consistently routed to the same back-end server. For details, see Client IP address stickiness.

Client IP address stickiness feature is under preview.

- **Support for creating client internal IP address pools**

  Support is added for creating client internal IP address pools. These IP address pools are essential for assigning a unique IP address to a user and the associated device to support the following use cases:

  - Server-to-client connections
  - Client IP address stickiness support

  For details, see Client internal IP address pools.

  > **Note:**
  >
  > Client internal IP address pools feature is in preview. To get this feature enabled, contact Citrix Support.

- **Support for server-to-client connections**

  Secure Private Access supports server-to-client connections wherein the servers in the customer's resource location can establish a TCP connection with the remote client. To enable server-to-client connection, Secure Private Access introduces the server-to-client app. This app can be configured with the client details (port, protocol) and the back-end server's IP CIDR range. For details, see Support for server-to-client connections.

  Server-to-client app support is under preview.

02 January 2025

- **CSV-based applications import tool**

  The Secure Private Access admin console includes a CSV-based import tool that allows administrators to bulk import multiple applications into the system using a CSV file. This tool is especially useful for organizations shifting from a traditional VPN to a more advanced solution like Secure Private Access. For details, see CSV-based applications import tool.

03 December 2024

- **Secure Private Access support for cloud-hosted multi-session VDI**

The Citrix Secure Access client for Windows now supports the use of Secure Private Access to achieve zero trust access to corporate resources from cloud-hosted multi-session VDIs. For more information, see Support for Multi-session Virtual Desktop Infrastructure.

25 November 2024

- **Secure Private Access sessions codes in DaaS Monitor**

  Secure Private Access sessions related codes are now displayed in DaaS Monitor. For the list of codes, see Secure Private Access sessions related codes in Monitor.

14 November 2024

- **Enhancements to the policy modeling tool**

  Admins can now view a comprehensive list of policies associated with each application and utilize the drilldown feature to understand the specific policy application logic, why a specific policy was applied and why others were not. For details, Drilldown into access policies.

08 November 2024

- **Secure Private Access integration with 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 Integration with DaaS monitor.

07 November 2024

- **Enhancements to the Secure Private Access graphical user interface**

  The Secure Private Access service now offers an improved graphical user interface (GUI) for a better user experience. The primary menu tree structure is replaced with a hover-to-display feature for easier navigation. Secondary menu items appear when hovered over, displaying a submenu for quicker selection.

  Also, you can collapse or expand the entire menu by clicking the icon.

23 September 2024

- **Support for context-based app routing and resource locations selection**

  The dynamic domain routing configuration in the access policy now allows admins to edit the internal routing type per URL based on the user context. Administrators can modify the resource locations so that the user requests are routed to the optimal data center, ensuring that user requests are handled efficiently and performance is optimized. For details, see Context-based app routing and resource locations selection.

15 August 2024

- **Option to configure a time duration for purging the entries in the blocked users list**

  Admins can now set a specific duration (1 to 99 days) for purging the entries in the blocked user list. For details, see Terminate active user sessions and add users to the user block list.

- **Additional security controls**

  The following additional security controls are now available for restricting application access.

  - Microphone
  - Webcam
  - Notifications
  - Pop-ups
  - Insecure content

- **Enhancements to the unsanctioned websites (web filtering) feature**

  The unsanctioned websites (web filtering) feature enables admins to block access to all unsanctioned traffic by default or allow it by default via Citrix Enterprise Browser.

16 July 2024

- **Additional security controls**

  The following additional security controls are available for restricting application access.

  - Download restriction by file type
  - Upload restriction by file type
  - Personal data masking

- Printer management
- Clipboard restriction for security groups

- **Display of embedded domains in the App discovery page**

  The App discovery feature enables admins to create new applications or add those domains to an existing application if a main domain or an embedded domain (HTTP/HTTPS) or the destination IP address (TCP/UDP) is not associated with an application. The **App discovery** page displays both the main domain and its underlying embedded domains in a tree structure. For details, see Discover domains or IP addresses accessed by end users.

11 June 2024

- **Policy modeling tool**

  The policy modeling tool (**Access policies > Policy modeling**) helps admins analyze and troubleshoot configuration issues from within the admin console. For details, see Policy modeling tool.

- **Support for filters in the Diagnostic logs chart**

  The filter option in the **Diagnostic logs** chart helps admins refine the search based on the various criteria such as app type, category, and description for easier logs analysis and troubleshooting. For details, see Diagnostic logs.

13 March 2024

- **Support to terminate active user sessions and add users to the disabled user list**

  Admins can now terminate all active end user sessions immediately and add the users to the disabled user list. Adding a user to this disabled user list terminates all active Secure Private Access application sessions and blocks future application access. For details, see Terminate active user sessions and add users to the disabled user list.

12 February 2024

- **General availability of the browser and antivirus scans**

  The browser and antivirus scans supported by the Device Posture service are now generally available. For details, see Scans supported by device posture.

23 January 2024

- **General availability of device certificate check with Device Posture service**

  Device certificate check with the Device Posture service is now generally available. For details, see Device certificate check with Device Posture service.

20 December 2023

- **General availability of Secure Private Access on-premises**

  Citrix Secure Private Access for on-premises is now generally available. For details, see What's new.

16 October 2023

- **Secure Private Access on-premises solution preview features**

  The Secure Private Access on-premises solution now offers the following:

  - Admin UI for the first-time setup.
  - Admin UI for configuring the applications and access policies.
  - Logs dashboard.

  For details, see Secure Private Access for on-premises.

- **Device Posture service preview features**

  Device Posture service now supports the following checks:

  - Device Posture service is now supported on the IGEL platforms.
  - Device Posture service now supports geolocation and network location checks.

  For details, see Device Posture.

11 September 2023

- **General availability of Device Posture Integration with Microsoft Intune**

  Device Posture Integration with Microsoft Intune is now generally available. For details, see Microsoft Intune integration with Device Posture.

30 August 2023

- **Manage Citrix Endpoint Analysis Client for Device Posture service**

  The EPA client can be used together with NetScaler and Device Posture. Some configuration changes are required to manage EPA client when used with NetScaler and Device Posture. For details, see Manage Citrix Endpoint Analysis Client for Device Posture service.

28 August 2023

- **Device Posture service support on iOS platforms**

  Device Posture service is now supported on iOS platforms. For details, see Device Posture.

  This feature is in preview.

22 August 2023

- **Device Certificate check with Citrix Device Posture service**

  Citrix Device Posture service can now enable contextual access (Smart Access) to Citrix DaaS and Secure Private Access resources by checking the end device's certificate against a corporate certificate authority to ascertain if the end device can be trusted. For details, see Device certificate check with Device Posture service.

  This feature is in preview.

17 August 2023

- **Device Posture events on Citrix DaaS™ Monitor**

  Device Posture service events and monitoring logs are now searchable on DaaS Monitor. For details, see Device posture events on Citrix DaaS Monitor.

07 June 2023

- **Tool for configuring Secure Private Access for on-premises**

  A simplified user interface is now available to configure the Secure Private Access for on-premises solution. The config tool can be run on a Citrix Virtual Apps and Desktops™ delivery controller to create a SaaS or Web application quickly. In addition, you can use this tool to set application restrictions, traffic routing, and NetScaler Gateway settings.

29 May 2023

- **General availability of creation of access policies with multiple rules**

  You can create multiple access rules and configure different access conditions for different users or user groups within a single policy. These rules can be applied separately for both HTTP/HTTPS and TCP/UDP applications, all within a single policy. For details, see Configure an access policy with multiple rules.

10 April 2023

- **Application discovery**

  Application discovery feature helps an admin get visibility into the internal private applications such as web apps and client server apps (TCP and UDP based apps) in their organization and the users accessing those applications. Admins can discover the apps by specifying the scope of the domains (wildcard domains) or IP subnets. For details, see Application discovery.

29 March 2023

- **Secure Private Access solution for on-premises deployments**

  As a Citrix StoreFront and NetScaler Gateway customer, you can now access the Web and SaaS apps seamlessly along with Citrix Virtual Apps and virtual desktops using the Citrix Secure Private Access solution for on-premises deployments. For details, see Secure Private Access for on-premises.

07 March 2023

- **Configure DNS suffixes**

  The DNS suffix feature of the Citrix Secure Private Access service can be used for the following use cases:

  - Enable the Citrix Secure Access™ client to resolve a non-fully qualified domain name (host name) to a fully qualified domain name (FQDN) by adding the DNS suffix domain for the back-end servers.

- Enable admins to configure applications using IP addresses (IP CIDR/IP range), so that the end users can access the applications using the corresponding FQDN under the DNS suffix domain.

For details, see DNS suffixes to resolve FQDNs to IP addresses.

23 January 2023

- **Device posture service**

  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). For details, see Device Posture.

- **Microsoft Endpoint Manager integration with Device Posture**

  In addition to the native scans offered by the Device Posture service, the Device Posture service can also be integrated with other third-party solutions. Device Posture is integrated with Microsoft Endpoint Manager (MEM) on Windows and macOS. For details, see Microsoft Endpoint Manager integration with Device Posture.

22 December 2022

- **Single sign-on support for the Workspace URL for users logged in via Citrix Workspace™ app**

  Citrix Secure Access client now supports single sign-on for the Workspace URL when already logged in via Citrix Workspace app. This SSO functionality enhances the user experience by avoiding multiple authentications. For details, see Single sign-on support for the Workspace URL.

- **Enable access to apps using access policies**

  To grant access to the apps for the users, admins are now required to create access policies with a matching user subscription list for the apps to be available for end users. Previously, admins had to add users as subscribers for enabling access. For details, see Create access policies.

03 October 2022

- **Access policies to grant access to the apps**

  The App Subscribers configuration option is removed from the Applications section in the configuration wizard. To grant access to the apps for the users, admins are required to create access policies. In access policies, admins add app subscribers and configure security controls. For details, see Create access policies.

- **Support for UDP apps**

  The Secure Private Access service now supports access to UDP apps. For details, see Preview features.

09 September 2022

- **Adaptive access based on user risk score**

  Admins can now configure an adaptive access policy with the user risk score provided by Citrix Analytics for Security (CAS). For details, see Adaptive access based on user risk score.

- **Adaptive access based on user's network location**

  Admins can now configure the adaptive 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. For details, see Adaptive access based on the location.

- **Enhanced adaptive access policy builder**

  Access to the apps is now enabled only after the configured conditions are met. Apps subscription alone does not provide your customers access to the applications. Admins must add access policies to provide access to the apps in addition to the app subscription. Also, users or groups is a mandatory condition in the access policies that must be met to access the apps. For details, see Create access policies.

- **Restrict file uploads into SaaS/web apps**

  This feature allows the customer admins to control (allow or restrict) who can upload files into their business-critical applications. With this, only authorized users can upload files into the applications. For details, see Create access policies.

- **Enhanced dashboard**

  The Secure Private Access dashboard now provides detailed visibility into several user metrics such as app usage, top app users, top apps accessed, diagnostic logs, and so on. For details, see Dashboard.

- **Library deprecation**

  The Secure Private Access applications are now not visible inside the Citrix Cloud™ Library. All Secure Private Access configured applications are inside the application section within the Secure Private Access service tile. This helps admins to easily navigate, edit, and configure the applications.

- **Audit logs for Secure Private Access**

  The Citrix Secure Private Access service related events are now captured in the **Citrix Cloud > System Log.** For details, see Audit logs.

- **Diagnostic logs for Enterprise Web and SaaS apps access**

  The Citrix Secure Private Access events are now integrated with Citrix Analytics. Citrix Analytics provides a public endpoint that enables admins to access and download the events. These events can be accessed through a PowerShell script. For details, see Diagnostic logs for Enterprise Web and SaaS apps access.

- **Troubleshooting Guide**

  The admins can use the troubleshooting guide to resolve configuration-related issues. For details, see Troubleshoot apps related issues.

01 June 2022

- **Adaptive Authentication service**

  Adaptive Authentication is now generally available (GA). For detailed information about Adaptive Authentication, see Adaptive Authentication service.

04 April 2022

- **Rebranding changes**

Citrix Secure Workspace Access service is now rebranded to Citrix Secure Private Access service.

- **Admin guided workflow for easy onboarding and set up**

  Secure Private Access now has a new streamlined admin experience with a step-by-step process to configure Zero Trust Network Access to SaaS apps, internal web apps, and TCP apps. It includes configuration of Adaptive Authentication, applications including user subscription, adaptive access policies, and others within a single admin console. For details see, Admin-guided workflow for easy onboarding and set up.

  This feature is now generally available (GA).

- **Secure Private Access dashboard**

  The Secure Private Access dashboard provides admins full visibility into their top apps, top users, connectors health status, bandwidth usage, and in a single place for consumption. This data is fetched from Citrix Analytics. For details, see Secure Private Access dashboard.

  This feature is now generally available (GA).

- **Direct access to Enterprise web apps**

  Customers can now enable Zero Trust Network Access (ZTNA) to internal web apps, directly from native web browsers such as Chrome, Firefox, Safari, and Microsoft Edge. For details, see Direct access to Enterprise web apps.

  This feature is now generally available (GA).

- **ZTNA agent-based access to TCP/HTTPS apps**

  Citrix customers can now enable Zero Trust Network Access (ZTNA) to all client-server applications and IP/Port based resources, in addition to internal web apps. For details, see Support for client-server apps.

  This feature is now generally available (GA).

- **Adaptive access and security controls for Enterprise Web, TCP, and SaaS applications**

  The Citrix Secure Private Access service adaptive access feature offers a comprehensive Zero Trust Network Access (ZTNA) approach that delivers secure access to the applications.

Adaptive access enables admins to provide granular level access to the apps that users can access based on the context. The term “context” here refers to:

- Users and groups (users and user groups)
- Devices (desktop or mobile devices)
- Location (geo-location or network location)
- Device posture (device posture check)
- Risk (user risk score)

For details, see Adaptive access and security controls for Enterprise Web, TCP, and SaaS applications.

This feature is now generally available (GA).

- **Audit logs for Secure Private Access**

  The Citrix Secure Private Access service related events are now captured in the **Citrix Cloud > System Log.** For details, see Audit logs.

  This feature is now generally available (GA).

- **Diagnostic logs for Enterprise Web and SaaS apps access**

  The Citrix Secure Private Access events are now integrated with Citrix Analytics. Citrix Analytics provides a public endpoint that enables admins to access and download the events. These events can be accessed through a PowerShell script. For details, see Diagnostic logs for Enterprise Web and SaaS apps access.

  This feature is now generally available (GA).

- **Adaptive authentication service**

  Citrix Cloud customers can now use Citrix Workspace to provide Adaptive Authentication to Citrix Virtual Apps and Desktops. Adaptive Authentication is a Citrix Cloud service that enables advanced authentication for customers and users logging in to Citrix Workspace. Adaptive Authentication service is a Citrix managed and Citrix Cloud hosted ADC. For details, see Adaptive Authentication service.

  This feature is in preview.

16 February 2022

- **Support for client-server apps** With the support for client-server applications within Citrix Secure Private Access, you can now eliminate the dependency on a traditional VPN solution to provide access to all private apps for remote users.

  For details, see Support for client-server apps - Preview

11 October 2021

- **Merger of Citrix Gateway service tile into a single Secure Private Access in Citrix Cloud**

  The Citrix Gateway service tile is now merged into a single Secure Private Access in Citrix Cloud.

  - All Secure Private Access customers, including Citrix Workspace Essentials™ and Citrix Workspace Standard, can now use one single Secure Private Access tile for configuring SaaS and Enterprise web apps, enhanced security controls, contextual policies, in addition to web filtering policies.
  - All Citrix DaaS customers can still enable the Citrix Gateway service as the HDX proxy from Workspace Configuration. However, the shortcut to enable Citrix Gateway service from the gateway service tile is removed. You can enable the Citrix Gateway service from **StoreFront Cloud > Access > External Connectivity**. For details, see External connectivity. There is no change in the functionality, otherwise.

30 July 2021

- **Contextual access and security controls for the Enterprise Web and SaaS apps based on user's geographic location**

  The Citrix Secure Private Access service now supports contextual access to the Enterprise Web and SaaS apps based on the user's geographic location.

- **Option to hide a specific Web or a SaaS app from Citrix Workspace portal**

  Admins can now hide a specific Web or SaaS app from the Citrix Workspace portal. When an app is hidden from the Citrix Workspace portal, the Citrix Gateway service does not return this app during enumeration. However, users can still access the hidden app.

09 June 2021

- **Route table to define the rules to route the app traffic**

  Admins can now use the route table to define the rules to route the app traffic directly to the internet or through the Citrix Gateway Connector. The admins can define the route type for the apps as External, Internal, Internal-Bypass Proxy, or External via Gateway Connector depending on how they want to define the traffic flow.

22 May 2021

- **Contextual access to Enterprise Web and SaaS applications**

  The Citrix Secure Private Access service contextual access feature offers a comprehensive zero-trust access approach that delivers secure access to the applications. Contextual access enables admins to provide granular level access to the apps that users can access based on the context. The term "context" here refers to users, user groups, and the platform (mobile device or a desktop computer) from which the user is accessing the application.

- **Rebranding of Citrix Gateway Connector user interface**

  The Citrix Cloud Gateway Connector™ user interface is rebranded as per the Citrix branding guidelines.

01 May 2021

- **Deletion of customer data from the Citrix Secure Private Access service datastore**

  Customer data, including backups, is deleted from the Citrix Secure Private Access service datastore after 90 days of service entitlement expiry.

- **Simplified steps to federate a domain from Azure AD to Citrix Workspace**

  The steps to federate a domain from Azure AD to Citrix Workspace app is now simplified for faster onboarding in Citrix Workspace. Domain federation can now be performed in the Citrix Gateway service user interface, from the Single sign on page.

- **Enhancement to the Connectivity Test tool**

The Connectivity Test tool in the Citrix Gateway Connector is enhanced to handle timeout errors and to generate the necessary logs.

15 March 2021

- **Platform enhancements**

  Various platform enhancements are made to increase reliability in propagating customer's admin configurations to the Citrix Gateway Connectors.

- **Improved web apps performance**

  The web apps performance when the web applications are accessed from the system browser using clientless VPN has been improved.

- **Enabling Citrix Gateway Connector to use TLS1.2 Grade A or above cipher suites**

  The Citrix Gateway Connector now uses TLS1.2 with Grade A or above cipher suites to connect to Citrix Cloud service and other back end servers.

11 November 2020

- **Renaming of Citrix Access Control™ service**

  The Access Control service is now renamed as Secure Private Access.

15 October 2020

- **Enhanced security option to launch SaaS and Enterprise Web apps within Remote Browser Isolation service**

  Admins can now use the enhanced security option, **Select Launch application always in Citrix Remote Browser Isolation™ service** to always launch an application in the Remote Browser Isolation service regardless of other enhanced security settings.

08 October 2020

- **Configure session timeouts for the Citrix Secure Private Access browser extension**

Admins can now configure session timeouts for the Citrix Secure Private Access browser extension. Admins can configure this setting from the **Manage** tab in the Citrix Gateway service user interface.

- **RBAC control on Citrix Secure Private Access browser extension admin settings**

  RBAC control is now enforced on Citrix Secure Private Access browser extension admin settings.

24 September 2020

- **Enable VPN-less access to Enterprise Web apps through a local browser**

  You can now use the **Citrix Secure Private Access** browser extension to enable VPN-less access to Enterprise Web apps through a local browser. The **Citrix Secure Private Access** browser extension is supported on both Google Chrome and Microsoft Edge browsers.

07 July 2020

- **Validate Kerberos configuration on Citrix Gateway Connector**

  You can now use the **Test** button in the **Single sign on** section to validate the Kerberos configuration.

19 June 2020

- **Read-only access to admins of the Citrix Gateway service and Citrix Secure Private Access service**

  Security admin teams using the Citrix Gateway service can now provide granular controls, such as read-only access to admins of the Citrix Gateway service and Citrix Secure Private Access service.

  - Admins with read-only access to the Citrix Gateway service have access to only view the app details.
  - Admins with read-only access to the Citrix Secure Private Access service can only view the content access settings.

08 May 2020

- **New troubleshooting tools in Citrix Gateway Connector 13.0**
  - **Network tracing:** You can now use the **Trace** feature to troubleshoot Citrix Gateway Connector registration issues. You can download the trace file and share it with the administrators for troubleshooting.
  - **Connectivity tests:** You can now use the **Connectivity Test** feature to confirm that there are no errors in the Gateway Connector configuration and the Gateway Connector is able to connect to the URLs.

V2019.04.02

- **Kerberos authentication support for Citrix Gateway Connector to outbound proxy**

  Kerberos authentication is now supported for the traffic from the Citrix Gateway Connector to the outbound proxy. Gateway Connector uses the configured proxy credentials to authenticate to the outbound proxy.

V2019.04.01

- **Web/SaaS apps traffic can now be routed via a corporate-network-hosted Gateway-Connector thus avoiding two factor authentication.** If a customer has published a SaaS app that is hosted outside the corporate network, support is now added to authenticate traffic for that app to go through an on-premises Gateway Connector.

  For example, consider that a customer has an Okta protected SaaS app (like Workday). The customer might want that even though the actual Workday data traffic is not routed via the Citrix Gateway service, the authentication traffic to the Okta server is routed through the Citrix Gateway service via an on-premises Gateway Connector. This helps a customer to avoid a second factor authentication from the Okta server as the user is connecting to the Okta server from within the corporate network.

- **Disabling Filtering Website Lists and Website Categorization**. Filtering Website Lists and Website Categorization can be disabled if the admin chooses not to apply these functionalities for a specific customer.

- **Automatic geo routing for Remote Browser Isolation service redirects.** Automatic geo routing is now enabled for Remote Browser Isolation service redirects.

V2019.03.01

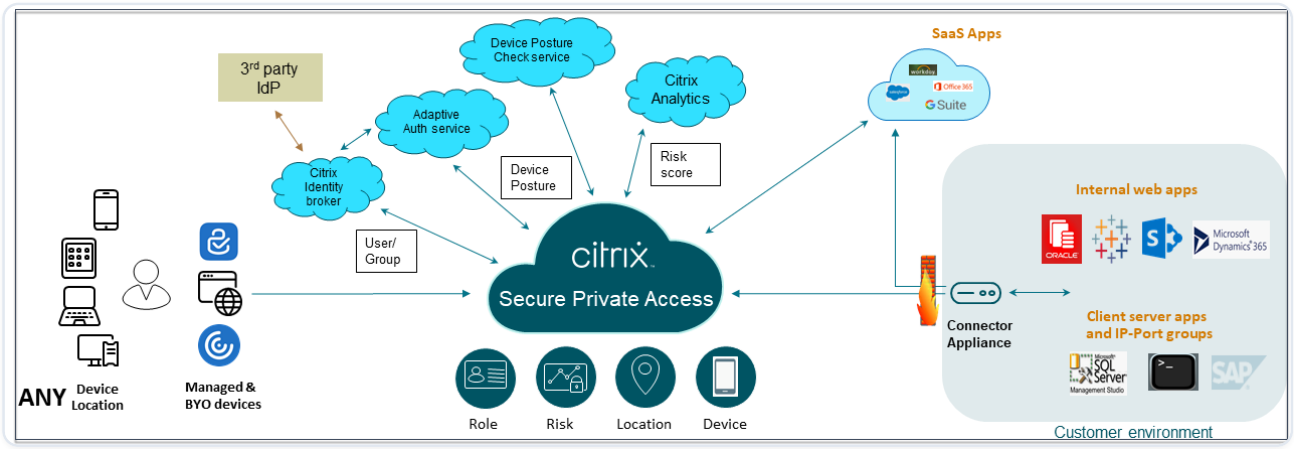
- **"Detect" button is added in the "Add a Gateway Connector" page.** The **Detect** button is used to refresh the list of connectors, allowing the newly added connector to reflect in the Web app connectivity section.

- **A new category "Malicious and Dangerous" is added in the "Access Control Web Filtering" categories.** A new category named **Malicious and Dangerous** in the **Access Control Web Filtering** categories is added under the **Malware and Spam** group.

Secure Private Access service solution overview

Traditional VPN solutions require end-user devices to be managed, provide access at the network level, and enforce static access control policies. Citrix Secure Private Access™ gives IT a set of security controls to protect against threats from BYO devices, giving users the choice to access their IT-sanctioned applications from any device, whether it's managed or BYO.

Citrix Secure Private Access offers Adaptive Authentication, single sign-on support, enhanced security controls for the applications. Secure Private Access also provides the capabilities to scan the end user device before establishing a session by using the Device Posture service. Based on the Adaptive Authentication or Device Posture results, admins can define the authentication methods for the apps.



Adaptive security

Adaptive Authentication determines the right authentication flow for the current request. Adaptive Authentication can identify the device posture, geographical location, network segment, user organization/department membership. Based on the information obtained, an admin can define how they want to authenticate users to their IT sanctioned apps. This allows organizations to implement the same authentication policy framework across every resource including public SaaS apps, private web apps, private client-server apps, and Desktops as a Service (DaaS). For details, see Adaptive Security.

Application access

Secure Private Access can create a connection to the on-premises web apps without relying on a VPN. This VPN-less connection uses an on-premises deployed Connector Appliance. The Connector Appliance creates an outbound control channel to the organization's Citrix Cloud subscription. From there, Secure Private Access can tunnel connections to the internal web apps without the need for a VPN. For details, see Application Access.

Single sign-on

With Adaptive Authentication, organizations can provide strong authentication policies to help reduce the risk of compromised user accounts. The single sign-on capabilities of Secure Private Access use the same Adaptive Authentication policies for all SaaS, private web, and client-server apps. For details, see Single Sign-On.

Browser security

Secure Private Access is integrated with Google Chrome Enterprise Premium (CEP), which includes features such as data loss prevention (DLP), malware and phishing protection, and URL filtering. 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. For details, see Integration with Google Chrome Enterprise Premium.

Device posture

Device posture service allows an admin to define policies to check the posture of endpoint devices trying to access corporate resources remotely. Based on the compliance status of an endpoint, the device posture service can deny access or provide restricted/full access to corporate applications and desktops.

When an end user initiates a connection from their store, the Device Posture client collects information about the endpoint parameters and shares this information with the Device Posture service to determine if the posture of the endpoint meets policy requirements.

The integration of the Device Posture service with Citrix Secure Private Access enables secure access to SaaS, Web, TCP and UDP apps from anywhere, delivered with the resiliency and scalability of Citrix Cloud. For details, see Device Posture.

Support for TCP and UDP applications

Sometimes remote users need access to private client-server apps that have their front-end on the endpoint and their back-end in a data center. Organizations can rightfully enforce strict security policies around these internal and private apps, making it difficult for remote users to access these applications without compromising security protocols.

Secure Private Access service addresses the TCP and UDP security vulnerabilities by enabling ZTNA to deliver secure access to these apps. Users can now access all private apps including TCP, UDP, and HTTPS apps either using the Chrome browser or a native client application via the Citrix Secure Access™ client running on their machines.

Users must install the Citrix Secure Access client on their client devices.

- For Windows, the client version (22.3.1.5 and later) can be downloaded from Downloads.
- For macOS, the client version (22.02.3 and later) can be downloaded from the App Store.

For details, see Support for client-server apps.

Sample use cases

- Access internal applications (Web/TCP/UDP) using a Zero-Trust approach without opening incoming traffic on the firewall
- Move to a Zero-Trust approach by discovering applications accessed by users
- Restrict access to SaaS applications to company-owned public IP addresses
- Enhanced Security to Azure-managed SaaS Apps
- Enhanced Security to Office 365
- Enhanced Security to Okta Apps

Reference articles

- Introduction to Secure Private Access
- Tech brief
- Reference Architecture
- Secure Private Access onboarding and set up

Reference videos

- Zero trust network access (ZTNA) to apps
- Private Web app access with Citrix Secure Private Access
- Public SaaS app access with Citrix Secure Private Access
- Private client-server app access with Citrix Secure Private Access
- Keylogger Protection with Citrix Secure Private Access
- Screen sharing protection with Citrix Secure Private Access
- End-user experience with Citrix Secure Private Access
- ZTNA versus VPN logon experience with Citrix Secure Private Access
- ZTNA versus VPN port scans with Citrix Secure Private Access

What's new in related products

- Citrix StoreFront Cloud: What's new
- Citrix DaaS: What's new
- Citrix Secure Access: Citrix Secure Access

Integration with Google Chrome Enterprise Premium

The following sections provide details about the integrated solution.

Solution overview

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 benefit of this integration is to provide agentless access from the Chrome browser to private web and SaaS applications by automated traffic steering through Citrix Secure Private Access infrastructure. When users access applications through Chrome, the system automatically sends their traffic to Citrix Secure Private Access via the Google Secure Gateway. This ensures secure and controlled network access without needing to install extra software on user devices. It also simplifies the deployment, reduces IT management, improves the user experience, and streamlines IT operations.

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.

Citrix Secure Access controls for Chrome Enterprise

The following value-adding features are supported with the Secure Private Access and Chrome Enterprise Premium integration.

- **RDP** - Enable secure RDP sessions directly within the browser. For details, see Remote Desktop control.
- **SSH** - Enable secure access to SSH apps within the browser. For details, see SSH control.
- **Anti-key logging** - Prevent keyloggers when accessing resources in CEP. For details, seeAnti-keylogging control.

- **Clipboard container** - Restrict or allow clipboard sharing between the browser and virtualized applications. For details, see Clipboard container control.
- **Session recording** - Record user sessions within the browser. For details, seeSession recording control
- **Browser session reauthentication** - Enforces periodic re-authentication of browser sessions after a configured time interval. For details, seeBrowser session reauthentication control.
- **Domain suffix** - Optimize the user experience by appending the domain to short URLs.For details, seeDomain suffix for web applications.

Prerequisites for successful integration

To ensure optimal integration between the Citrix Workspace™ app 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.

- Licenses, app versions, and extensions
- Google Admin console
- Secure Private Access service
- Chrome browser
- Synchronize user directory configured in Citrix Workspace with the Google Cloud user directory

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.

Important:

For Chrome Enterprise Premium (CEP), only HTTPS enterprise web and SaaS apps are supported. HTTP enterprise web and SaaS apps are not supported.

Legal

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

Related topics

- Secure Private Access onboarding and set up
- Update Google integration details post onboarding
- Apps configuration and management
- Tech Brief: Citrix Secure Access with Chrome Enterprise

Prerequisites for the integrated solution

To ensure optimal integration between the Citrix Workspace™ application and Chrome Enterprise Premium, the following prerequisites must be implemented. Successful completion of these prerequisites result 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.

- Licenses, app versions, and extensions
- Google Admin console
- Secure Private Access service
- Chrome browser
- Manage users
- Correlate user directory

- Bypass TLS inspection

Licenses, app versions, and extensions

- **Chrome Enterprise Premium license**: Ensure that you have an active Chrome Enterprise Premium license, available through the Citrix Cloud Platform License (CPL) program.
- **Citrix Workspace app (CWA) versions**:
  - Windows: 2025.07 and later
  - macOS: 2025.08 and later
  - ChromeOS: 25.7.0.25 and later

> **Note:**
>
> Citrix Workspace app is an optional requirement for this solution.

- **Citrix Endpoint Analysis (EPA) client versions:**
  - Windows: 25.9.1.9 and later
  - macOS: 25.10.3 and later

> **Note:**
>
> We recommend installing the Windows EPA client in administrator mode to support periodic device posture scans. In addition, periodic device posture scans must be enabled under Device Posture **Settings** page. For details, see Periodic scanning of devices.

- **Chrome browser version**: Endpoints must use the latest Google Chrome version.
- **Operating systems**: Windows, macOS, and ChromeOS.

Google 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.
- **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.

Secure Private Access service

- **IPv6 endpoints limitations**: The Citrix Secure Private Access service, when integrated with Google cloud endpoints, might receive traffic from end-user devices with IPv6 addresses. Currently, Secure Private Access Geo Location and Network Location access policies lack IPv6 support.

  Consequently, access policies with Geo Location or Network Location conditions might fail for end-user devices with an IPv6 address. Other access policies that do not leverage such conditions work for both IPv4 and IPv6 enabled end user devices.
- **Access restrictions are now configured in 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

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.

Manage users

For a seamless integration, there must be a correlation between users configured in Citrix Secure Private Access and Google Identity (Directory). This ensures that only authorized users can access their assigned applications. The following user directories are supported for integration:

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

Mandatory - Populate email address fields for users

Google Identity requires the email address field to be populated. Towards this end, a user object in the directory used by Secure Private Access must have one of the following:

- An email address, with a domain part that is configured and verified in the Google Admin console. For example, `Alice` with an email address `alice@example.com` is mapped as `alice@example.com` in Google Identity.
- An email address with a domain part that is not configured in the Google Admin console. For example, `Bob` has an email address `bob@example.internal.net`, which is not configured in Google. In this case, he is mapped as `bob@example.com` in Google Identity, `example.com` being a verified domain.
- Another directory field that can be used in the absence of email for domain mapping purposes. A typical approach is leveraging the User Principal Name (UPN), with or without domain substitution. For example, `Charlie` has a UPN `charlie@ADdomain.com` and is mapped as `charlie@example.com` in Google Identity.

There are significant limitations for users with a mismatch between their email address in the Secure Private Access directory and the Google directory. See the domain mapping considerations section for details.

Mandatory - Populate email address fields for user groups

Similarly to users, a group object in the directory used by Secure Private Access must have one of the following:

- An email address with a domain part that is configured and verified in the Google Admin console.
- An email address with a domain part that is not configured in the Google Admin console.
- Another directory field that can be used in the absence of an email address for domain mapping purposes. A typical approach is leveraging the Common Name (CN), appending the appropriate domain in Google Directory. For example, a group with CN `group1` is mapped as `group1@example.com` in Google Identity.

Domain mapping considerations for missing or inconsistent email address

Users:

In case a user's email address is missing on the Secure Private Access directory or is inconsistent between it and the Google Identity, the following considerations apply:

- A user without an email address will not be available for selection when configuring Secure Private Access policies within the Secure Private Access console.
- The Secure Private Access policies for a user with an email address that is not matching between the Secure Private Access directory and the Google directory will not work.
- Launching a web or SaaS app from cloud stores (using Citrix Workspace app or a web browser) is not supported for these users.

Groups:

In case a group's email address is missing on the Secure Private Access directory or is inconsistent between it and the Google Identity, an appropriate domain mapping configuration is required to make sure that Secure Private Access group-level policies work correctly.

Correlate user directory configured in Citrix Secure Private Access with the Google Cloud user directory

You must correlate the user directory configured in Citrix Secure Private Access with the Google Cloud directory. Specifically, the following user directories are supported:

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

Note that user directory correlation must occur periodically to ensure that application access is appropriately enforced. Only a minimal set of attributes are required for correlation.

Active Directory

For Active Directory, the Name, Email Address, Object Globally Unique Identifier (objectGUID), and Security Identifier (SID) must be correlated. Password and all other attributes are not required to be correlated with the Google Cloud Directory.

For details on how to correlate 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 and Active Directory User Account provisioning.

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

When configuring synchronization, you must consider the following requirements:

- **Email address:** The email address field must be populated for all users and groups. For details, see Manage users.
- **objectId attribute mapping:** The objectId attribute of Entra ID Users must be mapped to Google Directory.

  Do this mapping in the G-Suite Connector configuration:

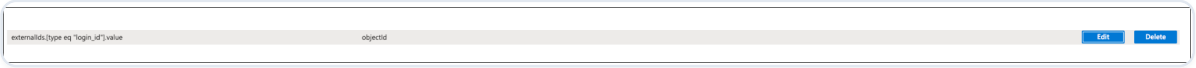
  a. From the left menu, click **Manage > Provisioning**.

  b. In the new menu click **Manage > Attribute Mapping**.

  c. Click **Provision Microsoft Entra ID Users**.

  d. Find the appropriate row for objectId.

  - Click **Edit** and under **Target attribute** select **externalIds**..value.
  - Verify that the resulting configuration matches the following screenshot.



- **Single Sign-On:** Single sign-on (SSO) configuration is optional. You can configure a separate password in the Google directory, configure SSO with Entra ID, or configure SSO with Open ID Connect with Citrix Identity.

Okta

You can use Okta as the identity source by provisioning users and groups from Okta into the Google Cloud user directory (Cloud Identity / Google Workspace). Once provisioned, correlation with Secure Private Access follows the same model as the other supported directories. Only a minimal set of attributes is required, and the email address field must be populated for all users and groups.

For details on provisioning from Okta into Google, see Okta user provisioning and single sign-on. You can follow the same guide to configure SSO against Okta, or see Open ID Connect with Citrix Workspace.

Google Cloud Identity (Google Directory)

When Google Cloud Identity is already your identity provider, the users and groups reside natively in the Google Cloud directory. No directory correlation or synchronization is required, because there is no separate external directory to reconcile against Google. Google is the source of identity for both Citrix Workspace and Chrome managed profiles.

> **Note:**
>
> Device Posture service integration for Chrome Enterprise Premium relies on the OpenID Connect (OIDC) flow, in which the Google Cloud directory acts as a relying party against Citrix Workspace. That flow is not supported when Google Cloud Identity is itself the underlying IdP. Hence, Device Posture service integration is not available in this configuration.

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 host names 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 host names 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`

Admin roles and privileges

The Citrix service account is used by Secure Private Access to onboard users to Chrome Enterprise Premium (CEP) and enable CEP integration. Therefore, you must assign a role with the required privileges to the service account in the Google Admin console.

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

System roles: These are the default roles provided by Google. Except for the super admin role, the remainder of the system roles does not include all the necessary privileges required for CEP integration with Secure Private Access.

Custom roles: These can include any subset of Admin API privileges. You must create a custom role that includes all privileges required for CEP integration with Secure Private Access.

You must be signed into the Google Admin console as a super administrator for this task.

> **Note:**
>
> Super administrator roles cannot be assigned to service accounts.

Google custom admin role privileges

For CEP and Secure Private Access integration, the Citrix service account must have a custom role in the Google Admin console with the following specific privileges:

REQUIRED ADMIN PRIVILEGE	WHY IS THIS PRIVILEGE NEEDED
Manage customer > Read customer	To read the Google customer organization-friendly name.
Organization Units > Read	To verify that the organization units configured are available in Google Directory.
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**).	To add the mandatory extensions, and configuration thereof, required for CEP and SPA integration at the user profiles.
Services > Chrome Management > Settings Managed Browsers > Read	To read the managed Chrome profiles and the managed browsers.
License Management > Read	To query the total number of Chrome Enterprise Premium-assigned licenses provisioned for the organization.
Reports	To read the users that are actively using their assigned licenses. To read the activity events when the Data Loss Prevention (DLP) rules are triggered. To read the failure events.

REQUIRED ADMIN PRIVILEGE	WHY IS THIS PRIVILEGE NEEDED
Groups > Read	To verify that the integration groups configured are available in Google Directory.
Services > Alert Center > Full access > View access	To read the security alerts for Data Loss Prevention and the login failure events.
Manage Devices and Settings	To read device metadata so as to display them in the Monitor network topology view.
Users > Read	To verify that the integration users configured are available in Google Directory.

Note:

- It is also required to grant the equivalent OAuth scopes for these admin privileges.
- All administrative privileges are now found in the **Admin privileges** section. This includes privileges previously listed in the **Admin console privileges** and **Admin API privileges** sections. This change does not affect how privileges are assigned, and existing privileges continue to work as they did before.
- 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.
- Citrix Secure Private Access deploys configurations to your Google account using the Citrix service account configured. After Citrix Secure Private Access and Google CEP integration is completed, open the Google Admin console and navigate to **Chrome Browser > Apps & Extensions**. Note that several browser extensions have been configured at the root org level. Those are inherited by the child OUs. When users onboard Google Chrome profiles with this tenant, these extensions are automatically provisioned.

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 Google custom admin role privileges.

   For more information related to roles and privileges, see the Google documentation.
4. Save the custom role.

Configure egress hub regions

Secure Private Access enables administrators to choose the egress regions that Chrome Enterprise Premium uses for SaaS application traffic. Each selected region provides a dedicated set of egress IP addresses, which administrators can add to their SaaS application allow lists to permit traffic routed through Google Secure Gateway. This feature is available for both cloud and hybrid deployments.

You can access the **Egress regions for SaaS applications** panel from one of the following paths.

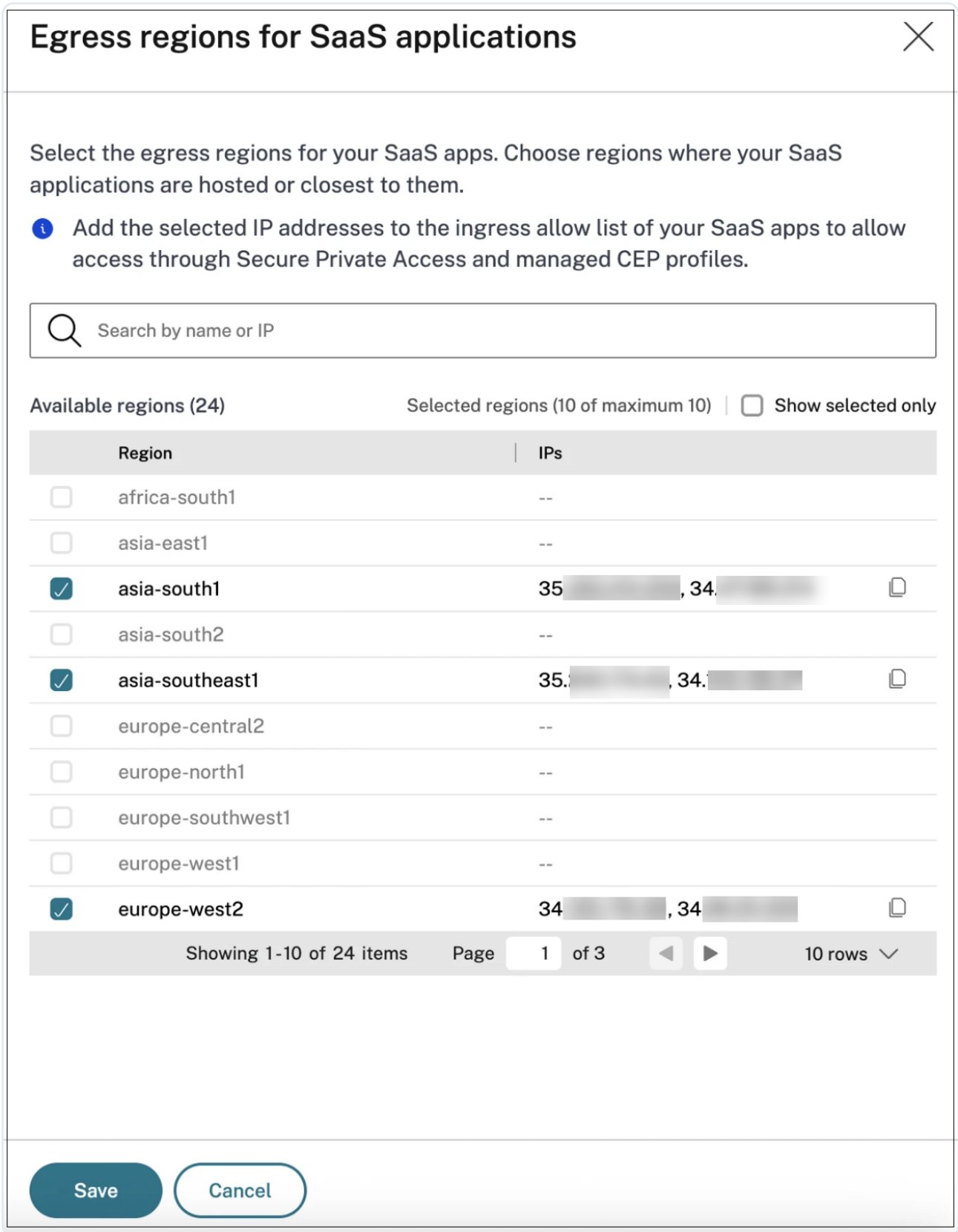
- Click the **Manage egress regions** button on the Chrome Enterprise Premium setup card.



- Click **Edit** in **Browser Settings > Browser Configure > Egress regions for SaaS applications**.

The Egress regions for SaaS applications panel

The **Egress regions for SaaS applications** panel displays the available egress regions and the IP addresses associated with each selected region. You can search for regions by the name or the IP address, and then copy a region's IP addresses to add them to your SaaS application allow lists.



IP addresses become available only after you select a region, save your changes, and Google completes the deployment. Until the deployment is complete, newly selected regions do not display any IP addresses. Deployment usually takes a few minutes, although the exact time may vary.

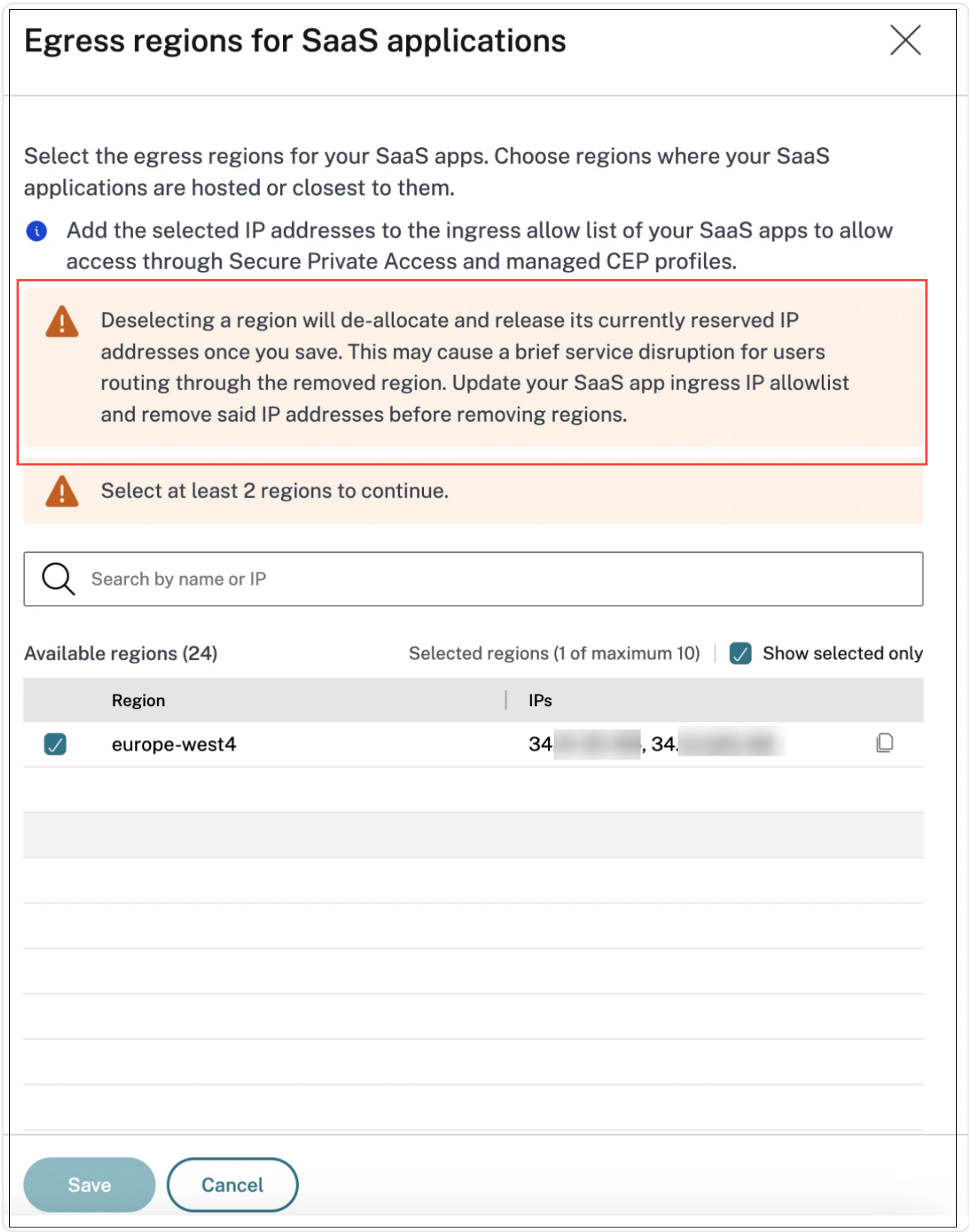
Select a region

Select the regions where your SaaS applications are hosted or the regions closest to them. To ensure redundancy during a regional outage, select at least two regions. You can select up to 10 regions.

After Google deploys the selected regions and the associated IP addresses become available, add those IP addresses to your SaaS applications' ingress allow lists.

De-select a region

De-selecting a region displays a warning message.



You must update your SaaS application allow lists before saving changes. If you select **Cancel**, all changes are discarded.

If you later de-select and re-select the same region, Google assigns a new set of egress IP addresses. These IP addresses typically differ from the ones previously assigned, so you must update your SaaS application allow lists accordingly.

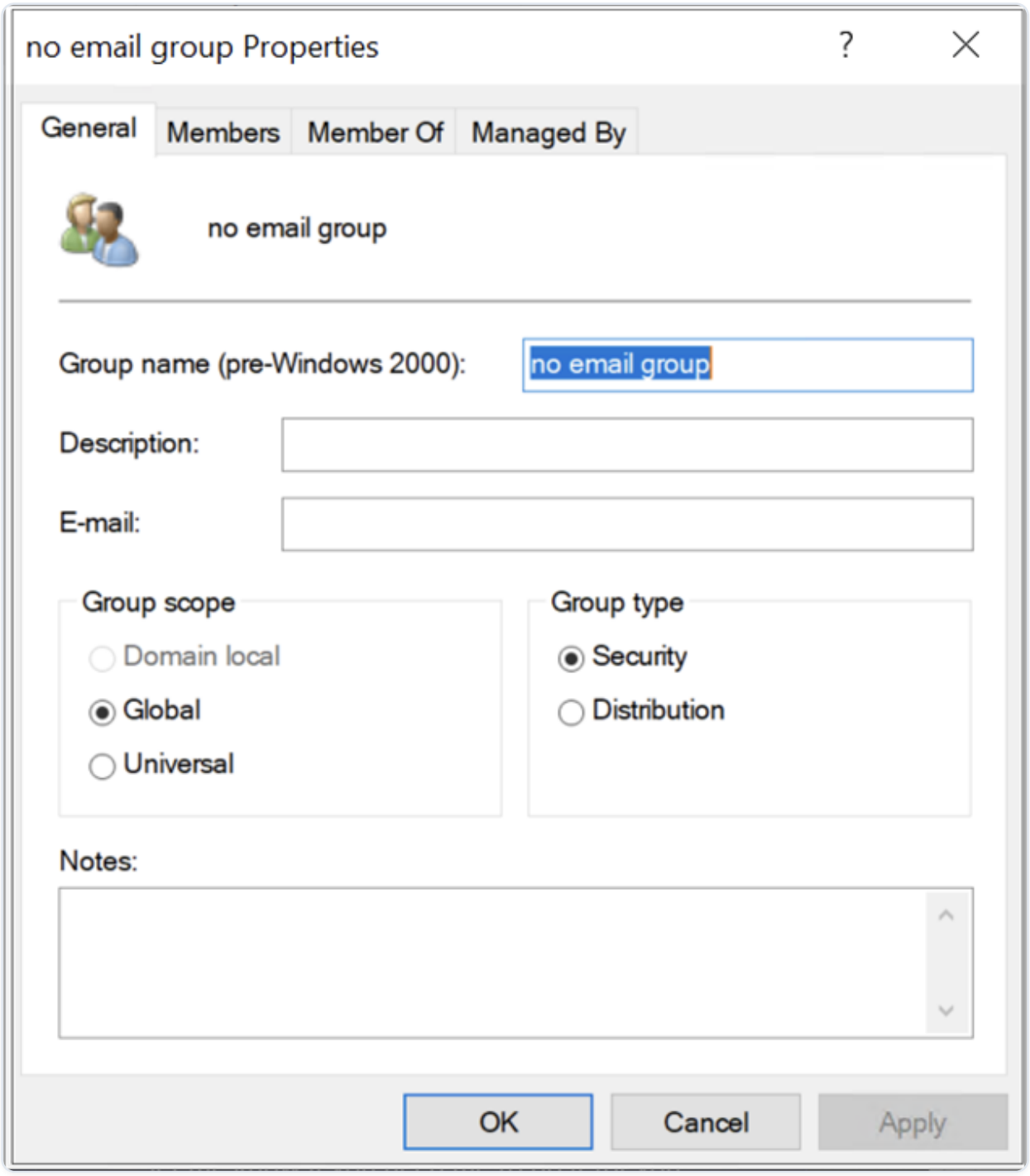
Domain mapping for user groups without email addresses

Google directory requires a verified email address for all user and group objects. However, this isn't always available for directories supported by Secure Private Access, specifically Active Directory (AD) and Microsoft Entra ID. AD and Microsoft Entra ID objects might lack an email address or have one pointing to an internal or special domain (for example, @fabrikam.onmicrosoft.com) that Google directory cannot verify.

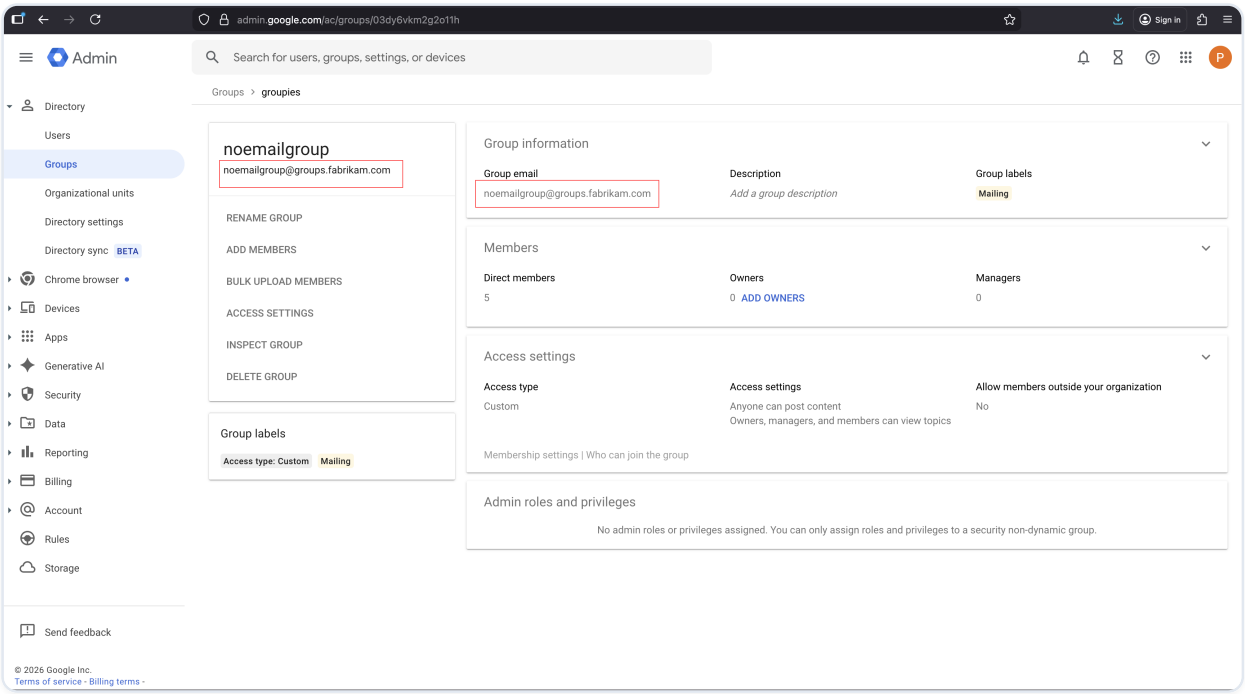
Because the email address normally serves as the common identifier between Secure Private Access and Google directory, groups from AD/Entra without a verified Google email address are typically unsupported for Secure Private Access policies. The Domain Mapping feature resolves this by allowing administrators to configure policies against groups even if they lack an email address or have an email address with an unverified domain.

How domain mapping works

- Consider a group in your AD without an email address.



- This group is replicated in the Google directory with an email address that is synthesized by the group common name (note that since “space” is not supported in an email address, it’s omitted) and a verified Google domain `@groups.fabrikam.com`. The effective Google group email address, `noemailgroup@groups.fabrikam.com` does not exist in the source directory.



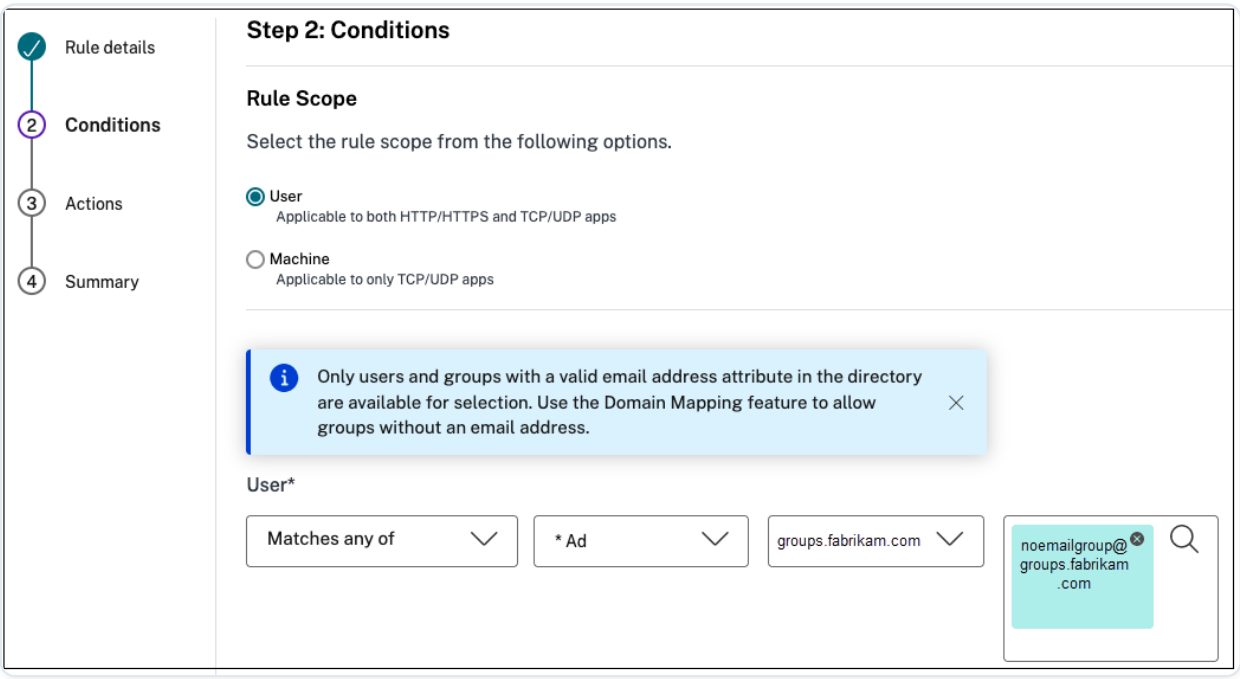
- The admin can configure domain mapping for groups without an email address.

  a. In the Secure Private Access admin console, navigate to **Browser settings > Domain Mapping**.

  b. Turn the **Include empty domain** toggle to ON to enable mapping of groups without email addresses.

  c. In the **Google domains > Domains** field, enter the target group domain (`groups.fabrikam.com` in this example). By adding the target group domain, you are enabling the admin to map groups without an email against the appropriate Google domain email (`groups.fabrikam.com`) when configuring policies.

When assigning groups to a policy, if you search for the group without an email address (`noemailgroup`), an email address is synthesized based on your Domain mapping configuration and `noemailgroup@groups.fabrikam.com` becomes available. This conversion is based on a predetermined conversion logic. For details, see Email address construction.



Email address construction

- For groups without an existing email address:
  - The email local part is populated using the lowercase version of the Group Common Name (cn), with “space” characters omitted.
  - The email domain part is populated using the lowercase version of the Google domain (google-domain).
  - Domain selection (when multiple Google domains are present): If a group is associated with multiple Google domains, the admin can select the appropriate domain for the email address.
- For groups with an existing onmicrosoft.com or otherwise email address in an unverified domain:
  - Email local part: The email local part is populated using the lowercase version of the existing email address' local-part.
  - Domain selection (when multiple Google domains are present): If a group is associated with multiple Google domains, the admin can select the appropriate domain for the email address.

Limitations

The Domain Mapping feature only supports groups with alphanumeric characters, dashes, underscores, and spaces.

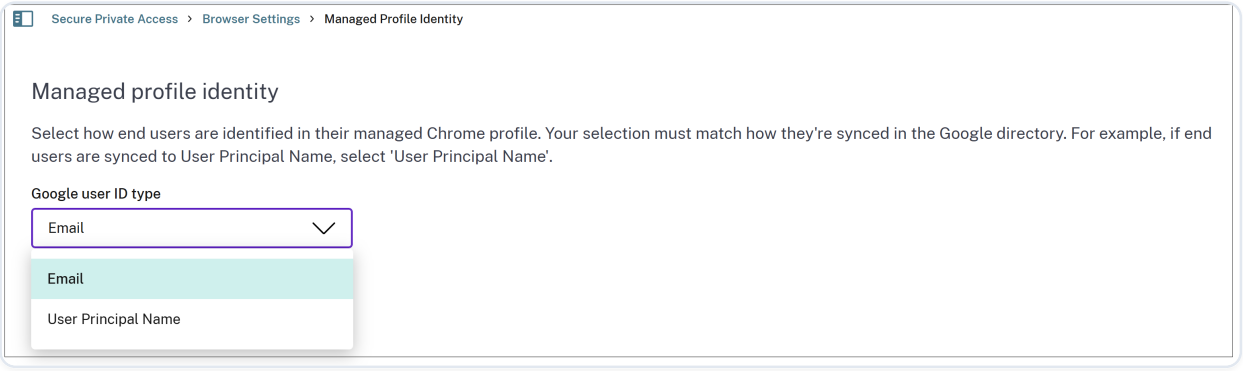
Managed profile identity

Google directory identifies every user account by a primary email address. When your organization synchronizes users from Active Directory or Microsoft Entra ID into the Google directory, you choose which source attribute becomes that address. Most organizations map the email address. Organizations that do not populate the email attribute for every user, may map the User Principal Name (UPN) instead, because the UPN is always present in Active Directory.

Secure Private Access must look up each user by the same attribute that your directory synchronization used as the primary address, otherwise it cannot match the user to their account in the Google directory. You can set up the attribute from the Managed profile identity page in the Secure Private Access admin console.

Set up the user attribute type

1. In the Secure Private Access admin console, navigate to **Browser Settings > Managed Profile Identity**.
2. In **Google user ID type**, select the attribute Secure Private Access uses to identify CEP end users.



   - **Email** - Secure Private Access identifies end users by their email address. This is the default value and the one used by existing deployments.
   - **User Principal Name** - Secure Private Access identifies end users by their User Principal Name (UPN).
3. Click **Save**.
4. In the **Update Google user ID type?** confirmation window, review the message and click **Update**.

A confirmation message appears when the setting is saved.

> **Note:**

- The **Google user ID type** setting applies to users only. Google groups do not have a User Principal Name, so group identity is unaffected. If your groups have no email address in the source directory, see Domain mapping for user groups without email addresses.
- The setting is applied tenant-wide. You cannot select a different identity attribute for individual users.

Open ID Connect with Citrix Identity and access management

You can configure Single Sign On (SSO) for Chrome Enterprise Premium (CEP) using OpenID Connect (OIDC) authentication provider for Citrix Cloud. OIDC integration with Citrix Identity provides the following benefits:

- **Device Posture service integration:** By integrating the Device Posture service with Google Chrome Enterprise Premium, you can extend device compliance checks to Chrome browser-based access scenarios. This integration enables organizations to enforce device posture policies when users access applications through their managed Google Chrome profiles. To use the Device Posture service for this integration, we recommend configuring periodic device posture scans.

  Note:

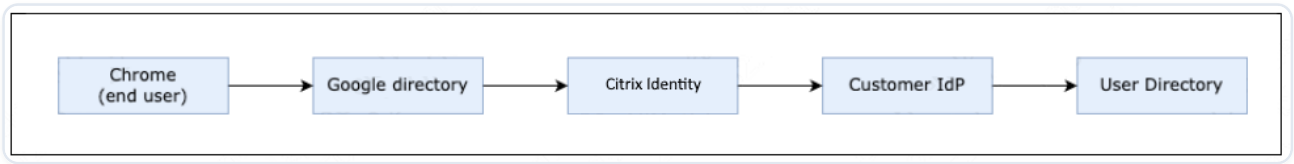
  This integration does not work when the Device Posture service is configured in multiple store mode.

  For more information about the Device Posture service, see Device Posture overview.

- **Unified sign-on experience:** While you can configure SSO for Chrome against most common identity providers, including but not limited to Active Directory (AD) and Microsoft Entra (formerly Azure AD), you can opt for a unified sign-on experience for both cloud stores and CEP.

Overview

OIDC enables SSO using Citrix Identity as an OIDC authentication provider. The components involved in OIDC are illustrated in the following diagram:



Google Chrome, when creating a managed profile, always tries to authenticate against the Google Directory. With OIDC, Google directory becomes essentially a relying party (RP) against Citrix Identity, which is an OIDC Connect Provider. In turn Citrix Identity enables the following:

- Device Posture capabilities
- A common and unified sign-in experience for Chrome and cloud stores.

Prerequisites

Before configuring the OIDC authentication with Citrix Identity, ensure that the following prerequisites are met:

- You have administrative access to the Google Admin console.
- You have configured and performed directory synchronization. For details, see Synchronize user directory configured in Citrix identity with the Google Cloud user directory.
- User identity provider (IdP) is set up and configured in Citrix Cloud Identity and Access Management. The following identity providers are supported:
  - Active Directory (AD) - Standard on-premises Active Directory integration
  - Active Directory with Token - AD integration with token-based authentication
  - Microsoft Entra ID - Cloud-based identity service (formerly Azure AD)
  - Okta
  - SAML 2.0

> **Note:**
>
> Single sign-on (SSO) for Chrome Enterprise Premium (CEP) that uses Citrix Cloud as the OpenID Connect (OIDC) authentication provider now supports conditional authentication.

- For more information about Citrix Cloud Identity and Access Management, see Identity and access management.

- You have configured how subscribers authenticate to their stores by selecting one of the previously mentioned Identity Providers. For instructions on how to Configure stores authentication, see Configure Authentication.
- You have already completed the initial setup and onboarding of Secure Private Access. For details, see Secure Private Access onboarding and set up.

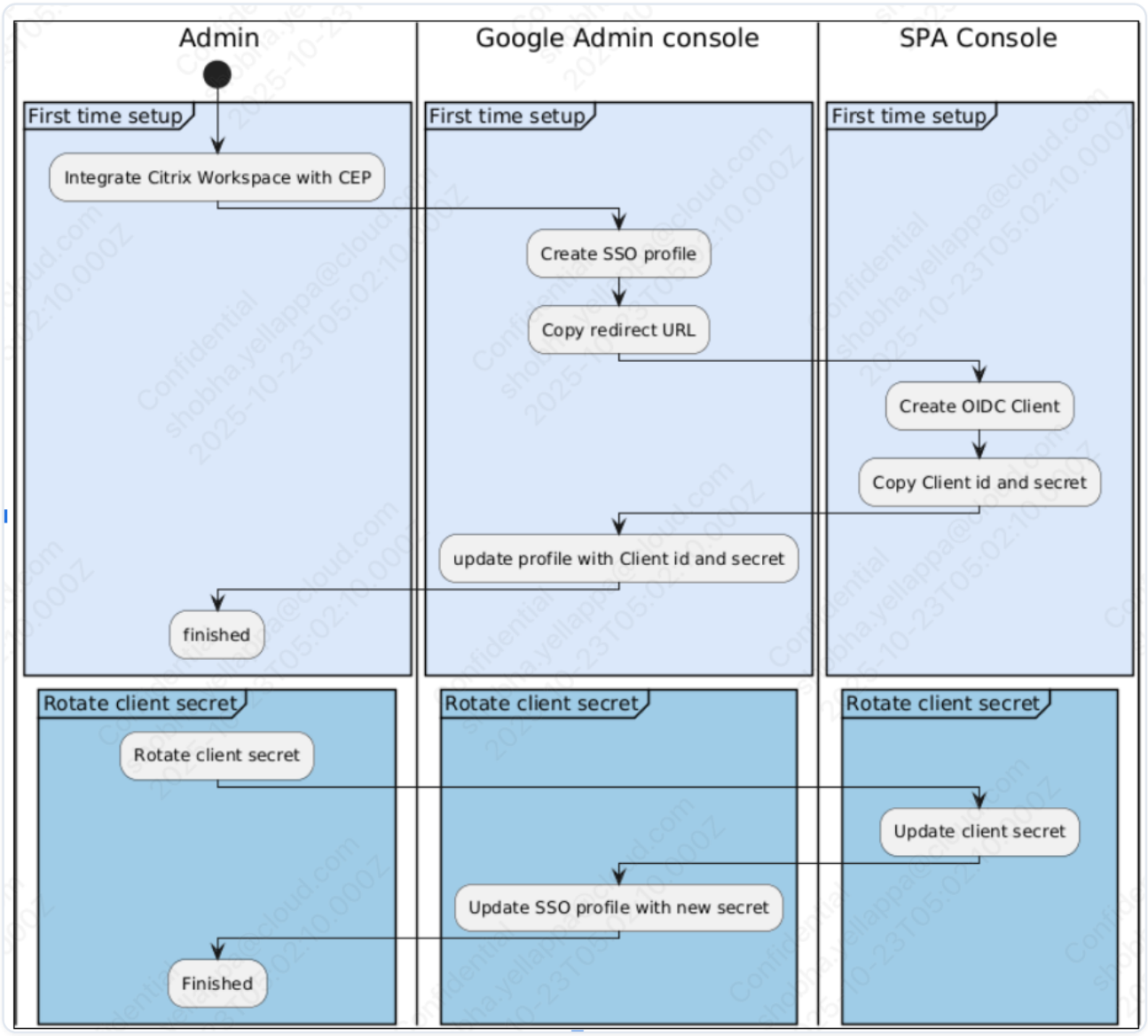
OIDC integration overview

To enable Google Chrome managed profile login to integrate with your configured Citrix Identity Provider, a Google OIDC SSO profile must be associated with a Citrix OIDC client. To do so, perform the following steps:

1. In the Google Admin console, create a new SSO profile by entering a profile name. You can leave the other fields blank for now. For details about creating a new SSO profile and redirect URL, see Create a Google OIDC SSO profile.
2. After the SSO profile is created, copy the redirect URL generated for this profile.
3. In the Secure Private Access console, create the Citrix OIDC client and paste the redirect URL (from the Google SSO profile) in the **Redirect URL** field. For details on creating a Citrix OIDC client, see Create a Citrix OIDC client.
4. Once the OIDC client is created, note the client ID, client secret, and issuer URL displayed in the Secure Private Access console.
5. Return to the Google Admin console and update the SSO profile with the client ID, client secret, and issuer URL from the Secure Private Access console.
6. In **Manage SSO profile assignments**, select the Google SSO profile you configured to complete the integration.

> **Note:**
>
> Post creation of the OIDC client, you can rotate the client secret in the Secure Private Access console and update the SSO profile in the Google Admin console.

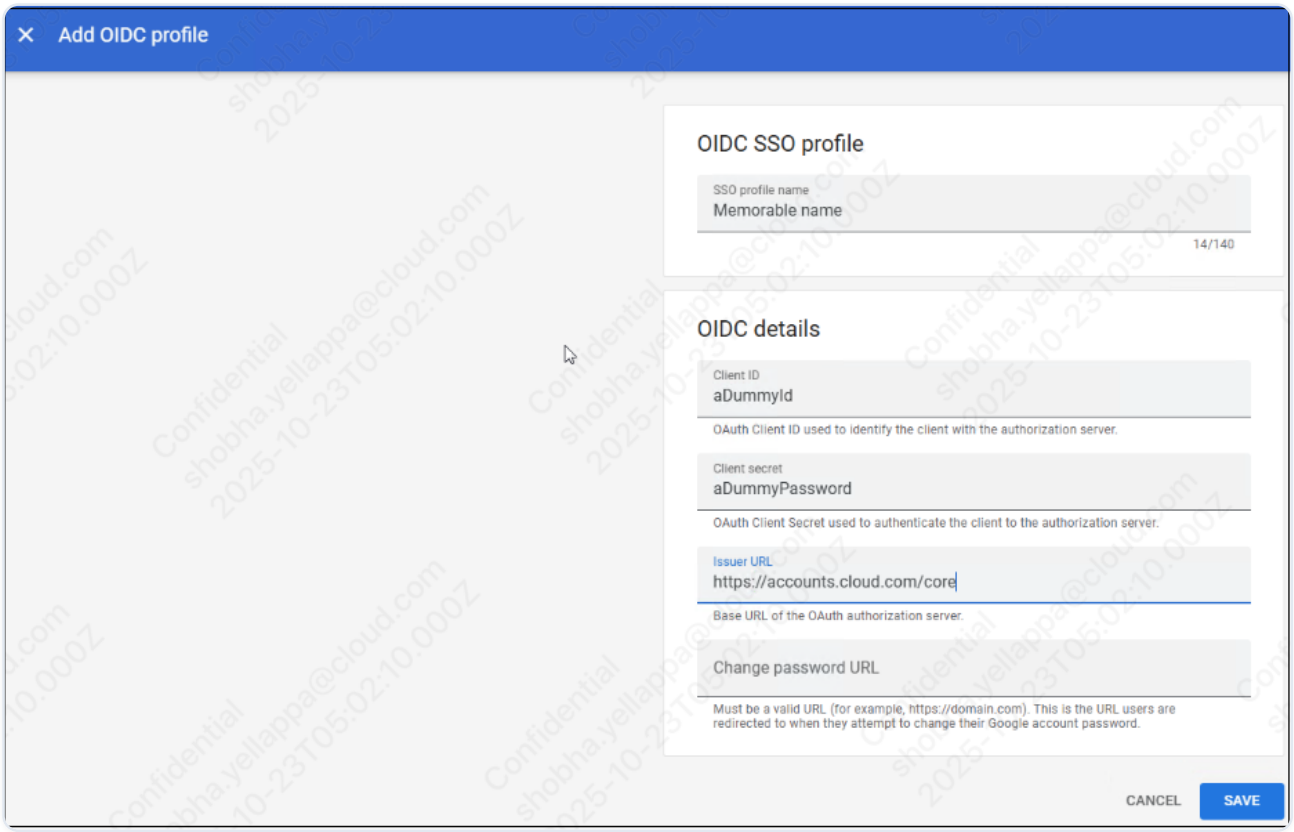
The following diagram illustrates the OIDC integration workflow:



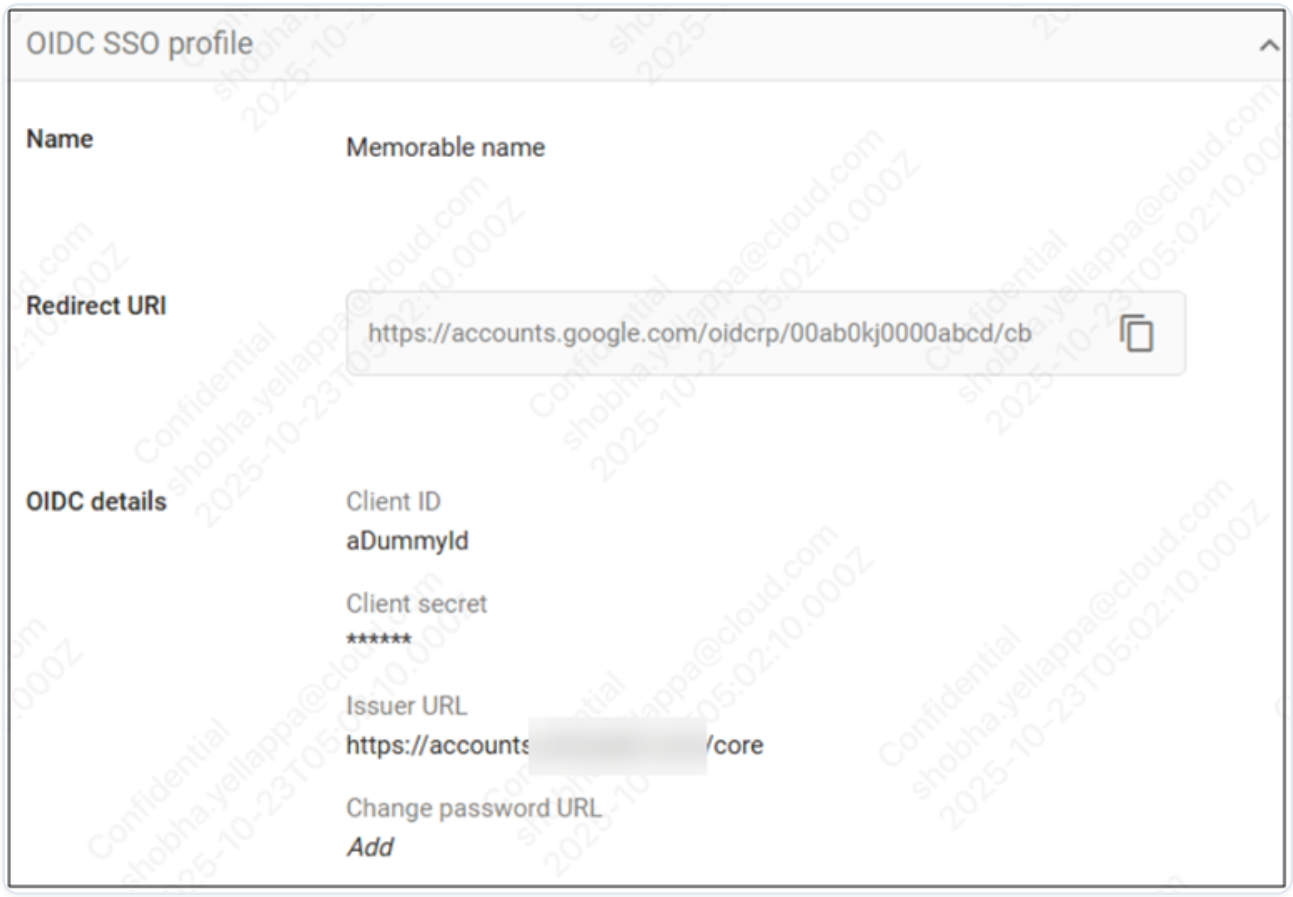
Create a Google OIDC SSO profile

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. Provide a name for the profile.
3. Assign a dummy value for client ID and client secret or leave these empty. These fields are updated later.
4. In **Issuer URL**, enter `https://accounts.cloud.com/core`.
5. Click **Save**.



After creating the profile, click it to obtain the redirect URI, which is needed for creating the OIDC client.



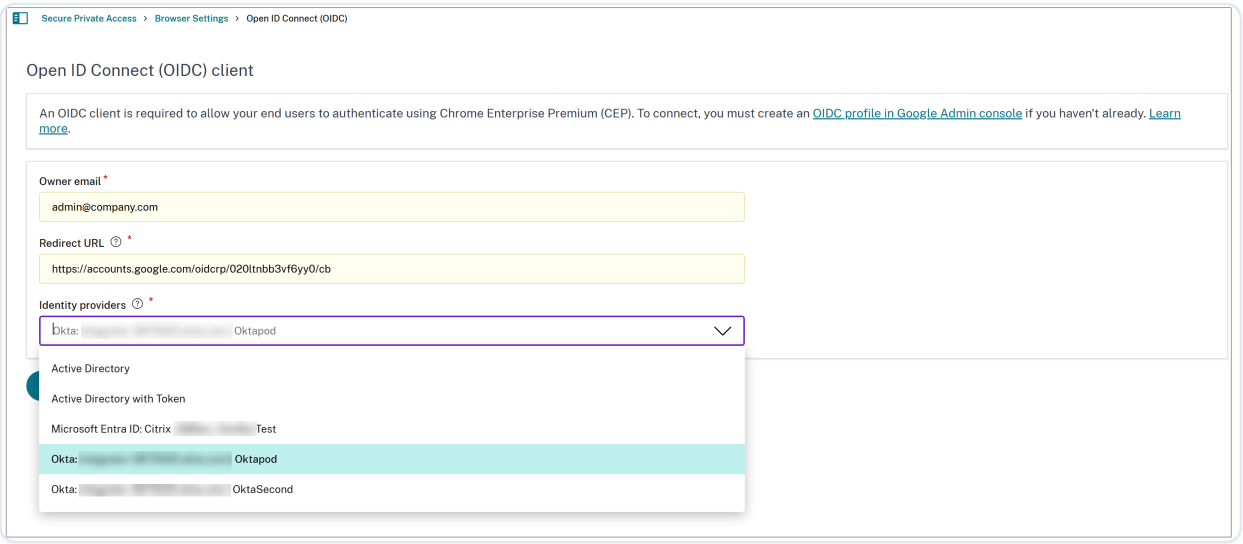
Create a Citrix OIDC client

Perform the following steps in the Secure Private Access admin console:

1. In the navigation pane, click **Browser Settings > Open ID Connect (OIDC)**.

   > **Note:**
   >
   > The **Open ID Connect (OIDC)** option in the **Browser settings** menu is available only after the onboarding process is completed.

2. In **Owner email**, enter the user's email ID address. This email ID address is required for sending alerts when the OIDC client secret expires.
3. In **Redirect URL**, enter the redirect URI that was generated in the Google Admin console when you created the Google OIDC SSO profile. The identity provider responds to user authentication requests using this URL.
4. Select the identity provider that is configured in your environment.
5. Click **Create**.



After successfully creating an OIDC client, a pop-up window displays the client ID, client secret, and issuer URL. You must copy these details to your Google Admin console configuration. You can retrieve the credentials by one of the following methods:

- Copying the values directly from the pop-up window
- Downloading the details as a CSV file for secure storage

> **Important:**

> The client secret is only visible during this initial setup step. You must retrieve the client secret before closing the pop-up window or proceeding to the next step. Once the window is closed, the client secret cannot be viewed again and you must rotate the secret to obtain a new one.

6. Click **Close**.

OIDC SSO profile assignment

Once the OIDC client is created and the Google OIDC SSO profile is updated with the Client ID and Secret, the OIDC SSO profile must be assigned to the users and groups for SSO to take effect.

1. In the Google Admin console, go to **Security > Authentication > SSO with 3rd party IdP**.
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 may assign the SSO profile to specific groups or OUs.

Update Citrix OIDC client

The Citrix OIDC client secret has a default lifetime of two years. You can maintain OIDC security, or respond to a potential security incident, by rotating the client secret. Client secret rotation is a critical security measure that must be performed when an existing secret is nearing its expiration or as part of proactive security maintenance. Each time you rotate a client secret, a new secret is generated. The old secret remains valid until its original expiration date, to ensure a smooth transition without an SSO authentication outage. Ensure to update your Google Admin console configuration with the new client secret as soon as possible after every rotation.

Perform the following steps to rotate the client secrets

1. In the admin console, click **Settings > Open ID Connect (OIDC) client** page.
2. Click **Rotate client secret** to generate a new secret. A confirmation message appears.
3. Enable the toggle switch to agree to the confirmation message, then click **Rotate**.

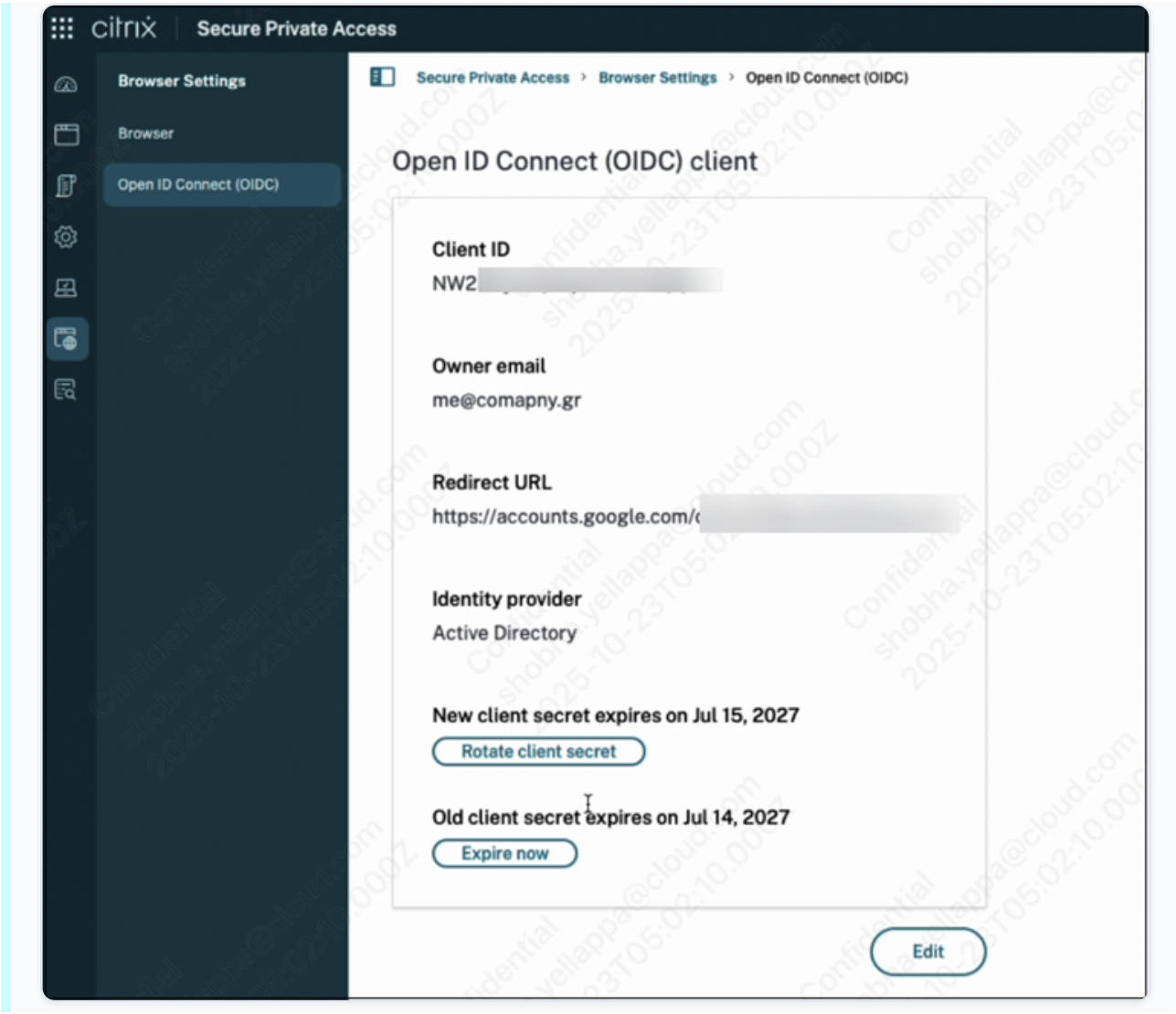
> **Note:**

- The old client secret remains valid until its expiration. This allows you to update Google Workspace without any authentication outage.
- If for security purposes you want to expire immediately, click **Expire now**.
- The Client ID remains unchanged during this process.

4. Click **Close**.
5. Update the new secret in your Google Workspace configuration immediately.

Important:

- You must update the new client secret in your Google OIDC SSO profile configuration prior to the previous secret's expiration to maintain uninterrupted OIDC authentication. Failure to update the secret in such a timely manner disrupts authentication and may cause access issues for users and services.
- Regular rotation of client secrets is recommended to mitigate unauthorized access risks and maintain authentication system integrity.
- Once you have updated the secret of the Google OIDC SSO profile, it's recommended that you expire the old secret.



Delete an OIDC client

A client secret cannot be rotated after it has expired. If the client secret expires before being rotated, it becomes invalid. In this case, you must delete the existing client and create a new one.

Perform the following steps in the Secure Private Admin console.

1. Click **Edit** in the Open ID Connect (OIDC) client page.
2. Click **Delete client**.

   A confirmation message appears.
3. Slide the toggle to ON and then click **Delete client**.

End user experience

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** - The native desktop application that provides the most secure and feature-rich access experience with full policy enforcement and single sign-on capabilities.
- **Store URL in a web browser** - Users can open their store in a web browser:
  - 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	STORE URL IN A WEB BROWSER	CITRIX WORKSPACE APP
Non-chrome browser	Access denied for SaaS apps (assuming that the SaaS apps have been configured with the appropriate IP address allow list).	Apps are enumerated in the user interface.	Not-applicable
	Private apps are unreachable.	The applications are launched in the appropriate Chrome managed profile.	
		A profile creation wizard is launched if the respective managed profile has	

	DIRECT	STORE URL IN A WEB BROWSER	CITRIX WORKSPACE APP
		not been created already.	
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
	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
Citrix Workspace app	Not-applicable	Not-applicable	Apps are enumerated in the user interface.
			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 extension for Chrome Enterprise Premium

The Citrix Secure Access 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.

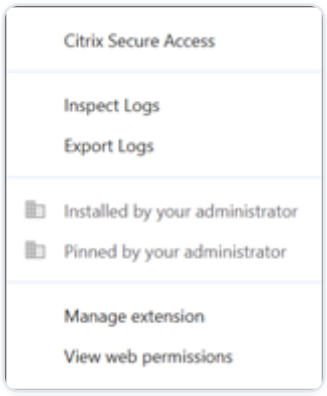


Secure Access extension logs

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.

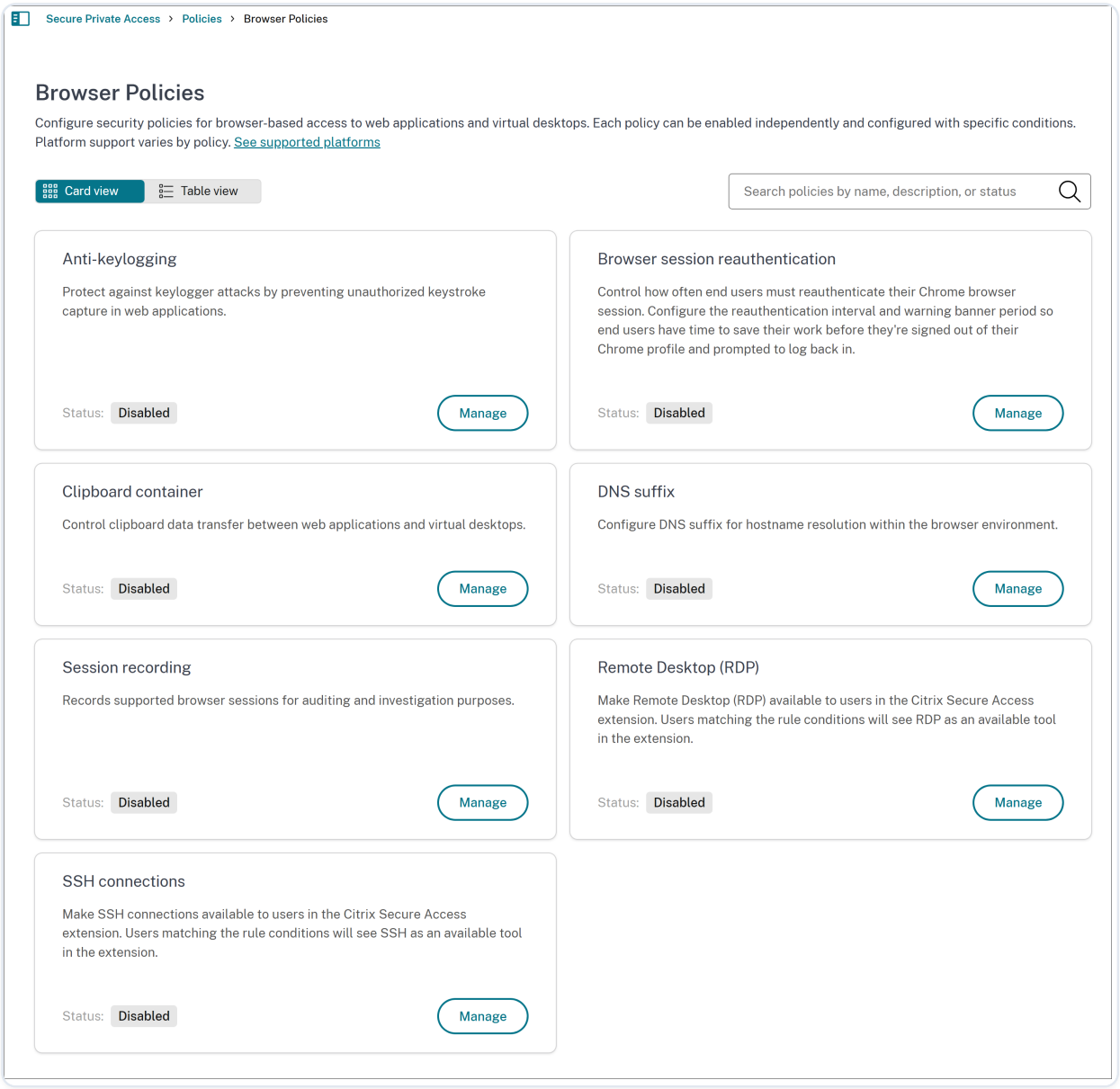


Citrix Secure Access controls for Chrome Enterprise

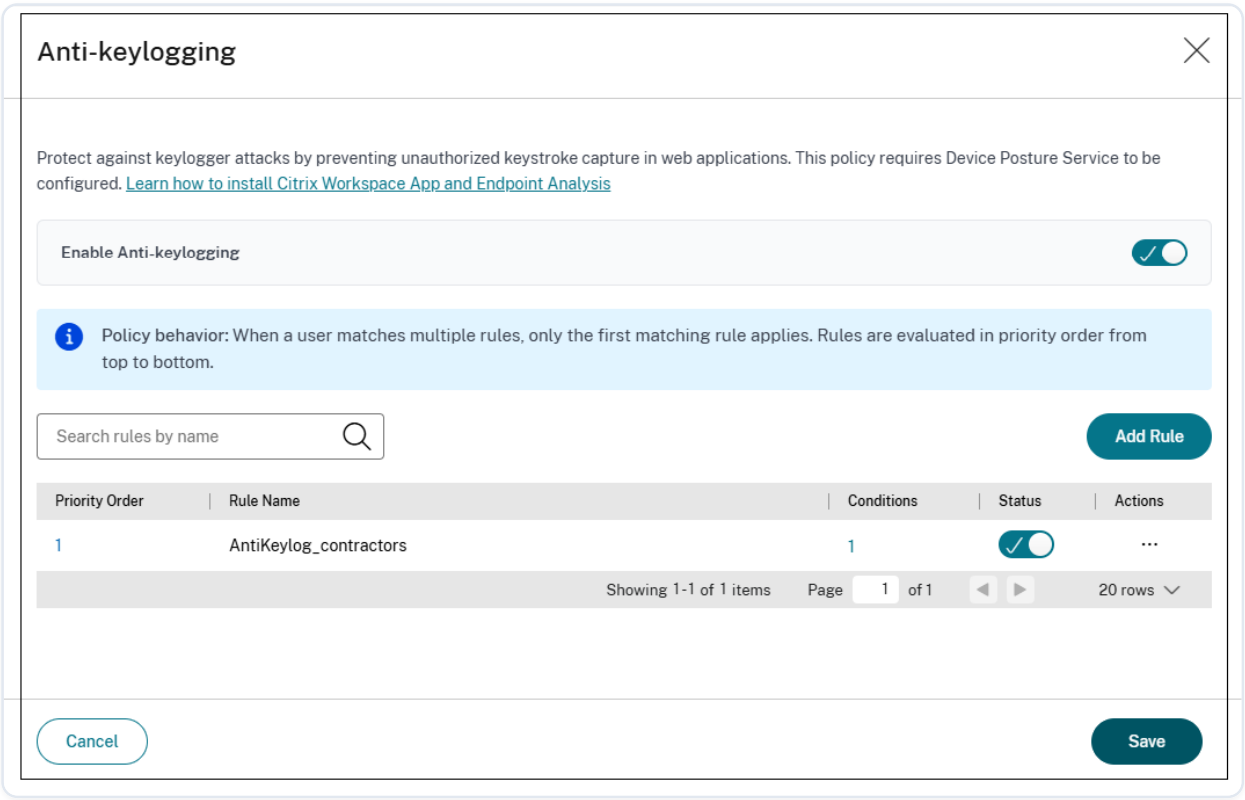
Citrix Secure Private Access supports security policies that are delivered to and enforced by the Citrix Secure Access extension for Google Chrome Enterprise Premium (CEP). For details, see Supported controls.

You can configure these policies from the Secure Private Access admin console.

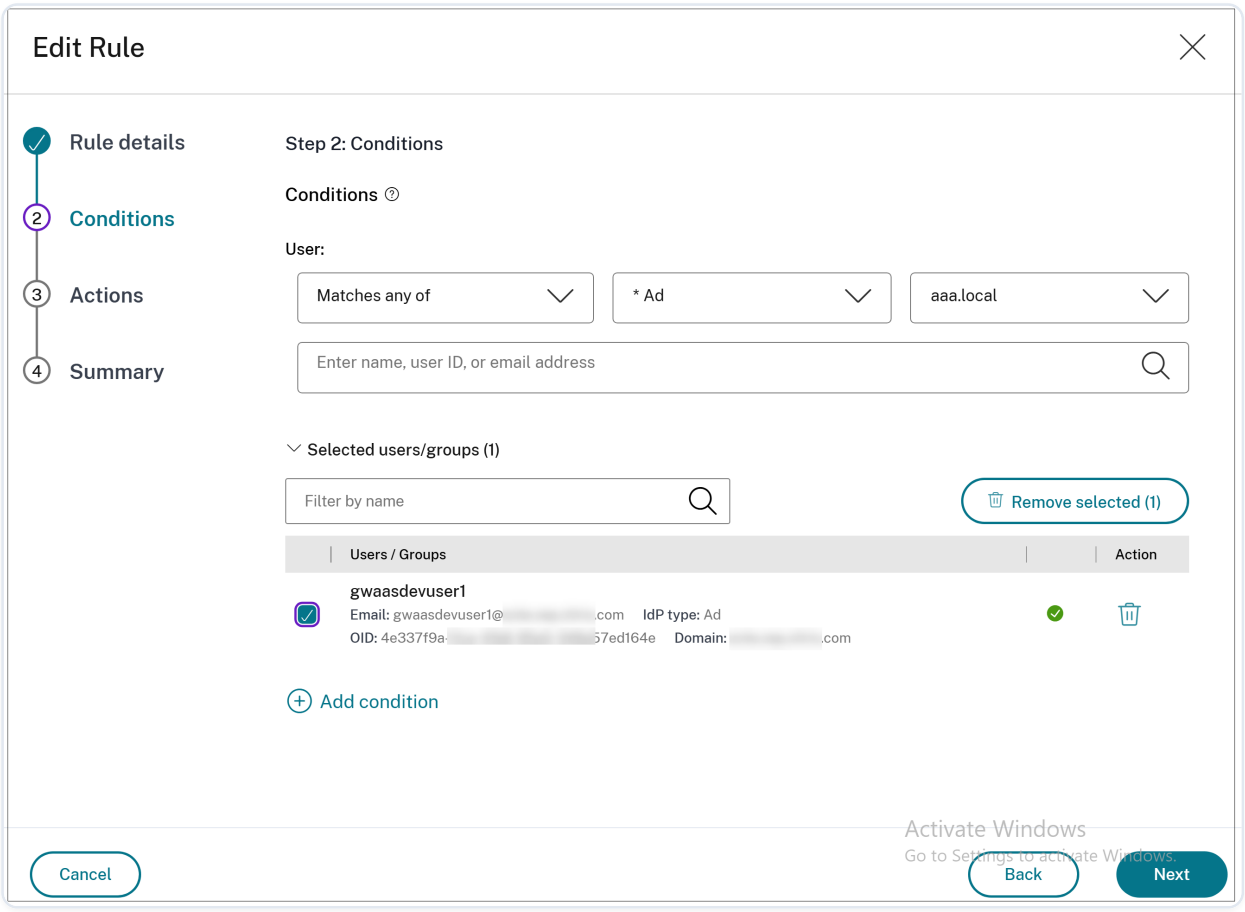
1. Go to **Policies > Browser policies**, and then click **Create browser policy**.
2. Select the policy and then click **Manage**.



3. Add rules for the policy.



4. Add an **Access Mode** condition to scope browser controls to browser sessions. For browser policies, the value is typically **Browser**. For more information about access modes, see Access mode-based policy enforcement.
5. Select the conditions for which the policy must be evaluated.



Note:

When selecting users or groups, administrators can verify whether entries from the selected user directory are synchronized with and correctly configured in Google Directory. Secure Private Access policies evaluate correctly only when they use synchronized users and groups. Otherwise, warnings might appear. For details, see Verify user and group synchronization.

For detailed configuration steps, see the documentation for each control.

Supported controls

Citrix supports the following Secure Access controls with the Secure Private Access and Chrome Enterprise Premium integration:

CONTROL	WHAT IT DOES
Anti-keylogging	Obfuscates keystrokes to prevent keylogger malware on the endpoint from capturing user input.
Clipboard container	Controls what users can copy and paste between the browser and other apps.
DNS suffix	Automatically completes short internal URLs (like “wiki/”) into full addresses.
Session recording	Records browser session activity for audit and compliance.
Browser session reauthentication	Enforces periodic re-authentication of browser sessions after a configured time interval.
SSH connections	Enables users to establish SSH connections directly within a browser tab, without requiring a terminal client.
Remote Desktop (RDP)	Enables users to launch Remote Desktop sessions directly within a browser tab, without requiring an RDP client.

Users and groups in policies

The following sections provide more information about users and groups:

Search for users or groups

The users and groups that you select appear in a grid. Each row in the grid displays the following identity details so that you can clearly distinguish between identically named users or groups across different domains, forests, or identity providers (IdPs):

- **Name** – The display name of the user or group.
- **Email** – The email address associated with the identity.
- **IDP type** – The identity provider, such as Azure AD, Active Directory, Okta, or Google.
- **OID** – The object ID or security identifier of the identity.
- **Domain** – The domain to which the user or group belongs.

You can filter the grid by name, remove individual rows, or select multiple entries and remove them together using **Remove selected**.

Use synchronized users and groups

When selecting users or groups, administrators can verify whether entries from the selected user directory are synchronized with and correctly configured in Google Directory. Secure Private Access policies evaluate correctly only when they use synchronized users and groups. Otherwise, the following warnings might appear:

- **Missing tenant account privileges.**

  Remediation: In the Google Admin console, assign the **Users > Read** and **Groups > Read** privileges to the tenant service account. SPA requires these privileges to verify that a user or group exists.

- **User or group not synchronized.**

  Remediation: The searched or selected user or group is not synchronized with Google Directory. Synchronize the directory entity with Google Directory before using it in an SPA policy.

- **Insufficient group access settings.**

  Remediation: In the Google Admin console, open the access settings for the selected group and make sure the **Who can view members** has at least the **Group members** option selected.

> **Note:**
>
> This feature is available only after the Google Chrome integration is successfully completed.

Anti-keylogging control

Cybercriminals use malicious software such as keyloggers to steal sensitive information, such as passwords, credit card numbers, and confidential company data.

The Citrix Secure Access browser extension for Chrome Enterprise Premium (CEP) supports anti-keylogging to help protect your data. This feature scrambles keystrokes so that if a malicious program attempts to capture typed input, it records only unreadable characters while the actual text is securely delivered to your work applications.

Supported deployments: Citrix Secure Private Access service and hybrid deployments.

Supported platforms: Windows 11 and later.

> **Note:**
>
> Anti-keylogging is not supported for native RDP sessions.

Prerequisites

Ensure that the following prerequisites are met before enabling anti-keylogging:

- CWA version 2603 and later is installed.
- Integration between Citrix Secure Access and Chrome Enterprise Premium (CEP) is complete.

Configure the anti-keylogging policy

1. Log in to the Secure Private Access admin console.
2. Go to **Policies > Browser Policies**, and then click **Create browser policy**.
3. Select **Anti-keylogging**, and then click **Manage**.
4. Click **Add Rule** to add rules for the users to enable anti-keylogging.
    a. Enter the name for the rule and click **Next**.
    b. Select conditions based on your requirement such as user or group. You can also add conditions such as **Geo-location**, **Network location**, and **Device posture check**.
    c. Click **Next**.
5. Click **Save**.

    The number of rules configured for the anti-keylogging policy appears in the **Browser Policies > Anti-keylogging** tab.

Clipboard container control

Deployments that use Chrome for web access and VDI for native applications can use the Clipboard container feature to control data sharing between the browser and VDI sessions. Clipboard data is transferred directly between Citrix sessions without being written to the local endpoint clipboard. This improves security while still giving users flexibility to work across both environments.

Supported deployments: Secure Private Access service and hybrid deployments.

Supported platforms: Windows.

Prerequisites

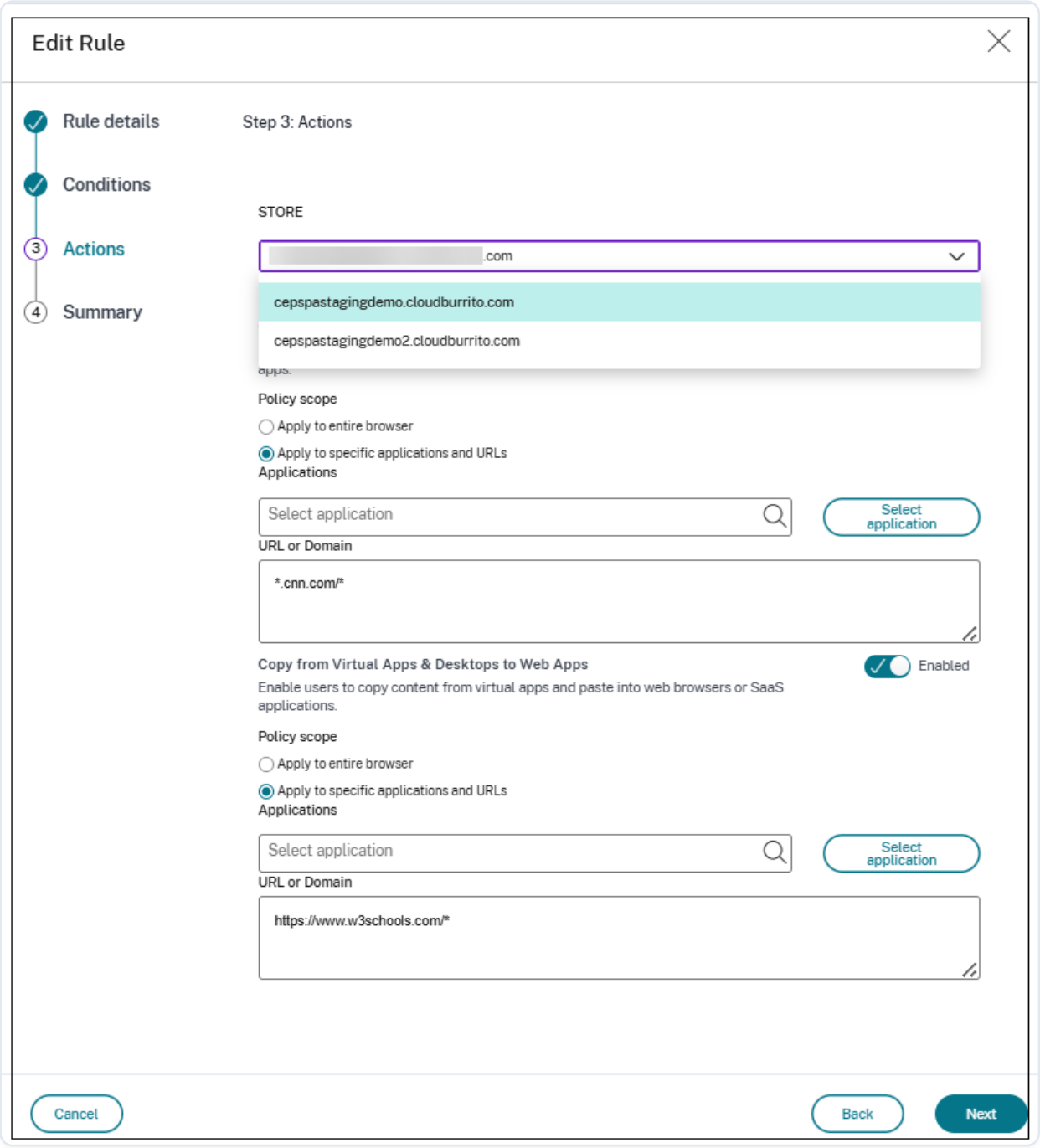
Ensure that the following prerequisites are met:

- Integration between Citrix Secure Access and Chrome Enterprise Premium (CEP) is complete.
- Citrix Workspace app 2603.10 or later.
- Windows VDA running 2607 LTSR or later (GA version for Clipboard Sharing Scope). For details, see Clipboard Sharing Scope.
- Windows VDA running 2507 LTSR (Preview version for Clipboard Sharing Scope), enable the following:
  - **Cross clipboard container with DaaS** feature. For details, see Cross clipboard container with DaaS. This feature is currently available as a preview in DaaS.
  - **Clipboard Sharing Scope** registry. For details, see Enable the Clipboard Sharing Scope registry.

Enable Clipboard Container control

1. Log in to the Secure Private Access admin console.
2. Go to **Policies > Browser Policies**, and then click **Create browser policy**.
3. Select **Clipboard container**, and then click **Manage**.
4. Click **Add Rule** to add rules for the clipboard share between VDA and browser.
   a. Enter the name for the rule and click **Next**.
   b. Select conditions based on your requirement such as user or group. You can also add conditions such as **Geo-location**, **Network location**, and **Device posture check**.
   c. Click **Next**.
   d. Define the URL and Secure Private Access applications to allow clipboard sharing.
   e. Select the policy scope.
      - **Apply to entire browser** — The policy governs all clipboard activity in the managed profile.
      - **Apply to specific applications and URLs** — The policy is limited to selected applications and the URL/domain patterns entered.

- **Select Application** — Select the specific published applications using the application picker.
- **URL or Domain** - Enter the URL or the domains of the specific application.



5. Click **Save**.

   The number of rules configured for the clipboard container policy appears in the **Browser Policies > Clipboard container** tab.

Enable Clipboard Sharing Scope

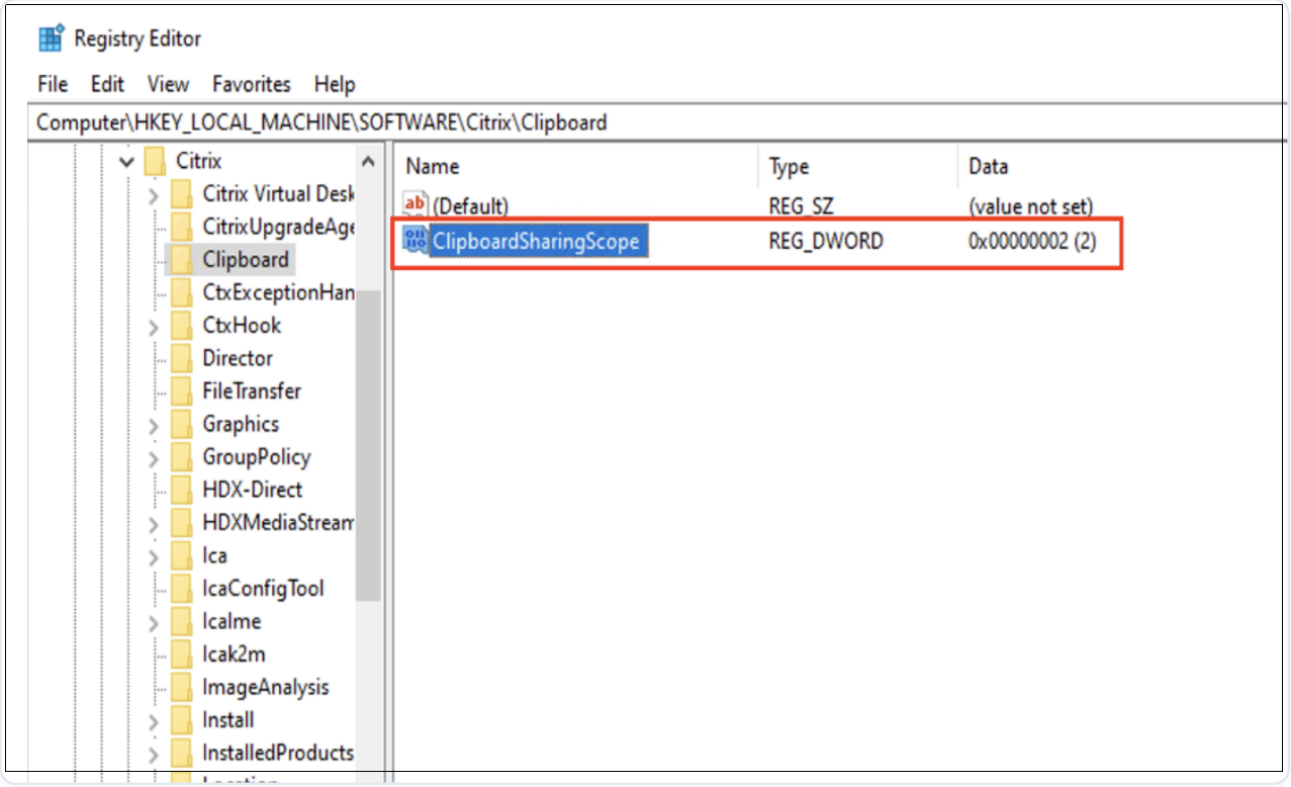
For VDA version 2607:

See How it works.

For VDA version 2507:

Enable this registry **Clipboard Sharing Scope** registry.

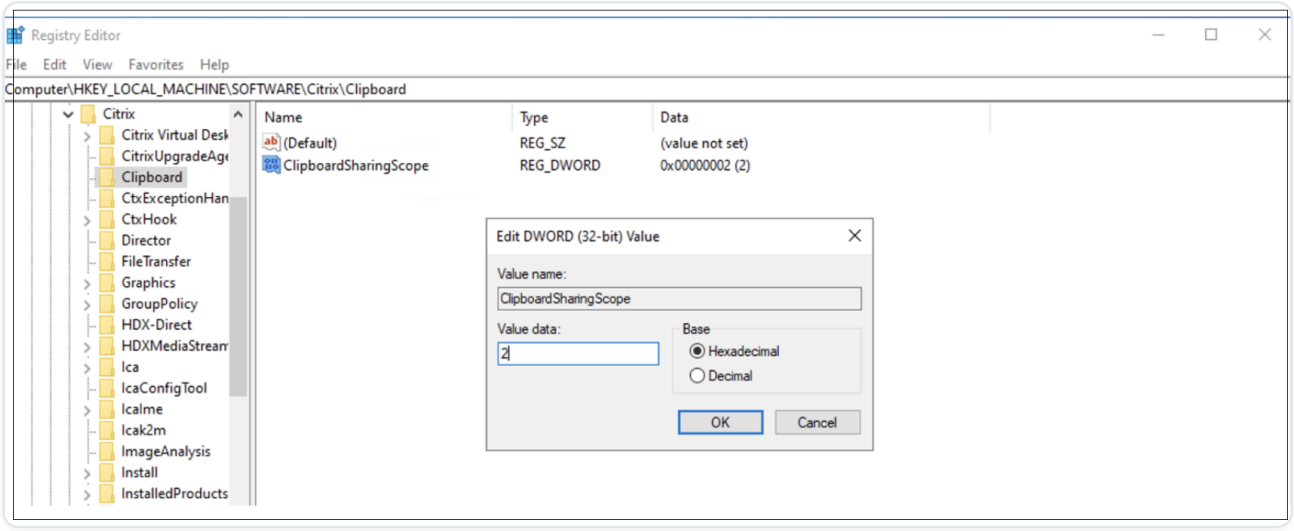
1. Open the Windows Registry Editor using regedit.exe.
2. Navigate to HKEY_LOCAL_MACHINE\Software\Citrix\Clipboard\.
3. Create a REG_DWORD value named `ClipboardSharingScope`.



The `ClipboardSharingScope` policy controls where VDA clipboard data can be shared. Until the new DDC policy is available, this setting can be configured using the preceding registry key.

SUPPORTED VALUE	SCOPE	DESCRIPTION
0	Unlimited	Clipboard data is copied to the client system clipboard and can be accessed by the Client, VDA, and CEP.
1	VDA only	Clipboard data is accessible only to the VDA. The client system clipboard and CEP cannot access the clipboard content.

SUPPORTED VALUE	SCOPE	DESCRIPTION
2	CEP only	Clipboard data is accessible only to CEP. The client system clipboard and VDA cannot access the clipboard content.
3	VDA and CEP	Clipboard data is accessible to both the VDA and CEP. The client system clipboard cannot access the clipboard content.



Note:

- The CEP only (2) and VDA and CEP (3) modes are designed to work with the Clipboard Container feature in the CEP extension.
- When the Clipboard Container policy is enabled, only administrator-configured URLs are allowed to exchange clipboard data with the VDI.

```
>-  Content copied from the approved web applications can be pasted into
the VDI.

>-  Content copied from the VDI can be pasted only into administrator-
configured, paste-allowed URLs.
```

```
>-  If a user attempts to paste VDI clipboard content into a website that
is not included in the policy, the paste operation is blocked and an error
message appears.
```

Domain suffix for web applications

In scenarios where users enter short, internal host names in the browser (for example, `sw` or `server001`), the domain suffix feature automatically appends the DNS suffix and converts them into Fully Qualified Domain Names (FQDNs) using browser-managed DNS suffix policies instead of relying on the operating system's DNS suffix configuration.

The DNS suffix feature is supported on both **Windows** and **macOS** platforms, and consistently applies across common URL entry formats, including:

- `sw`
- `http://sw`
- `https://sw/`
- `sw/`
- `http://sw/`
- `https://sw/`

Supported deployments: Secure Private Access service and hybrid deployments.

Supported platforms: Windows and macOS.

Prerequisites

Ensure that the integration of Citrix Secure Access with Chrome Enterprise is configured. For details, see Integration with Google Chrome Enterprise Premium.

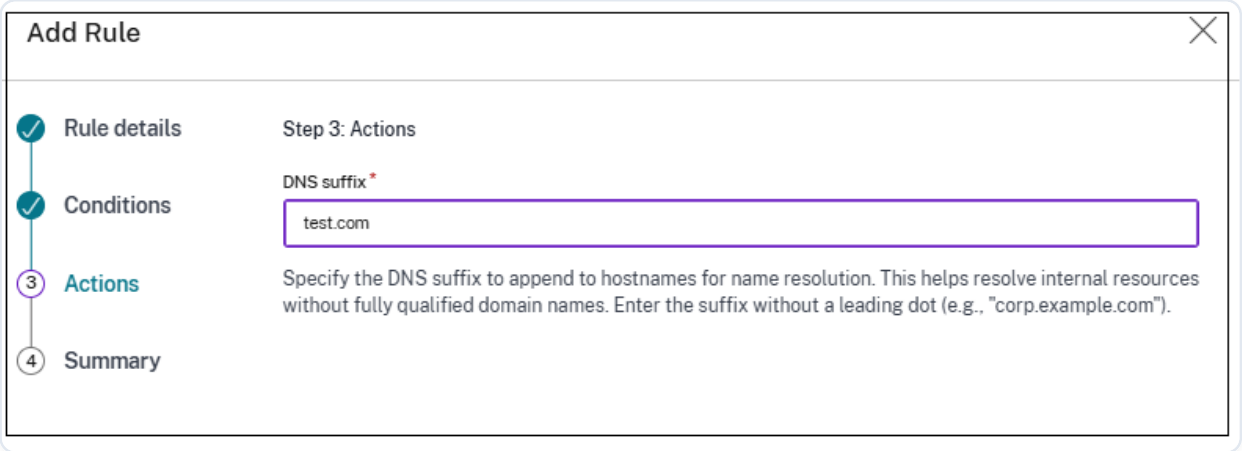
Configure DNS suffix

1. Log in to the Secure Private Access admin console.
2. a. Go to **Policies > Browser Policies**, and then click **Create browser policy**.
3. Select **DNS suffix**, and then click **Manage**.
4. Click **Add Rule** to add rules for the domain to be added to your URL.
    a. Enter the name for the rule and click **Next**.

b. Select conditions based on your requirement such as user or group. You can also add conditions such as **Geo-location**, **Network location** and **Device posture check**.

c. Click **Next**.

d. Define the domain that you want to append for access.



5. Click **Save**.

   The number of rules configured for the DNS suffix policy appears in the **Browser Policies > DNS suffix** tab.

Session recording control

Session recording records, catalogs, and archives sessions for retrieval and playback.

Session recording offers the following key benefits:

- Provides flexible policies to trigger recordings of application and desktop sessions automatically.
- Enables IT personnel to monitor and examine user activity, and supports internal controls for regulatory compliance and security monitoring.
- Aids technical support by speeding up problem identification and reducing time-to-resolution.

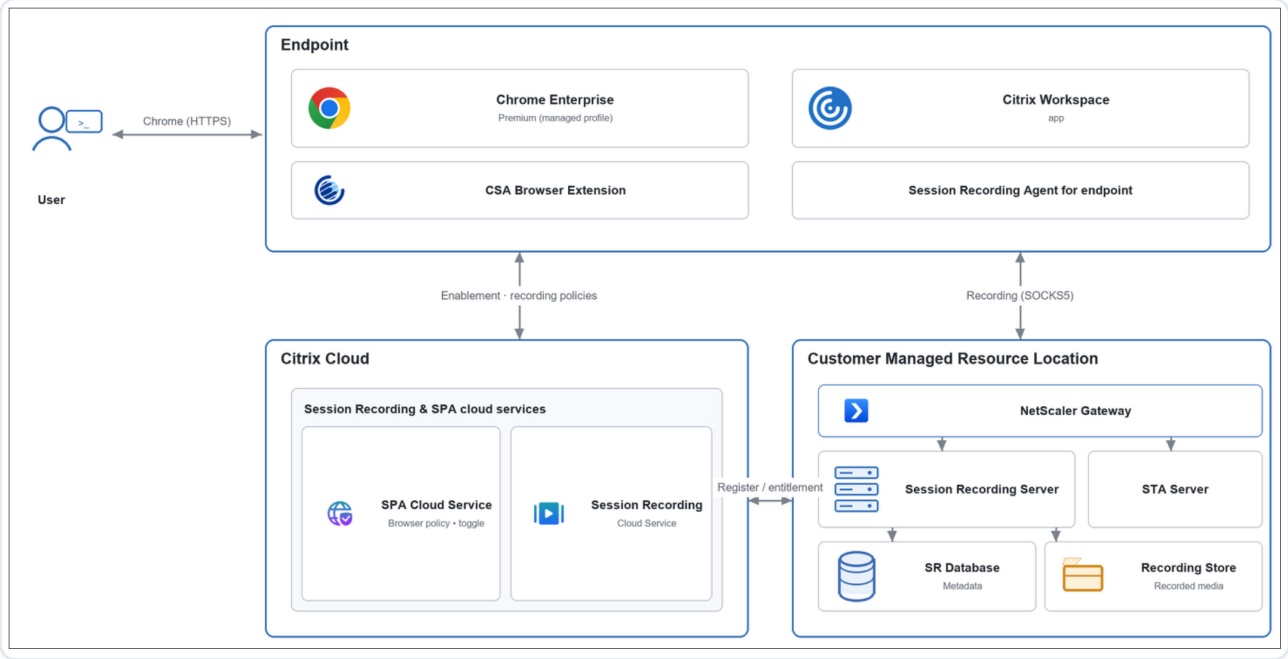
For details, see Benefits.

Architecture

The session recording solution spans three planes:

- The endpoint with the managed Chrome profile, Citrix Secure Access extension, and Session Recording Agent for endpoints.

- The Citrix Cloud control plane, which houses the Secure Private Access and Session Recording cloud services.
- The customer-managed resource location, which encompasses NetScaler Gateway, the STA server, the Session Recording server, and its database and recording stores.



Prerequisites

- Citrix Workspace app for Windows 2603.10 or later
- Endpoint analysis (EPA) version: 26.5.1.7 and later

System requirements

- Citrix Secure Private Access, deployed in either service or hybrid mode combined with Chrome Enterprise Premium (with managed profile).
- Session Recording Cloud service with Session Recording server 2511 or later. For details, see Get started.
- Windows 64-bit or 32-bit endpoints with the following components:
  - Citrix Endpoint Analysis (EPA) plug-in 26.5.1.7 or later.
  - Citrix Workspace app for Windows, version 2603.10 or later, with the Session Recording Endpoint Agent installed

Set up the environment

Complete the following steps to enable and validate endpoint recording for Chrome Enterprise sessions.

Configure the Session Recording site

Follow the steps documented in Configure endpoint recording policies.

> **Note:**
>
> NetScaler Gateway is required for endpoint recording. It routes recording traffic to the Session Recording Server through the STA in both Secure Private Access deployment types. Even with the Secure Private Access service, where NetScaler does not manage user-to-application access, you must provide a gateway URL for recording traffic.

Configure the Session Recording browser policy in Secure Private Access

1. Log in to the Secure Private Access admin console.
2. Go to **Policies > Browser Policies**, and then click **Create browser policy**.
3. Select **Session recording**, and then click **Manage**.
4. Click **Add Rule**, enter a name for the rule, and then click **Next**.
5. Set the conditions (users and groups). (Optional) Add **Geo-location**, **Network location** and **Device posture check**, and then click **Next**.
6. Click **Save**. The rule count appears on the **Browser Policies > Session recording** tab.

Install the Workspace App with Session Recording Agent for endpoints

Follow the steps documented in Session Recording add-on support.

Replay recorded sessions

Recordings are viewable in the Session Recording console.

- All windows associated with the user's Chrome work profile are recorded.
- Multiple windows across one or more monitors are recorded.
- Windows that are out of focus or obscured by another application are still recorded in their entirety.
- Minimized windows and windows with anti-screen capture enabled appear as black rectangles during playback.

Best practices

- **Keep one global site**. Use a single global endpoint-recording site and document the configuration. Changing it can unintentionally disable the other sites' configured policies.

- **Align regions**. Keep the Session Recording cloud service URL, cloud client, and back end in the same Citrix Cloud region to avoid latency and data-residency issues.
- **Plan storage**. Full-screen web/SaaS recording can be storage-intensive. Size the server, Session Recording database, and recording storage accordingly, and monitor storage consumption closely.
- **Validate entitlement and roles first**. Mismatched Citrix DaaS and Citrix Secure Private Access entitlements are the most common cause of deployment failure. Confirm that a single active customer record exists and that the required administrative roles are assigned before enabling policies.

Browser session reauthentication control

Citrix Secure Private Access allows administrators to enforce session timeout policies for Chrome Enterprise Premium (CEP) browser sessions. Users are required to re-authenticate after a configured session duration, regardless of browser activity. This strengthens Zero Trust access controls for applications accessed through the Google Chrome work profile.

Once a session expires, users must re-authenticate with enterprise credentials and multifactor authentication (MFA). Successful reauthentication restores their last active page and restarts the session timer.

Supported deployments: Secure Private Access service and hybrid deployments.

Supported platforms: Windows, macOS, Linux, ChromeOS.

Prerequisites

Ensure that the following prerequisite is met:

- Integration between Citrix Secure Access and Chrome Enterprise Premium (CEP) is complete.

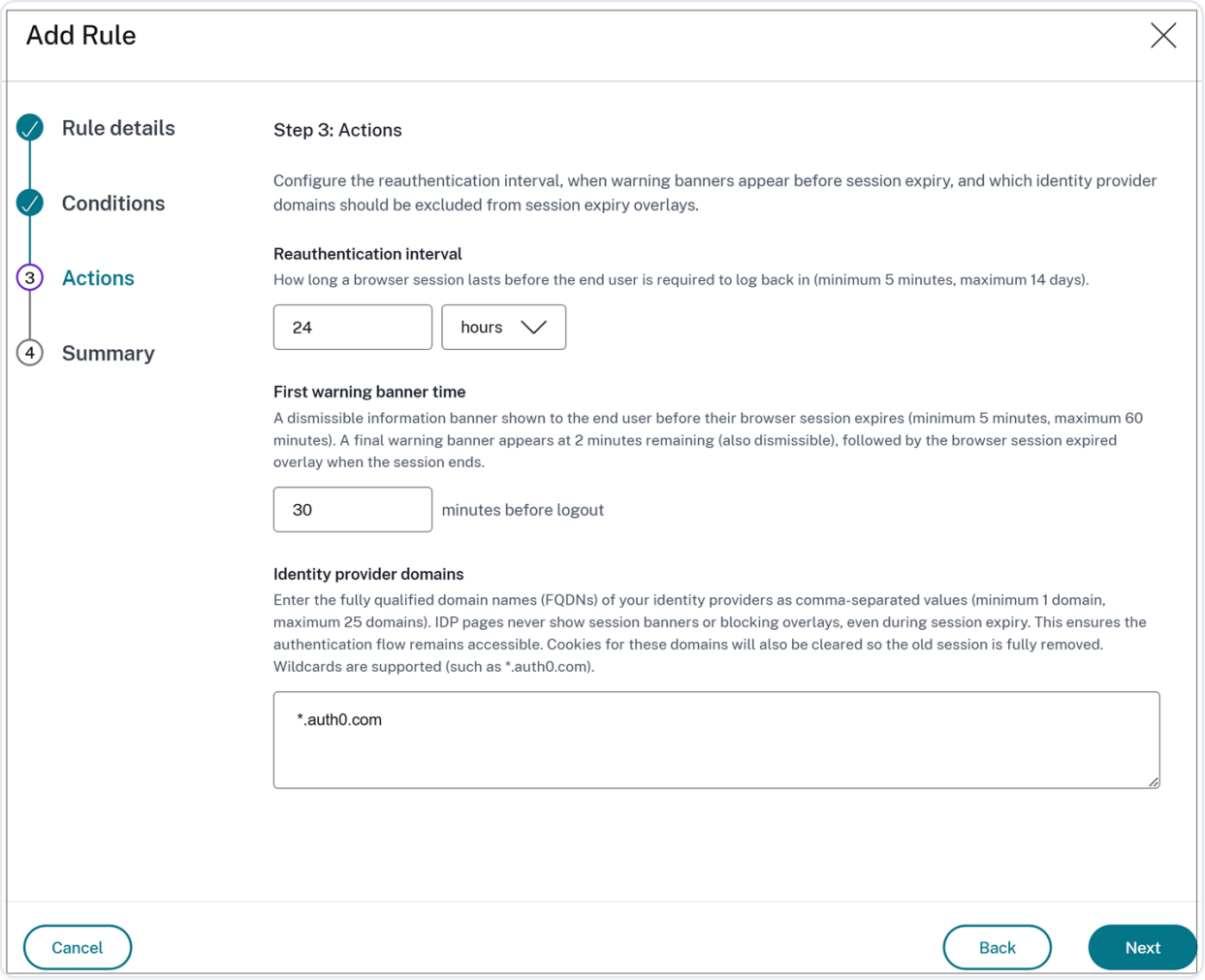
Enable Browser session reauthentication control

1. Log in to the Secure Private Access admin console.
2. Go to **Policies > Browser Policies**, and then click **Create browser policy**.
3. Select **Browser session reauthentication**, and then click **Manage**.
4. Click **Add Rule** to add rules to enable browser session reauthentication.
    a. Enter the name for the rule and click **Next**.
    b. Select conditions based on your requirement such as user or group. You can also add conditions such as **Geo-location**, **Network location**, and **Device posture check**.

c. Click **Next**.

d. Configure the following:

- **Reauthentication interval**: The duration of a browser session before the user is required to re-authenticate. The interval can be set between 5 minutes and 14 days, and configured in minutes, hours, or days.
- **First warning banner time**: A dismissible warning banner to be displayed to the user before their browser session expires. The value can be set between 5 and 60 minutes before expiry. A second warning banner appears when 2 minutes are left, followed by a session-expired overlay when the session ends.
- **Identity provider domains**: The fully qualified domain names (FQDNs) of your identity providers as comma-separated values. You can specify between 1 and 25 domains. Session banners and blocking overlays are suppressed on IdP pages to ensure that the authentication flow remains uninterrupted. Cookies for these domains are cleared when the session expires to ensure that the old session is fully removed. Wildcards are supported (for example, *.auth0.com).



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

The number of rules configured for the clipboard container policy appears in the **Browser Policies > Browser session reauthentication** tab.

SSH control

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

Configure the SSH policy

1. Log in to the Secure Private Access admin console.
2. Go to **Policies > Browser Policies**, and then click **Create browser policy**.
3. Select **SSH**, and then click **Manage**.
4. Click **Add Rule** to add rules for the users to enable SSH.
5. Enter the name for the rule and click **Next**.
6. Select conditions based on your requirement such as user or group. 1. You can also add conditions such as **Geo-location, Network location**, and **Device posture check**.
7. Click **Next**.
8. Click **Save**.

The number of rules configured for the anti-keylogging policy appears in the **Browser Policies > SSH** tab.

Remote Desktop control

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

Configure the remote desktop policy

1. Log in to the Secure Private Access admin console.
2. Go to **Policies > Browser Policies**, and then click **Create browser policy**.
3. Select **Remote Desktop**, and then click **Manage**.
4. Click **Add Rule** to add rules for the users to enable remote desktop.

5. Enter the name for the rule and click **Next**.
6. Select conditions based on your requirement such as user or group. 1. You can also add conditions such as **Geo-location, Network location**, and **Device posture check**.
7. Click **Next**.
8. Click **Save**.

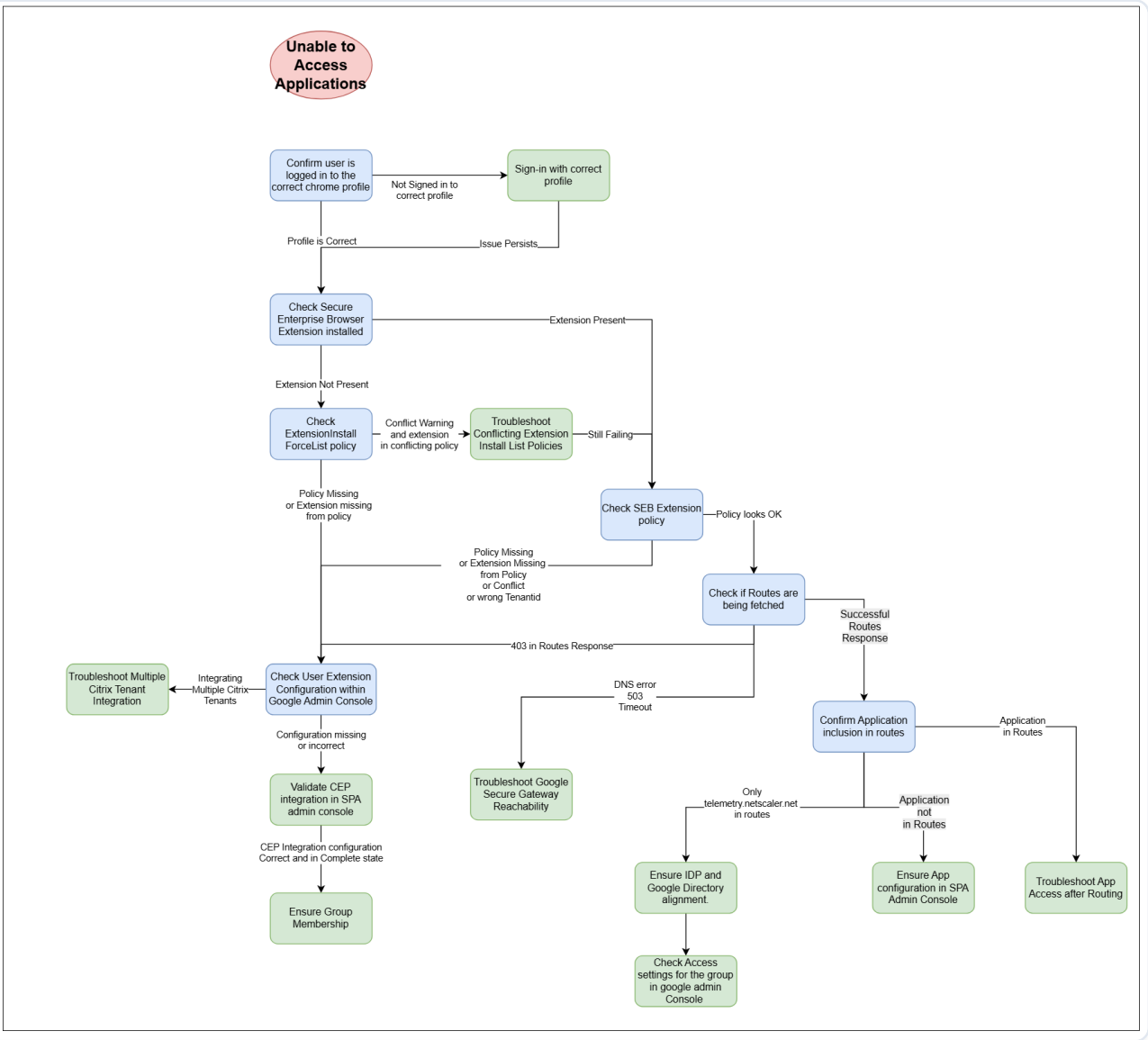
The number of rules configured for the anti-keylogging policy appears in the **Browser Policies > Remote desktop** tab.

Troubleshoot CEP integration issues

This article provides a troubleshooting workflow for customer admins who have completed Chrome Enterprise Premium (CEP) integration with Citrix Secure Private Access and are unable to access applications.

Basic assumptions:

- The customer administrator has completed directory synchronization with Google Directory.
- The customer has successfully completed Chrome Enterprise onboarding in Secure Private Access.
- Applications and access policies are configured in the Secure Private Access admin console to allow access to the relevant applications for the user or a group the user belongs to.
- The user is logging in to the onboarded domain.
- The browser has internet connectivity.



Diagnostic logs for CEP troubleshooting

To streamline investigation, collect the following diagnostic information before opening a support case and include it with every submission.

1. Export Chrome policies.
    a. Open Chrome and navigate to chrome://policy/.
    b. Click **More Actions** and then select **Export to JSON**.
    c. Attach the exported file to your support case.
2. Enable Verbose Logging for the Secure Enterprise Browser extension.
    a. Click the ellipsis icon next to the Secure Enterprise Browser extension.
    b. Click the options and then set **Log level** to **All**.

c. Close and reopen Chrome.

d. Go back to the extension options (ellipsis icon), and then click **Download the log**.

3. Collect the extension Log.

a. Close and reopen Chrome.

b. Repeat step 2 to access the **Extension** options, then click **Download the log**.

c. Attach the downloaded file to your support case.

4. Capture a network log.

a. In Chrome, navigate to chrome://net-export/ and click **Start Logging to Disk** (the default file name is chrome-net-export-log.json).

b. Access a few SaaS and web applications, then return to chrome://net-export/ and click **Stop Logging**.

c. Attach the resulting file to your support case.

Confirm that user is logged in to the correct Chrome profile

How to check: On the top right corner of the Chrome browser, click the profile icon. It must show the correct user and correct domain for the profile through which you intend to access your applications.

Also, ensure that the profile doesn't show **Paused** or **Click to Sign-in**. If it does, you must re-authenticate.

- **Profile is correct and authenticated:** Proceed to Check Secure Enterprise Browser Extension installed.
- **Profile is incorrect or not authenticated:** Log in or re-authenticate with the correct profile. Ensure that the domain suffix of the user's email aligns with the domain of the Google Admin account that is installed with Secure Private Access.

Check Secure Enterprise Browser extension installed

How to check: On the top right corner of the Chrome browser, there must be a green shield icon that corresponds to the Secure Enterprise Browser extension. You might need to click the jigsaw puzzle piece to see all the extensions.

- **Extension present:** Proceed to Check Secure Enterprise Browser Extension policy.
- **Extension not present:** Proceed to Check ExtensionInstallForcelist policy.

Check ExtensionInstallForcelist policy

How to check: Navigate to chrome://policy and under **Chrome Policies** look for a policy named **ExtensionInstallForcelist**. Click **show more** at the end of the corresponding row to see the details of the policy.

Within this force list, you expect to see an extension with the ID: `ekajlcmdfcigmdbphhifahdfjbkciflj`. This corresponds to the Secure Enterprise Browser extension.

It is possible that you are presented with a warning suggesting that there are two conflicting policies.

- **Conflict warning and extension in conflicting policy:** Proceed to Troubleshoot conflicting extension install list policies.
- **Policy missing:** Complete absence of the policy suggests that the user is not configured to use Secure Enterprise Browser and you must Check user extension configuration within Google Admin Console.
- **Extension missing from policy:** Proceed to Check user extension configuration within Google Admin Console.

Troubleshoot conflicting extension install list policies

Having conflicting policies isn't necessarily a blocker for supporting CEP with Secure Private Access. However, the effective policy must force the installation of the following three extensions:

- Secure Enterprise Browser (`ekajlcmdfcigmdbphhifahdfjbkciflj`)
- Citrix Secure Access (`loifegnemklkgbmonigcdkmniboielgl`)
- Endpoint Verification (`callobklhcbilhphinckomhgkigmfocg`)

To resolve extension policy conflicts for Secure Private Access, follow these steps based on Chrome Policy Hierarchy Guide.

1. **Identify the conflict:** Navigate to `chrome://policy`. Locate **ExtensionInstallForcelist** and check the **Status** and **Source**.
2. **Analyze precedence:** Note that machine-level policies (GPO) generally supersede cloud/user-level policies.
3. **Harmonize:** Ensure the highest-precedence policy includes all three required extension IDs (it's OK if additional extensions are included). Alternately, if the browser and the profile are

managed by the same Google Workspace organization, you can use the Policy Merging feature.

4. **Verify:** Click **Reload policies**. The **Applies to** and **Level** columns must confirm that the required extensions are **Mandatory** and active at the effective level.

If the issue persists even after correcting the extension install list policy, then proceed to Check Secure Enterprise Browser Extension policy.

Check Secure Enterprise Browser Extension policy

How to check: Navigate to chrome://policy and under **Secure Enterprise Browser** look for a policy named **securityGateway**. Click **Show More** to display the full policy configuration. Its value is expected to have the following format:

```
{
  "authentication": {},
  "context": {
    "resource": "projects/project-<tenant_id>-<random-hex-characters>/
locations/global/securityGateways/securitygateway-<tenant_id>-<random-hex-
characters>"
  },
  "externalHelper": {
    "id": "com.citrix.device_posture_context_provider",
    "metadata": {
      "action": "device/metadata",
      "input": [
        {
          "key": "tenantId",
          "stringValue": "<tenant_id>"
```

```
        }
      ]
    }
  },
  ...
}
```

Ensure that the `tenant_id` field has a value that corresponds to your Citrix Cloud Tenant ID. If this value is different, it might be that a second tenant is configured to integrate with this Google Account.

- **Policy missing or empty:** Complete absence of the policy suggests that the Secure Enterprise Browser extension is configured not only by Secure Private Access but by the customer as well, and the user is picking up the extension empty configuration from a previous or manual configuration. You must Check user extension configuration within Google Admin Console.
- **Policy is populated with wrong Citrix Tenant ID:** If the policy is present but the value doesn't line up with the example, either the tenant ID is different or there are two conflicting policies. Proceed to Check user extension configuration within Google Admin Console.
- **Policy looks correct:** Proceed to Check if routes are being fetched.

Check user extension configuration within Google Admin Console

How to check: Navigate to https://admin.google.com. From here, go to **Chrome Browser > Apps & Extensions**. Within this view, you must find all policy configurations that are being applied.

Click the **Overview** tab (assuming it is present) and select the **Secure Enterprise Browser** app. To the left, under **Installation policy** it must read **Force installed and pinned in \<primary domain\>**, where \<primary domain\> corresponds to the top-level Organizational Unit of your Google Admin Console.

When clicking through to see the extension **Deployment Settings**, look for the **Policy for extensions** configuration. This must look like what is described in the Check Secure Enterprise Browser Extension policy section.

- **Single policy that appears correct:** If the policy for the parent OU looks correct, you must ensure the user that you are testing with belongs to the account in question and also that there is no other configuration at a sub-OU or group level that might be overriding the parent OU's policy. If the membership is confirmed but still the issue persists, reach out to Citrix Support.
- **Policy missing:** Complete absence of the policy suggests that this Google account is not configured to use Secure Enterprise Browser and you must Validate CEP integration in the Secure Private Access admin console.
- **Multiple policies - Multiple Citrix accounts:** If you see multiple configurations for the Secure Enterprise Browser extension, then this might be a cause for incorrect configuration of the associated policy. Associating multiple Citrix accounts to the same Google account is not prohibited but might cause the integration not to function.
- **Multiple policies - Single Citrix account:** If you are integrating only one Citrix tenant, you must ensure that no other admin functions in your organization might be configuring this extension. If you are confident there is no one else providing policy configuration for this extension, you can proceed to remove those policy configurations that don't correspond to the Citrix tenant against which you have integrated through the Secure Private Access Admin Console.

  If you remove the superfluous extension configurations and, after restarting the browser you are still unable to access your applications, reach out to Citrix Support.

Check if routes are being fetched

How to check: Navigate to chrome://extensions/?options=ekajlcmdfcigmdbphhifahdfjbkciflj or right-click the Secure Enterprise Browser extension and select **Options**.

Set log level to **ALL** and click **SHOW LOG**. Once the log shows up, close the browser and repeat the process to go to the log page. This ensures that you have retrieved the full set of logs necessary for troubleshooting.

Within the log, search for a log line containing:

```
Calling 'https://api.prod.securegateway.goog/api/v1/routes'
```

This must be followed by a response such as:

```
[260220 17:07:51.64] [SG.ApiClient] [DEBUG] Response: {expirationTime:
'2026-02-20T15:37:51Z', proxyUrl: 'https://api.prod.securegateway.goog',...
```

- **Contextual Routes show a 403 status code in the logs:** This 403 might be returned by an intercepting firewall such as Zscaler, Umbrella, and so on.
  - In this case, ensure that the traffic bound for Google Security Gateway is allowed as per Prerequisites for the integrated solution.
  - If not, then it is likely an authentication issue with the user profile and might imply incomplete integration of Secure Private Access with CEP. Proceed to Validate CEP integration in the Secure Private Access admin console.
- **Contextual Routes show timeout, a DNS error or 503 error:** Proceed to Troubleshoot Google Secure Gateway reachability.
- **Contextual Routes appears successful (200 OK):** Proceed to Confirm Application inclusion in routes.

Validate CEP integration in the Secure Private Access admin console

Visit the **Browser Settings** section within Secure Private Access of the Citrix Cloud console.

In this section, verify the following:

- **Google Chrome integration status** must read as **Complete**. If you find that it has failed, ensure that you have completed the prerequisite steps for CEP integration per the documentation and retry. If the issue persists, reach out to Citrix Support.
- **Customer ID** must have a value that corresponds to the Google account you are integrating with. You can find the value in your Google Admin Console under **Account > Account settings**.

If all the above values are correct but you are still not getting the correct extension configuration in your Chrome browser, reach out to Citrix Support.

Troubleshoot Google Secure Gateway reachability

How to check: Copy the URL `https://api.prod.securegateway.goog/api/v1/routes` and navigate to this URL in the browser location bar. You must get an HTTP 401 error response. This is an expected behavior and indicates that a network connection to the Google Secure Gateway can be successfully established.

- **DNS Resolution error:** This suggests that your company might have some restrictive DNS resolution configuration in place that prevents lookup of the Google Security Gateway FQDN. However, this is a prerequisite for the use of this feature and the respective FQDN must be resolvable.

- **The request hangs or is presented with a timeout error page:** This strongly suggests that a firewall between the browser and the internet is dropping traffic bound for Google's Security Gateway. Follow the Prerequisites for the integrated solution to ensure that the prerequisite internet locations are reachable from your network.

If you are still not receiving the correct routes, reach out to Citrix Support.

Confirm application inclusion in routes

A successful routes response includes FQDNs that correspond to applications configured by your Secure Private Access admin. For example:

```
[260318 06:42:38.99] [SG.ApiClient] [DEBUG] Response: {expirationTime:
'2026-03-18T14:15:05Z', proxyUrl: 'https://via.prod.securegateway.goog',
endpointMatchers: [{hostname: 'telemetry.netscalergateway.net'},
{hostname: 'www.workday.com'}, {hostname: '*.workday.com'}, {hostname:
'jira.internal.corp'}, {hostname: '*.jira.internal.corp'}]}.
```

Does this line include the application you are trying to access?

- **The inaccessible application is included in the routes response:** Proceed to Troubleshoot routed application access.
- **Only telemetry.netscalergateway.net is included in the routes response:** Try configuring an additional application and inclusive application policy. If you are still not seeing it in the routes, this strongly suggests an issue with group membership or a misalignment of groups between your IdP configured in Citrix and Google Directory. Proceed to Ensure IdP and Google Directory alignment.
- **The inaccessible application is not included in the routes response:** This suggests that the application is not correctly configured in the Secure Private Access Admin console. Verify that the application exists and has a policy associated (either to allow or deny access). If you are certain that the application is configured but it is still missing from the preceding routes, contact Citrix Support.

Troubleshoot routed application access

When attempting to access your application (that does show up in the routes list), what is the observed behavior?

- **You are getting a domain resolution error (ERR_NAME_NOT_FOUND)**

This most likely suggests that the application is not correctly configured or the contextual routes are not received correctly.

- **A cream-yellow page showing "Access Denied"**

  This suggests that the policy configuration in the Secure Private Access console is not configured to include the current user.

- **A cream-yellow page showing "Oops! Something went wrong."**

  The most common cause for this error page is the Connector being unable to reach the target application. In this case, troubleshoot connector access to internal applications as per Citrix documentation. Common issues include:

  - Internal DNS reachability
  - Backend service is down
  - Firewall rules

- **A white page showing "Service Unavailable" in a large red font**

  This can be a transient error and might resolve after a few minutes.

  If the issue persists, reach out to Citrix Support.

- **Timeout**

  - First, verify that `via.prod.securegateway.goog` is reachable by entering it in Chrome's address bar. You must receive a 401 response. If it times out, an intermediate firewall or proxy is blocking access and must be resolved before applications can be accessed.
  - Another potential cause for an application timeout is a firewall blocking traffic to the internet and to the Google Security Gateway in particular. This is common in scenarios where a customer requires an explicit proxy to reach the internet. The Secure Private Access integration with Chrome Enterprise Premium does not support this proxy configuration.

- **Certificate error**

  Application might be using a private CA certificate and as such the browser might throw an "untrusted certificate error". Through Chrome Enterprise Premium configuration, the customer can push their trusted root CA to the browser. For details, see Use Chrome Enterprise Premium to manage root certificate configurations.

Ensure IdP and Google Directory alignment

For Secure Private Access integration with Chrome Enterprise Premium, the synchronization of your directory to Google Directory has to follow some specifications covered in Prerequisites for the integrated solution.

If the user and user group emails are correct and line up with what is configured in your source directory, proceed to Check access settings for the group in Google Admin Console.

Check access settings for the group in Google Admin Console

In Google Admin Console, navigate to **Directory > Groups** and select the group against which you have configured your access policy and against which your application is not loading.

From there, select **Access settings** and ensure that the row **Who can view members** has the option **Group Members** enabled. This configuration must apply to all groups you want to create policies against in Secure Private Access.

If this option is already enabled, reach out to Citrix Support.

Known issues with the CEP integration

The following known issues exist in the Secure Private Access integration with Chrome Enterprise Premium.

Secure Private Access user interface

- **Issue:** Session policy configuration currently allows users to add only two simulate conditions, even though three conditions are available. This limits flexibility in policy creation.

  Workaround: Create two separate session policies; one with two of the simulate conditions and another policy with the remaining condition.

- **Issue:** The TCP/UDP server-to-client configuration option is not available in the application configuration UI across all customer environments. This limits the ability to define server-to-client traffic behavior.

Adaptive access policy configuration

- **Issue:** Access policy creation fails when Okta groups are specified in the rules. This issue only affects groups that are present in the Okta directory.

Workaround: You can use Okta as an identity provider but not as a directory. To use Okta as an IdP, you must first integrate your on-premises AD with Okta. For details, see Connect Okta as an identity provider to Citrix Cloud.

Google Chrome browser

- **Issue:** If the Google profile picker is open and the user tries to launch an app from CWA or a non-Chrome browser when there is no existing profile, the profile creation workflow is not triggered.

  Workaround: Close the profile picker and relaunch the app.

- **Issue:** Logging into CWA with a managed Chrome profile and launching an app does not take the user to the original internal app URL after profile creation.

  Workaround: After the profile creation, relaunch app.

- **Issue:** Users part of a group is not auto synced when synced a group from Google Admin console. The `whoCanViewGroupMembership` setting is explicitly overridden to `ALL_MANAGERS_CAN_VIEW` during the sync. So, the restricted visibility is expected.

  Workaround: Manually update the google group permission on the Google Admin console or usomg via API. For details, see `<https://developers.google.com/workspace/admin/groups-settings/manage>`.

- **Issue:** Users are prompted to authenticate with a user name and password through a proxy pop-up when accessing published SaaS/Web applications through a managed Chrome profile. This typically occurs after a period of inactivity:

  Causes:

  - A proxy token is unavailable or the proxy token is available but has subsequently expired.
  - The SEB extension requires re-initialization due to delayed initialization.

  Workaround: Relaunch the Chrome session in a new window.

- **Issue:** Users might experience intermittent "Service Unavailable" errors when accessing external SaaS applications through Managed Chrome profiles or Citrix Workspace App. This issue is due to an unresolved backend issue on Google's infrastructure.

  Workaround: Contact the Google team for support.

Open ID Connect (OIDC)

Issue: When a customer has more than one Microsoft Entra ID connection to the same Azure tenant, the Entra ID IdPs cannot be reliably distinguished during OIDC client configuration. This issue affects only the reliability of IdP selection. The OIDC client configuration and authentication behavior are unaffected.

Get started with Citrix Secure Private Access

This document walks you through how to get started with onboarding and setting up the SaaS apps delivery for the first time. This document is intended for application administrators.

System requirements

- **Operating systems support:** Citrix Workspace app is supported on:
  - Windows 7, 8, 10, and 11
  - macOS - 10.11 and above
- **Browser support:** Access apps through the cloud store URL using the latest versions of Edge, Chrome, Firefox, or Safari.
- **Citrix Workspace™ app support:** Access stores using Citrix Workspace app for any of the desktop platforms (Windows, Mac).
- If users access their store using a custom URL then they must use the following minimum versions:
  - Citrix Workspace app for Windows: 2503.10 or later
  - Citrix Workspace app for Mac: 2505.10 or later
  - Citrix Secure Access app for Mac: 26.04.1.1 and later
  - Citrix Secure Access app for iOS: 26.04.1 and later

How it works

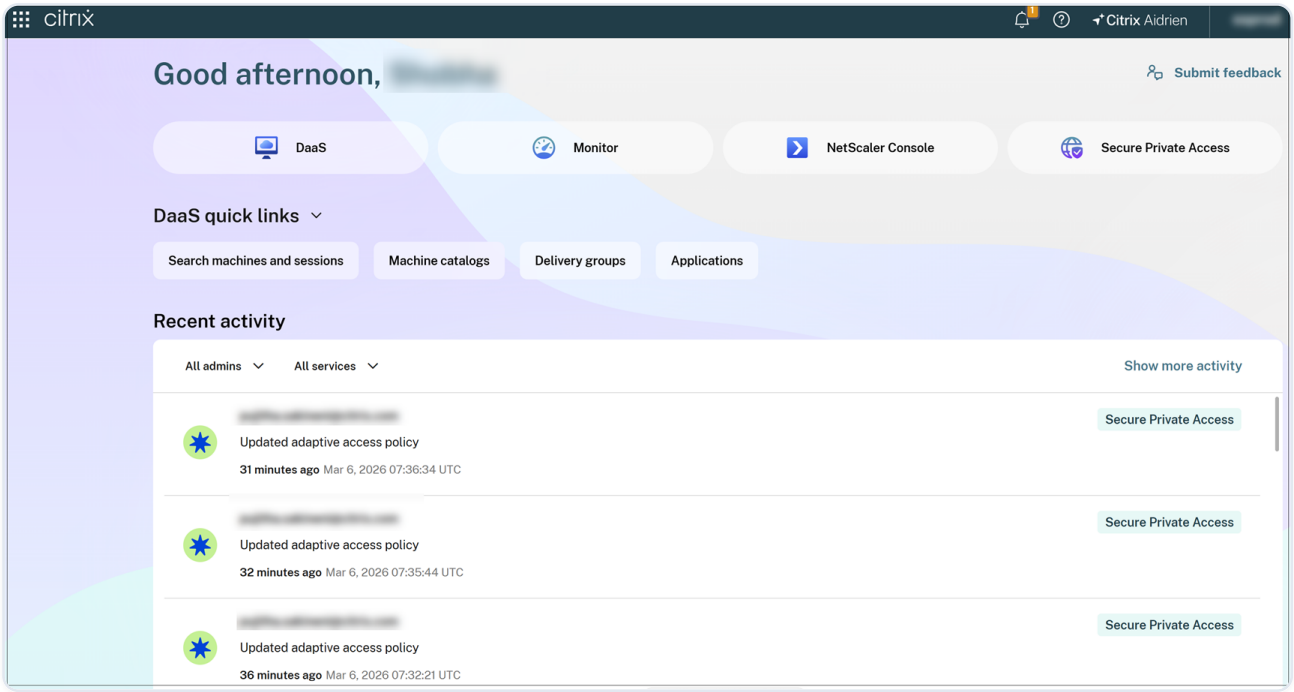
Citrix Secure Private Access helps IT and security admins to govern authorized end-user access to sanctioned SaaS and enterprise hosted web apps. User identities and attributes are used to determine access privileges and access control policies determine the privileges that are required to perform operations. Once a user is authenticated, access control then authorizes the appropriate level of access and allowed actions associated with that user's credentials.

Citrix Secure Private Access combines elements of several Citrix Cloud™ services to deliver an integrated experience for end users and administrators.

FUNCTIONALITY	SERVICE/COMPONENT PROVIDING THE FUNCTIONALITY
Consistent user interface to access apps	StoreFront Cloud
SSO to SaaS and Web apps	Citrix Gateway Service Standard
Web filtering and categorization	Web filtering service
Enhanced security policies for SaaS	Cloud app control
Secure browsing	Remote Browser Isolation service
Visibility into website access and risky behavior	Citrix Analytics

Get started with the Citrix Secure Private Access service

1. Sign up for Citrix Cloud.
2. Request for the Secure Private Access service entitlement.
3. After the entitlement is granted, the Secure Private Access service is provisioned for your account.
4. Access the Secure Private Access service admin UI.
5. Configure the store that end users use to view and launch their apps in StoreFront Cloud.



Note:

- For your end users to use the store and access the apps, they must download and use the Citrix Workspace app or open the store URL from their web browser. You must have a few SaaS apps published to your store to test the Citrix Secure Private Access solution. The Workspace app can be downloaded from Downloads. In the **Find Downloads** list, select **Citrix Workspace app**.
- If you have an outbound firewall configured, ensure that access to the following domains is allowed.
    - *.cloud.com
    - *.nssvc.net
    - *.netscalergateway.net

    More details are available at Cloud Connector Proxy and Firewall Configuration and Internet Connectivity Requirements.

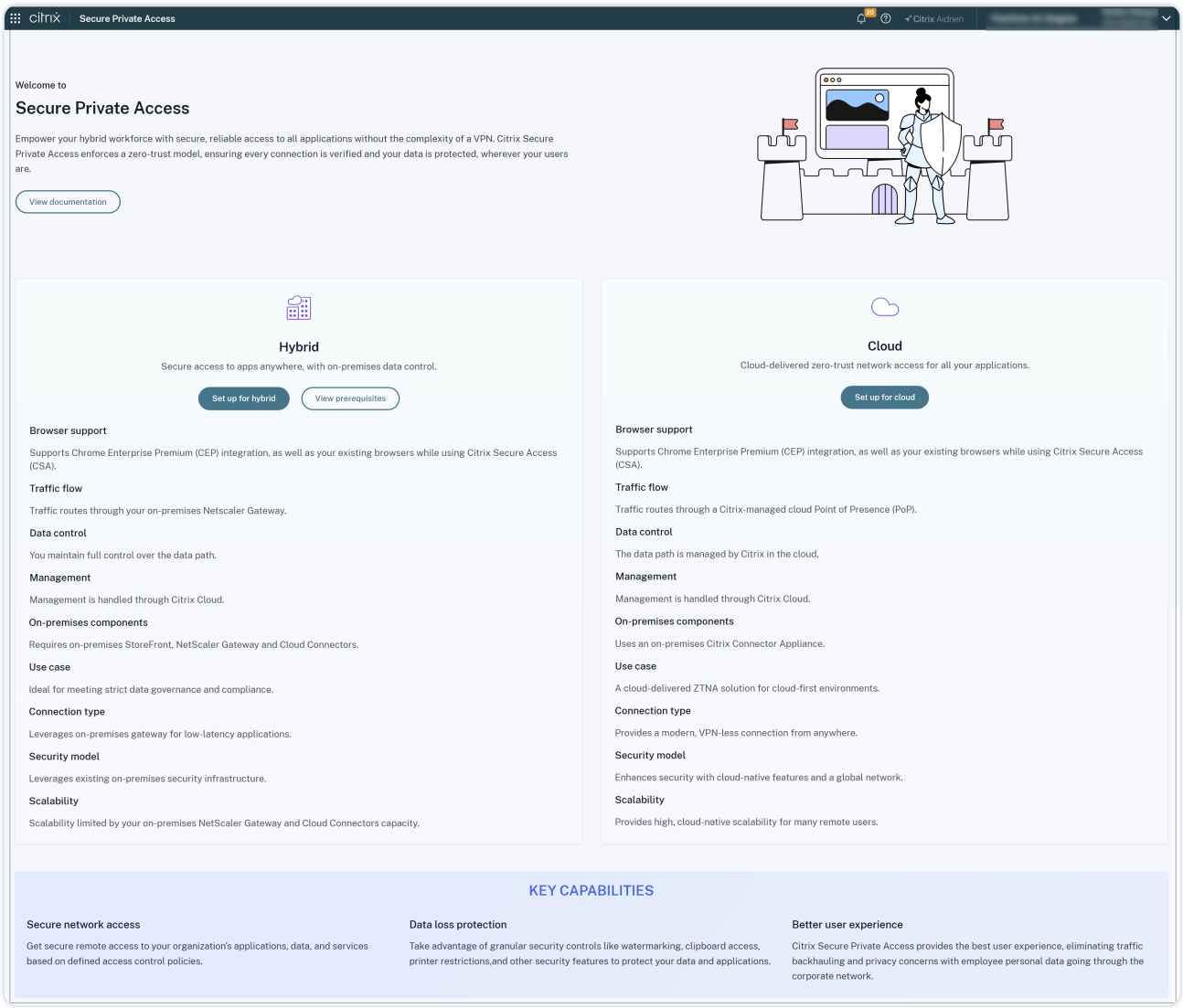
Secure Private Access service deployment models

The secure Private Access service is available to customers in two architectural options.

- **Hybrid service architecture:** Hybrid service architecture allows you to use your on-premises StoreFront and NetScaler Gateway components, ensuring that all user traffic remains under your control. Also, the site management components are hosted and managed by Citrix. For details, see Hybrid deployment.
- **Cloud native service architecture:** Cloud native service architecture is a cloud delivered ZTNA solution that delivers adaptive access to IT-sanctioned applications whether they are deployed on-premises or in the cloud. For details, see Citrix Secure Private Access.

You can choose these options from the Secure Private Access service admin console.

1. Log in to Citrix Cloud™ and then click **Secure Private Access**.
2. Select **Setup for hybrid** or **Setup for cloud** as per your requirement.



Points of Presence (PoPs) locations for Citrix Secure Private Access™ service

Citrix is adding more PoPs globally to ensure business continuity and quality service for the Citrix Secure Private Access customers.

Secure Private Access management PoPs

The following is the list of Secure Private Access management PoP locations.

POP NAME	ZONE	REGION
az-eu-w-mgmt	Azure westeurope	Netherlands
az-in-s-mgmt	Azure southindia	Chennai
az-us-e-mgmt	Azure eastus	Virginia

Secure Private Access data PoPs

The following is the list of Secure Private Access data PoP locations.

POP NAME	ZONE	REGION
az-us-e	Azure eastus	Virginia
az-us-w	Azure westus	California
az-us-sc	Azure southcentralus	Texas
az-aus-e	Azure australiaeast	New South Wales
az-eu-n	Azure northeurope	Ireland
az-eu-w	Azure westeurope	Netherlands
az-jp-e	Azure japaneast	Tokyo, Saitama
az-bz-s	Azure brazilsouth	Sao Paulo State
az-asia-se	Azure southeastasia	Singapore
az-uae-n	Azure uaenorth	Dubai
az-in-s	Azure southindia	Chennai
az-asia-hk	Azure eastasia	Hong Kong
az-nw-e	Azure norwayeast	Norway

Secure Private Access onboarding and set up

The Secure Private Access™ admin console enables administrators to onboard and manage SaaS, web, and TCP/UDP applications, and define granular access policies that govern how users interact with those applications.

Citrix Secure Private Access is integrated with Google Chrome Enterprise Premium, which allows customers to securely access private web and SaaS applications using Google Chrome Enterprise Premium as their enterprise browser.

The high-level steps to onboard and set up Secure Private Access are:

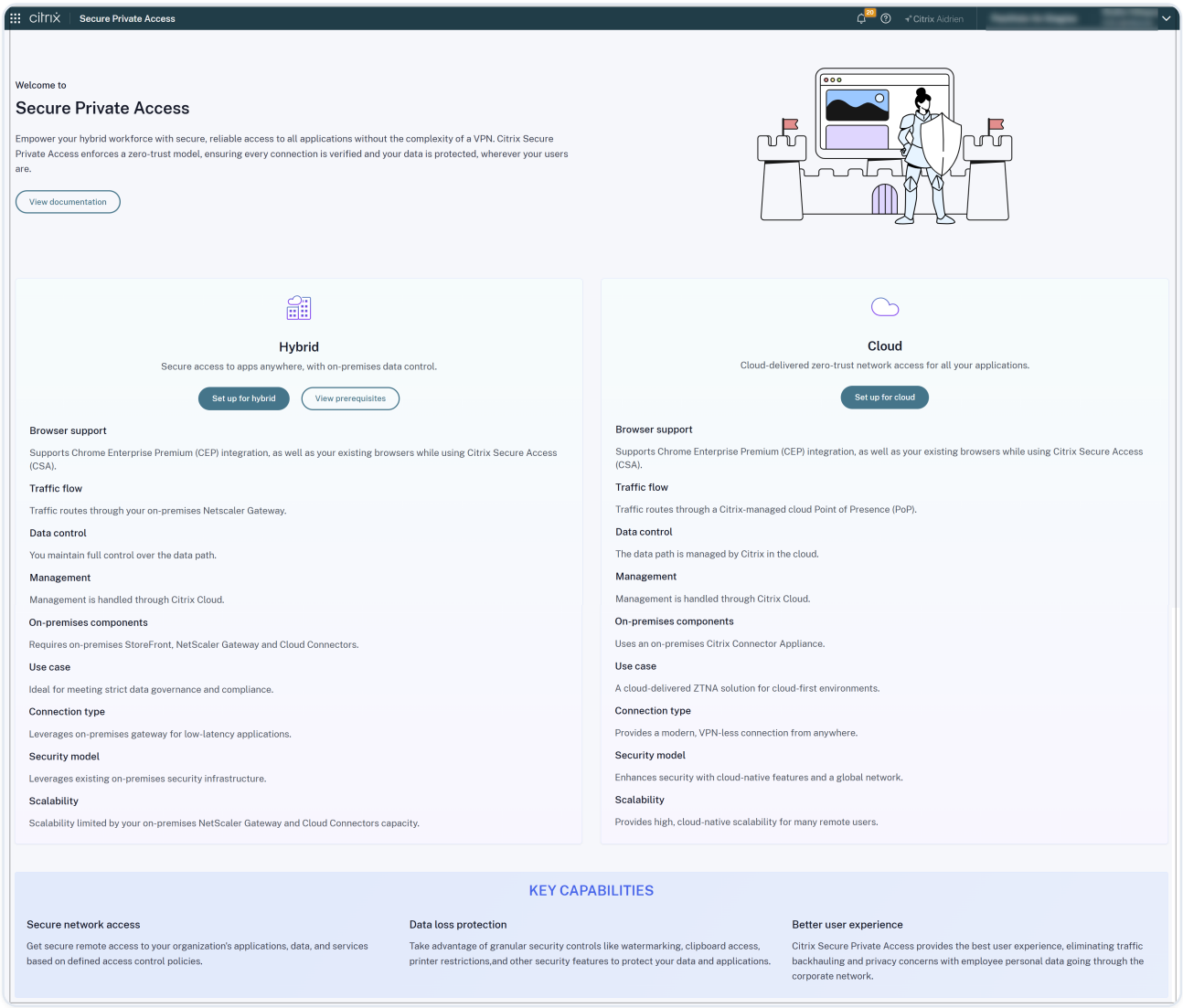
1. Onboard users to Secure Private Access
2. Configure the store URL in Citrix® StoreFront Cloud
3. Setup Google Chrome integration.
4. Configure Connector Appliance
5. Add apps for your users.
6. Assign permissions for app access by creating the required access policies.

> **Important:**
>
> You can set Google Chrome as your enterprise browser. For details, see the following topics.
>
> - Set Google Chrome as your enterprise browser
> - Considerations prior to switching browser

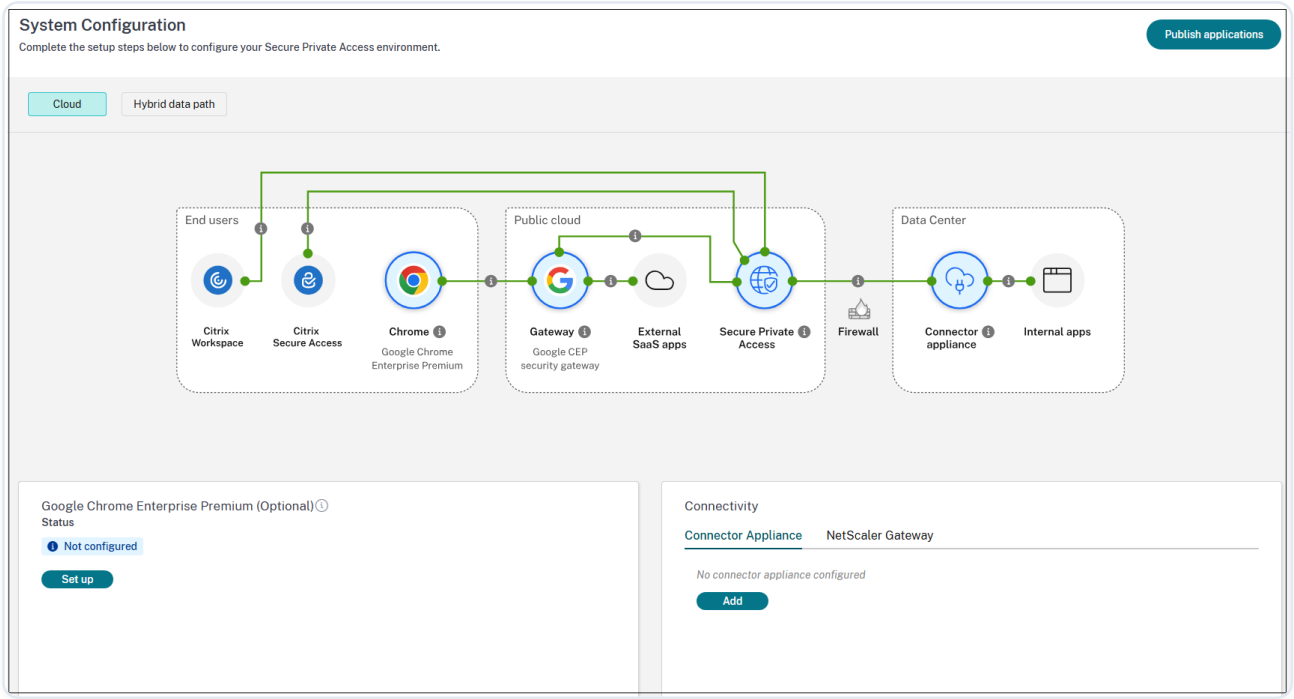
Onboard users to Secure Private Access

Perform the following steps to onboard your users to Secure Private Access.

1. Log in to Citrix Cloud™ and then click **Secure Private Access**.
2. Select **Setup for cloud** and then click **Continue**.



The topology diagram shows the components used in Secure Private Access cloud deployments. You can click the help icon to view a short description of each component in the flow.



- **For new customers**, selecting the Secure Private Access service in the Citrix Cloud console opens the setup page, allowing them to configure Connector Appliance and CEP.
    - To configure Connector Appliance, click **Add** in the **Connector Appliance Configuration** pane. For details, see Configure Connector Appliance.
    - To configure Google Chrome Enterprise Premium (CEP), click **Set up** in the **Google Chrome Enterprise Premium** pane and follow the on-screen instructions. For details, see Setup Google Chrome integration.

  Once the setup is completed, during the subsequent visits, the administrators are redirected to the Secure Private Access dashboard when they click Secure Private Access in the Citrix Cloud console.
- **For existing customers**, the system checks:
    - Connector Appliance availability
    - Chrome Enterprise Premium status

  Connector Appliance check: The system checks whether one or more Connector Appliances are configured and how many are available. This check helps administrators understand that configuring a Connector Appliance is mandatory for users to successfully connect to internal corporate applications (Web, TCP/UDP). The Connector Appliance enables end-user connectivity through the native Citrix Secure Access client, supporting any browser of the customer's choice.

  Chrome Enterprise Premium configuration check: The Chrome Enterprise Premium configuration check helps administrators determine whether the integration between Citrix Secure Private Access and Chrome Enterprise Premium is enabled. This integration allows end users to securely access corporate web applications through the Chrome browser, without requiring the native Citrix Secure Access client.

> **Note:**
>
> The Google Chrome Enterprise Premium setup is optional and can be skipped.

Configure store URL in Citrix StoreFront Cloud

You can integrate the Secure Private Access service with Citrix® StoreFront Cloud. You provide your users with a store URL which they can open in a web browser or Citrix Workspace™ app. The store provides a unified user experience for the configured SaaS apps, web apps, virtual apps and other configured resources.

By default, a store is created with URL `customerid.cloud.com`. You can change this URL, or add your own custom URL for example `store.company.com`. To configure the stores, see Configure access to stores.

Setup Google Chrome integration

In the Google Chrome Integration page, perform the following steps:

1. Copy the autogenerated service account email and paste it into the appropriate field in the Google Admin console.
    a. In the Google Admin console, go to **Admin Roles**.
    b. Select the role that is created for the Secure Private Access service and apply the recommended privileges. For the list of privileges, see Admin roles and privileges.
    c. Under **Admins**, select **Assign service accounts**.
    d. Paste the Citrix service account (`tenant-sa-<random-string>.iam.gserviceaccount.com`) and select **Add**. Then select **Assign Role**.

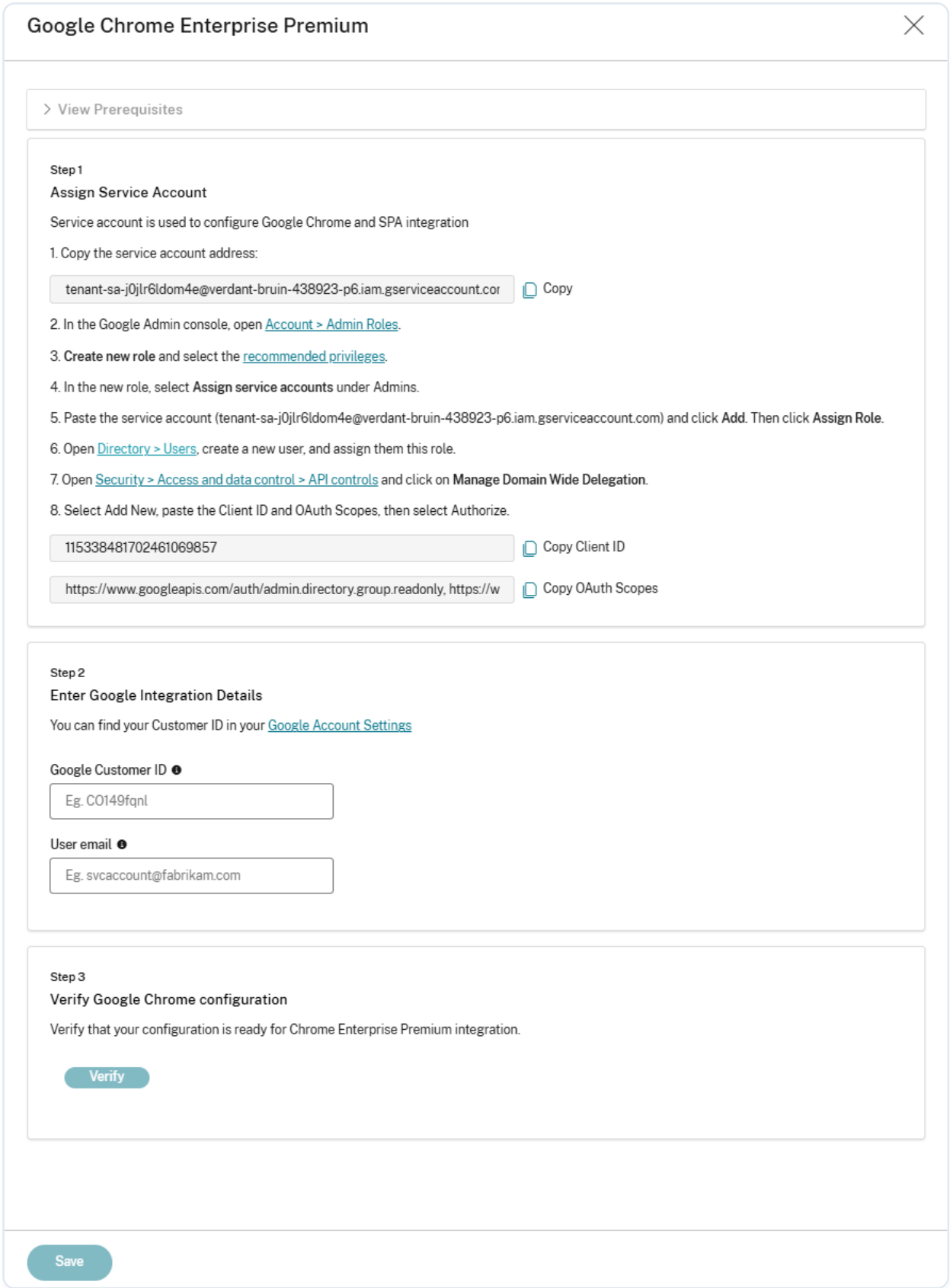
    For details about roles, see About administrator roles.
    e. In the Google Admin console, navigate to **Directory > Users**.
    f. Click **Add new user** and create a new user (First name: Citrix Service, Last name: Account, Primary email: caccount). Keep the email of the newly created user.
    g. Once the new user is created, select it and go to **User details**. In the **Admin roles and privileges** select and assign to this user the same role.
    h. Go to **Security > Access and data control > API controls** and click **Manage Domain Wide Delegation**.
    i. On **API clients**, click **Add new** and fill in the Client ID and OAuth scopes with the respective information provided in the Google Chrome Integration page.

j. Copy the Google Customer ID that is available in **Google Account Settings** within the Google Admin console into the **Google Customer ID** field in the **Google Chrome Integration** page.

k. Fill in the **User email field** in the Google Chrome Integration page with the email of the previously created user.

2. Click **Run CEP verification** to verify your Google Workspace configuration to ensure that it is ready for Chrome Enterprise Premium integration before proceeding with the next step.

   - If the verification returns a failure or a warning, see Known verification failures and warnings for troubleshooting guidance.
   - Once the CEP verification is successful, the Secure Private Access service successfully connects to the Google customer ID and a Secure Gateway is created.
   - Upon successful creation of the Secure Gateway, the system displays the egress IP addresses assigned to it. Administrators can select the egress regions that Chrome Enterprise Premium uses for SaaS application traffic. For details, see Configure Egress hub regions.
   - When a user attempts to access a SaaS application, the request does not go directly to the SaaS provider. Instead, the traffic is first routed through the Secure Gateway, which functions as a partner connector. This gateway acts as an intermediary, inspecting and securing all traffic before it reaches the destination application.



3. Click **Save**.

Important:

- You can also update the integration details after the customer is onboarded to CEP. For details, see Update Google integration details post onboarding.
- You can apply the CEP configuration to selected Google Directory organizational units during onboarding, in addition to all users and user groups. For details, see Configure CEP for Google Directory organizational units.

- For more details about Secure Private Access integration with Google Chrome Enterprise Premium, see Integration with Google Chrome Enterprise Premium.

Add IP addresses of SaaS apps

After onboarding customers to Secure Private Access and Chrome Enterprise Premium, you must allow the list of the IP addresses used by your SaaS applications. This step is critical to ensure that:

- Users can access SaaS applications without connectivity issues or blocks caused by network security controls.
- Traffic from Citrix Secure Private Access and Chrome Enterprise Premium is recognized as legitimate and not inadvertently filtered or denied.

Note:

For an application routed via Connector Appliance using the "Internal via Connector" routing type, customers must use the Citrix IP allow list.

Principal access boundary policies configuration

Principal access boundary policies can prevent end users from accessing the Citrix-managed Google Secure Gateway.

If your GCP organization has a principal access boundary policy that blocks access to cross-tenant resources by default, create a principal access boundary policy that allows access to the Google Secure Gateway. You can retrieve the Secure Gateway identifier from the **Browser settings > Browser** page. For details on configuring an appropriate policy, see Google Cloud IAM - Principal access boundary policies documentation.

Update Google integration details post onboarding

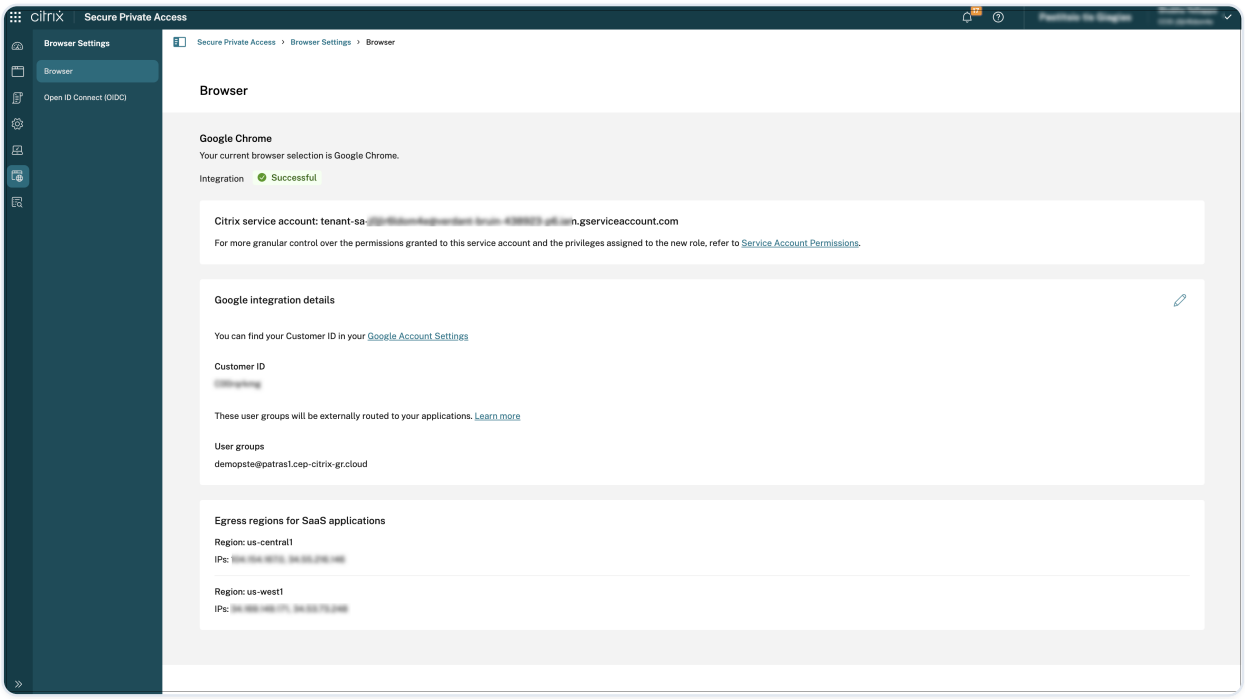
Once customers are successfully onboarded to Chrome Enterprise Premium, Secure Private Access allows for post-onboarding management of their integration details. This includes the ability to update critical identifiers such as the customer ID and to modify associated user groups.

Perform the following steps to update the integration details post onboarding:

1. In the Secure Private Access admin console, go to **Browser settings > Browser**.

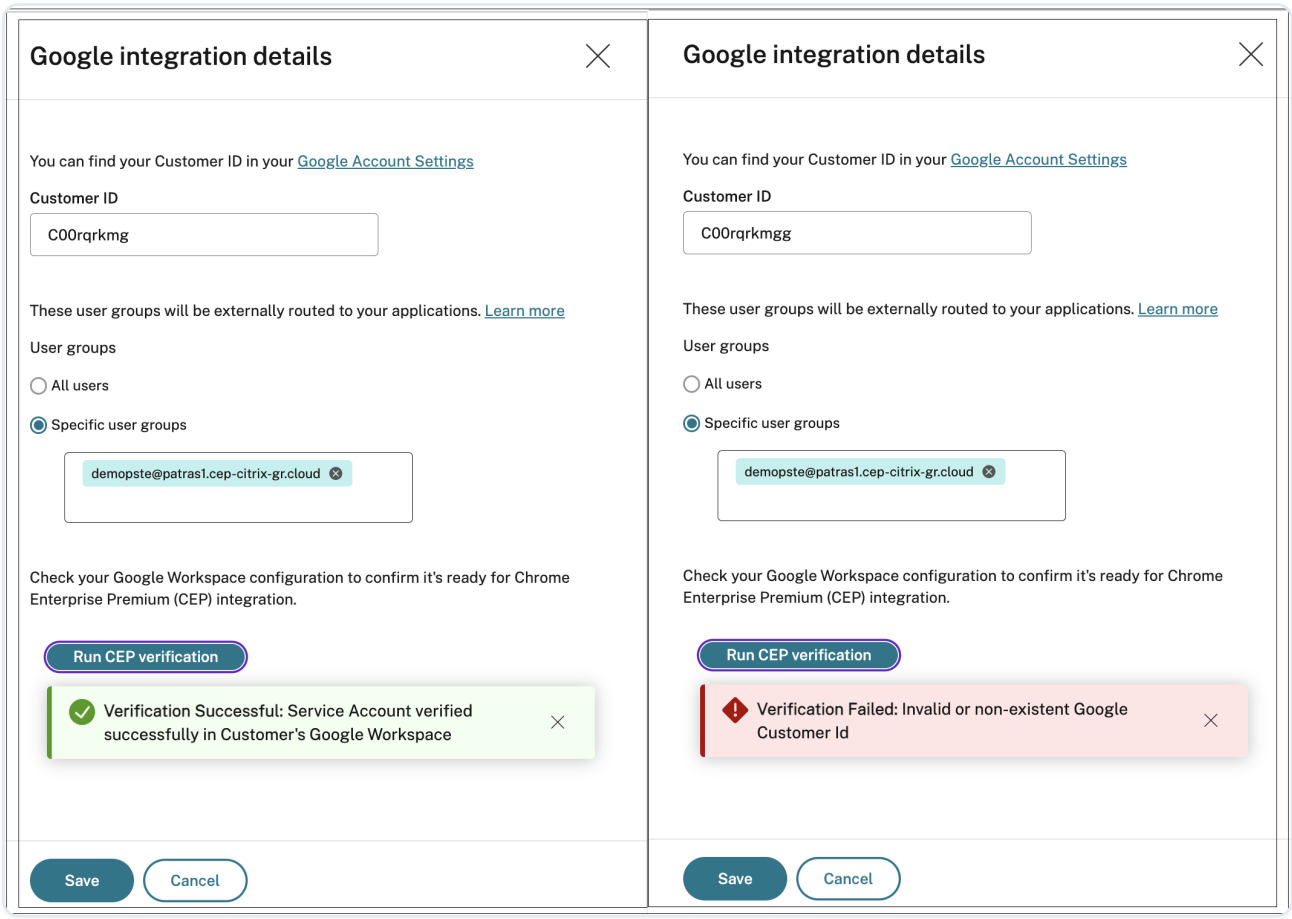
   The Browser page displays the Google Chrome integrations details.

   The system also displays the egress IP addresses associated with the Secure Gateway. Each time a user tries to access a Software as a Service (SaaS) application within this integration, traffic is routed through the Google Secure Gateway, which acts as a partner connector, instead of directly connecting to the SaaS application. This gateway inspects and secures the traffic, enforcing security policies and access controls, and ensuring compliance with the organization's security posture.



2. Click the edit icon and update the customer ID or the user groups or both.
3. Click **Run CEP verification** to verify your Google Workspace configuration is ready for Chrome Enterprise Premium integration.

   If there are issues with the integration details, CEP verification displays a failure or warning message with details to help you resolve them. For guidance, see Known verification failures and warnings.



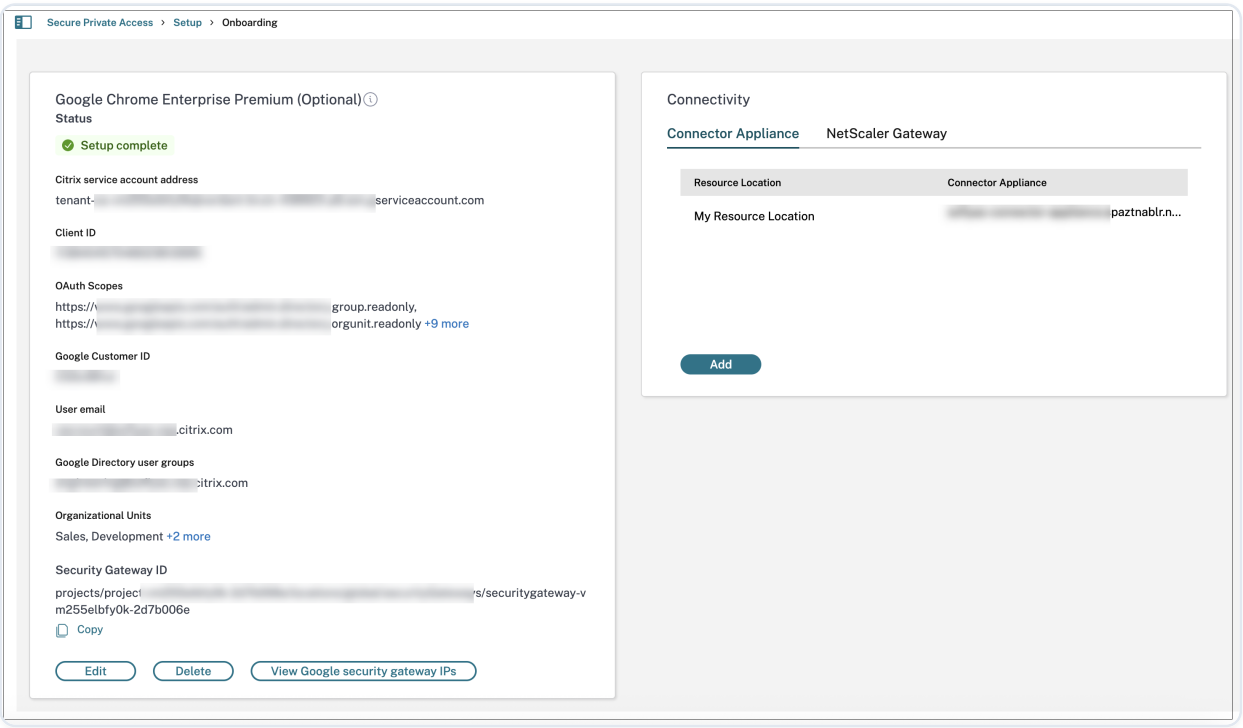
Configure CEP for Google Directory organizational units

In addition to all users and Google Directory user groups, you can apply a Chrome Enterprise Premium (CEP) configuration to selected Google Directory organizational units. User groups and organizational units are not mutually exclusive, so a single configuration can target both. You can also save a configuration that uses organizational units only, with no user groups selected. This option is available for both Secure Private Access cloud and hybrid deployments.

A selected organizational unit is inherited: the configuration applies to the users in that organizational unit and to all of its child organizational units, including any that are created later.

Organizational units are selected in the same panel as the Google Directory user groups. Perform the following steps:

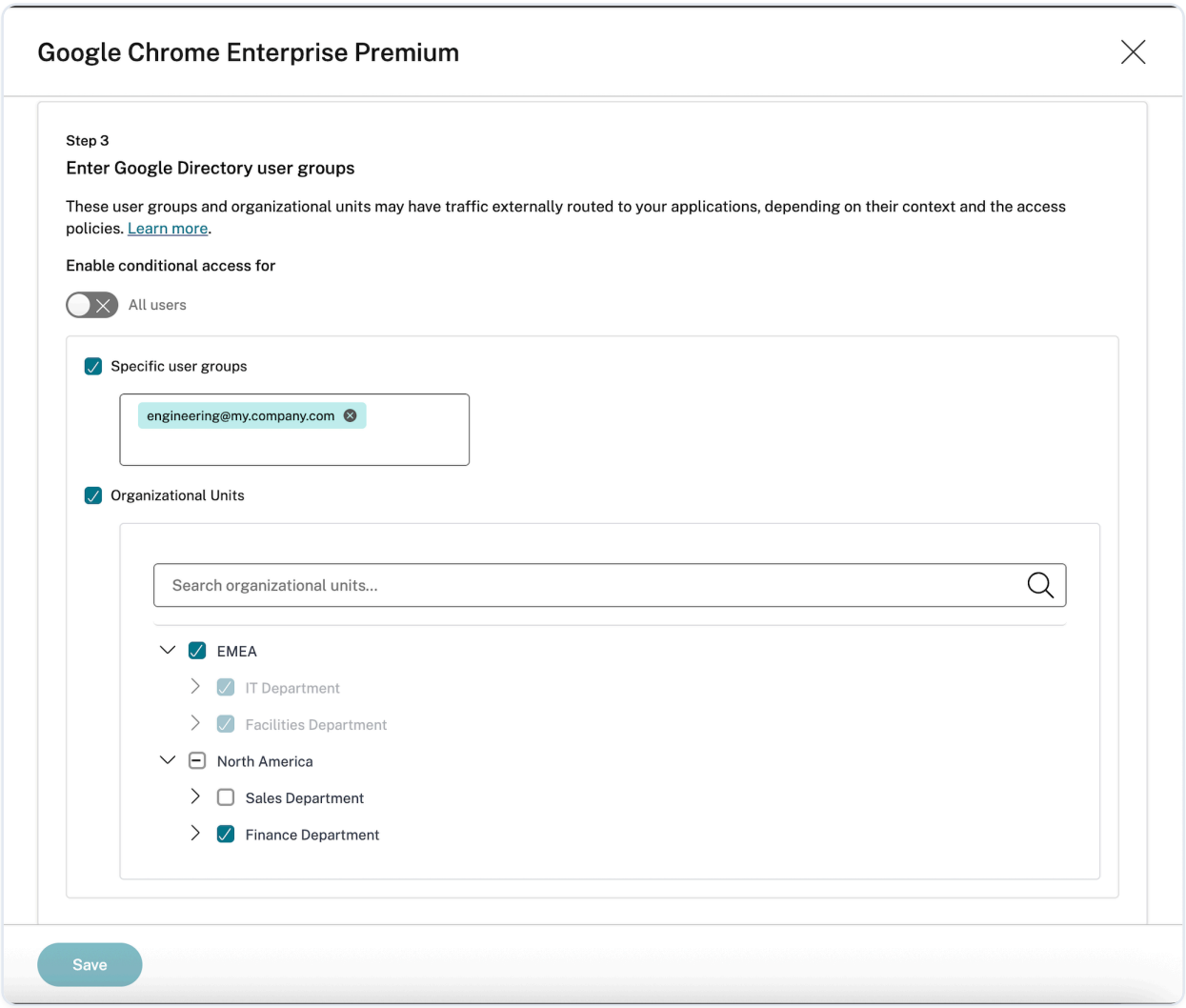
1. On the Chrome Enterprise Premium setup card, click **Edit**.



Alternatively, in the Secure Private Access admin console, go to **Browser settings > Browser** and click the edit icon.

The card lists the organizational units that are currently selected.

2. Click **Organizational Units** to display your Google Directory hierarchy as a tree of check boxes.



Note:

- The root organizational unit is not shown in the tree. To enable CEP integration for everyone, select All users.
- The hierarchy is read from your Google Directory using the Citrix service account. If the service account does not have the **Organization Units > Read privilege**, the hierarchy cannot be loaded and an error appears in place of the tree. For details, see Google admin roles and privileges.

3. Select the organizational units to include.

   Selecting an organizational unit also selects its child organizational units. The child units appear selected and are grayed out. They cannot be cleared individually. To include only a subset, clear the parent and select the specific child organizational units that you want.

4. Click **Run CEP verification**, and then click **Save**. If you change the selection after a successful verification, run the verification again before you save. For the failures and warnings that verification reports, see Known verification failures and warnings.

   When you reopen the panel, the tree expands to display your saved selection. Organizational units that have been deleted in Google Directory are removed from the panel.

Known verification failures and warnings

When verifying the CEP configuration, Secure Private Access flags any failures or warnings identified for the selected setup before allowing the configuration to be completed.

You must resolve all identified failures before continuing with the configuration. Use the following table to identify and fix specific failures detected during verification:

FAILURE MESSAGE	ACTION
Invalid Google Customer ID or service account lacks permissions to access Google Workspace.	Verify that the Google Customer ID is correct.
\^	Ensure that the required privileges are assigned to the service account. For details, see Admin roles and privileges.
Service account lacks permissions to access Chrome Extension Policies.	Ensure that the required privileges are assigned to the service account. For details, see Admin roles and privileges.
\^Service account lacks permissions to access Chrome Extension Policies for User Group.	\^
\^Service account lacks permissions to access Chrome Client Certificates Policy.	\^
Null or Empty User Group ID found in Google Workspace.	This can be a temporary issue. If it persists, there might be a problem with the Google group.
\^	If the issue continues for multiple Google groups, contact Citrix Support.

FAILURE MESSAGE	ACTION
Invalid or non-existent User Group	Check for spelling errors in the Google group name.
\^	Verify in the Google Admin console that the group still exists.
Service account lacks permission to apply Chrome extension policies to the organizational unit.	Ensure that the required privileges are assigned to the service account. For details, see Admin roles and privileges.

Any identified warnings must be noted and investigated, but they do not prevent the configuration from being completed. The following list describes common warnings and how to address them:

WARNING MESSAGE	ACTION
Google Customer ID is already in use	Your organization has multiple Citrix Secure Private Access tenants using the same Google Customer ID for Chrome Enterprise Premium integration. Configure this carefully, because overlapping Google groups (including selecting 'All users' for one or more tenants) can override or partially override existing Chrome Enterprise Premium settings in your other Citrix tenants.
Overlapping Google Directory user groups detected	Review the Chrome Enterprise Premium integration on your other Citrix tenants for the given Google groups.
\^	Decide which Citrix tenant must have the Chrome Enterprise Premium set up for each of the relevant Google groups.
\^	Remove the respective setup from the other Citrix tenants.
\^	Reapply the Google group setup for the selected Citrix tenant if it was removed during cleanup.

WARNING MESSAGE	ACTION
The 'All users' option may interfere with other customers linked to this Google Customer ID	Configuring Chrome Enterprise Premium for 'All users' (the root Google organizational unit) can override other Secure Private Access setups that use the same Google Customer ID.
\^	Use this setting only if the other Citrix tenants are not actively used by users.
The 'All users' option is used by at least one customer linked to this Google Customer ID	If another Citrix tenant has configured Chrome Enterprise Premium for 'All users' (the root Google organizational unit), it can override Google group integrations planned for this Citrix tenant.
\^	Confirm whether the other Citrix tenant requires the 'All users' integration. If not, change that tenant to a specific Google group.
Overlapping Google Directory organizational units detected	Another customer linked to this Google Customer ID already uses the organizational unit, or an organizational unit in its path.
\^	The overlap applies to the organizational unit and all of its child organizational units. Review the Chrome Enterprise Premium integration on your other Citrix tenants for the listed organizational units.
Service Account is missing permission `Services > Chrome Management > Settings > Managed Browsers > Read`	Confirm that the respective privilege has been assigned. If yes, verify that you have a subscription for either Chrome Enterprise Core or Chrome Enterprise Premium in your Google Admin Console (under Billing > Subscriptions)

Provisioning failure issue with multiple user groups

When configuring Chrome Enterprise Integration in Secure Private Access (while onboarding or from the **Browser settings** page), specifying more than eight user groups might cause provisioning failures. As a workaround, do the following:

- Use a dedicated directory parent group that encompasses all required groups.

- Configure this parent group during onboarding.
- If group membership changes in the directory, repeat the synchronization process to Google's Directory.

Next steps

After you configure Connector Appliance and Chrome Enterprise Premium, you can configure the applications and policies for your users.

- Configure applications.
- Configure access policies.

Data regionalization

Data regionalization in Citrix Secure Private Access enables customers to control where their data is stored by selecting a preferred geographic region. Customers can choose the region where their data is stored, with options including Global, Europe (EU), APAC (Asia Pacific), and North America (NA). All configuration data at rest remains within the selected region, ensuring that it does not leave the designated geography.

For any user access request, application traffic is processed within the selected region and does not traverse or leave that geographic region. This applies regardless of the user’s location. Even if users are distributed globally, each user’s traffic is routed through the selected region and does not traverse any other geography.

The data regionalization feature delivers the following benefits:

- Ensures strong data residency control by keeping all configuration data within the selected region.
- Ensures strong data residency control by keeping configuration data and applicable management and supporting service data within the selected region, with regional data PoPs and management endpoints used for customer deployments.
- Ensures that user access request traffic for any application remains within the selected region by leveraging geo-location-based routing, which directs user traffic to specific PoPs regardless of the user's location.
- Helps organizations meet regulatory and data sovereignty requirements.
- Reduces risk by preventing data from leaving designated geographies.
- Supports flexible global deployments with region-specific needs, enabling customers to confidently adopt cloud-delivered secure access aligned with their residency policies.

> **Note:**

> Without data regionalization, organizations operating across regions might face strict data residency and compliance requirements while lacking control over where their service data is stored. Without regional data boundaries, configuration data might be stored outside required

> geographies, increasing regulatory risk and limiting adoption of cloud-delivered secure access solutions.

Supported deployments

This feature applies to all Citrix Secure Private Access deployments, including both service and hybrid models, and is especially relevant for organizations with regional data residency, compliance, and regulatory requirements.

Configuration

Selecting a region is a one-time setting during onboarding of the Secure Private Access service or a hybrid deployment. After it is set, all data remains in the selected region, with no impact on ongoing operations or user workflows.

1. Log in to Citrix Cloud and then click **Secure Private Access**.
2. Select **Setup for cloud** or **Hybrid** and then click **Continue**.
3. In **Select deployment region**, select the region where your data must be stored. The available regions are based on your Citrix Cloud account region.
4. Click **Continue**.

Limitations

Some of the limitations of data regionalization are:

- Data regionalization applies to customer-owned configuration data at rest and user access request for application data. Other data types (such as telemetry or in-transit data) might not be restricted to the selected region.
- There are dependencies on other Citrix Cloud services that operate globally, which might not follow the same regional boundaries.
- This is a one-time configuration during onboarding and cannot be changed later.
- The feature is available for new customers only.

Apps configuration and management

Citrix Secure Private Access provides a user-friendly, centralized platform for configuring and managing access to a diverse range of applications (SaaS/Web and TCP/UDP). The Secure Private Access console simplifies administration by providing a single point of control for various configuration tasks. Using the configuration wizard, administrators can easily set up Adaptive Authentication, configure applications, define access policies to control user permissions, and implement security restrictions to protect sensitive data, all within the same console. Additionally, Secure Private Access supports agentless access to Enterprise web apps without the need for installing a VPN client.

For details, see the following topics:

- Support for Enterprise web apps
- Agentless access to Enterprise web apps
- Support for Software as a Service apps
- Support for client-server apps
- Support for server-to-client connections
- Citrix Secure Access client
- Best practices for Web and SaaS application configurations
- End user app access - Explained

Configure enterprise web apps

Web app delivery using the Secure Private Access service enables enterprise-specific applications to be delivered remotely as a web-based service. Commonly used web apps include SharePoint, Confluence, OneBug, and so on.

You can integrate the Secure Private Access service with Citrix® StoreFront Cloud. Users access their cloud store from a web browser or Citrix Workspace™ app. The store provides a unified user experience for the configured SaaS apps, configured virtual apps, or any other resources.

System requirements

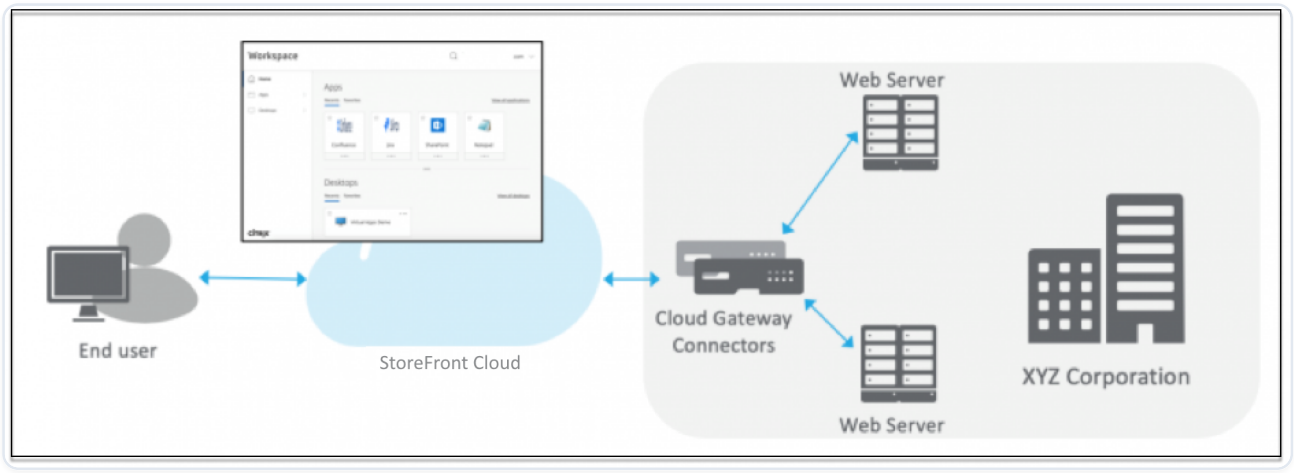
Connector Appliance - Use the Connector Appliance with the Citrix Secure Private Access service to support VPN-less access to the enterprise web apps in the customers' data center. For details, see Connector Appliance for Secure Private Access.

How it works

The Citrix Secure Private Access™ service securely connects to the on-premises data center using the connector, which is deployed on-premises. This connector acts as a bridge between enterprise web apps deployed on-premises and the Citrix Secure Private Access service. These connectors can be deployed in an HA pair and require only an outbound connection.

A TLS connection between the Connector Appliance and the Citrix Secure Private Access service in the cloud secures the on-premises applications that are enumerated into the cloud service. Web applications are accessed and delivered through their store using a VPN-less connection.

The following figure illustrates accessing web applications from their store using StoreFront Cloud.

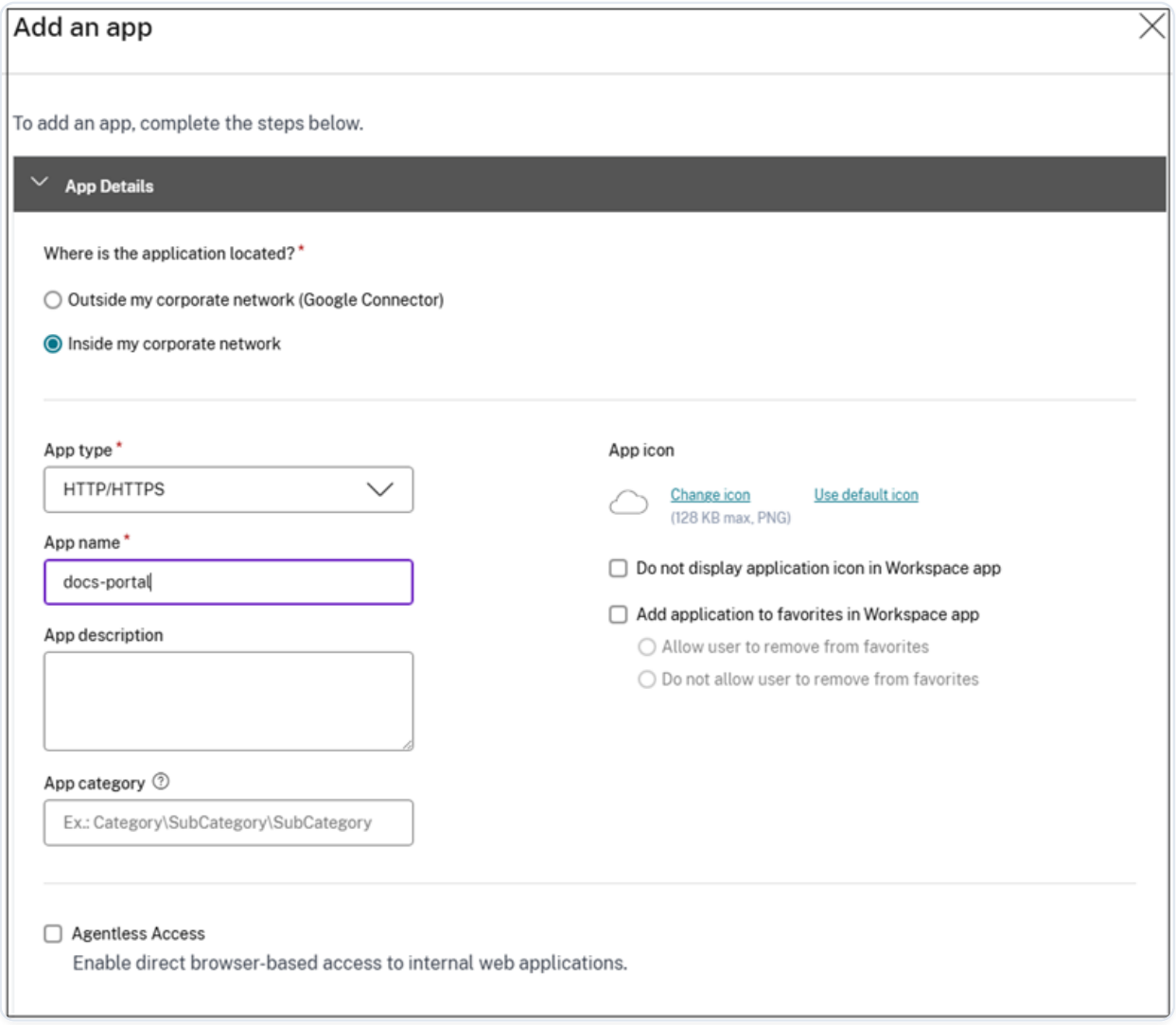


Configure a Web app

1. Log in to Citrix Cloud and select **Secure Private Access**.
2. Click **Applications > App Configuration** and then click **Add an app**.
3. In the **Choose a template** section, click **Skip**. Templates are available only for SaaS apps.
4. In **Where is the application location?**, select **Inside my corporate network**.
    - Select **Inside my corporate network** for applications hosted within your organization's private network infrastructure, behind firewalls and accessible only through internal network connection.

- Select **Outside my corporate network (Google Connector):** For applications hosted outside your organization's private network infrastructure. Traffic routing occurs directly from users to the external application via the Google Cloud Connector.

5. Enter the following details in the **App Details** section and click **Next.**



- **App type** – Select the app type.

> **Note:**
>
> For Chrome Enterprise Premium (CEP), only HTTPS enterprise web and SaaS apps are supported. HTTP enterprise web and SaaS apps are not supported.

- **App name** – Name of the application.
- **App description** - A brief description of the app. This description is displayed to your users in the store.

- **App category** - Add the category and the subcategory name (if applicable) under which the app that you're publishing must appear in the store UI. You can add a new category for each app or use existing categories from the store UI. Once you specify a category for a web or a SaaS app, the app shows up in the store UI under the specific category.
  - The category/subcategories are admin configurable and admins can add a new category for every app.
  - The **App category** field is applicable for HTTP/HTTPS apps and is hidden for TCP/UDP apps.
  - The category/subcategories names must be separated by a backslash. For example, **Business And Productivity\Engineering**. Also, this field is case sensitive. Admins must ensure that they define the correct category. If there's a mismatch between the name in store 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 store 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. If you do not change the icon, the default icon is displayed.

  If you do not want to display the app icon, select **Do not display application icon to users.**
- Select **Agentless Access** to enable users access the app directly from a client browser. For details, see Direct access to Enterprise web apps.
- **URL** – URL with your customer ID. The URL must contain your customer ID (Citrix Cloud™ customer ID). To get your customer ID, see Sign up for Citrix Cloud. In case SSO fails or you do not want to use SSO, the user is redirected to this URL.

  Customer domain name and **Customer domain ID** - Customer domain name and ID are used to create the app URL and other subsequent URLs in the SAML SSO page.

  For example, if you're adding a Salesforce app, your domain name is `salesforceformyorg` and ID is 123754, then the app URL is `https://salesforceformyorg.my.salesforce.com/?so=123754.`

  Customer domain name and Customer ID fields are specific to certain apps.

- **Related Domains** – The related domain is auto-populated based on the URL that you've provided. Related domain helps the service to identify the URL as part of the app and route traffic accordingly. You can add more than one related domain.

  > **Note:**
  >
  > A warning message appears if duplicate related domains are added or if a related domain is also added as a URL for a different app. To avoid these issues, see Best Practices for Web and SaaS application configurations.

- **Import HAR** – You can upload a HAR file to automatically discover the domains that an application accesses. Review the discovered domains and select the ones you want to add to the application's related-domain configuration. This simplifies application onboarding by reducing the need to manually identify and configure related domains. For more information, see Discover related domains using a HAR file.
- **Maintain consistent connection** - Select this checkbox to enable consistent connection to the same Connector Appliance. For details about consistent connections, see Maintain consistent connection.

  > **Note:**
  >
  > When the **Maintain consistent connection** option is selected, the routing type for the application must be set to **Internal via Connector** in the App Connectivity section.

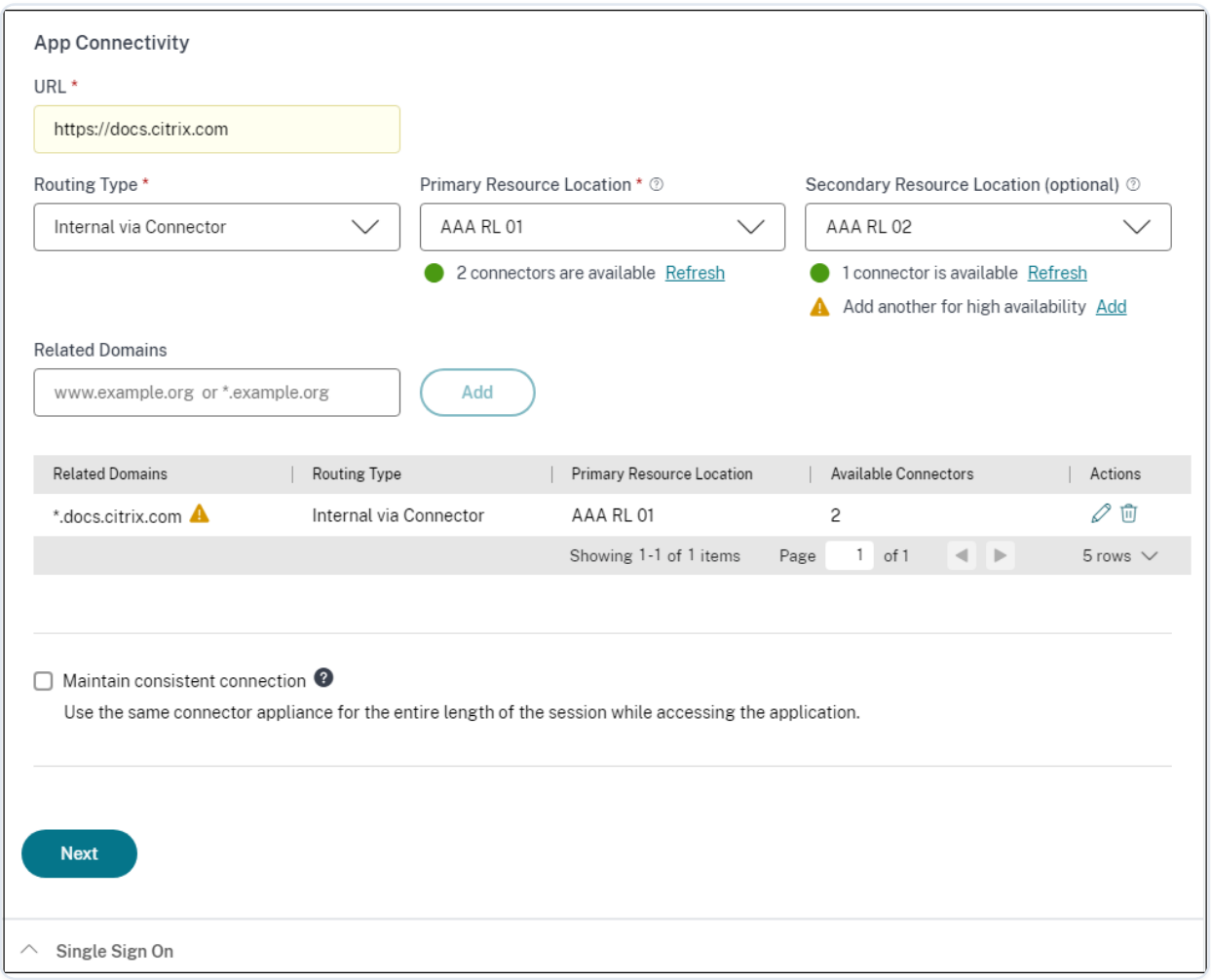
- Click **Add application to favorites Workspace app** to add this app as a favorite app in Citrix Workspace app.
  - Click **Allow user to remove from favorites** to allow app subscribers to remove the app from the favorites apps list in Citrix Workspace app. When you select this option, a yellow star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

If you remove the apps marked as favorites from the Secure Private Access service console, then users must manually remove the app from the favorites list in their store. The apps aren't auto deleted from the store if removed from the Secure Private Access service console.

Important:

- To enable zero-trust-based access to the apps, apps are denied access by default. Access to the apps is enabled only if an access policy is associated with the application.
- If multiple apps are configured with the same FQDN or some variation of the wildcard FQDN, this might result in a conflicting configuration.
- These issues can be resolved by following some of the best practices. For details, see Best practices for Web and SaaS application configurations.

6. In the **App Connectivity** section, you define routing for the related domains of applications, if the domains must be routed externally or internally through Citrix Connector™ Appliance.



- **Routing Type** - Select one of the following:
  - **Internal – bypass proxy** - The domain traffic is routed through Connector Appliance™, bypassing the customer's web proxy configured on the Connector Appliance.
  - **Internal via Connector** - The apps can be external but the traffic must flow through the Connector Appliance to the outside network.
  - **External** – The traffic flows directly to the internet.
- **Primary and secondary resource locations** - Admins can ensure high availability of applications even during disruptions by configuring a secondary resource location or by using the **First Available** option.
  - **Primary Resource Location:** Select the primary resource location where the application is hosted. Alternatively, admins can select the option **First Available** in **Primary Resource Location**.
  - **First available:** The **First Available** option ensures that a working resource location is used. When **First Available** is selected, the system automatically routes traffic to the first available location. This ensures continuous application access without manual

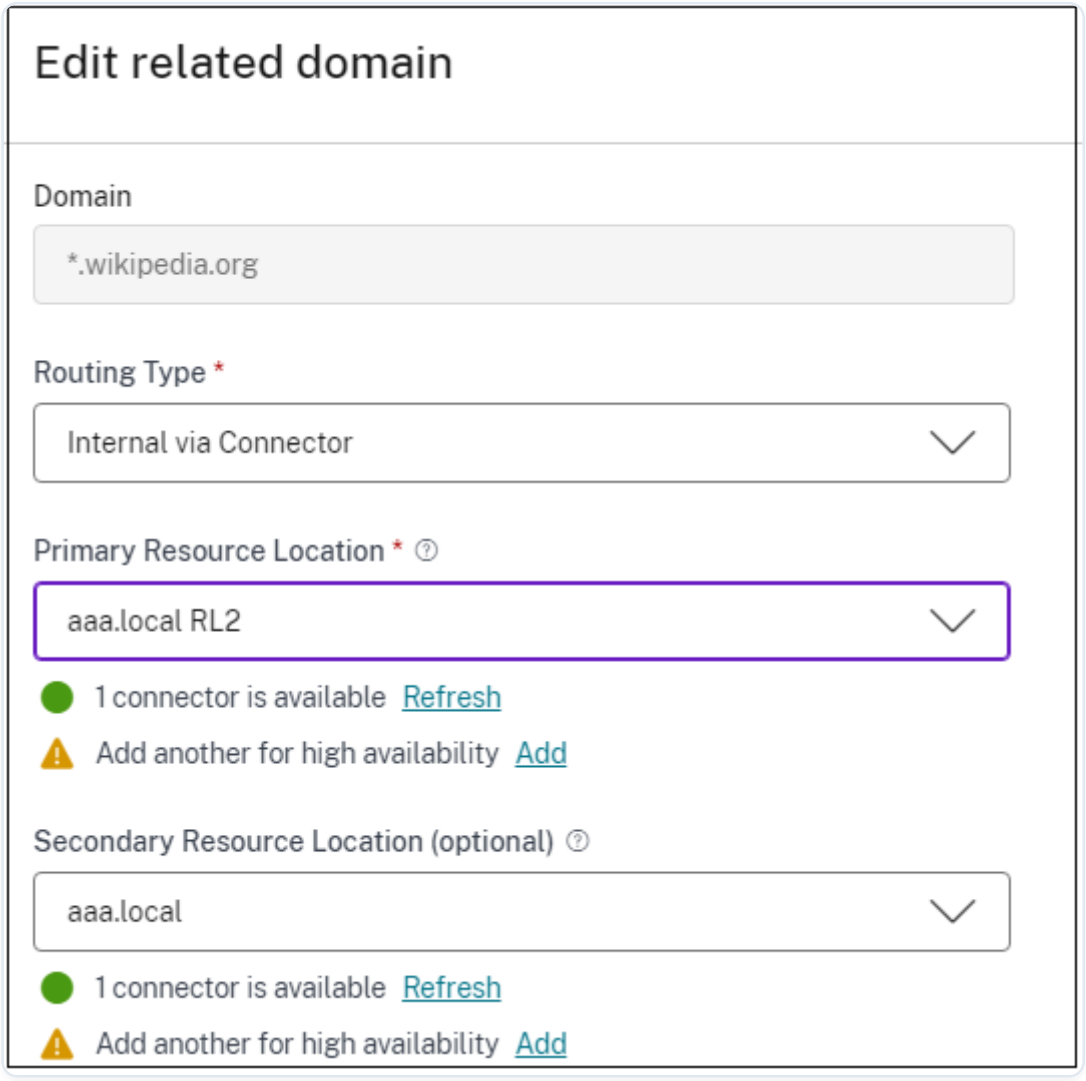
intervention. For instance, if ResourceLocation1 is unavailable but ResourceLocation2 is reachable, then ResourceLocation2 is selected by default to front-end the application.

- **Secondary Resource Location** - The **Secondary Resource Location** option becomes available only if a primary resource location is explicitly specified. If the primary resource location becomes unavailable, for reasons such as a Connector Appliance or data center failure, the application fails over to the specified secondary resource location. The secondary resource location can also act as a failover even when the application is hosted in another data center.

You can also set a primary and secondary resource location or select the **First Available** option for each of the related domains.

a. Click the edit icon in the **Actions** column of the Related Domains table.

b. Set the primary and secondary resource location or choose the **First Available** option.



Note:

- Setting the backup resource location and using the **First Available** option feature is currently in Preview.
- When you delete an application, its routing entries are removed automatically. For more information, see Automatic cleanup of routing entries on application deletion.

- **Maintain consistent connection** - Select this checkbox to enable consistent connection to the same Connector Appliance. For details about consistent connections, see Maintain consistent connections.

Note:

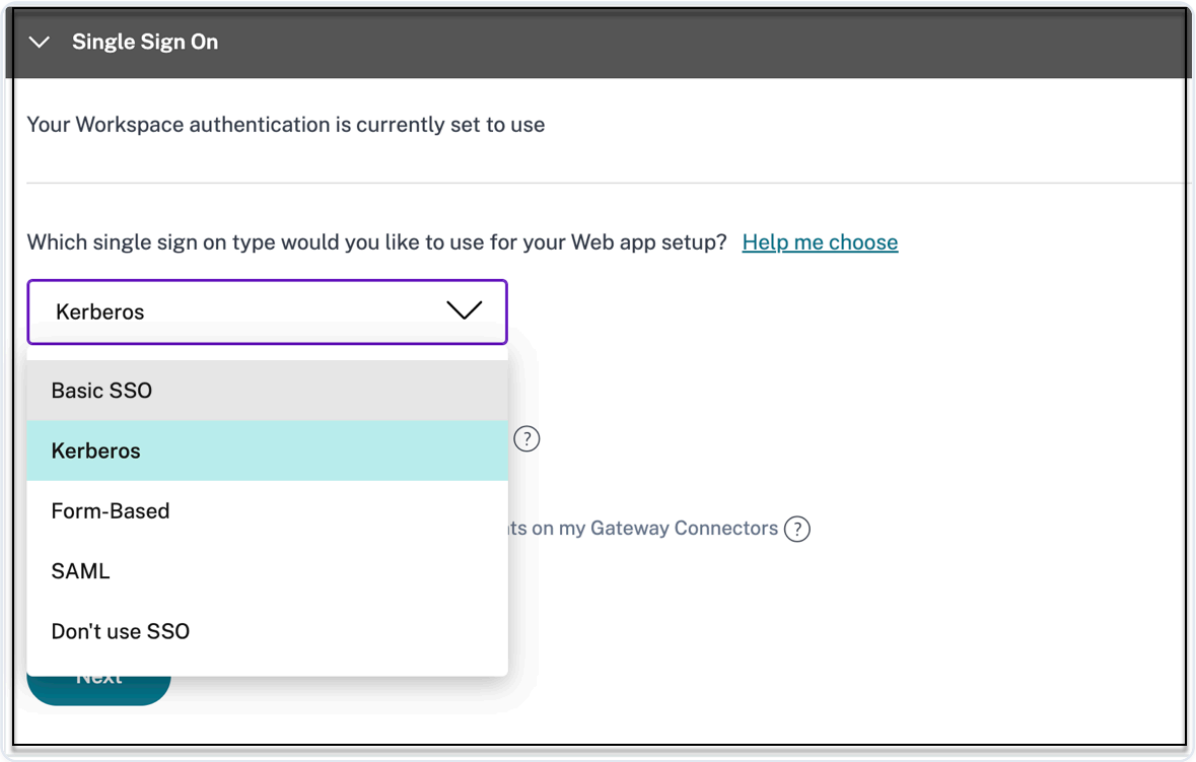
When the **Maintain consistent connection** option is selected, the routing type for the application must be set to **Internal via Connector** in the App Connectivity section.

7. Set the preferred sign-on method.

Note:

The single sign-on option is not applicable for Citrix Secure Access with Chrome Enterprise (CEP).

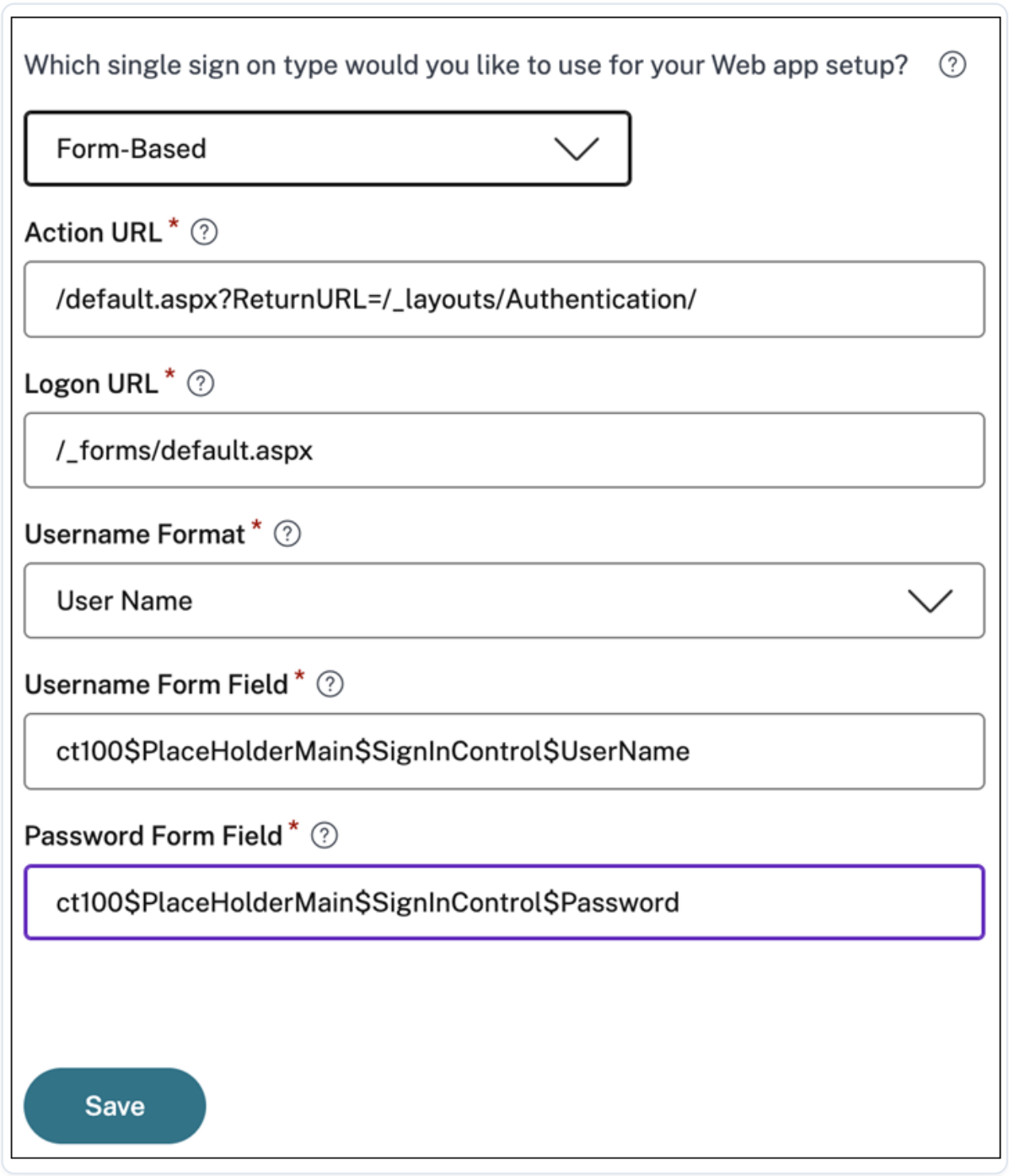
a. In the **Single Sign On** section, select your preferred single sign-on type to be used for your application and click **Save.** The following single sign-on types are available.



- **Basic** – If your back-end server presents you with a basic-401 challenge, choose **Basic SSO**. You do not need to provide any configuration details for the **Basic** SSO type.
- **Kerberos** – If your back-end server presents you with the negotiate-401 challenge, choose **Kerberos**. You do not need to provide any configuration details for the **Kerberos** SSO type.
- **Form-Based** – If your back-end server presents you with an HTML form for authentication, choose **Form-Based**. Enter the configuration details for the **Form-Based** SSO type.
- **SAML** - Choose **SAML** for SAML-based SSO into web applications. Enter the configuration details for **SAML** SSO type.
- **Don't use SSO** – Use the **Don't use SSO** option when you do not need to authenticate a user on the back end server. When the **Don’t use SSO** option is selected, the user is redirected to the URL configured under the **App details** section.

Form based details:

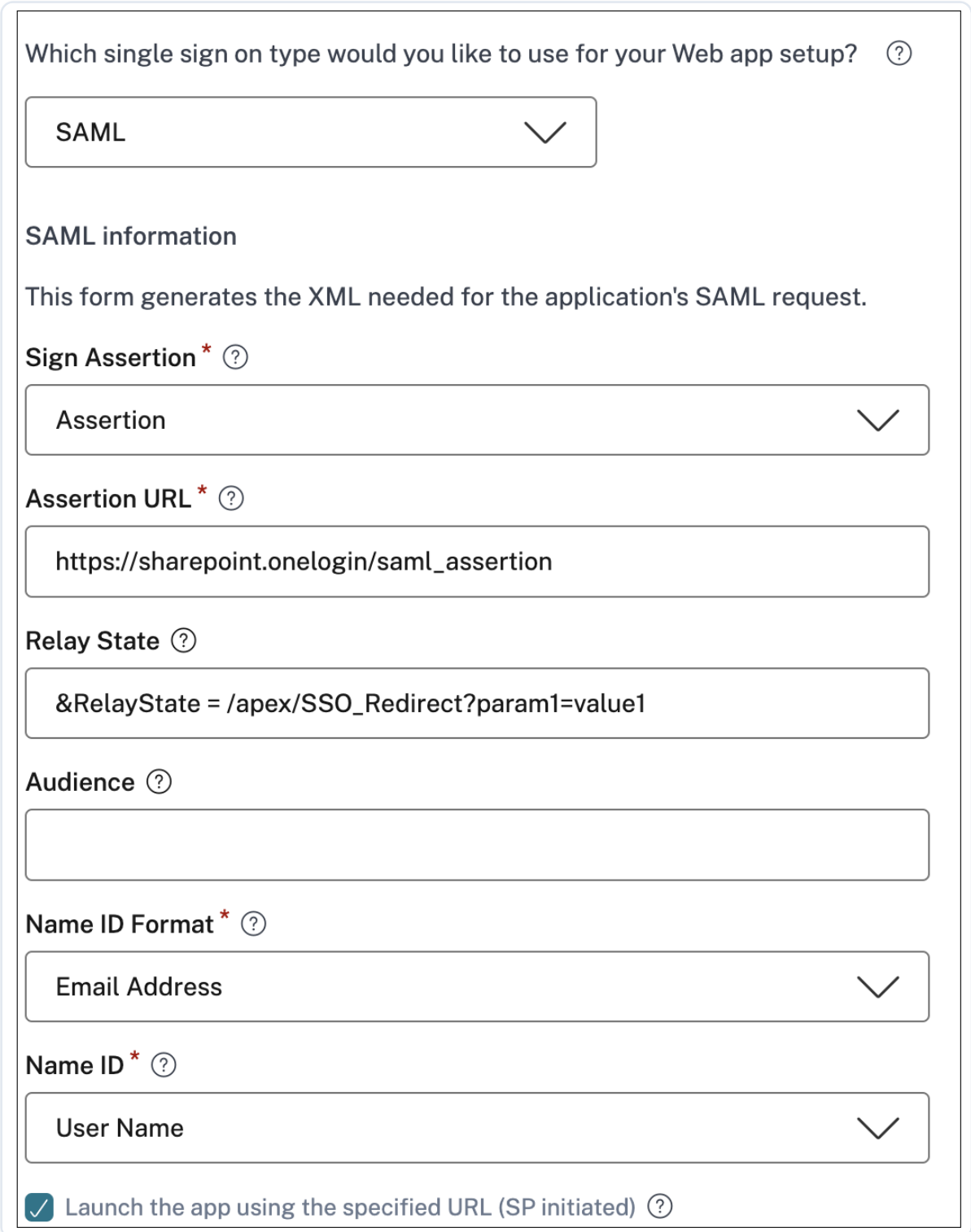
Enter the following form-based configuration details in the Single Sign On section and click **Save.**



- **Action URL** - Type the URL to which the completed form is submitted.
- **Logon form URL** – Type the URL on which the logon form is presented.
- **Username Format** - Select a format for the user name.
- **Username Form Field** – Type a user name attribute.
- **Password Form Field** – Type a password attribute.

SAML:

Enter the following details in the Sign sign on section and click **Save.**



- **Sign Assertion** - Signing assertion or response ensures message integrity when the response or assertion is delivered to the relying party(SP). You can select **Assertion, Response, Both,** or **None**.
- **Assertion URL** – Assertion URL is provided by the application vendor. The SAML assertion is sent to this URL.
- **Relay State** – The Relay State parameter is used to identify the specific resource the users access after they’re signed in and directed to the relying party's federation server.

Relay State generates a single URL for the users. Users can click this URL to log on to the target application.

- **Audience** – Audience is provided by the application vendor. This value confirms that the SAML assertion is generated for the correct application.
- **Name ID Format** – Select the supported name identifier format.
- **Name ID** – Select the supported name ID.

i. In **Advanced attributes (optional)** add additional information about the user that is sent to the application for access control decisions.

ii. Download the metadata file by clicking the link under **SAML Metadata.** Use the downloaded metadata file to configure SSO on the SaaS apps server.

- You can copy the SSO login URL under **Login URL** and use this URL when configuring SSO on the SaaS apps server.
- You can also download the certificate from the **Certificate** list and use the certificate when configuring SSO on the SaaS apps server.

8. Click **Save** and then click **Finish.**

After you click **Finish**, the app is added to the Applications page. You can edit or delete an app from the Applications page after you've configured the application. To do so, click the ellipsis button on an app and select the actions accordingly.

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

Important:

- To grant access to the apps for the users, admins are required to create access policies. In access policies, admins add app subscribers and configure security controls. For details, see Create access policies.

Automatic cleanup of routing entries on application deletion

When you configure an application, its destinations (FQDNs or application domains) are added to the routing table, which Secure Private Access uses for routing decisions. When you delete an application, Secure Private Access cleans up the routing entries based on the following rules:

- **Unreferenced entries are removed** - If a routing entry (FQDN or application domain) associated with the deleted application is not referenced by any other application, Secure Private Access removes it from the routing table automatically.
- **Shared entries are retained** - If a routing entry is used by more than one application, deleting one of those applications does not remove the shared entry. The entry remains in the routing table for as long as at least one active application references it.
- **No retroactive removal** - Routing entries are evaluated and removed only as part of an application deletion. Existing entries are not removed retroactively unless they are confirmed to be unused by any application.

Note:

- The cleanup runs automatically when an application is deleted from the Applications page (using the ellipsis (...) menu). No administrator action is required.
- Because shared routing entries are preserved, deleting an application does not disrupt access to other applications that share the same destination.

Configure SaaS apps

Software as a Service (SaaS) is a software distribution model that delivers software remotely as a web-based service. Commonly used SaaS apps include Salesforce, Workday, Concur, GoToMeeting, and so forth.

You can integrate the Secure Private Access service with Citrix® StoreFront Cloud. Users access their cloud store from a web browser or Citrix Workspace™ app. The store provides a unified user experience for the configured SaaS apps, configured virtual apps, or any other resources. SaaS app delivery using the Secure Private Access service provides you an easy, secure, robust, and scalable solution to manage the apps.

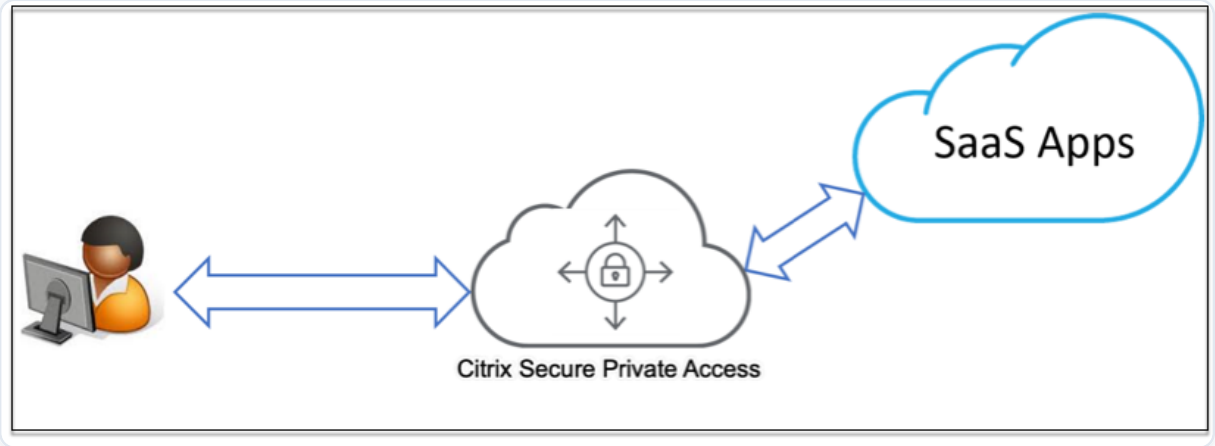
How SaaS apps are supported with the Secure Private Access service

1. Customer admin configures SaaS apps using the Secure Private Access service UI.
2. Admin provides the store URL to the end users.
3. To launch the app, a user clicks the enumerated SaaS app icon.

4. SaaS app trusts the SAML assertion provided by the Secure Private Access service and the app is launched.

Note:

- To grant access to the apps for the users, admins are required to create access policies. In access policies, admins add app subscribers and configure security controls. For details, see Create access policies.
- Configured SaaS apps are aggregated along with virtual apps and other resources in the store for a unified user experience.



Configure a SaaS app

1. Log in to Citrix Cloud and select **Secure Private Access**.
2. Click **Applications > App Configuration** and then click **Add an app**.

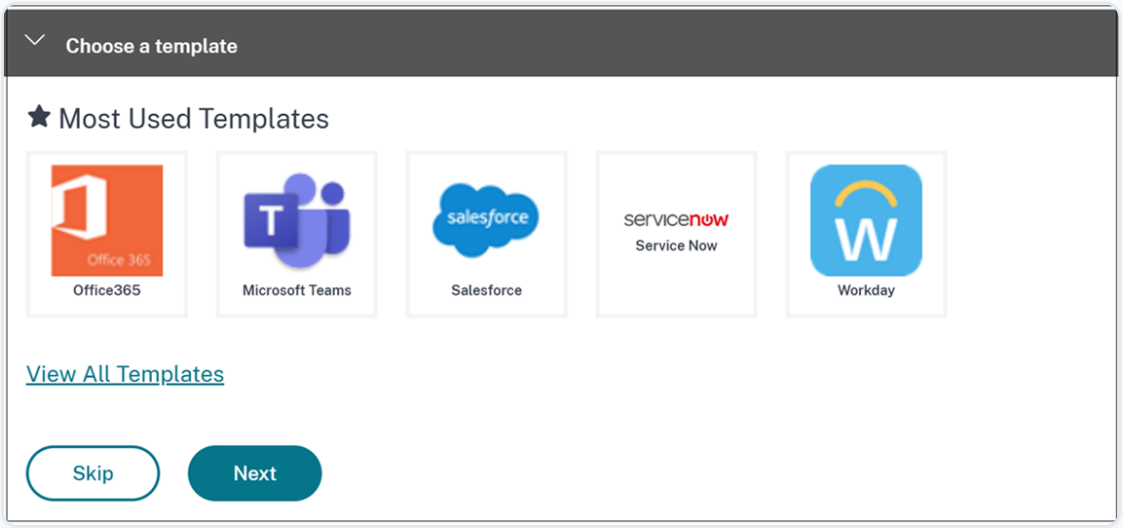
Note:

You can configure an app manually or by using a template. Templates prefill most application settings, but you must still provide customer-specific details.

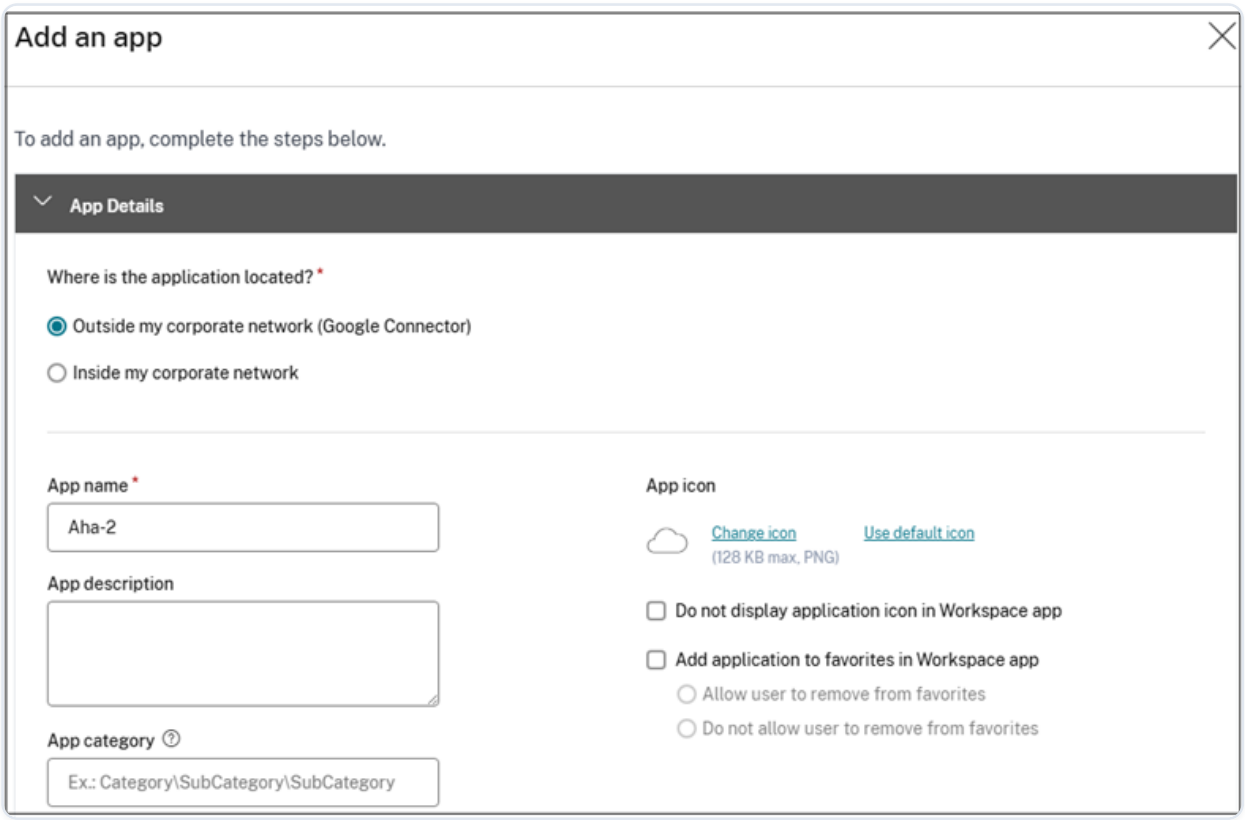
Manual configuration: Click **Skip** in **Choose a template** section and then configure the application in the **App Details** section. Start from step 3.

Template-based configuration: Click **Choose a template**, select a template, and click **Next**. Review and update the app details as needed.

- The app configuration page highlights the five most-used templates to simplify and accelerate app onboarding.
- Select **View the templates** to browse templates for other supported SaaS apps.



3. In **Where is the application location?**, choose the location of the target application to determine the routing path, policies, and access mechanisms that must be applied. For SaaS apps, select **Outside my corporate network (Google Connector)**.
   - **Outside my corporate network (Google Connector):** For applications hosted outside your organization's private network infrastructure. Traffic routing occurs directly from users to the external application via Citrix Cloud.
   - **Inside my corporate network**: For applications hosted within your organization's private network infrastructure, behind firewalls and accessible only through internal network connections.
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 store.
- **App category** - Add the category and the subcategory name (if applicable) under which the app that you're publishing must appear in the store UI. You can add a new category for each app or use existing categories from the store UI. Once you specify a category for a web or a SaaS app, the app shows up in the store UI under the specific category.
  - The category/subcategories are admin configurable and admins can add a new category for every app.
  - The **App category** field is applicable for HTTP/HTTPS apps and is hidden for TCP/UDP apps.
  - The category/subcategories names must be separated by a backslash. For example, **Business And Productivity\Engineering**. Also, this field is case sensitive. Admins must ensure that they define the correct category. If there's a mismatch between the name in the store 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 store 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. If you do not change the icon, the default icon is displayed.

  If you do not want to display the app icon, select **Do not display application icon to users**.

- **URL** – URL with your customer ID. The URL must contain your customer ID (Citrix Cloud™ customer ID). To get your customer ID, see Sign up for Citrix Cloud. In case SSO fails or you do not want to use SSO, the user is redirected to this URL.
- **Customer domain name** and **Customer domain ID** - Customer domain name and ID are used to create the app URL and other subsequent URLs in the SAML SSO page.

  For example, if you're adding a Salesforce app, your domain name is `salesforceformyorg` and ID is 123754, then the app URL is `https://salesforceformyorg.my.salesforce.com/?so=123754.`

  Customer domain name and Customer ID fields are specific to certain apps.

- **Related Domains** – The related domain is auto-populated based on the URL that you've provided. Related domain helps the service to identify the URL as part of the app and route traffic accordingly. You can add more than one related domain.

  > **Note:**
  >
  > A warning message appears if duplicate related domains are added or if a related domain is also added as a URL for a different app. To avoid these issues, see Best Practices for Web and SaaS application configurations.

- **Import HAR** – You can upload a HAR file to automatically discover the domains that an application accesses. Review the discovered domains and select the ones you want to add to the application's related-domain configuration. This simplifies application onboarding by reducing the need to manually identify and configure related domains. For more information, see Discover related domains using a HAR file.
- **Maintain consistent connection** - Consistent connection to the Connector Appliance is supported for SaaS apps. Select the **Maintain consistent connection** checkbox and

choose **Internal via Connector** as the connectivity type in the **App Connectivity** section. For details about consistent connections, see Maintain consistent connection.

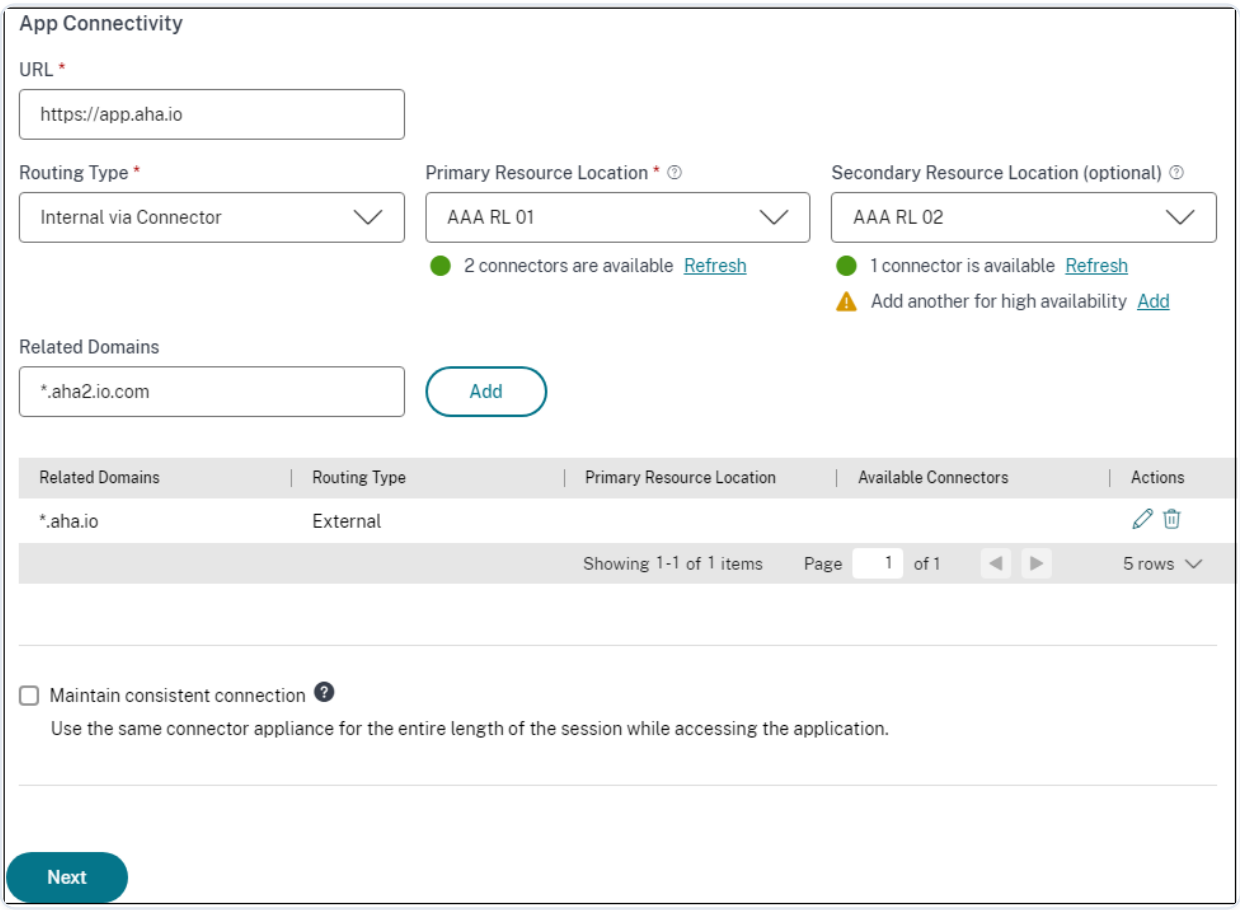
- Click **Add application to favorites in Workspace app** to add this app as a favorite app in Citrix Workspace app.
  - Click **Allow user to remove from favorites** to allow app subscribers to remove the app from the favorites apps list in Citrix Workspace app. When you select this option, a yellow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

  If you remove the apps marked as favorites from the Secure Private Access service console, then users must manually remove the apps from the favorites list in their store. The apps aren't auto deleted from the store if removed from the Secure Private Access service console.

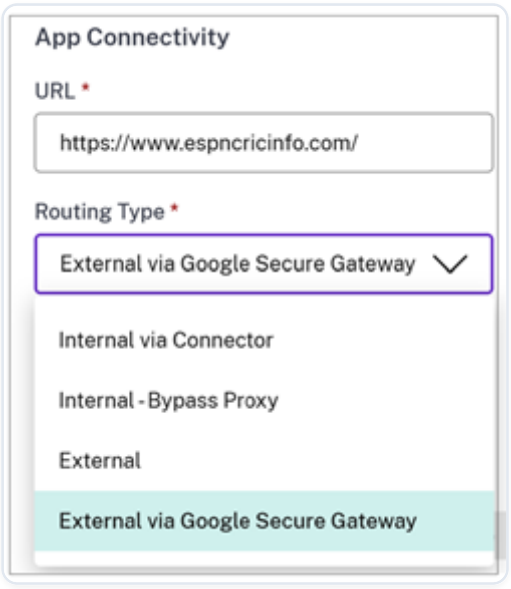
Important:

- Access to a SaaS app is governed by its access policy. An app is granted access, blocked, or left unmanaged based on the access policy rule that matches the user. If no rule matches the user, or no access policy is associated with the app, the app is not blocked. It is left unmanaged and the browser connects to it directly. To block an app for users who are not covered by any rule, add an All Users > Deny access rule at the lowest priority. For more information, see Block SaaS applications by default.
- If multiple apps are configured with the same FQDN or some variation of the wildcard FQDN, this might result in a conflicting configuration.
- These issues can be resolved by following some of the best practices. For details, see Best practices for Web and SaaS application configurations.

5. In the **App Connectivity** section, you define routing for the related domains of applications, if the domains must be routed externally or internally through Citrix Connector™ Appliance.



- **Routing Type** - Select one of the following:
  - **Internal – bypass proxy** - The domain traffic is routed through Connector Appliance™, bypassing the customer's web proxy configured on the Connector Appliance.
  - **Internal via Connector** - The apps can be external but the traffic must flow through the Connector Appliance to the outside network.
  - **External** – The traffic flows directly to the internet.
  - **External via Google Secure Gateway** — The traffic flows to the internet through the Google Secure Gateway. For more information, see Routing via Google Secure Gateway.

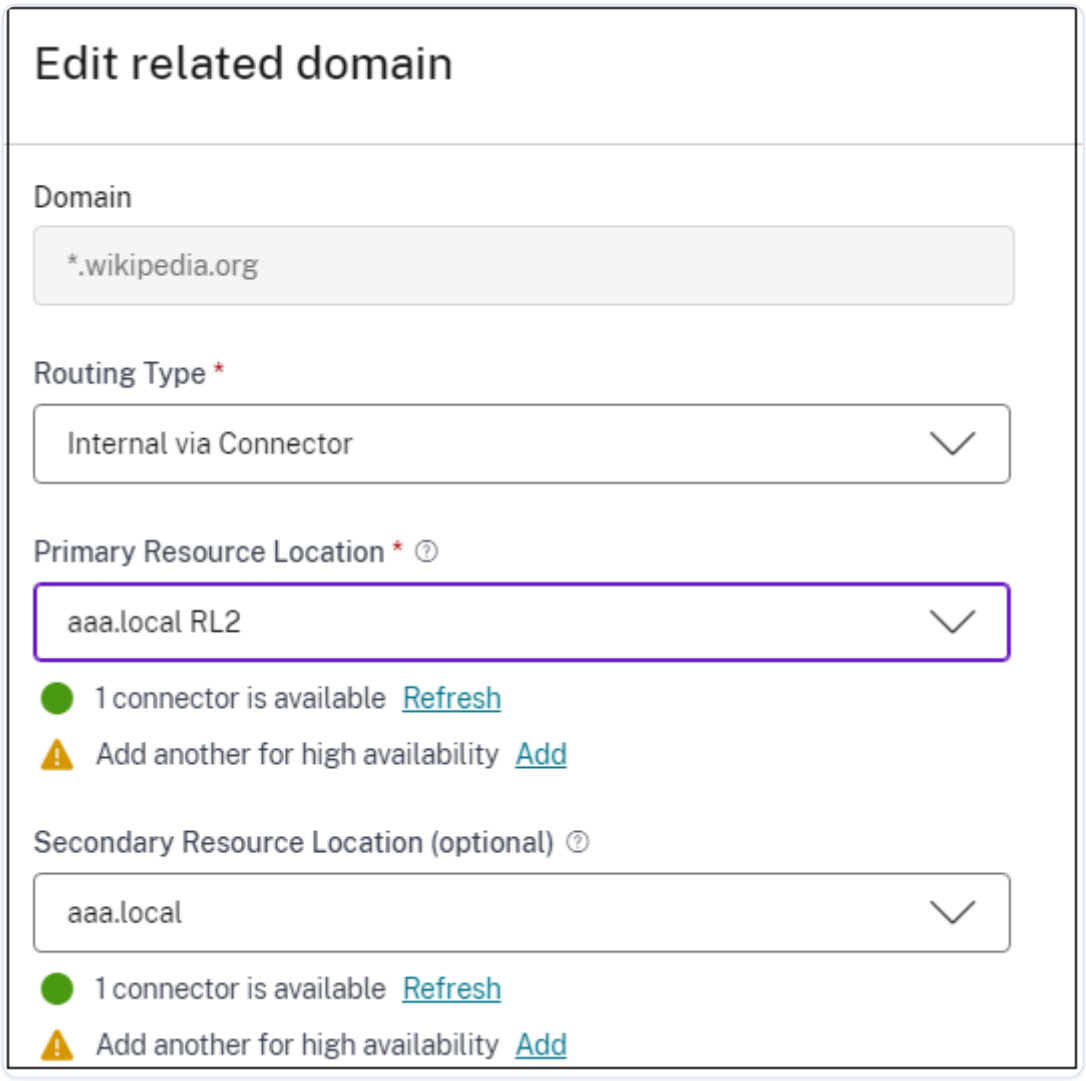


- **Primary and secondary resource locations** - Admins can ensure high availability of applications even during disruptions by configuring a secondary resource location or by using the **First Available** option.
  - **Primary Resource Location:** Select the primary resource location where the application is hosted. Alternatively, admins can select the option **First Available** in **Primary Resource Location**.
  - **First available:** The **First Available** option ensures that a working resource location is used. When **First Available** is selected, the system automatically routes traffic to the first available location. This ensures continuous application access without manual intervention. For instance, if ResourceLocation1 is unavailable but ResourceLocation2 is reachable, then ResourceLocation2 is selected by default to front-end the application.
  - **Secondary Resource Location** - The **Secondary Resource Location** option becomes available only if a primary resource location is explicitly specified. If the primary resource location becomes unavailable, for reasons such as a Connector Appliance or data center failure, the application fails over to the specified secondary resource location. The secondary resource location can also act as a failover even when the application is hosted in another data center.

You can also set a primary and secondary resource location or select the **First Available** option for each of the related domains.

a. Click the edit icon in the **Actions** column of the Related Domains table.

b. Set the primary and secondary resource location or choose the **First Available** option.



> **Note:**
>
> - Setting the backup resource location and using the **First Available** option feature is currently in Preview.
> - When you delete an application, its routing entries are removed automatically. For more information, see Automatic cleanup of routing entries on application deletion.

- **Maintain consistent connection** - Select this checkbox to enable consistent connection to the same Connector Appliance. For details about consistent connections, see Maintain consistent connections.

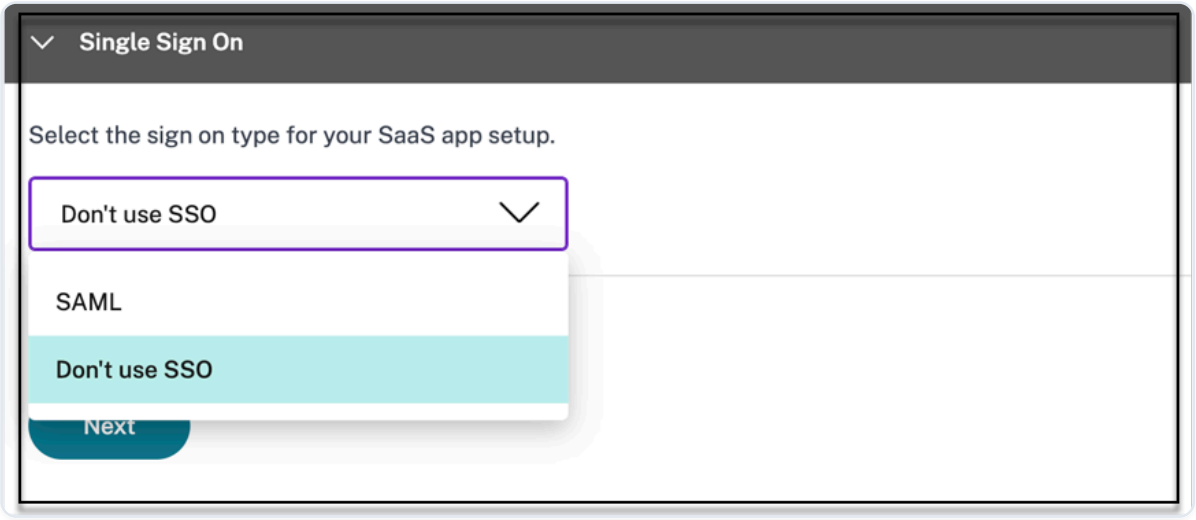
> **Note:**

> When the **Maintain consistent connection** option is selected, the routing type for the application must be set to **Internal via Connector** in the App Connectivity section.

6. Set a preferred sign-on method.

> **Note:**
>
> The single sign-on option is not applicable for Citrix Secure Access with Chrome Enterprise (CEP).

a. In the **Single Sign On** section, select your preferred single sign-on type to be used for your application and click **Save.** The following single sign-on types are available.



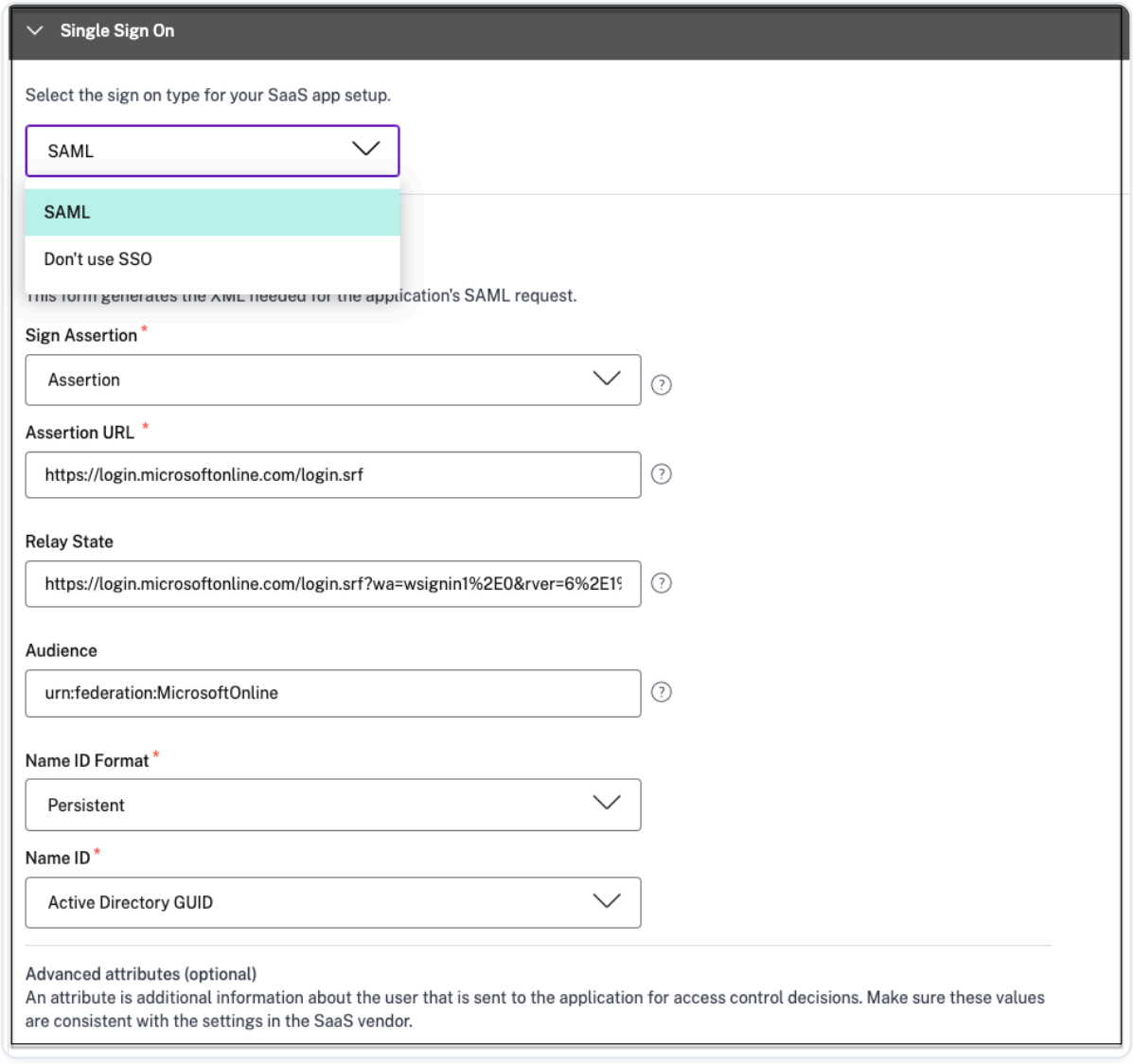
- **Don't use SSO** – Use the **Don't use SSO** option when you do not need to authenticate a user on the back end server. When the **Don’t use SSO** option is selected, the user is redirected to the URL configured under the **App details** section.
- **SAML** - Choose **SAML** for SAML-based SSO into web applications. Enter the configuration details for **SAML** SSO type.

Enter the following details in the Sign sign on section and click **Save**.

- **Sign Assertion** - Signing assertion or response ensures message integrity when the response or assertion is delivered to the relying party(SP). You can select **Assertion, Response, Both,** or **None**.
- **Assertion URL** – Assertion URL is provided by the application vendor. The SAML assertion is sent to this URL.

- **Relay State** – The Relay State parameter is used to identify the specific resource the users access after they're signed in and directed to the relying party's federation server. Relay State generates a single URL for the users. Users can click this URL to log on to the target application.
- **Audience** – Audience is provided by the application vendor. This value confirms that the SAML assertion is generated for the correct application.
- **Name ID Format** – Select the supported name identifier format.
- **Name ID** – Select the supported name ID.
- Select **Launch the app using the specific URL (SP initiated)** to override the identity provider-initiated flow and use only the service provider-initiated flow.

b. In **Advanced attributes (optional)**, add additional information about the user that is sent to the application for access control decisions.



c. Download the metadata file by clicking the link under **SAML Metadata**. Use the downloaded metadata file to configure SSO on the SaaS apps server.

- You can copy the SSO login URL under **Login URL** and use this URL when configuring SSO on the SaaS apps server.
- You can also download the certificate from the **Certificate** list and use the certificate when configuring SSO on the SaaS apps server.

7. Click **Save** and then click **Finish.**

After you click **Finish**, the app is added to the Applications page. You can edit or delete an app from the Applications page after you've configured the application. To do so, click the ellipsis button on an app and select the actions accordingly.

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

Routing via Google Secure Gateway

When you set a SaaS app's routing type to **External via Google Secure Gateway**, traffic for that app is routed to the internet through Google Secure Gateway instead of directly from the client.

- You can set this routing type during app configuration, where it becomes the default routing for that app.
- You can also set it as a routing exception in an access policy, where it applies only to users in that policy and overrides the app's default routing.
- This routing type is available only for SaaS apps and only for customers integrated with Google Chrome Enterprise Premium. It is not available for internal web apps.
- In the Citrix Secure Access client, this option behaves the same as **External**. During import, set the **Routing type** value to **External via Google Secure Gateway**.

> **Note:**
>
> For SaaS apps accessed through Citrix Enterprise Browser™, the **Routing Type** appears as **External via Google Secure Gateway** instead of **External**. This is only a UI display difference and does not change the routing behavior. The traffic continues to flow directly to the internet.

Automatic cleanup of routing entries on application deletion

When you configure an application, its destinations (FQDNs or application domains) are added to the routing table, which Secure Private Access uses for routing decisions. When you delete an application, Secure Private Access cleans up the routing entries based on the following rules:

- **Unreferenced entries are removed** - If a routing entry (FQDN or application domain) associated with the deleted application is not referenced by any other application, Secure Private Access removes it from the routing table automatically.
- **Shared entries are retained** - If a routing entry is used by more than one application, deleting one of those applications does not remove the shared entry. The entry remains in the routing table for as long as at least one active application references it.
- **No retroactive removal** - Routing entries are evaluated and removed only as part of an application deletion. Existing entries are not removed retroactively unless they are confirmed to be unused by any application.

> **Note:**
>
> - The cleanup runs automatically when an application is deleted from the Applications page (using the ellipsis (...) menu). No administrator action is required.
> - Because shared routing entries are preserved, deleting an application does not disrupt access to other applications that share the same destination.

SaaS app server specific configuration

Following are the links to the documents that have guidance on app server specific configuration using a template. Citrix presently supports the following SaaS apps and is continually adding support for more apps.

- 15Five - Continuous performance management tool to coach employees.
- 10000 ft - Project management tool to plan for growth.
- 4me - Service management tool for collaboration between internal, external, and outsourced teams.
- Abacus - Real-time expense reporting software.
- Absorb - Learning management tool.
- Accompa - Requirements management tool to build products.

- Adobe Captivate Prime - Learning management system to deliver personalized learning experiences across devices.
- Aha - Product roadmap and marketing planning tool to build products and launch campaigns.
- AlertOps - Collaboration incidence response tool to manage IT incidents.
- Allocadia - Marketing performance management tool to manage an organization’s marketing planning process.`
- Ana plan - Planning tool to help organizations with decision making by connecting data, people, and plans.
- &frankly - An engagement tool to drive change in the workplace.
- Anodot - An AI platform that monitors times series data, detects anomalies and forecasts business performance in real time.
- App Follow - Product management tool for accelerating global app growth and increasing customer loyalty.
- Assembla - Version control and source code management tool for software development.
- Automox - Patch management tool to track, control, and manage the patching process.
- Azendoo - Collaboration tool for teams to converse and collaborate.
- BambooHR - Human resources management tool to manage employee data.
- Bananatag - Tool to track and schedule emails, track files and create email templates
- Base CRM - Sales management tool to manage emails, phone calls, and notes.
- Beekeeper - Tool to integrate multiple operational systems and communication channels in one Secure Hub that is accessible from desktop and mobile devices.
- BitaBIZ - Absence and vacation planning and communication tool for leave and absence management.
- BlazeMeter - Testing suite.
- Blissbook - Policy management tool to create employee handbooks.
- BlueJeans - Video conferencing solution.
- Bold360 - Live chat tool for customer engagement.
- Bonusly - Employee recognition and reward management tool to recognize team contributions.
- Box - Content management and file sharing tool to manage, share, and access your content.
- Branch - A mobile linking platform powering deep links and mobile.
- Brandfolder - Digital asset management tool to store and share digital assets.

- Breezy HR - Recruiting software and applicant tracking system.
- `Buddy Punch` - Time management tool to monitor employee attendance.
- Bugsnag - Monitoring tool to manage application stability and report errors and diagnostic data.
- Buildkite - Infrastructure tool for continuous integration software development.
- Bullseye Locations - Store locator tool to locate a store or dealer on a device.
- CA Flowdock - Collaboration tool for teams to converse and collaborate.
- CakeHR - Human resources management tool for attendance and performance management.
- Cardboard - Collaborative product planning tool to track disorganized information.
- Citrix Cedexis - Traffic management tool for large websites to leverage multivendor sourcing of data centers, cloud providers, and content delivery networks.
- CipherCloud - Platform that provides an end-to-end data protection and advanced threat protection, and comprehensive compliance capabilities for an enterprise embracing cloud-based applications.
- Celoxis - Project management tool to create project plans, automate work, and collaborate.
- CircleHD - Training, learning, and collaboration tool to share videos and slides within the organization.
- Circonus - Data analytics and monitoring tool to deliver alerts, graphs, dashboards, and machine-learning intelligence.
- Cisco Umbrella - Cloud security platform to provide the first line of defense against threats on the internet.
- ClearSlide - Sales engagement tool to let users share content and sales material for customer interaction.
- Cloudability - Cloud cost management platform to improve visibility, optimization, governance across cloud environments.
- CloudAMQP - Message queue tool to pass messages between processes and other systems.
- CloudCheckr - Cost management, security, reporting, and analytics tool to help users optimize their AWS and Azure deployments.
- CloudMonix - Tool for cloud and on-premises resources monitoring and automation.
- CloudPassage - Visibility and continuous monitoring tool to reduce cyber risk and maintain compliance.

- CloudRanger - Tool to streamline your backups, disaster recovery, and server control for AWS Cloud.
- Clubhouse - Project management tool for software development.
- Coggle - Mind mapping web application to create hierarchically structured documents, like a branching tree.
- Comm100 - Customer service software and communication tool for customer service professionals.
- Confluence - Content collaboration tool to help teams collaborate and share knowledge.
- ConceptShare - Proofing tool to deliver content faster, quicker, and cheaper.
- Concur - Travel and expense management tool to manage expenses on the go.
- ConnectWise Control - Business management tool to provide remote support and access.
- Contactzilla - Contact management tool to access up to date contact information.
- ContractSafe - Contract management tool to track, store, and manage contracts.
- Contentful - Software for content to create, manage, and distribute content to any platform.
- Convo - Team communication and collaboration tool for internal conversations.
- Copper - CRM tool.
- Cronitor - Monitoring tool for cron jobs.
- Crowdin - Solution that provides seamless and continuous localization for developers.
- Dashlane - Password management tool that also manages digital wallets.
- Declaree - Travel and expense management tool for business travel.
- Dell Boomi - An integration tool to connect cloud and on-premises applications and data.
- Deskpro - Help desk tool to facilitate ticket management, customer self-help, and customer feedback.
- Deputy - Workforce management tool for scheduling and tracking employees' time, tasks, and communication.
- DigiCert - Certificate management and troubleshooting tool for SSL certificates for websites.
- Dmarcian - Email monitoring tool to filter spam, malware, and phishing.
- DocuSign - An online signature tool for different documents, such as insurance, medical, and real estate.
- DOME9 ARC - Security and compliance tool to manage public cloud environments.
- Dropbox - Cloud storage tool for secure file sharing and storage.

- Duo - Security tool to provide secure access to your applications.
- Dynatrace - Medical laboratory services.
- Easy Projects - Project Management tool.
- EdApp - Learning management tool for workspace learning.
- EduBrite - Learning management tool to create, deliver, and track training programs.
- Ekarda - Electronic card designing tool.
- Envoy - Visitor management tool to manage people and packages.
- Evernote - Application for note taking, organizing, task lists, and archiving.
- Expensify - Expense management tool for expense report management, receipt tracking, and business travel.
- ezeep - Print infrastructure management tool to print from any device, any location to any printer in the Cloud.
- EZOfficeInventory - Inventory management tool to track all your assets and equipment.
- EZRentOut - Equipment rental tool to track equipment quality and availability.
- Fastly - Edge cloud platform to serve and secure applications closer to the users.
- Favro - Planning and collaboration tool for organizational flow.
- Federated Directory - Cross-company contact directory tool to search through the corporate address books of different companies.
- Feeder
- Feedly - News aggregation tool to compile news feeds from different sources.
- FileCloud - Software solution that provides a robust and secure file hosting and sharing platform for organizations.
- Fivetran - Tool to help analysts replicate data into a cloud warehouse.
- Flatter Files - Digital flat file cabinet for drawings and documents to provide a secure and simple way for providing access to content.
- Float - Resource planning tool for project scheduling and managing the teams' utilization.
- Flock - Collaboration tool.
- Formstack - An online form builder and data collection tool.
- FOSSA - Automated open source license scanning and vulnerability management tools built natively into CI/CD.
- Freshdesk - Customer support tool to help support the needs of customers.

- Freshservice - IT help desk tool to simplify IT operations.
- FrontApp - Collaboration tool to manage all conversations in one place.
- Frontify - Platform to facilitate and streamline day-to-day branding, marketing, and development operations.
- Fulcrum - Mobile data collection platform that allows you to easily build mobile forms and collect data.
- Fusebill - Billing management and recurring billing software.
- G-Suite - Set of intelligent apps to connect the people in your company.
- GetGuru - Knowledge management software.
- GitBook - Tool to create and maintain your documentation.
- GitHub - A web-based hosting service for version control using Git for repositories hosted behind a corporate firewall.
- GitLab - A complete DevOps platform, delivered as a single application.
- GlassFrog - Software to Holacracy practice.
- GoodData - An embedded BI and analytics platform that provides fast, reliable, and easy to use analytics
- GotoMeeting - Online meeting software with HD Video Conferencing capabilities.
- HackerRank - Provides competitive programming challenges for consumers and businesses.
- HappyFox - Online help desk software and web based support ticket system.
- Helpjuice - Knowledge management solution to create and maintain knowledge bases.
- Help Scout - Customer service software and knowledge base tool for customer service professionals.
- Hello sign - E-signing interface to enable signing from anywhere, at any time, on any device.
- HelpDocs - knowledge base software to guide your users when they are stuck.
- Honeybadger - Application health monitoring tool.
- Harness - Tool for continuous delivery and integration for Java, .NET apps in AWS, GCP, Azure, and Bare Metal.
- HelpDocs - Tool to create an authoritative knowledge base to guide your users when they're stuck.
- Helpmonks - A collaborative email platform for team collaboration.
- Hoshinplan - Tool to visualize your strategic plans and track statuses in one canvas.

- Hosted Graphite - Tool to monitor your website, app, server, and container performance.
- Humanity - Online employee scheduling software to manage shifts, schedules, payroll, and time clocking.
- Igloo - Digital workplace and intranet solution provider to solve IT challenges across your organization.
- iLobby - Cloud-based visitor registration management solution.
- Illumio - Security system to prevent spread of breaches inside data center and cloud environments.
- Image Relay - Digital asset management and brand management software to securely organize and share digital files.
- Informatica - Tool for SaaS apps integration and a platform for developing and deploying custom integration services.
- Intelligent contract - Contract management software.
- iMeet Central - Project management software for marketers, creative agencies, and enterprise businesses.
- InteractGo - Tool to measure real-time and historical data on system performance.
- iQualify One - Learning and management tool to deliver authentic learning experiences.
- InsideView - Data and intelligence solutions to solve sales, marketing, and other business challenges.
- Insightly - A cloud-based customer relationship management (CRM) and project management tools for small and medium size businesses.
- ITGlue - A cloud-based IT documentation platform to help MSPs standardize documentation, create knowledge bases, manage passwords. and track devices.
- Jitbit - Help desk software and ticketing system to manage and track incoming support request emails and their associated tickets.

JupiterOne - Software platform to create and manage your entire security process.

- Kanbanize - An online portfolio Kanban software for lean management.
- Klipfolio - An online dashboard platform for building powerful real-time business dashboards for your team or your clients.
- Jira - Tool to plan, track, and manage your issues and projects.

- Kanban Tool - Visual management software to improve your team performance and boost productivity.
- Keeper Security - Password manager and security software to protect your passwords and private information.
- Kentik - Tool to apply big data for network and performance monitoring, DDoS protection, and real-time ad-hoc network flow analytics.
- Kissflow - Workflow tool and business process workflow management software to automate your workflow process.
- KnowBe4 - Tool to provide security awareness training and simulated phishing.
- KnowledgeOwl - Knowledge base and authoring tool.
- Kudos - Retail, job, project, and fulfillment process systems.
- LaunchDarkly - Feature management platform to enable dev and ops teams to control the feature lifecycle.
- Lifesize - Video conferencing solution.
- Litmos - Learning management system for employee training, customer training, compliance training, and partner training.
- LiquidPlanner - Online project management software for your business.
- LeanKit - Lean-based, enterprise process and work management software to help enterprises visualize work, optimize processes, and deliver faster.
- LiveChat - Live chat and help desk software for businesses.
- LogDNA - Tool to collect, monitor, parse, and analyze logs from all sources in one centralized logging tool.
- Mango - Team collaboration software to consolidate and streamline siloed applications into one single platform.
- Manuscript - A writing tool to help you plan, edit, and share your work.
- Marketo - Automation software to help marketing teams master the art and science of digital marketing.
- Matomo - A Web analytics platform that evaluates the entire user-journey of everyone who visits the website.
- Meisterplan - Software that helps organizations create project portfolios.
- Mingle - Am agile project management and collaboration tool to provide a combined workplace for the entire team.

- MojoHelpdesk - Help desk software and ticketing system.
- Monday - Team management software to plan, track, and collaborate all your work in one tool.
- Mixpanel - System to track user interactions with web and mobile.
- MuleSoft - Integration software to connect SaaS and enterprise applications in the cloud and on-premises.
- MyWebTimesheets - Online time tracking system to track time spent on various projects/jobs/activities.
- New Edge - Secure application networking service for Hybrid IT.
- NextTravel - Corporate travel management software tool.
- N2F - Expense report management tool to manage your business and travel expenses.
- New Relic - Digital intelligence platform to measure and monitor the performance of applications and infrastructure.
- Nmbrs - Cloud HR and payroll software for businesses.
- Nuclino - Collaboration software to collaborate and share information in real-time.
- Office365 - Microsoft's cloud-based subscription service.
- OfficeSpace - a Cloud-based platform that helps organizations allocate workspace.
- OneDesk - Project management and help desk software to connect with and support your customers.
- OpsGenie - An Incident management platform for DevOps and IT Ops teams to streamline alerts and incident resolution processes.
- Orginio - An online organizational chart creation tool to visualize the organizational structure.
- Oomnitza - IT Asset Management platform solution to track and manage assets.
- OpenEye - Mobile app for viewing live and recorded videos on the Apex recorder.
- Oracle ERP Cloud - Cloud-based software application suite to manage enterprise functions.
- Pacific Timesheet - Web-based timesheet tool for payroll, project hours, and expenses.
- PagerDuty - Digital operations management system.
- PandaDoc - A mobile app for iPhone users access to their documents, analytics, and dashboard directly on their mobile phones.
- Panopta - Infrastructure monitoring tool.
- Panorama9 - Cloud-based IT management platform for enterprise network monitoring.
- Papyrs - Editor to design your own intranet pages.

- ParkMyCloud - Single-purpose SaaS tool to connect to AWS, Azure Services, or GCP.
- Peakon - Tool to measure and improve employee engagement.
- People HR - HR software system for all key HR functions.
- Pingboard - Tool to build organization charts for organizing teams and workforce planning.
- Pigeonhole Live - Interactive Q&A platform.
- Pipedrive - Sales CRM and pipeline management software.
- PlanMyLeave - Leave management system for managing and tracking employee's leave of absence.
- PlayVox - Customer service quality monitoring tool.
- Podbean - Podcast service provider.
- Podio - A web-based tool to organize team communication, business processes, data, and content in project management workspaces.
- POPin - Crowd-solving platform and mobile app that operationalizes team engagement for problem-solving
- Postman - API development environment.
- Prescreen - Applicant tracking tool to publish job vacancies online and offline.
- ProductBoard - Product management tool.
- ProdPad - Product management software to develop product strategies.
- Proto.io - Application prototyping platform to create fully interactive, high-fidelity prototypes.
- Proxyclick - Cloud-based visitor management solution to manage visitors, build their brand image, and ensure the security.
- Pulumi - Cloud native development platform for containers, serverless, infrastructure, and Kubernetes.
- PurelyHR - Leave management tool for accessing employee leave data.
- Promapp - Business process management (BPM) tool.
- Prescreen - Cloud-based applicant tracking system to publish job vacancies online and offline.
- QAComplete - Software test management tool.
- Qualaroo - Feedback tool to gain insights from customers.
- Quality Built, LLC - Insurance, financial, and construction industry for providing reliable and innovative Third Party Quality Assurance Services.
- Qubole - Self-service platform for Big Data analytics built on Amazon.

- Questetra BPM Suite - Web-based business process platform for routine workflows.
- QuestionPro - Online survey software to create surveys and questionnaires.
- Quandora - Question and answer based knowledge management solution.
- Quip - Collaborative productivity software suite for mobile and the Web.
- Rackspace - Managed cloud computing services.
- ReadCube - Tool for web, desktop, and mobile reference management.
- RealtimeBoard - Whiteboard Collaboration tool for organizations to collaborate beyond formats, tools, locations, and time zones.
- Receptive - Tool to gather feedback from customers, teams, and the market at one place.
- Remedyforce - IT service management and help desk system.
- Retrace - An Application performance management tool that provides bug tracking, data aggregation, and automatic alerts.
- Robin - Workplace experience tools to schedule conference meeting rooms and desk bookings.
- Rollbar - Real-time error alerting and debugging tools for developers.
- Really Simple Systems - Cloud-based CRM software for small businesses to manage their sales and marketing.
- Reamaze - Customer support software to support, engage, and convert customers with chat, social, SMS, FAQ, and email on a single platform.
- Resource Guru - Resource management software to schedule people, equipment, and other resources.
- Retrace - Application performance management to integrate code profiling, error tracking, application logs, and metrics.
- Roadmunk - Product roadmap software and roadmap tool to create product roadmaps.
- Runscope - Tool to create, manage, and run functional API tests and monitors.
- Salesforce – CRM tool to manage customer contact information, integrate social media, and facilitate real-time customer collaboration.
- SalesLoft - Sales engagement platform for efficient and revenue-boosting sales
- Salsify - Product experience management (PXM) platform.
- Samanage - Tool for IT service management.
- Samepage - Collaboration software to manage online projects.
- Screencast-O-Matic – Tool to screencast and edit video.

- ScreenSteps –Tools to create visual documents centered on screen captures.
- SendSafely – Encryption platform for secure exchange of files and emails.
- Sentry - Open-source error tracking software.
- ServiceDesk Plus - Tool for IT service desk.
- ServiceNow - Cloud platform to create digital workflows.
- SharePoint – Collaborative platform used for document management and storage.
- Shufflrr - Presentation management tool to create, update, share, and broadcast presentations.
- Sigma Computing – An Analytics tool to explore, analyze, and visualize data.
- Signavio – A business process modeling tool.
- Skeddly - Tool to automate AWS resources.
- Skills Base - Talent management tool to track and document employee's performance and skills.
- Skyprep - Learning management system (LMS) to train customers and employees.
- Slack - Collaboration tool to communicate and share information.
- Slemma - Data analysis tool to create data reports from multiple data sets.
- Sli.do - Interaction tool for meetings, events, and conferences.
- SmartDraw - Diagram tool used to make flowcharts, organization charts, mind maps, project charts, and other business visuals.
- SmarterU - Learning management system (LMS) to train customers and employees.
- Smartsheet - Collaboration tool to assign tasks, track project process, manage calendars, and share documents.
- SparkPost - Email delivery service.
- Split - Bill splitting application.
- Spoke - Service desk tool to file service tickets.
- Spotinst - A SaaS optimization platform that helps companies purchase and manage cloud infrastructure capacity.
- SproutVideo - Platform to host business videos.
- Stackify - Troubleshooting tool that provides support with a suite of tools including Prefix and Retrace.
- StatusCast - Hosted page to keep your employees and customers aware about downtime and website maintenance.

- StatusDashboard - Communications platform for hosting status dashboards and broadcasting incident notifications to customers.
- Status Hero - Tool for tracking status updates and daily goals from your team.
- StatusHub - Platform to host the service state page.
- Statuspage - Tool to communicate status and incidents.
- SugarCRM - CRM tool for Salesforce automation, marketing campaigns, customer support, collaboration, Mobile CRM, Social CRM, and reporting.
- Sumo Logic - Data analytics software that focuses on security, operations, and BI use cases.
- Supermood - HR platform to gather employee's feedback in real-time.
- Syncplicity - Tool to share and synchronize files.
- Tableau - Tool to create interactive data visualization.
- TalentLMS - Learning management system (LMS) to facilitate online seminars, courses, and other training programs.
- Tallie – Tool to capture and upload receipts, generate expense reports, and customize expense details.
- Targetprocess - Agile project management software to Scrum, Kanban, SAFe, and so on.
- Teamphoria - Software to provide real-time employee engagement metrics, employee reviews, and recognition.
- TeamViewer - Proprietary software application for remote control, desktop sharing, online meetings, web conferencing, and file transfer between computers.
- Tenable.io - Tool that provides data to identify, investigate, and prioritize the remediation of vulnerabilities and misconfigurations in your IT environment.
- Testable - Tool to create behavioral experiments and surveys.
- TestingBot - Tool to provide various browser versions for live and automated testing.
- TestFairy - Mobile testing platform, to provide companies with video recordings, logs, and crash reports of mobile sessions.
- TextExpander - Communication tool to insert snippets of text from a repository of emails, and other content, as you type.
- TextMagic - Messaging service to connect with customers.
- ThousandEyes - Tool to monitor network infrastructure, troubleshoot application delivery, and map internet performance.
- Thycotic Secret server - Account management software tool to manage passwords.

- TimeLive – Tool to provide timesheets and track time.
- Tinfoil Security - Security solution software to check for vulnerabilities.
- Trisotech - Tool that allows customers to discover, model, analyze their digital enterprise.
- Trumba - Tool to publish online, interactive, calendars of events.
- TwentyThree - Video marketing platform to integrate and add videos to the marketing stack.
- Twilio - A developer platform for communications.
- Ubersmith - Business management software for usage-based billing, quoting, order management, infrastructure management, and help desk ticketing solutions.
- UniFi - Communication and collaboration software with voice, web collaboration, and video conferencing capabilities.
- UPTRENDS – Website monitoring solution to track website uptime and performance.
- UserEcho - Community forum tool that helps businesses manage customer feedback.
- UserVoice - Product feedback management software to enable businesses to make data-driven product decisions.
- VALIMAIL - Email authentication software to authenticate legitimate emails and block phishing attacks.
- Veracode - Source code analyzer and code scanner protect enterprises from cyber threats and application backdoors.
- Velpic - Learning management system (LMS) designed to streamline workplace training.
- VictorOps - Incident management software to provide DevOps observability, collaboration, and real-time alerting.
- VIDIZMO - Enterprise live and on-demand video streaming software.
- Visual Paradigm - Visual modeling and diagramming online platform for team collaboration.
- Vtiger - CRM tool that enables sales, support, and marketing teams to organize and collaborate.
- WaveMaker – Software for building and running custom apps.
- Weekdone - Tool to create managers' dashboard and team management service for companies.
- Wepow - Tool to connect recruiters, job candidates, and employers through a mobile and video interviewing solution.
- When I Work - Tool for employee scheduling and time tracking.
- WhosOnLocation – Tool to track the flow of people through sites and zones.

- Workable - Applicant tracking system.
- Workday - Tool for financial management, human resources, and planning.
- Workpath - Tool to manage the goals and performance of the organization.
- Workplace - Collaboration tool by Facebook to help employees communicate through a familiar interface.
- Workstars - Platform for social and peer employee recognition programs.
- Workteam - Tool to track employee time and attendance.
- Wrike - Social project management and collaboration software.
- XaitPorter - Document co-authoring software for bids and proposals and other business documents.
- Ximble - Tool for employee scheduling and time tracking.
- XMatters - Collaboration platform with an alerting software that integrates with other tools creating seamless process and effective communication.
- Yodeck - Tool to manage screens remotely, through the web or mobile.
- Zendesk - Software to request for customer service and to log support tickets.
- Ziflow - Tool for creative production teams.
- Zillable – Collaboration platform with communication capabilities.
- Zing tree - A toolkit for creating interactive decision trees and troubleshooters.
- ZIVVER - Tool that allows secure email and file transfer from your familiar email program.
- Zoho - Business application suite.
- Zoom - Communication and collaboration software with voice, web collaboration, and video conferencing capabilities.
- Zuora - A subscription-based software that enables a company launch, manage, and transform into a subscription business.

End-to-end app configuration

For a complete end-to-end configuration of an app, see Admin-guided workflow for easy onboarding and set up.

Agentless access to enterprise web apps

Enterprise web applications like SharePoint, JIRA, Confluence, and others hosted by the customer on-premises or on public clouds can now be accessed directly from a client browser. End users no longer need to initiate access to their enterprise web apps from the store. This feature also enables end users to access web apps by clicking links from emails, collaboration tools, or browser bookmarks, providing a true zero-footprint solution to customers.

How it works

- Add a new DNS record or modify an existing DNS record for the configured enterprise web apps.
- An IT administrator adds a new public DNS record or modify an existing public DNS record for the configured enterprise web app FQDN to redirect the user to the Citrix Secure Private Access™ service.
- When the end-user initiates access to the configured enterprise web app, the app traffic is steered to the Citrix Secure Private Access service, which then will proxy the access to the app.
- Once the request lands on the Citrix Secure Private Access service, it checks for user authentication and application authorization, including contextual access policies checks.
- Upon successful validation, the Citrix Secure Private Access service communicates with Citrix Cloud Connector™ Appliances, deployed at the customer's environment (either in on-premises or cloud) to enable access to the configured enterprise web app.

Configure Citrix Secure Private Access for agentless access to enterprise web apps

Prerequisites:

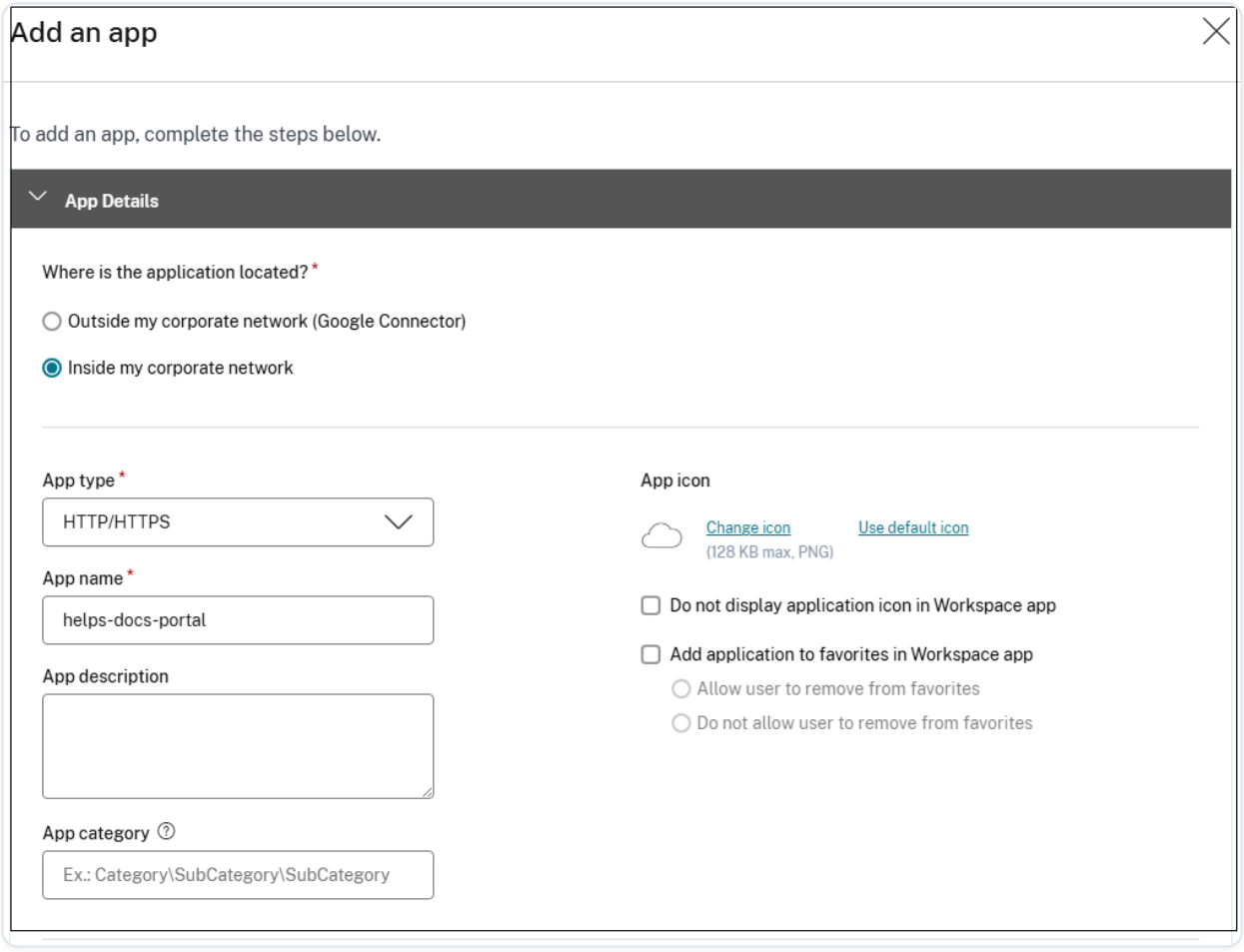
Before you begin, you need the following for the application to be configured.

- Application FQDN
- SSL certificate – Public certificate for the app to be configured
- Resource location – Install Citrix Cloud™ Connector Appliances
- Access to the public DNS record to update it with the canonical name (CNAME) provided by Citrix® during the app configuration.

Configure agentless access to enterprise web apps:

1. Log in to Citrix Cloud and select **Secure Private Access**.

2. Click **Applications > App Configuration** and then click **Add an app**.
3. In the **Choose a template** section, click **Skip**. Templates are available only for SaaS apps.
4. In **Where is the application location?**, select **Inside my corporate network**.
    - Select **Inside my corporate network** for applications hosted within your organization's private network infrastructure, behind firewalls and accessible only through internal network connection
    - Select **Outside my corporate network (Google Connector):** For applications hosted outside your organization's private network infrastructure. Traffic routing occurs directly from users to the external application via the Google Cloud Connector.
5. Enter the following details in the **App Details** section and click **Next**.



- **App type** – Select the app type (HTTP or HTTPS).

> **Note:**

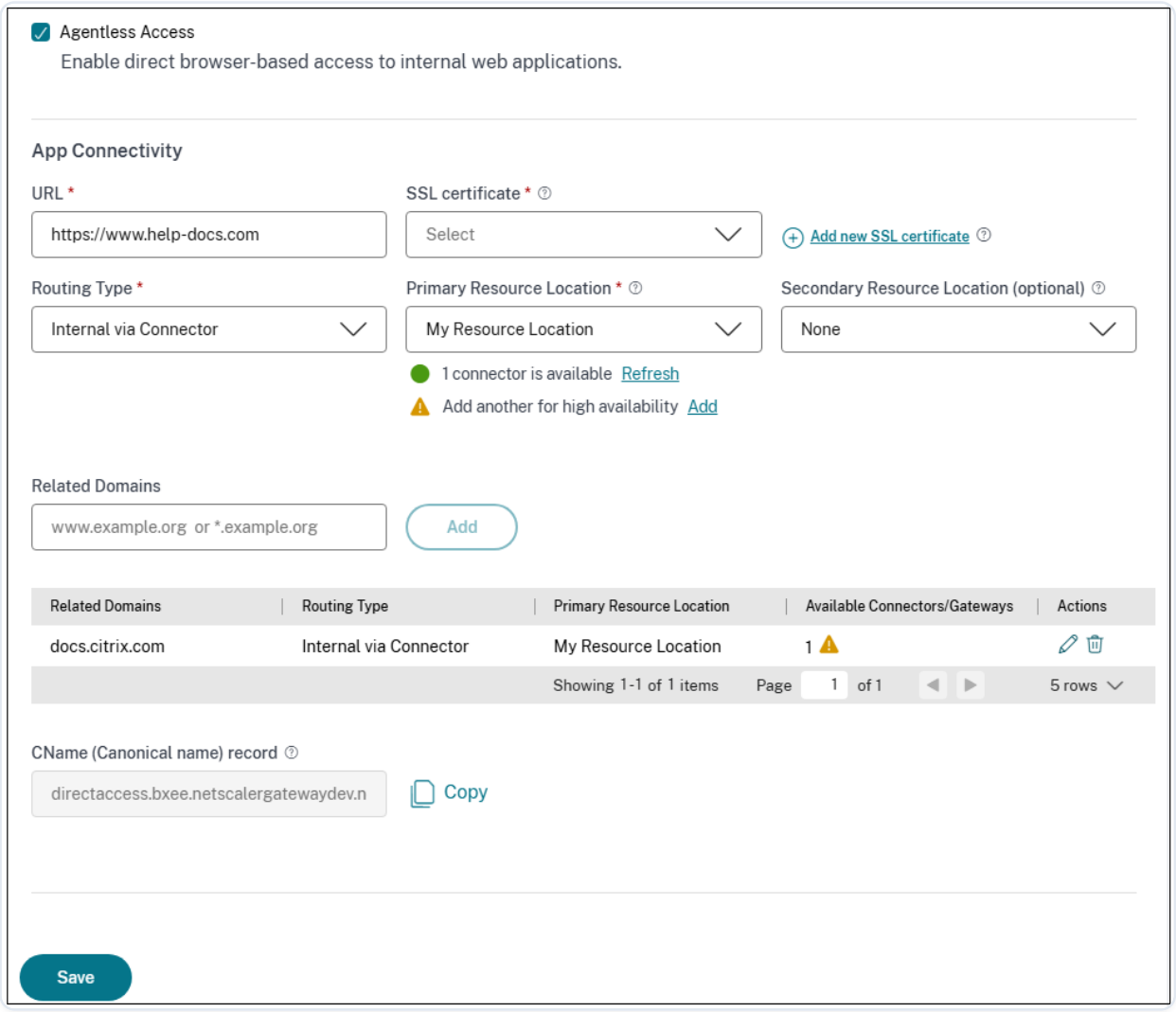
> For Chrome Enterprise Premium (CEP), only HTTPS enterprise web and SaaS apps are supported. HTTP enterprise web and SaaS apps are not supported.

- **App name** – Name of the application.
- **App description** - A brief description of the app. This description is displayed to your users in the store.
- **App icon** – Click **Change icon** to change the app icon. The icon file size must be 128x128 pixels. If you do not change the icon, the default icon is displayed.

  If you do not want to display the app icon, select **Do not display application icon to users**.

6. Select **Agentless Access** to enable users access the app directly from a client browser. Enter the following details.

   The **Agentless Access** option is available only for enterprise web apps.



- **URL** – URL for the back-end application. The URL must be in HTTPS format and a corresponding DNS entry must be added by the admin.
- **SSL certificate** – Select an existing SSL certificate from the drop-down menu or add a new SSL certificate by clicking **Add New SSL Certificate**.
  - Only a public or a trusted CA certificate is supported.
  - A full chain of certificates must be uploaded.

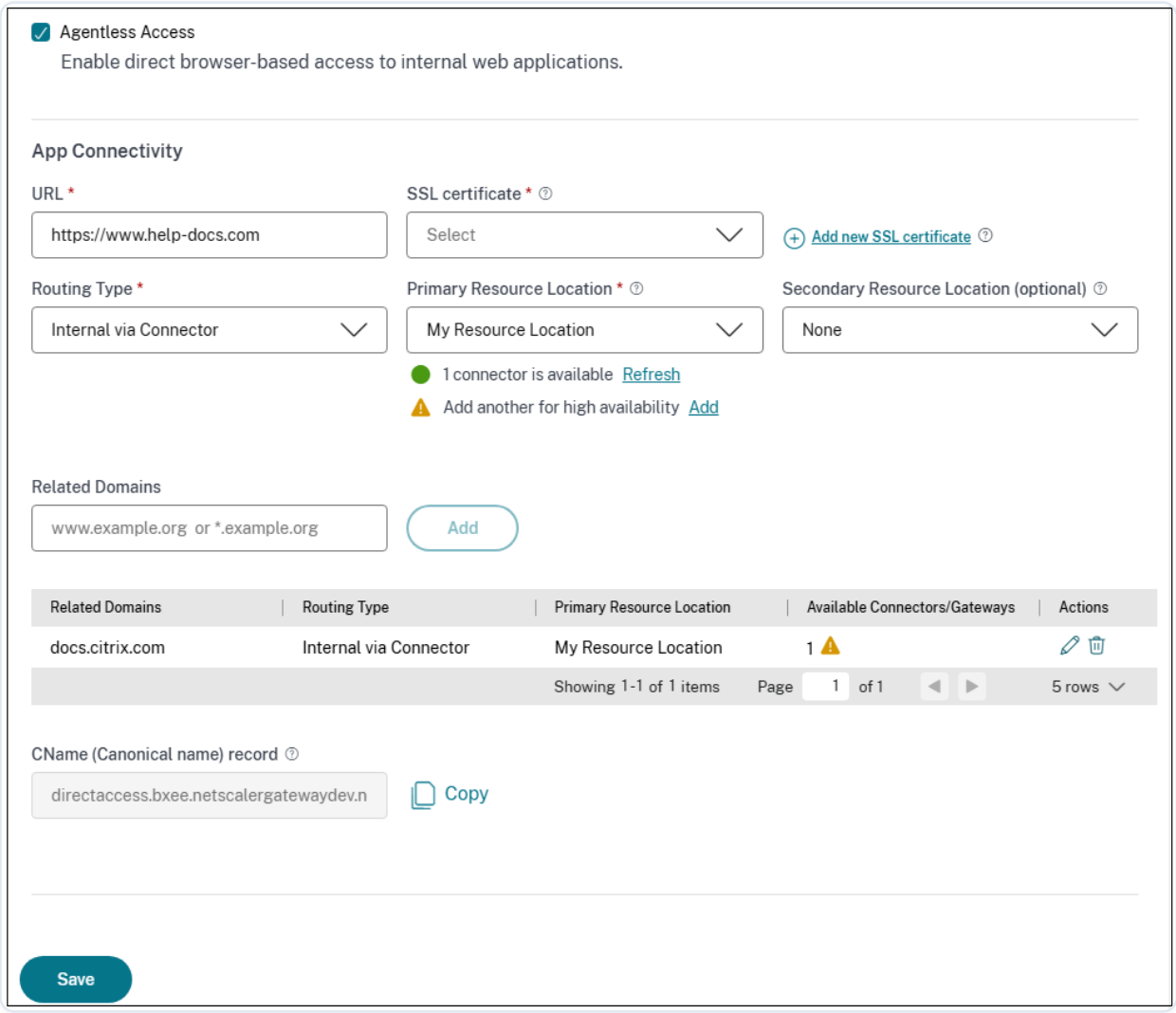
> **Important:**
>
> - Administrators must upload certificates directly to the Secure Private Access console, as Secure Private Access manages its own certificate store. For details, see Manage certificates in the Secure Private Access console.
> - Certificates added to the NetScaler® console can no longer be used in Secure Private Access as the certificates are not synchronized between the two systems.

- **Related Domains** – The related domain is auto-populated based on the URL that you've provided. Related domain helps the service to identify the URL as part of the app and route traffic accordingly. You can add more than one related domain. You can bind an SSL certificate to each related domain, this is optional.

> **Note:**
>
> A warning message appears if duplicate related domains are added or if a related domain is also added as a URL for a different app. To avoid these issues, see Best Practices for Web and SaaS application configurations.

- **Import HAR** – You can upload a HAR file to automatically discover the domains that an application accesses. Review the discovered domains and select the ones you want to add to the application's related-domain configuration. This simplifies application onboarding by reducing the need to manually identify and configure related domains. For more information, see Discover related domains using a HAR file.
- **CName record** – Auto generated by Secure Private Access. This is the value that must be entered in the DNS to enable agentless access to the application.

7. In the **App Connectivity** section, you define routing for the related domains of applications, if the domains must be routed externally or internally through Citrix Connector™ Appliance.

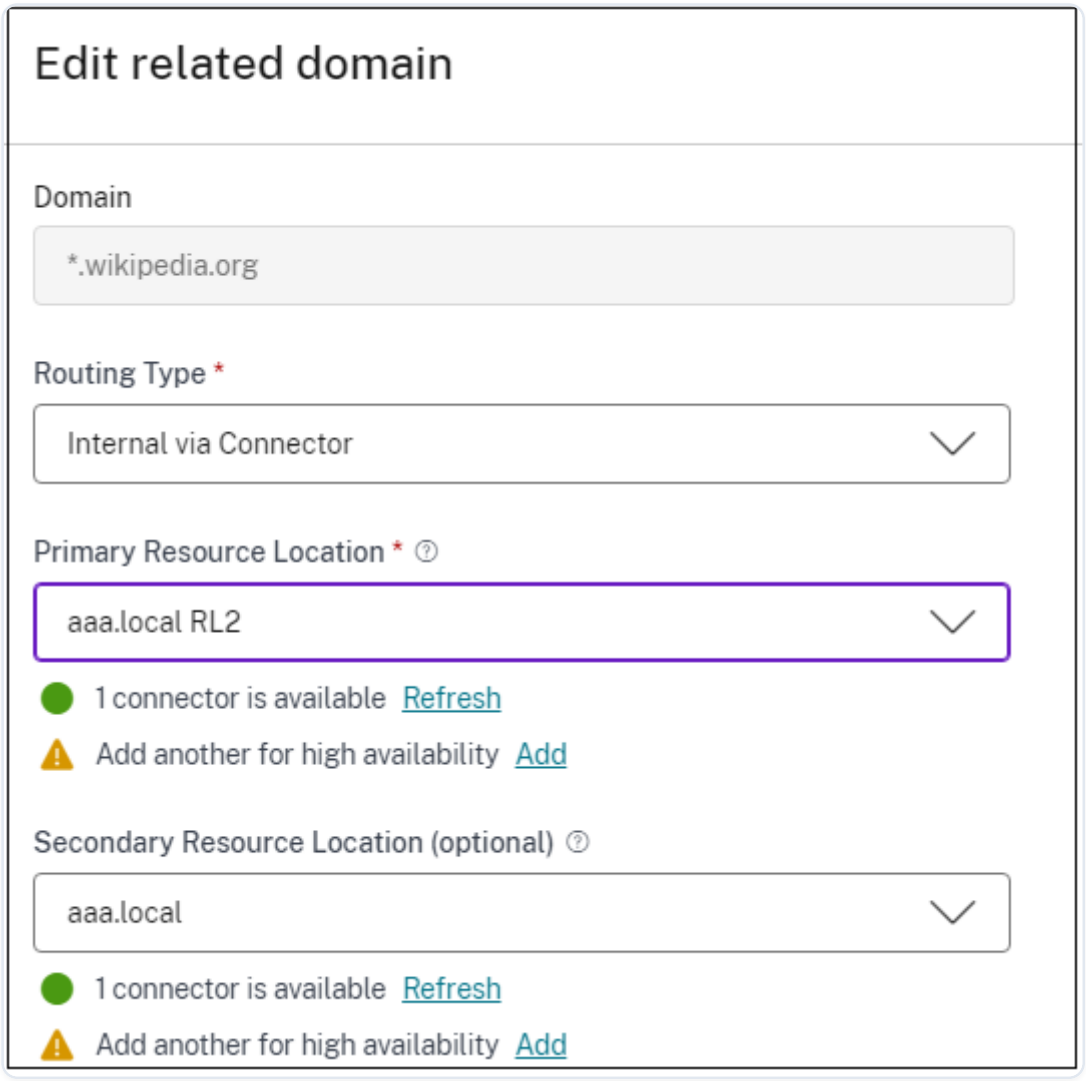


- **Routing Type** - Select one of the following:
  - **Internal – bypass proxy** - The domain traffic is routed through Connector Appliance™, bypassing the customer's web proxy configured on the Connector Appliance.
  - **Internal via Connector** - The apps can be external but the traffic must flow through the Connector Appliance to the outside network.
  - **External** – The traffic flows directly to the internet.
- **Primary and secondary resource locations** - Admins can ensure high availability of applications even during disruptions by configuring a secondary resource location or by using the **First Available** option.
  - **Primary Resource Location:** Select the primary resource location where the application is hosted. Alternatively, admins can select the option **First Available** in **Primary Resource Location**.

- **First available:** The **First Available** option ensures that a working resource location is used. When **First Available** is selected, the system automatically routes traffic to the first available location. This ensures continuous application access without manual intervention. For instance, if ResourceLocation1 is unavailable but ResourceLocation2 is reachable, then ResourceLocation2 is selected by default to front-end the application.
- **Secondary Resource Location** - The **Secondary Resource Location** option becomes available only if a primary resource location is explicitly specified. If the primary resource location becomes unavailable, for reasons such as a Connector Appliance or data center failure, the application fails over to the specified secondary resource location. The secondary resource location can also act as a failover even when the application is hosted in another data center.

You can also set a primary and secondary resource location or select the **First Available** option for each of the related domains.

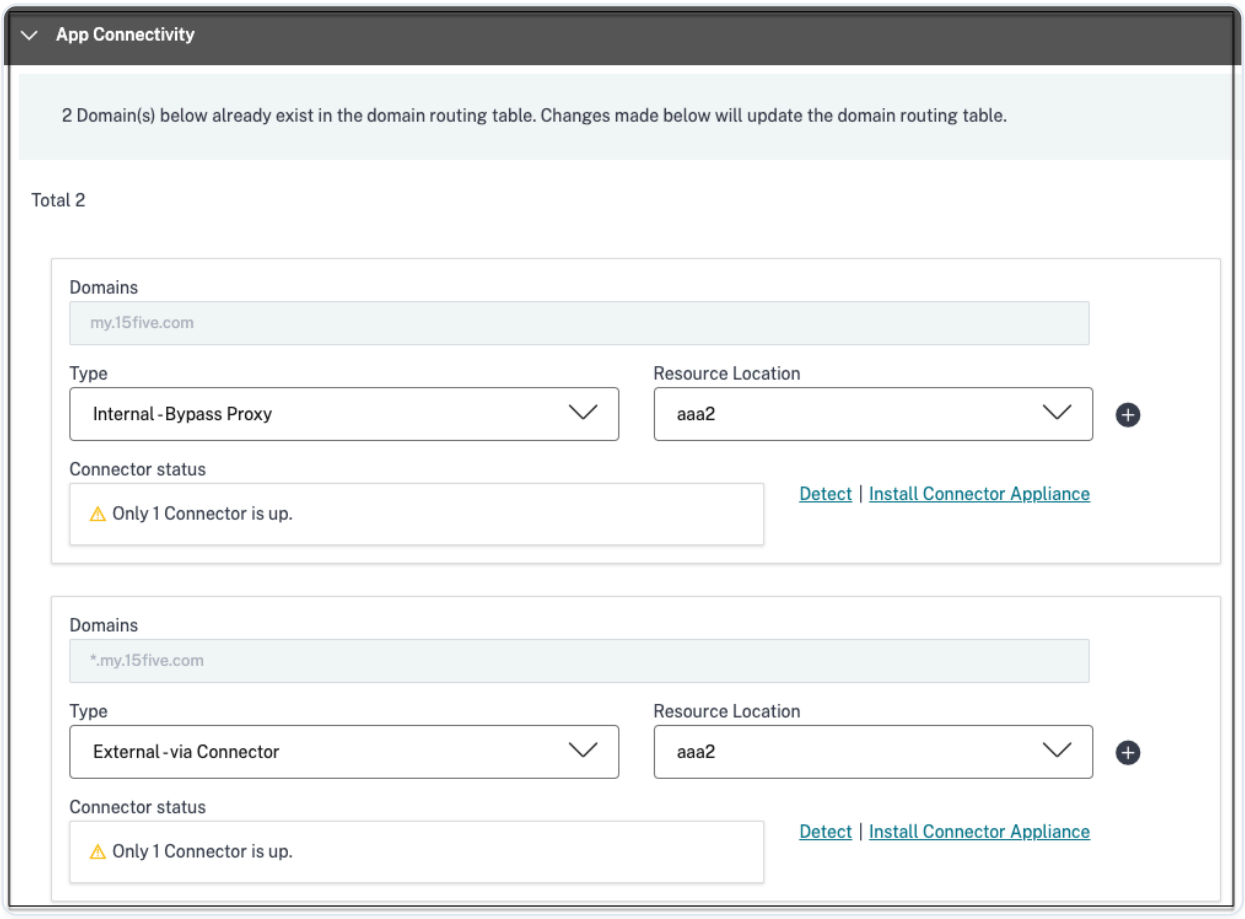
a. Click the edit icon in the **Actions** column of the Related Domains table.
b. Set the primary and secondary resource location or choose the **First Available** option.



Note:

- Setting the backup resource location and using the **First Available** option feature is in Preview.
- When you delete an application, its routing entries are removed automatically. For more information, see Automatic cleanup of routing entries on application deletion.

8. In the **App Connectivity** section,section, you define routing for the related domains of applications, if the domains must be routed externally or internally through Citrix Connector™ Appliance.



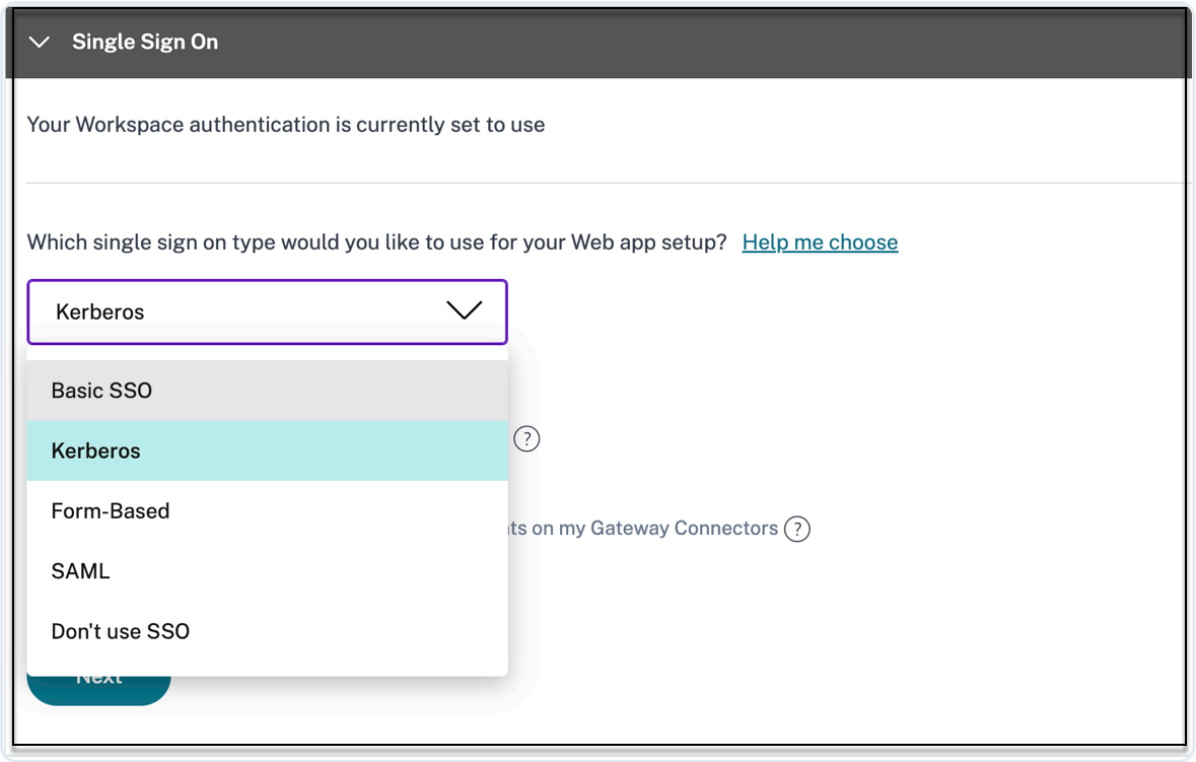
9. **Maintain consistent connection** - Select this checkbox to enable consistent connection to the same Connector Appliance. For details about consistent connections, see Maintain consistent connection.

> **Note:**
>
> When the **Maintain consistent connection** option is selected, the routing type for the application must be set to **Internal via Connector** in the App Connectivity section.

10. Set the preferred sign-on method.

> **Note:**
>
> The single sign-on option is not applicable for Citrix Secure Access with Chrome Enterprise (CEP).

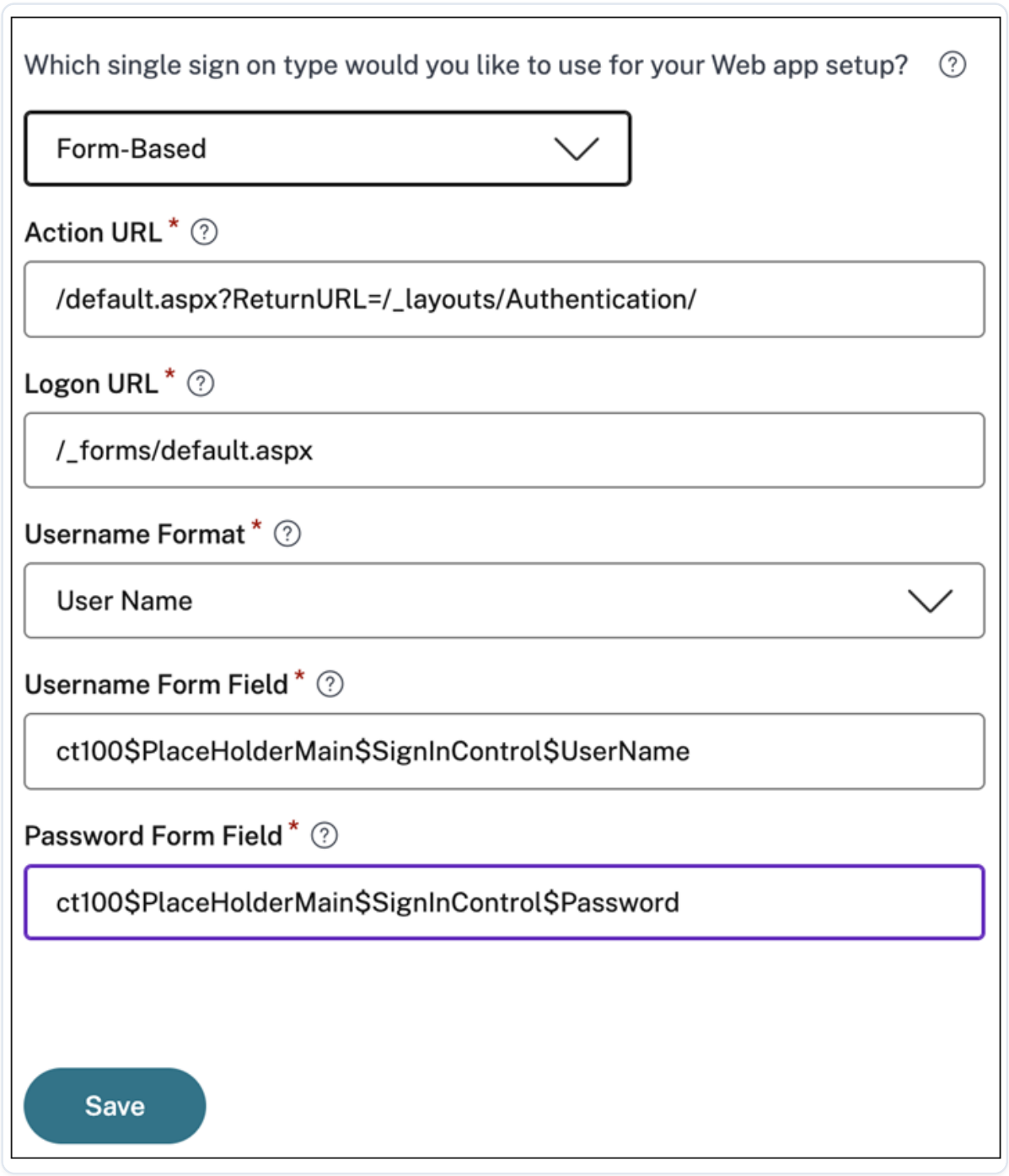
   a. In the **Single Sign On** section, select your preferred single sign-on type to be used for your application and click **Save.** The following single sign-on types are available.



- **Basic** – If your back-end server presents you with a basic-401 challenge, choose **Basic SSO**. You do not need to provide any configuration details for the **Basic** SSO type.
- **Kerberos** – If your back-end server presents you with the negotiate-401 challenge, choose **Kerberos**. You do not need to provide any configuration details for the **Kerberos** SSO type.
- **Form-Based** – If your back-end server presents you with an HTML form for authentication, choose **Form-Based**. Enter the configuration details for the **Form-Based** SSO type.
- **SAML** - Choose **SAML** for SAML-based SSO into web applications. Enter the configuration details for **SAML** SSO type.
- **Don't use SSO** – Use the **Don't use SSO** option when you do not need to authenticate a user on the back end server. When the **Don’t use SSO** option is selected, the user is redirected to the URL configured under the **App details** section.

Form based details:

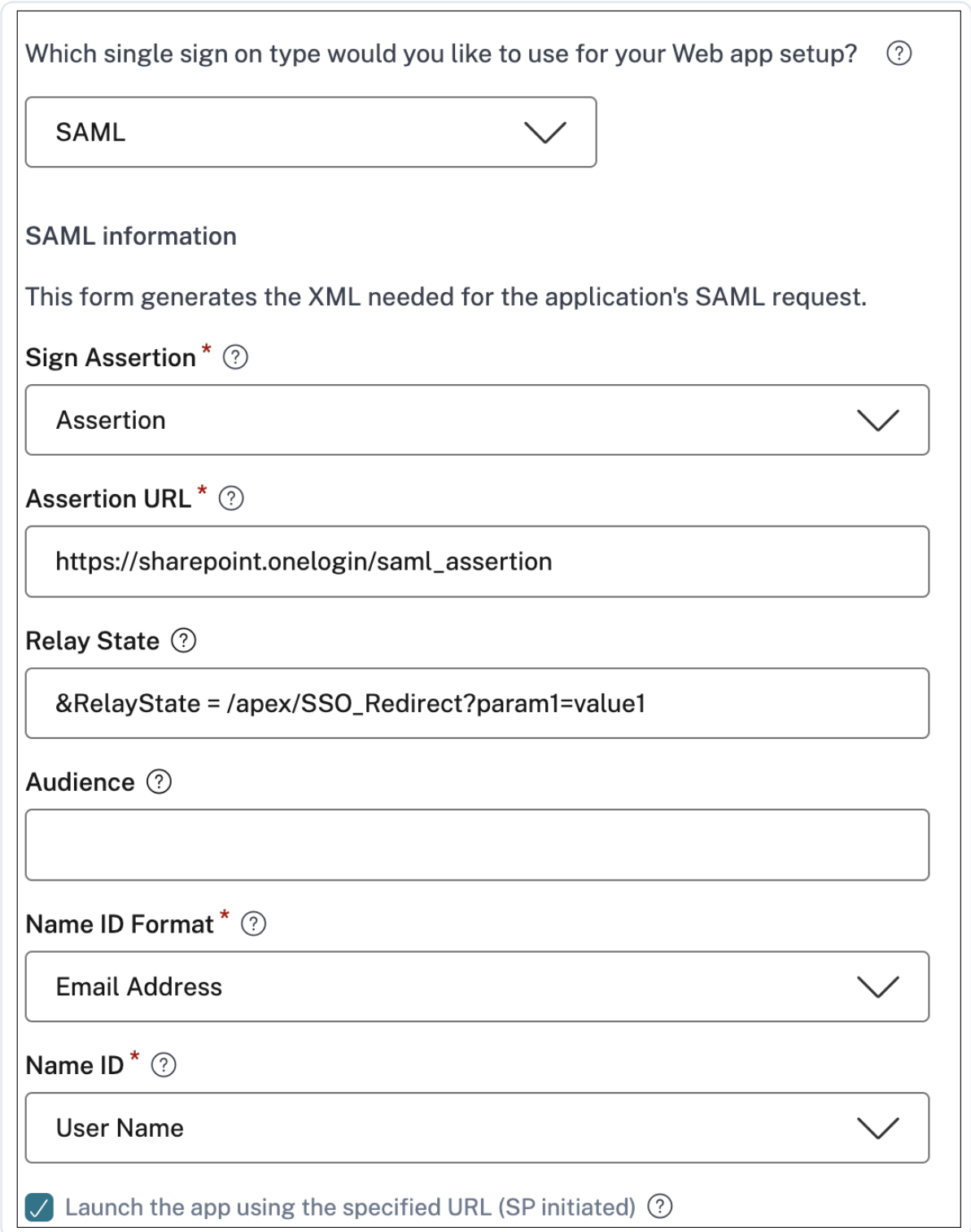
Enter the following form-based configuration details in the Single Sign On section and click **Save.**



- **Action URL** - Type the URL to which the completed form is submitted.
- **Logon form URL** – Type the URL on which the logon form is presented.
- **Username Format** - Select a format for the user name.
- **Username Form Field** – Type a user name attribute.
- **Password Form Field** – Type a password attribute.

SAML:

Enter the following details in the Sign sign on section and click Save.**



- **Sign Assertion** - Signing assertion or response ensures message integrity when the response or assertion is delivered to the relying party(SP). You can select **Assertion, Response, Both,** or **None**.
- **Assertion URL** – Assertion URL is provided by the application vendor. The SAML assertion is sent to this URL.
- **Relay State** – The Relay State parameter is used to identify the specific resource the users access after they’re signed in and directed to the relying party's federation server.

Relay State generates a single URL for the users. Users can click this URL to log on to the target application.

- **Audience** – Audience is provided by the application vendor. This value confirms that the SAML assertion is generated for the correct application.
- **Name ID Format** – Select the supported name identifier format.
- **Name ID** – Select the supported name ID.

i. In **Advanced attributes (optional)** add additional information about the user that is sent to the application for access control decisions.

ii. Download the metadata file by clicking the link under **SAML Metadata.** Use the downloaded metadata file to configure SSO on the SaaS apps server.

- You can copy the SSO login URL under **Login URL** and use this URL when configuring SSO on the SaaS apps server.
- You can also download the certificate from the **Certificate** list and use the certificate when configuring SSO on the SaaS apps server.

11. Click **Save** and then click **Finish**. The app is added to the Applications page. You can or edit or delete an app from the Applications page after you've configured the application. To do so, click the ellipsis button on an app and select the actions accordingly.

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

Important:

- To enable zero-trust-based access to the apps, apps are denied access by default. Access to the apps is enabled only if an access policy is associated with the application. For details on creating access policies, see Create access policies.
- If multiple apps are configured with the same FQDN or some variation of the wildcard FQDN, this might result in a conflicting configuration. To prevent conflicting configurations, see Best practices for Web and SaaS application configurations.

Automatic cleanup of routing entries on application deletion

When you configure an application, its destinations (FQDNs or application domains) are added to the routing table, which Secure Private Access uses for routing decisions. When you delete an application, Secure Private Access cleans up the routing entries based on the following rules:

- **Unreferenced entries are removed** - If a routing entry (FQDN or application domain) associated with the deleted application is not referenced by any other application, Secure Private Access removes it from the routing table automatically.
- **Shared entries are retained** - If a routing entry is used by more than one application, deleting one of those applications does not remove the shared entry. The entry remains in the routing table for as long as at least one active application references it.
- **No retroactive removal** - Routing entries are evaluated and removed only as part of an application deletion. Existing entries are not removed retroactively unless they are confirmed to be unused by any application.

> **Note:**
>
> - The cleanup runs automatically when an application is deleted from the Applications page (using the ellipsis (...) menu). No administrator action is required.
> - Because shared routing entries are preserved, deleting an application does not disrupt access to other applications that share the same destination.

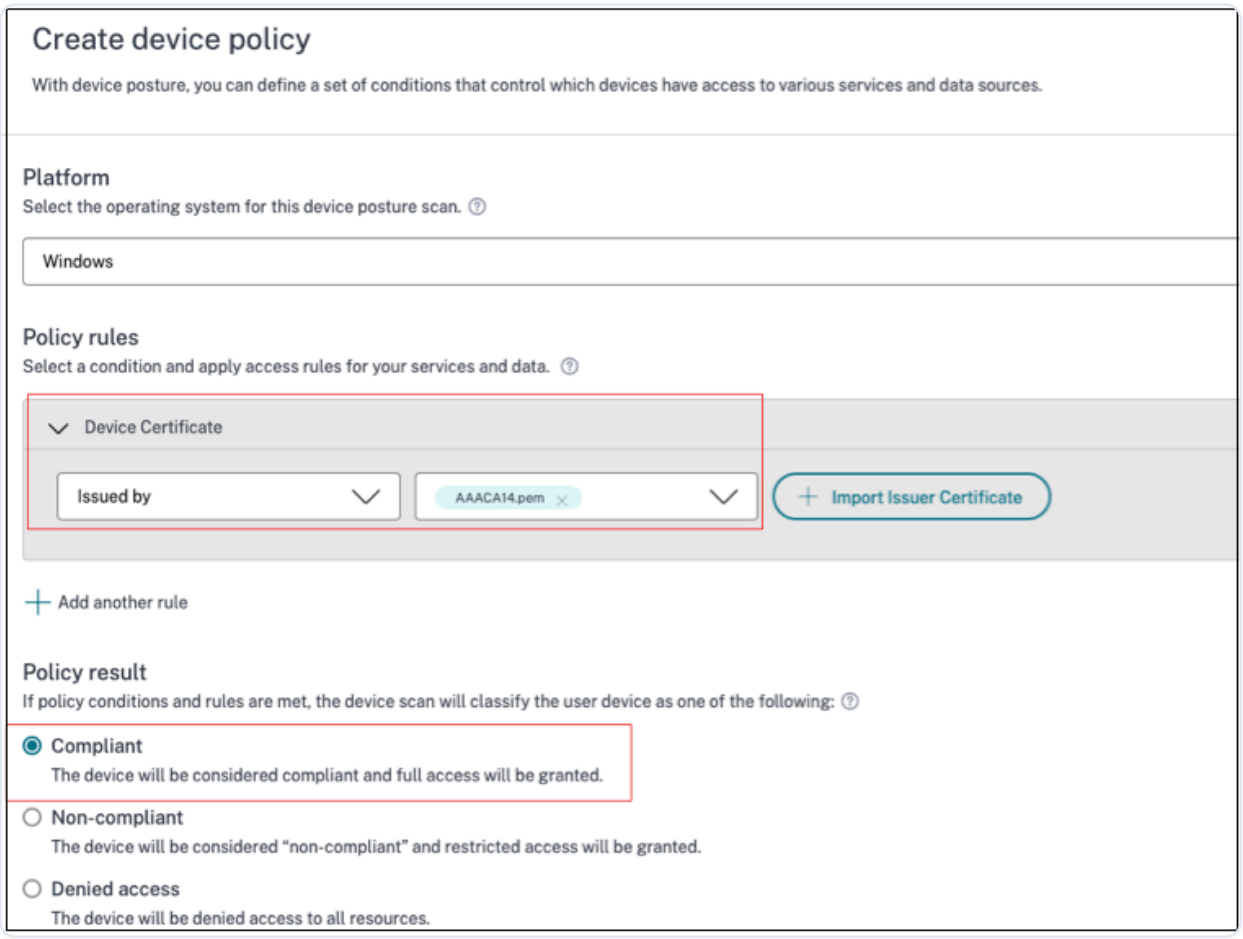
Device Posture service with agentless access apps

Citrix Secure Private Access with agentless access apps when combined with the Device Posture service can ensure that only compliant devices access sensitive applications through agentless access. Admins can block access to non-compliant or non-managed devices based on the Device Posture service scan results.

Steps to enable agentless access for compliant devices only

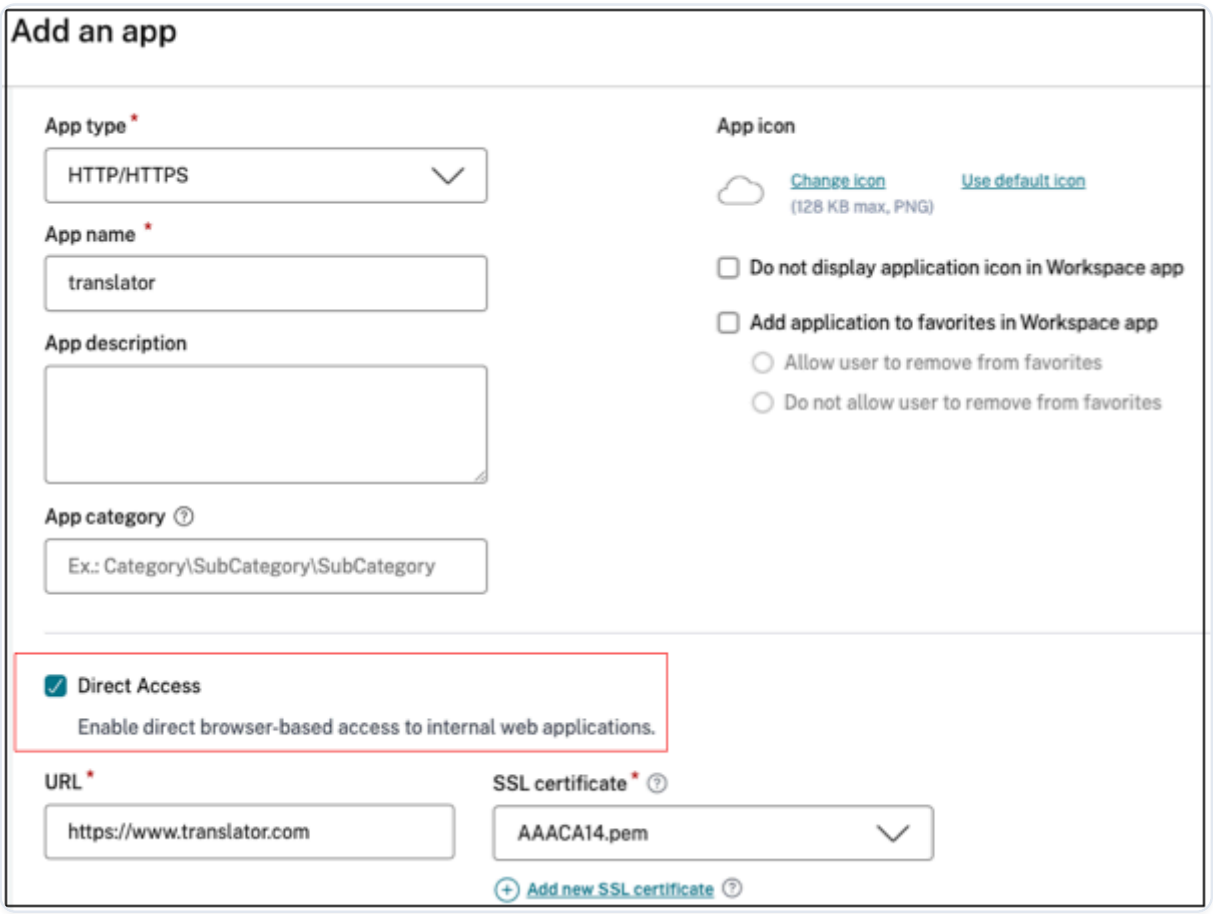
To enable agentless access to only compliant devices, the admin must perform the following steps:

1. From the Device Posture service admin console, create a device posture policy to check for the device posture scan conditions such as device certificate, antivirus, browser and then select **Compliant** as the policy result action. For details, see Configure device posture.



2. From the Secure Private Access admin console, perform the following:

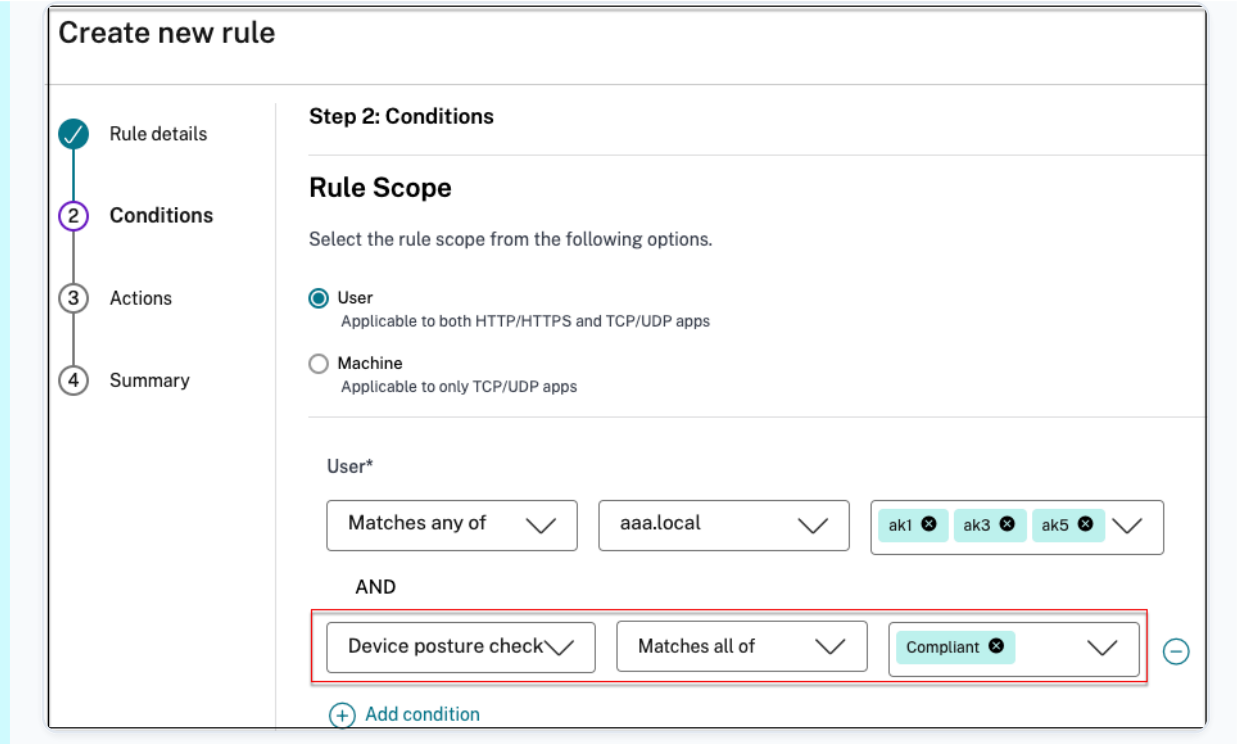
   - Create an application for which you want to enable agentless access. For details, see Direct access to Enterprise web apps.



- Configure Secure Private Access with Device Posture. In **Rule Scope**, select **Device posture check > Matches any of** and enter the tag **Compliant**. This tag is sent from the Device Posture service.

Note:

The tag must be entered exactly as captured earlier, using initial caps (Compliant). Otherwise, the device posture policies do not function as intended. For details, see Citrix Secure Private Access configuration with Device Posture.



Once this configuration is performed, based on the device posture scan results, the device is tagged as compliant, non-compliant, or denied login and app access is enabled accordingly.

Example:

Consider that you have created a device posture policy to check for the presence of a device certificate on an endpoint device and determine its login status. Once the device posture policies are set and device posture is enabled, the following actions occur when an end user logs into their store.

1. The device posture scan checks the endpoint device for the presence of a device certificate.
   - If the device certificate is present on the device, the device is tagged as **compliant**.
   - If the device certificate is not present on the device, the device is tagged as **non-compliant**.
2. This information is then passed to the Citrix Secure Private Access service as tags.
3. The access policy is evaluated based on the device classification.
   - If the device is compliant, agentless access is allowed for the apps.
   - If the device is non-compliant, agentless access is disabled for the apps.

End user experience

The end user experience is based on the classification of the device as compliant or non-compliant.

- **Compliant device:**

  The user can launch the agentless access app from the store or from the browser using the app URL.

- **Non-compliant device:**
  - The app is not enumerated in the store.
  - The user cannot launch the app from the browser using the app URL.
  - An access blocked page is displayed to the user.

Support for TCP/UDP apps

Secure Private Access service enables you to access TCP/UDP applications that are present in your on-premises environment either using a native browser or a native client application through the Citrix Secure Access client running on your machine. For details, see the following sections:

- Prerequisites
- Configure Secure Private Access for TCP/UDP apps
- Admin Configuration – Citrix Secure Access client-based access to HTTP/HTTPS apps
- Adaptive access to TCP/UDP and HTTP(S) apps
- Troubleshoot application domains IP address conflict

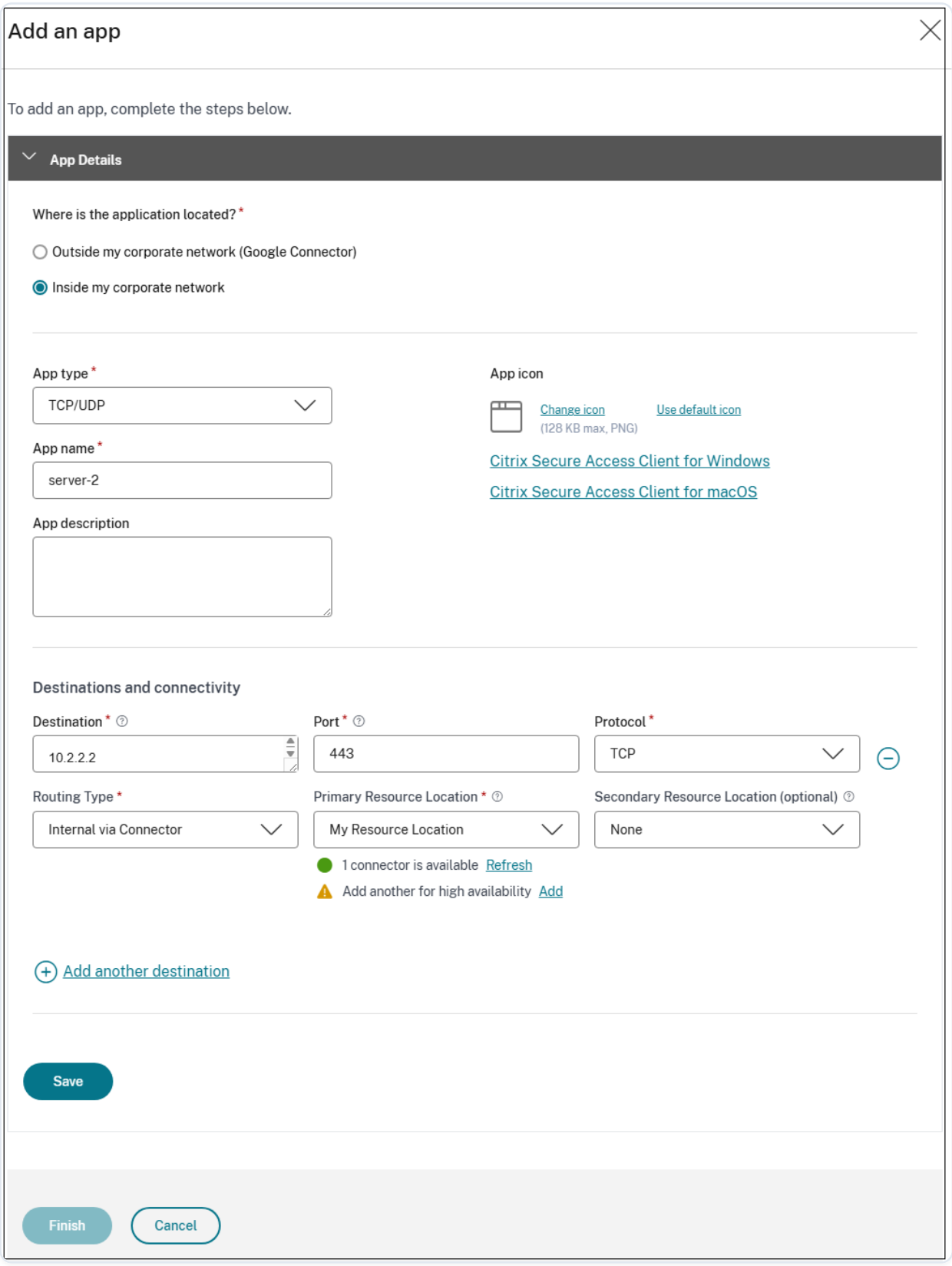
Prerequisites

- Citrix Secure Access client - For details, see Citrix Secure Access client.
- Connector Appliance – Citrix recommends installing two Connector Appliances in a high availability set-up in your resource location. The connector can be installed either on-premises, in the data center hypervisor, or in public cloud. For more information on Connector Appliance and its installation, see Connector Appliance for Cloud Services. You must use a Connector Appliance for TCP/UDP apps. The Connector Appliance must have a DNS server configuration for DNS resolution.

Configure Secure Private Access for TCP/UDP apps

1. Log in to Citrix Cloud and select **Secure Private Access**.
2. Click **Applications > App Configuration** and then click **Add an app**.
3. In the **Choose a template** section, click **Skip**. Templates are available only for SaaS apps.

   App is a logical grouping of destinations. We can create an app for multiple destinations – Each destination means different servers in the back end. For example, one app can have one SSH, one RDP, one Database server, and one Web server. You don't have to create one app per destination, but one app can have many destinations.
4. In the **App Details** section, select **Inside my corporate network**, enter the following details, and click **Next**.



- **App type** – Select TCP/UDP.
- **App name**– Name of the application.
- **App icon**– An app icon is displayed. This field is optional.
- **App description** – Description of the app you are adding. This field is optional.

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

> **Important:**
>
> End users can access the apps using FQDN even if the admin has configured the apps using the IP address. This is possible because the Citrix Secure Access™ client can resolve an FQDN to the real IP address. The following table provides examples of various destinations and how to access the apps with these destinations:

DESTINATION INPUT	HOW TO ACCESS THE APP
10.10.10.1-10.10.10.100	End user is expected to access the app only through IP addresses in this range.
10.10.10.0/24	End user is expected to access the app only through IP addresses configured in the IP CIDR.
10.10.10.101	End user is expected to access the app only through 10.10.10.101
`*.info.citrix.com`	End user is expected to access subdomains of `info.citrix.com` and also `info.citrix.com` (the parent domain). For example, `info.citrix.com`, `sub1.info.citrix.com`, `level1.sub1.info.citrix.com` **Note:** The wildcard must always be

DESTINATION INPUT	HOW TO ACCESS THE APP
	the starting character of the domain and only one *. is allowed.
info.citrix.com	End user is expected to access `info.citrix.com` only and no subdomains. For example, `sub1.info.citrix.com` is not accessible.

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

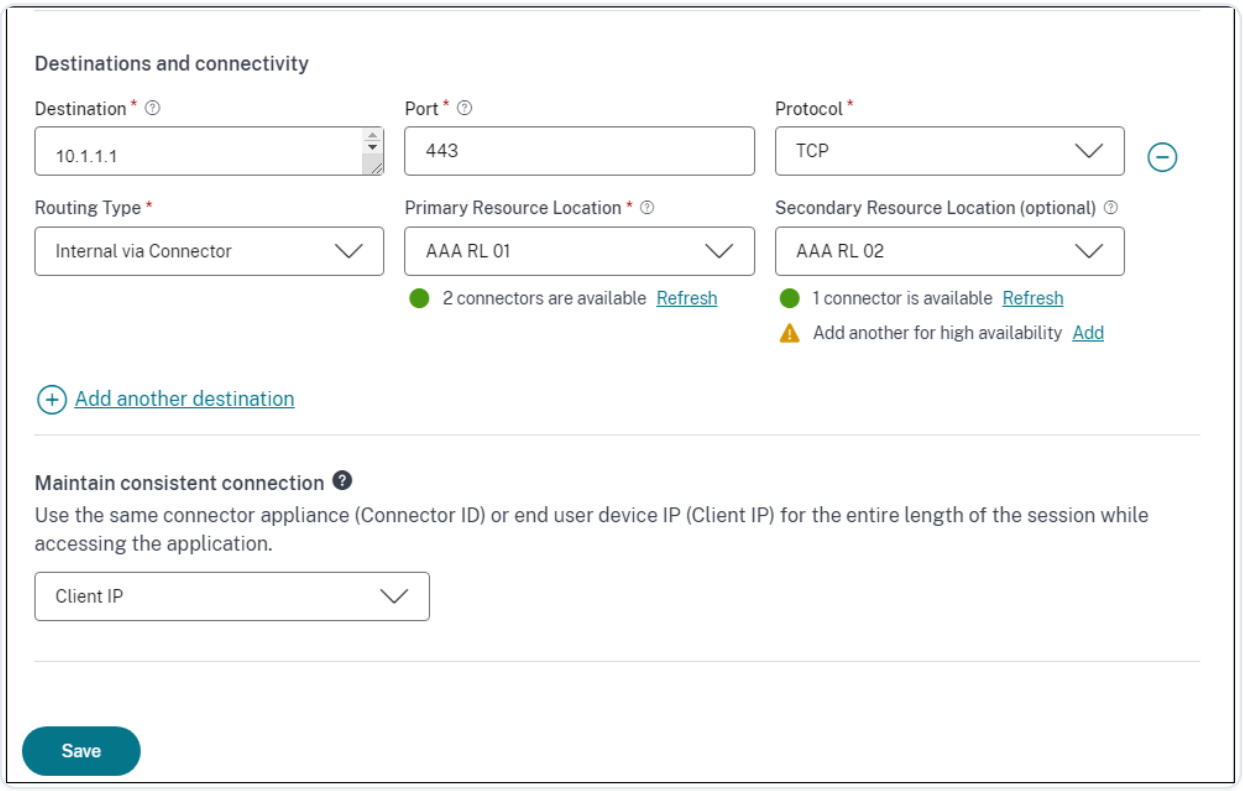
  The following table provides examples of ports that can be configured for a destination.

PORT INPUT	DESCRIPTION
*	By default, the port field is set to `"*"` (any port). The port numbers from 1 to 65535 are supported for the destination.
1300–2400	The port numbers from 1300 to 2400 are supported for the destination.
38389	Only the port number 38389 is supported for the destination.
22,345,5678	The ports 22, 345, 5678 are supported for the destination.
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

5. In the **App Connectivity** section, you define routing for the applications, if the domains must be routed externally or internally through Citrix Connector™ Appliance.

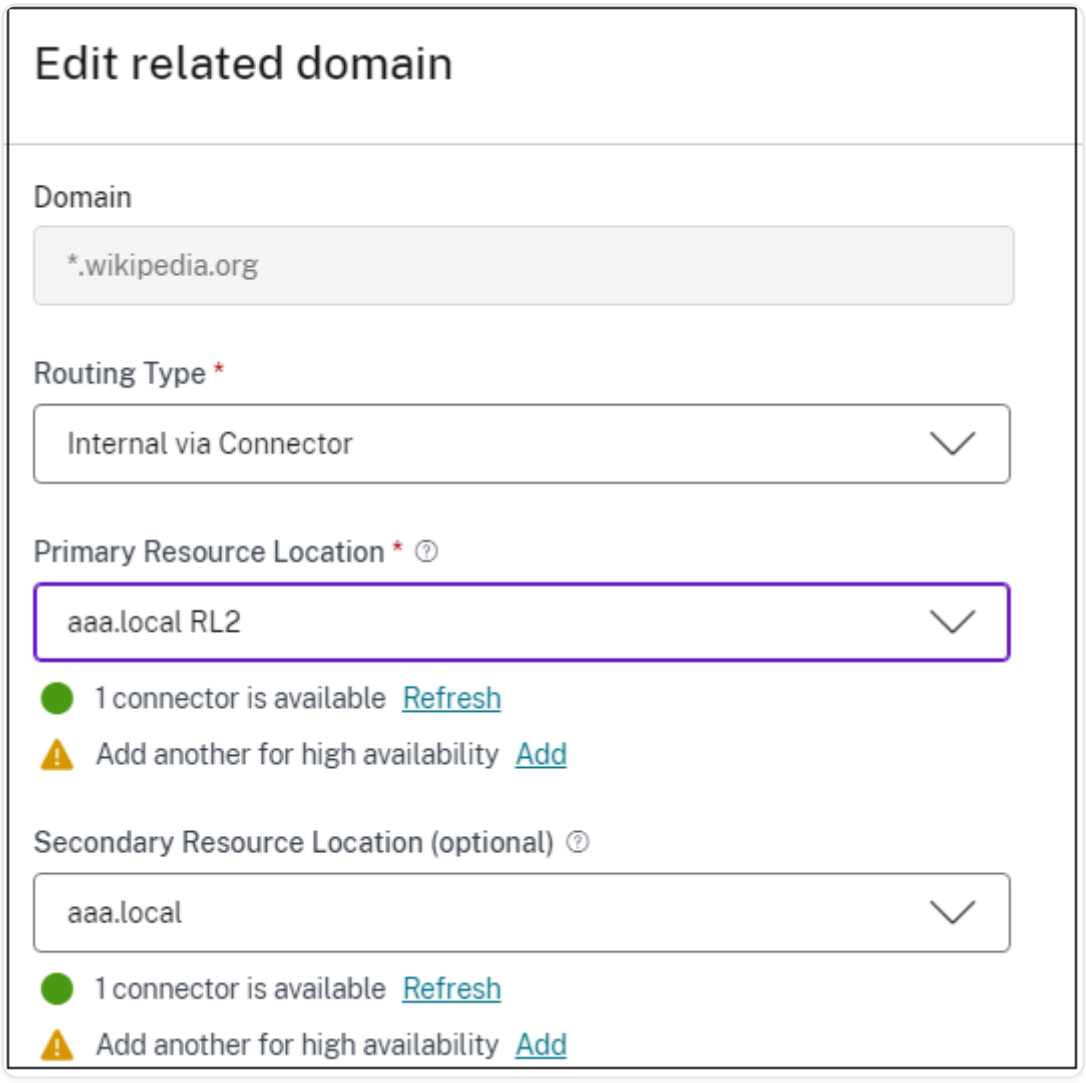


- **Routing Type** - Select one of the following:
  - **Internal via Connector** - The apps can be external but the traffic must flow through the Connector Appliance to the outside network.
  - **External** – The traffic flows directly to the internet.
- **Primary and secondary resource locations** - Admins can ensure high availability of applications even during disruptions by configuring a secondary resource location or by using the **First Available** option.
  - **Primary Resource Location:** Select the primary resource location where the application is hosted. Alternatively, admins can select the option **First Available** in **Primary Resource Location**.
  - **First available:** The **First Available** option ensures that a working resource location is used. When **First Available** is selected, the system automatically routes traffic to the first available location. This ensures continuous application access without manual intervention. For instance, if ResourceLocation1 is unavailable but ResourceLocation2 is reachable, then ResourceLocation2 is selected by default to front-end the application.
  - **Secondary Resource Location** - The **Secondary Resource Location** option becomes available only if a primary resource location is explicitly specified. If the

primary resource location becomes unavailable, for reasons such as a Connector Appliance or data center failure, the application fails over to the specified secondary resource location. The secondary resource location can also act as a failover even when the application is hosted in another data center.

You can also set a primary and secondary resource location or select the **First Available** option for each of the related domains.

a. Click the edit icon in the **Actions** column of the Related Domains table.
b. Set the primary and secondary resource location or choose the **First Available** option.



Note:

Setting the backup resource location and using the **First Available** option feature is currently in Preview.

- **Maintain consistent connection** - You can enable connector stickiness or client IP stickiness for the TCP/UDP apps. Select the **Maintain consistent connection** checkbox and then select on the following options:
  - **Do not use:** The application does not require any persistence. The application can work with any source IP address.
  - **Client IP:** The application uses the same source IP address for the client with each connection.
  - **Connector ID:** The application connects to the same connector appliance with each session.Select one of the following options:

  For details about consistent connections, see Maintain consistent connection.

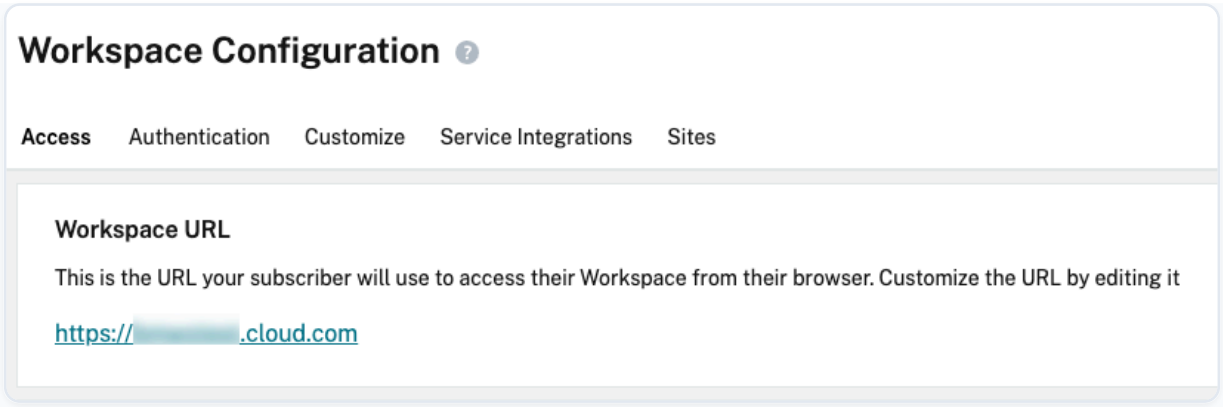
6. Click **Save** and then click **Finish**.

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

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

Note:

- To grant access to the apps for the users, admins are required to create access policies. In access policies, admins add app subscribers and configure security controls. For details, see Create access policies.
- To configure the authentication methods required for the users, see Setup identity and authentication.
- To obtain the store URL to be shared with the users, from the Citrix Cloud™ menu, click **StoreFront Cloud**, and select the **Access** tab.



Admin Configuration – Citrix Secure Access client-based access to HTTP/HTTPS apps

Note:

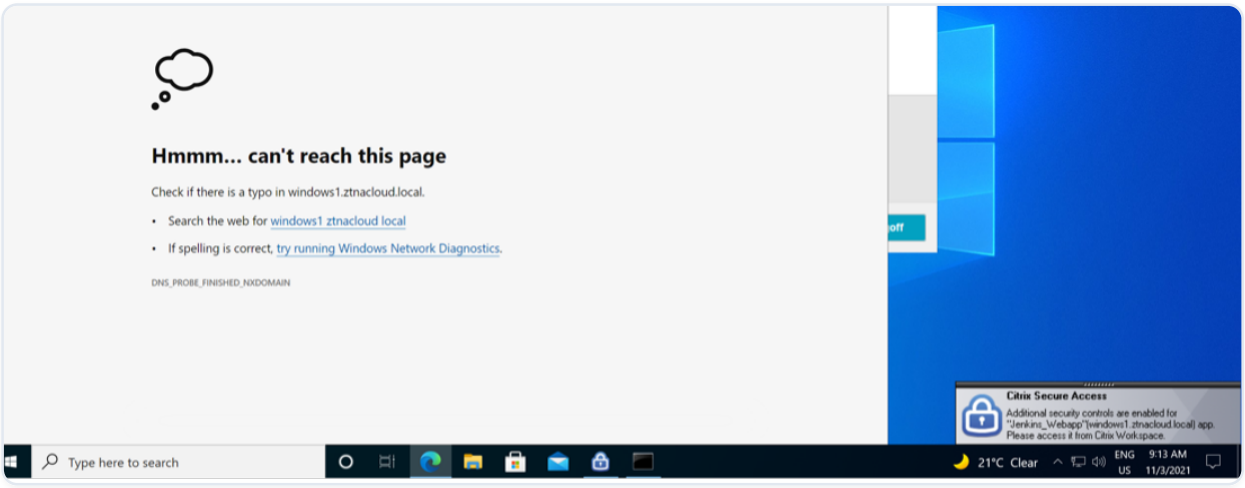
To access existing or new HTTP/HTTPS apps using the Citrix Secure Access client, you must install at least one (recommended two for high-availability) Connector Appliance in your resource location. The connector appliance can be installed on-premises, in the data center hypervisor, or in the public cloud. For details of Connector Appliance and its installation, see Connector Appliance for Cloud Services.

Prerequisites

- Access to Citrix Secure Private Access in Citrix Cloud.

Points to note

- Internal web apps enforced with enhanced security controls cannot be accessed through the Citrix Secure Access client.
- SaaS apps cannot be accessed via the Citrix Secure Access client.
- If you try to access an HTTP(S) application, which has enhanced security controls enabled, then the following pop-up message is displayed. **Additional security controls are enabled for "app name"(FQDN) app. Please access it from Citrix Workspace.**



- If you want to enable SSO experience, access the web apps using Citrix Workspace app or web portal.

The steps to configure HTTP(S) apps remain the same as existing functionality explained under Support for Enterprise web apps.

Adaptive access to TCP/UDP and HTTP(S) apps

Adaptive access provides the ability for admins to govern access to business-critical apps based on multiple contextual factors like device posture check, user geo-location, user role, and the Citrix Analytics service provided risk score.

Note:

- You can deny access to TCP/UDP applications, admins create policies based on the users, user groups, the devices from which the users access the applications, and the location (country) from where an application is accessed. Access to applications is allowed by default.
- The user subscription made for an app is applicable for all the TCP/UDP app destinations configured for the ZTNA application.

To create an adaptive access policy

Admins can use the admin-guided workflow wizard to configure Zero Trust Network Access to SaaS apps, internal web apps, and TCP/UDP apps in the Secure Private Access service.

Note:

- For details on creating an adaptive access policy, see Create access policies.
- For an end-to-end configuration of Zero Trust Network Access to SaaS apps, internal web apps, and TCP/UDP apps in the Secure Private Access service, see Admin-guided workflow for easy onboarding and set up.

Login and logout script configuration registries

The Citrix Secure Access client accesses the login and logout script configuration from the following registries when the Citrix Secure Access client connects to the Citrix Secure Private Access cloud service.

Registry: HKEY_LOCAL_MACHINE>SOFTWARE>Citrix>Secure Access Client

- Login script path: SecureAccessLogInScript type REG_SZ
- Logout script path: SecureAccessLogOutScript type REG_SZ

Troubleshoot application domains IP address conflict

Destinations added while creating an app are added to a main routing table. The routing table is the source of truth for making the routing decision to direct connection establishment and traffic to the correct resource location.

- The destination IP address must be unique across resource locations.
- Citrix recommends that you avoid overlap of the IP addresses or domains in the routing table. In case you encounter an overlap, you must resolve it.

Following are the types of conflict scenarios. **Complete Overlap** is the only error scenario that restricts admin configuration until the conflict is resolved.

CONFLICT SCENARIOS	EXISTING APPLICATION DOMAIN ENTRY	NEW ENTRY FROM APP ADDITION	BEHAVIOR
Subset Overlap	10.10.10.0-10.10.10.255 RL1	10.10.10.50-10.10.10.60 RL1	Allow; Warning info - Subset overlap of IP domain with existing entries
Subset Overlap	10.10.10.0-10.10.10.255 RL1	10.10.10.50-10.10.10.60 RL2	Allow; Warning info - Subset overlap of IP

CONFLICT SCENARIOS	EXISTING APPLICATION DOMAIN ENTRY	NEW ENTRY FROM APP ADDITION	BEHAVIOR
			domain with existing entrieS
Partial Overlap	10.10.10.0-10.10.10.100 RL1	10.10.10.50-10.10.10.200 RL1	Allow; Warning info - Partial overlap of IP domain with existing entries
Partial Overlap	10.10.10.0-10.10.10.100 RL1	10.10.10.50-10.10.10.200 RL2	Allow; Warning info - Partial overlap of IP domain with existing entries
Complete Overlap	10.10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL1	Error; `<Completely overlapping IP domain's value>` IP domain completely overlaps with existing entries.Change the existing routing IP Entry or configure a different destination
Complete Overlap	10.10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL2	Error; `<Completely overlapping IP domain's value>` IP domain completely overlaps with existing entries. Change the existing routing IP Entry or configure a different destination
Exact Match	20.20.20.0/29 RL1	20.20.20.0/29	Allow; Domains already exist in the domain routing table.

CONFLICT SCENARIOS	EXISTING APPLICATION DOMAIN ENTRY	NEW ENTRY FROM APP ADDITION	BEHAVIOR
			Changes update the domain routing table

Note:

- If the destinations added results in a complete overlap, an error is displayed while configuring the app in the **App Details** section. The admin must resolve this error by modifying the destinations in the **App Connectivity** section.

  If there are no errors in the **App Details** section, the admin can proceed to save the app details. However, in the **App Connectivity** section, if the destinations have a subset and partial overlap with each other or existing entries in the main routing table, a warning message is displayed. In this case, the admin can choose to either resolve the error or continue with the configuration.
- Citrix recommends keeping a clean **Application Domain** table. It is easier to configure new routing entries if the IP address domains are broken into appropriate chunks without overlaps.

Points to note

- Access to an existing web app for which enhanced security is enabled is denied via the Secure Access client. An error message suggesting to log in using Citrix Workspace app is displayed.
- Policy configurations for web app based on user risk score, device posture check and so on via Citrix Workspace app are applicable while accessing the app via the Secure Access client.
- The policy bound to an application is applicable for all the destinations in the application.

Always On before Windows Logon

The Secure Private Access Always On connectivity ensures that a managed device is always connected to an enterprise network before (machine tunnel only) and after Windows Logon. The Always On feature establishes a machine-level VPN tunnel before a user logs in to a Windows system. After the user logs on, the machine-level VPN tunnel is replaced by a user-level VPN

tunnel. The application access is based on policies assigned to the machine for the machine-level tunnel and to the user for the user-level tunnel.

The Secure Private Access Always On before Windows Logon (machine-tunnel) feature is supported on the following machines:

- Active Directory domain joined Windows machines
- Microsoft Entra ID hybrid domain joined Windows machines

The Always On before Windows Logon is authenticated by using the computer device certificate-based authentication with Active Directory.

The device certificate is issued by an Active Directory Enterprise Certificate Authority (CA). The device certificate is unique for each domain joined Windows machine.

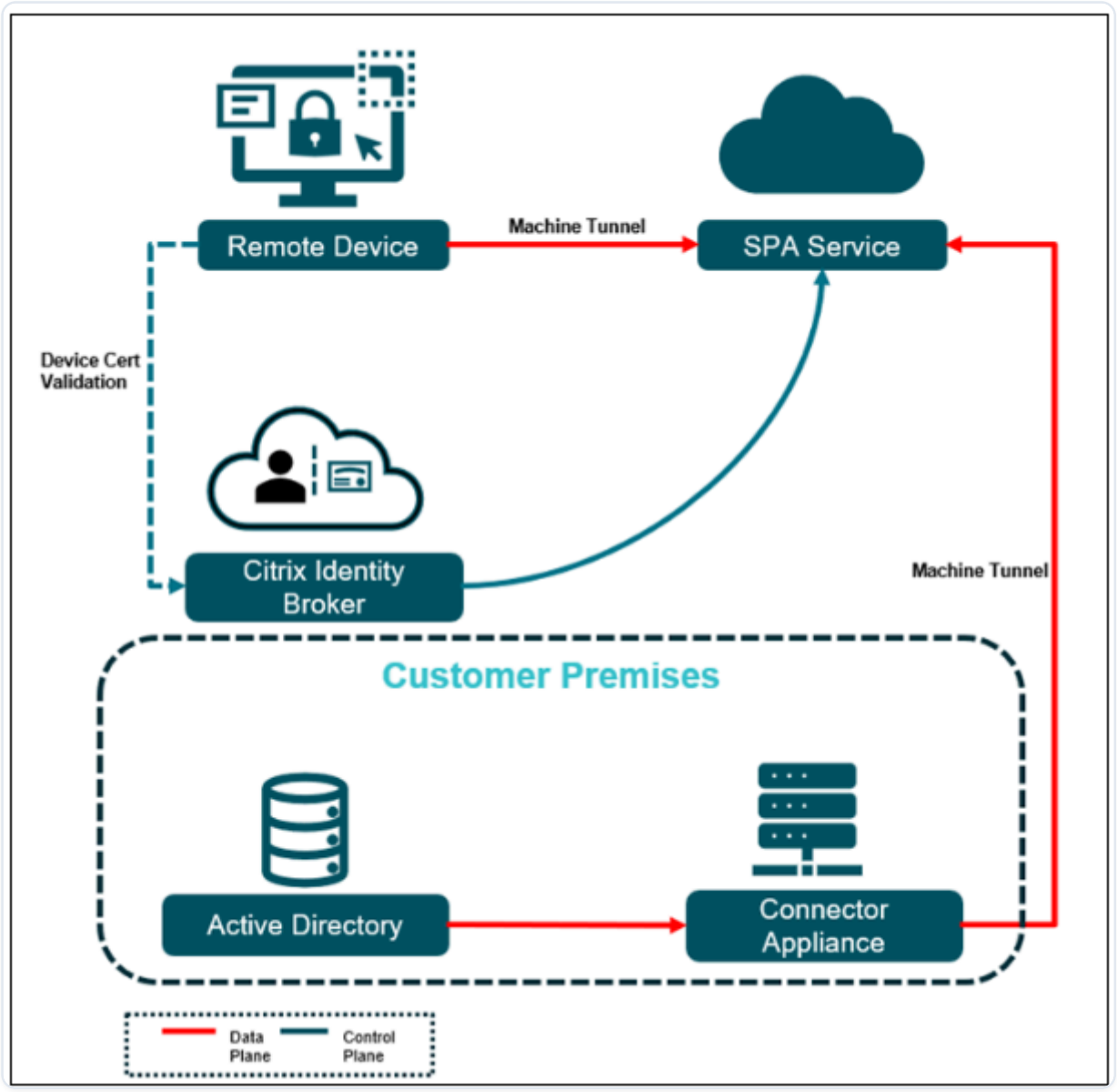
Note:

- The one-tier to multi-tier Microsoft Enterprise Certification Authority is supported.
- The Secure Private Access Always On after Windows Logon (user tunnel) is achieved by one of the following auto logon authentication methods for Active Directory:
  - Single sign-on (SSO) to Citrix Secure Access™ client using the Active Directory credentials provided during Window Logon. SSO does not work if a second factor is configured.
  - Kerberos-based SSO with Citrix Gateway. For details, see Connect an on-premises Citrix Gateway as an identity provider to Citrix Cloud and Provision Adaptive Authentication.
  - Adaptive Authentication configuration. For details, see Provisioning Adaptive Authentication.
- The Secure Private Access Always On after Windows Logon (user tunnel) is achieved by the following autologon authentication method for Microsoft Entra ID hybrid joined machines, SSO with Primary Refresh Token (PRT) of Microsoft Entra ID authentication.

  Disable Always prompt end users for their credentials.

How does Always On work?

The following diagram illustrates the workflow of the Always On before Windows Logon feature.



- The Citrix Identity Broker verifies the device certificate to authenticate the device immediately after bootup. The following are the device certificate verification steps:
  - The client presents the device certificate based on CA certificates uploaded to the Secure Private Access admin console.
  - The Citrix identity provider does device certificate-based authentication.
  - The Citrix identity provider verifies the following details:
    - Device certificate signature
    - CRL-based device certificate revocation check
    - Validate device certificate against Active Directory Computer object
- On successful verification of the device certificate, a secure machine tunnel is established between the device and the resources in the corporate premises based on the access policy.

- On allowing access to Active Directory, Windows Logon authenticates user credentials with Active Directory and supports password expiry and password change.
- After Windows Logon, the machine-level tunnel is automatically replaced by the user tunnel with autologon. On user tunnel failure/disconnect, the connection falls back to the machine tunnel.
- The autologin feature is supported for the Active Directory and hybrid Microsoft Entra ID environment.

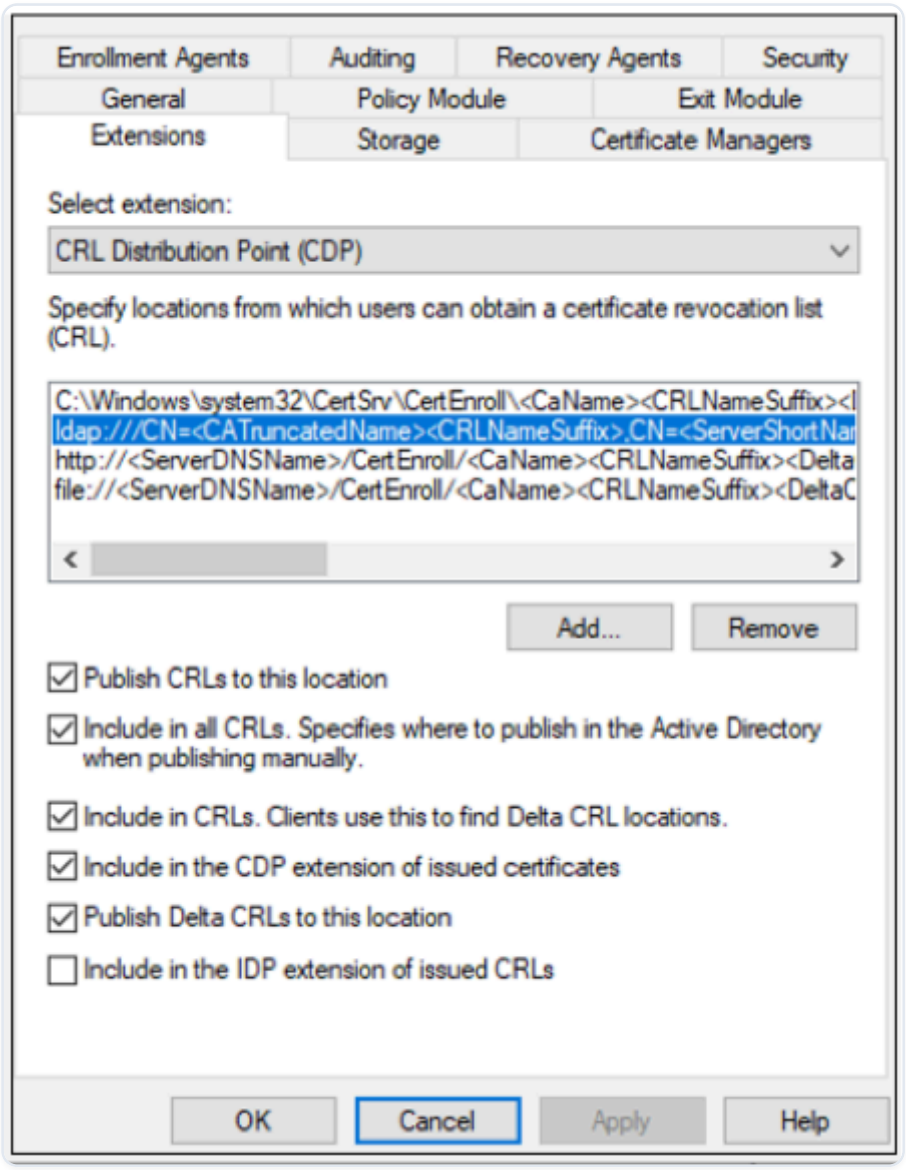
Active Directory and Microsoft Entra ID Hybrid AD configuration

The Windows machines must be Active Directory or Microsoft Entra ID Hybrid joined as a prerequisite for Always On. The Active Directory Enterprise Certificate Authority is required to issue the device certificate for Always On machine authentication. The certificate revocation is verified based on the CDP extension with LDAP URL configuration in the certificate authority.

Device certificate enrollment configuration

The following steps are involved in device certificate enrollment:

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

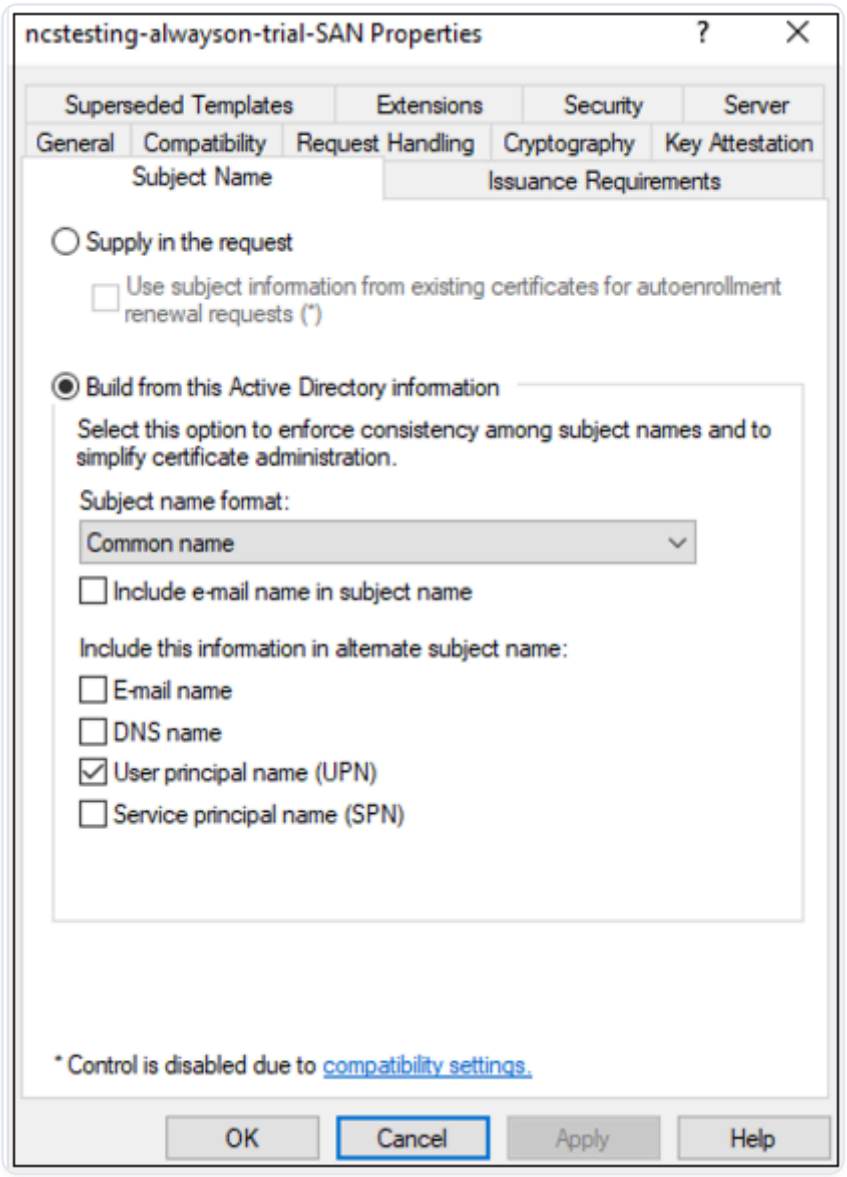


3. A certificate template in this certificate authority must be created to enroll the device certificate with the following details.

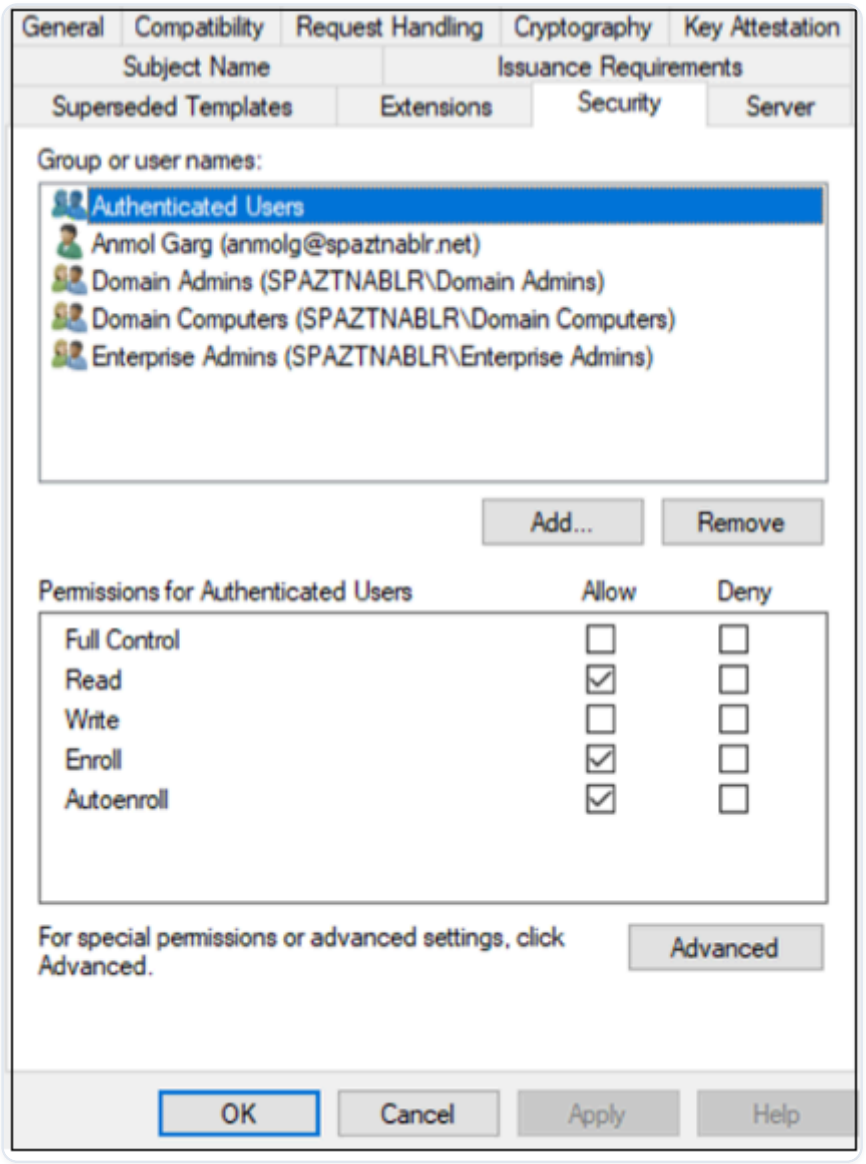
   a. Open the certification template snap-in and duplicate either the **Computer** or **Workstation Authentication** (preferred) template.

   b. Provide a new name for the certificate.

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

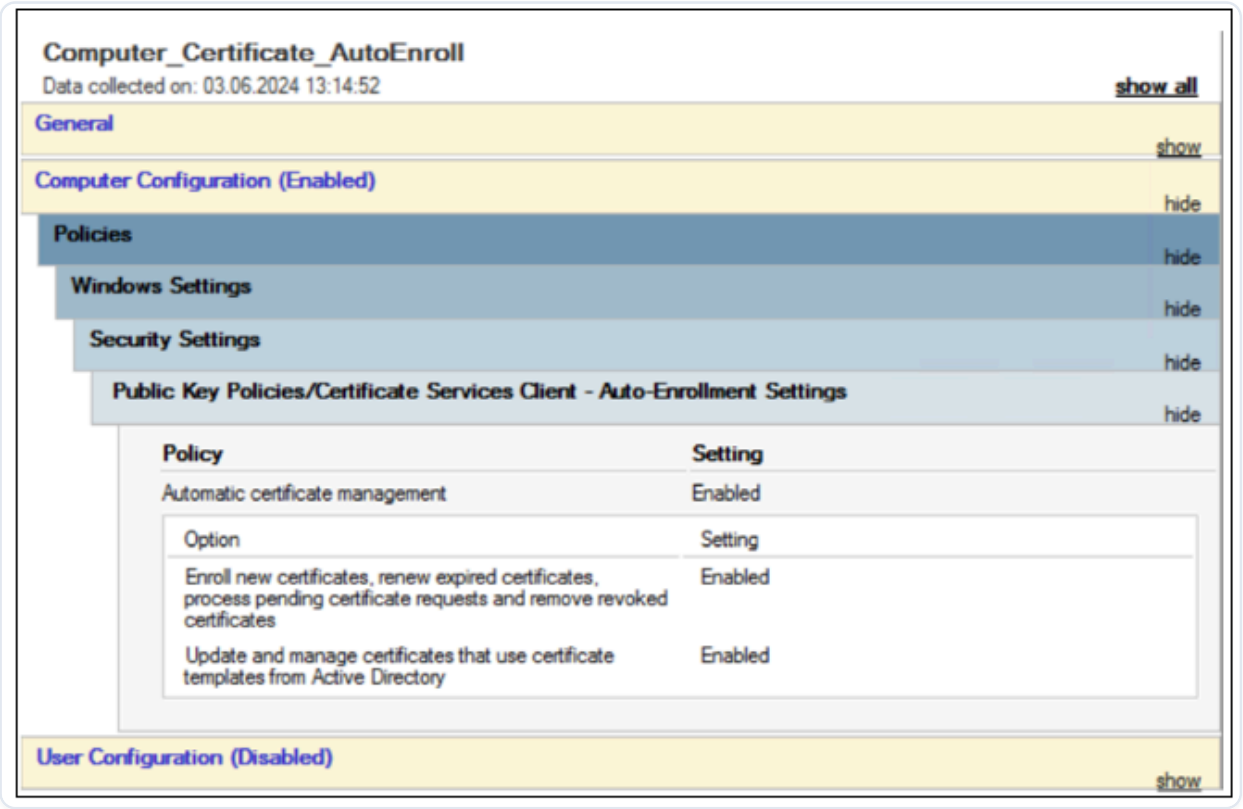


d. Switch to the **Security** tab and add a security group (containing only computer accounts) to which you want to autoenroll the new certificate template. Select the added group and select **Allow** for **Autoenroll**.



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

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



Secure Private Access configuration

The following sections provide more information about configuring Secure Private Access.

Configure Always On before Windows Logon (machine tunnel)

1. In the Secure Private Access admin console, navigate to **Settings > Certificate Store**.

   > **Note:**
   >
   > We recommend that you use the **Machine Based Authentication** option found under **Settings > Certificate Store** instead of **Settings > Machine Based Authentication**. The option **Settings > Machine Based Authentication** is scheduled for removal in the upcoming service release.

2. In the **Certificates** page, click the **Machine Authentication** tab.

   The **Enforce machine level tunnel before users log on** toggle switch is enabled by default for the Always On before Windows Logon feature.

3. Upload a CA certificate: Click **Add certificate**, select the certificate, and click **Open**.
4. In **Name**, enter a name for the certificate.

5. In **Certificate file**, browse to your local drive and upload the certificate file.

   - Certificates for both root CA and intermediate CA are supported. The certificates to be uploaded must be in the PEM format and include the whole chain. The certificate must be generated starting from the intermediate certificate all the way to the root CA.
   - If the certificate is in a CER format, run the following command on a Linux or Mac terminal to convert the certificate into PEM format. After converting the certificate into PEM format, upload the certificate in the Secure Private Access user interface.

     ```
     openssl x509 -in /Users/t_abhishes2/Downloads/cert12.crt out/Users/t_abhishes2/Downloads/cer_pem12_ao.pem
     ```

6. Click **Save**.

   The certificate is added to the list of available certificates in the **Machine authentication** tab.

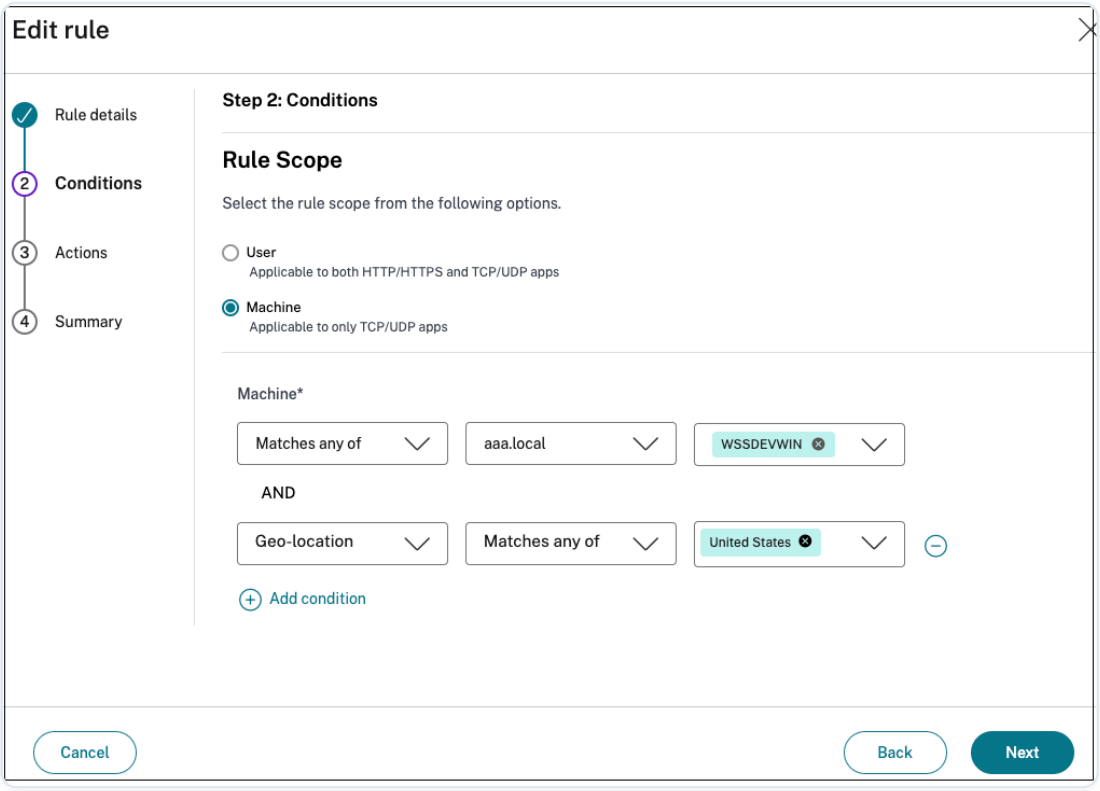
7. Create a TCP/UDP application to access Active Directory as a TCP/UDP server. For example, Active Directory domain, IP address, and Ports. This is for Windows user logon with AD credentials. For details on creating a TCP/UDP app, see Admin Configuration – Citrix Secure Access client-based access to TCP/UDP apps.
8. Create additional applications if needed to be accessed before Windows Logon and before user-level tunnel migration.
9. Create an access policy and provide access for the domain joined machine or its AD group.

   a. In the Secure Private Access admin console, click **Access Policies,** and then click **Create Policy**.
   b. Enter the policy name and description of the policy.
   c. In **Applications**, select the app or set of apps for which this policy must be enforced.
   d. Click **Create Rule** to create rules for the policy.

      - Enter the rule name and a brief description of the rule, and then click **Next**.
      - In the **Rule scope**, select **Machine**.

      > **Note:**
      >
      > When you select a machine, the access privileges are limited as the machine-level tunnel is based on single-factor authentication.

- Select the matching condition, and the domain, and search for the machine/groups to which the policy must be applied. Add more conditions if needed. When finished, click **Next**.
  - **Matches any of** – Only the machines/groups that match any of the names listed in the field and belonging to the selected domain are allowed access.
  - **Does not match any** – All machines/groups except those listed in the field and belonging to the selected domain are allowed access.



10. Select one of the following actions to be applied based on the condition evaluation.
    - **Allow access**
    - **Deny access**
11. Click **Next,** and then click **Finish**.
12. (Optional) Create additional rules for the geo-location and network location, and so on. For details, see Configure an access policy.

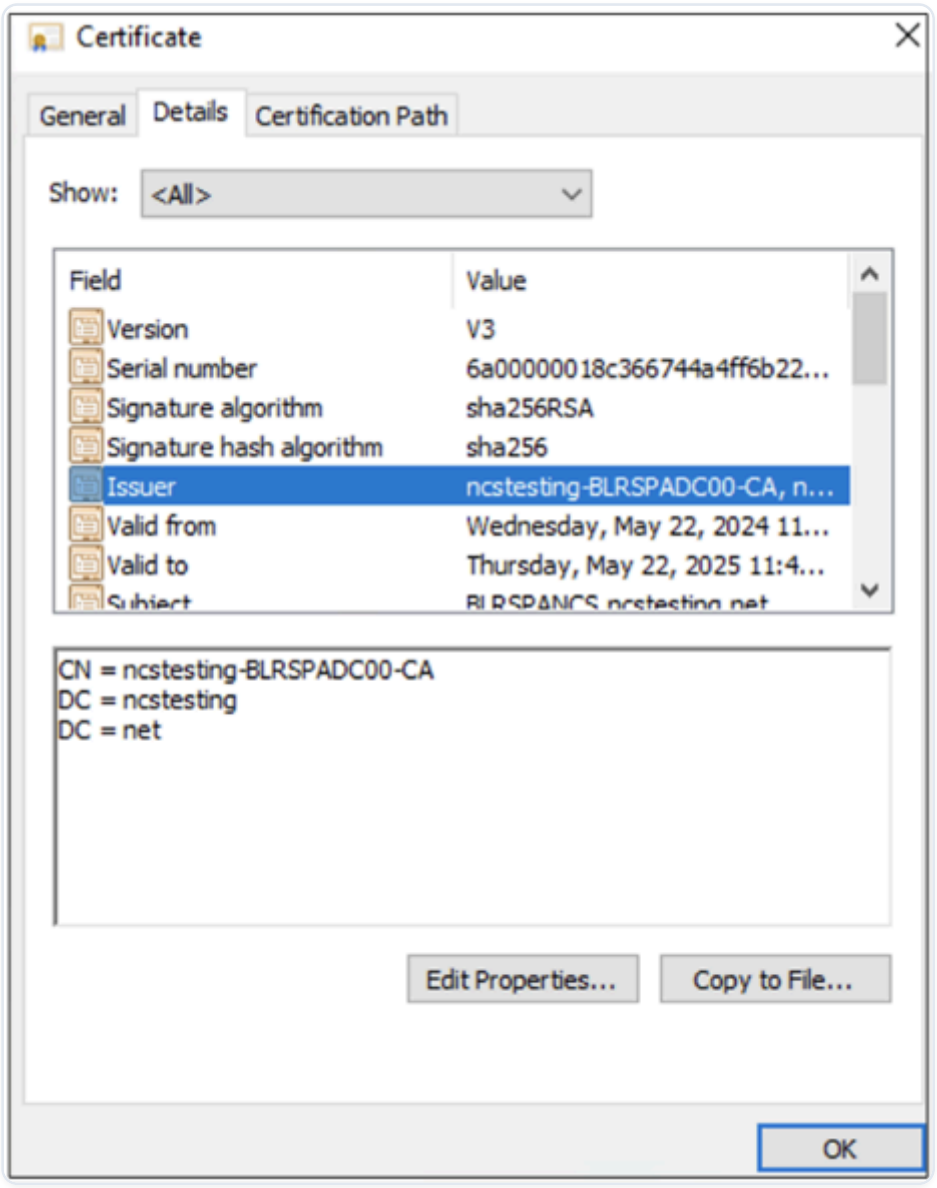
    The policy is listed on the Access Policies page. A priority order is assigned to the policy, by default. The priority with a lower value has the highest preference. The policy with the lowest priority number is evaluated first. If the policy does not match the conditions defined, the next policy is evaluated. If the conditions match, the other policies are skipped.

Connector Appliance Configuration

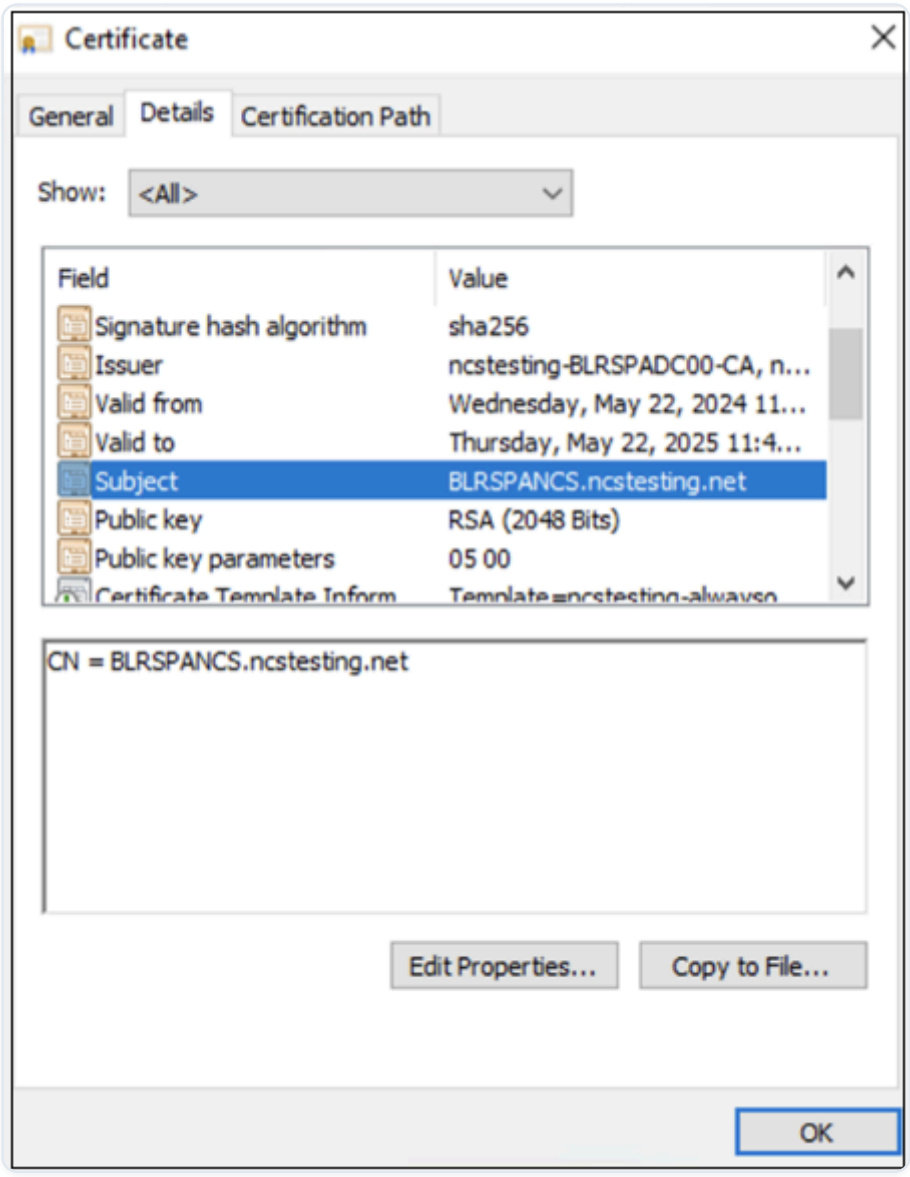
Connector Appliance performs device certificate validation, certificate revocation check (CRL), and device object verification for Always On Device certificate authentication. Connector Appliance must be domain joined to the Active Directory domain for Device certificate authentication to be supported.

Client configuration

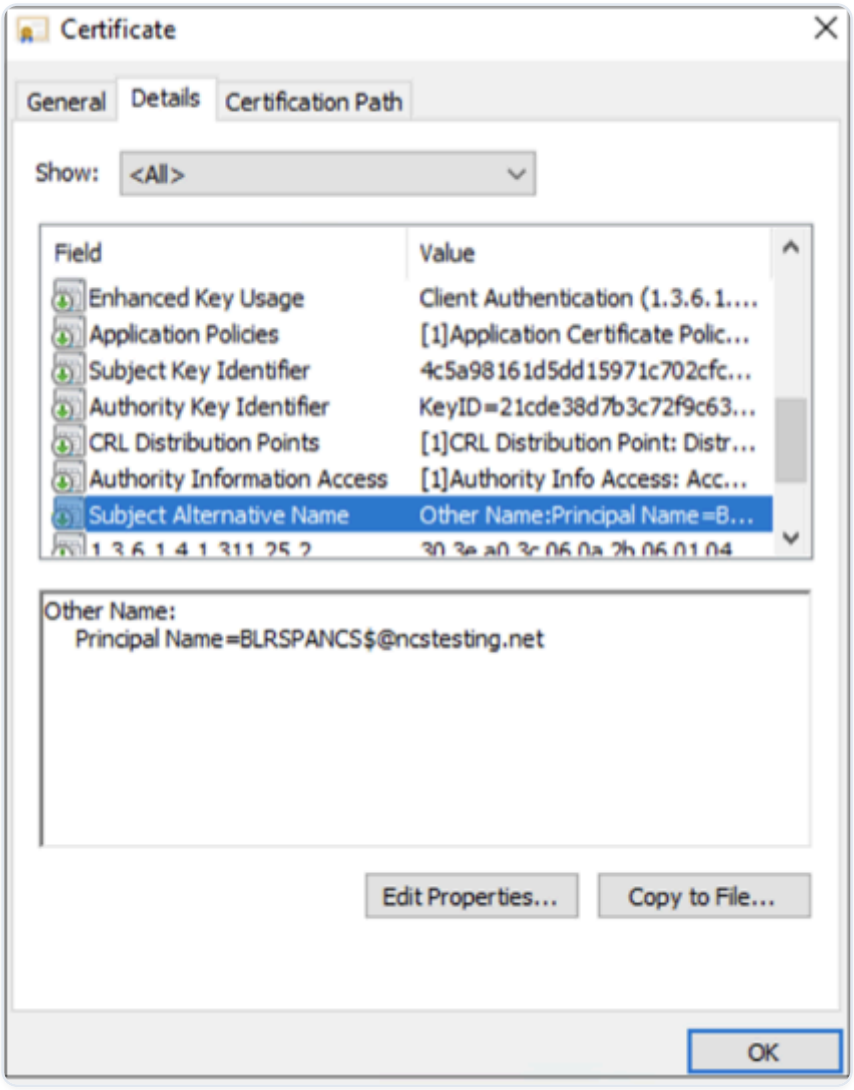
- The Windows machine that needs Always On support must be domain joined to Active Directory or Entra ID hybrid.
- The Windows machine must enroll a device certificate from the Enterprise Certificate Authority for Secure Private Access Always On.
- The device certificate attributes must include the following details.
    - The issuer name in the device certificate must match the common name of the CA certificate uploaded to the Secure Private Access admin console.



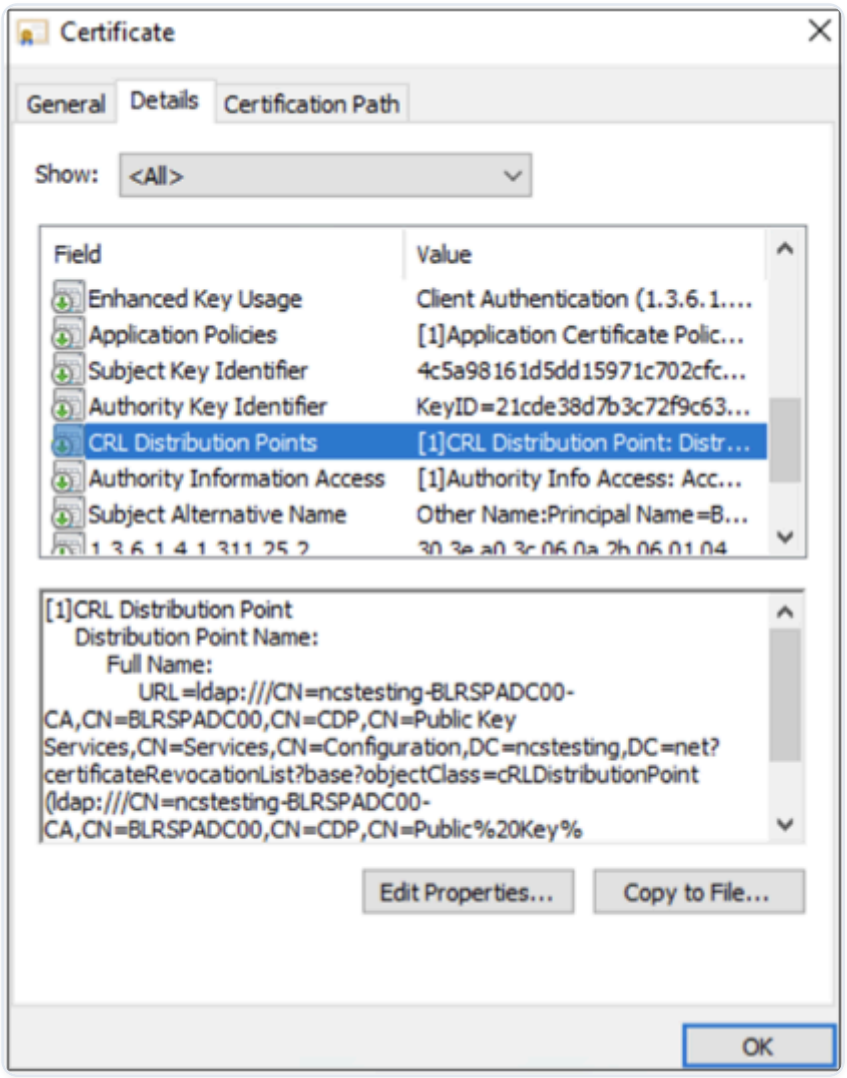
- Subject must contain the common name of the computer.



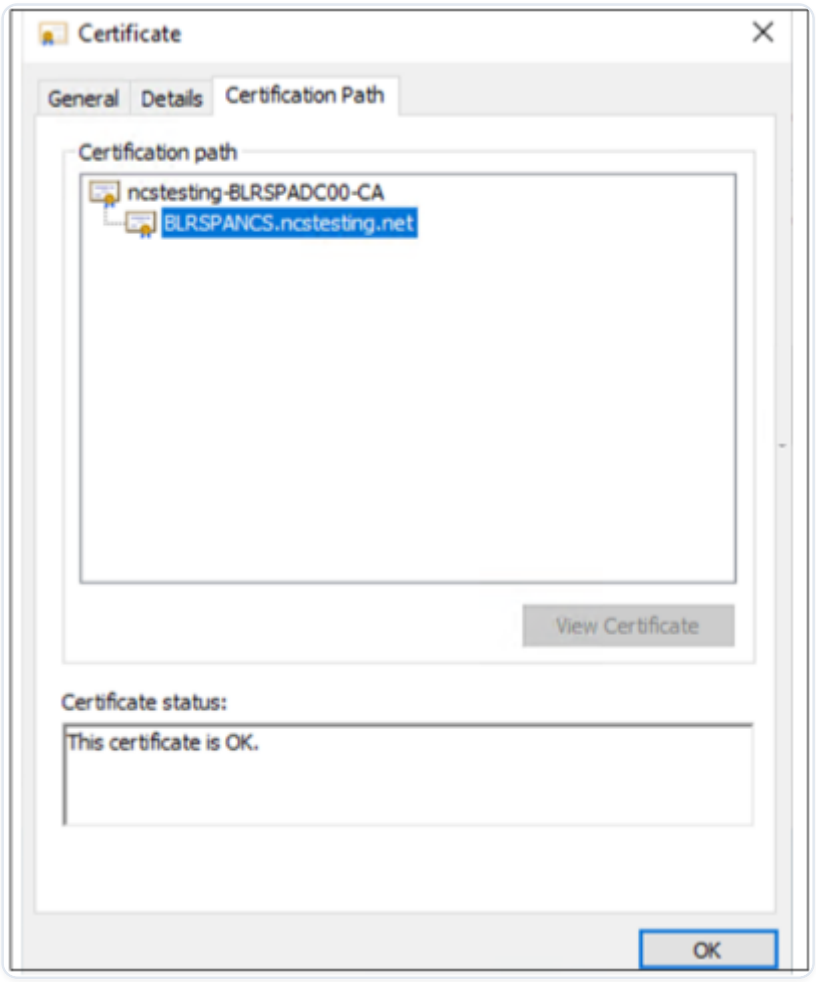
- Subject Alternate Name (SAN) must contain the UPN of the computer.



- CRL distribution point must contain the appropriate LDAP URL.



- The certification path must be appropriate to the certificate authority chain.



- Install the Citrix Secure Access client for Always On.
- The following registries must be created on the client to enable Always On before Windows Logon.
    - **CloudAlwaysOnURL** in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client.

      Registry Type - STRING

      Registry Value - `<Customer store FQDN>` (For example, company.cloud.com)
    - **AlwaysOnService** in HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client.

      Registry Type - DWORD

      Registry Value - 0x00000002

Configure Always On after Windows Logon (machine/user tunnel)

After successful Windows Logon, the machine tunnel continues until the user login is successful with the Citrix Secure Access client.

- If user auto login is successful, the machine tunnel is migrated to a user tunnel.
- If user auto login fails, the machine tunnel continues.
- If the user tunnel gets disconnected, the connection automatically falls back to the machine tunnel.

User Autologon after Windows Logon is supported for the following authentication methods in the StoreFront Cloud authentication configuration.

- Authentication with Active Directory (with no second factor) - AD credential SSO
- Authentication with Citrix Gateway/Adaptive Auth configured with Kerberos SSO
- Authentication with Azure Active Directory (SSO with Primary Refresh Token (PRT) of Microsoft Entra ID authentication).

> **Note:**
>
> Disable Always prompt end users for their credentials.

Limitations

- Computer UPN host name must not exceed 15 characters.
- Windows Auto Logon (First Time User (FTU)) case is supported only if the machine is domain joined and the device certificate is present.
- The Always On before Windows Logon feature is supported only on Windows 10 or later versions.
- The Always On before Windows Logon feature is not supported for Windows Server Operating Systems.
- The Always On before Windows Logon feature is not supported with Cloud Connector. Even if you have not selected Connector Appliance as a preferred connector, the machine tunnel traffic goes via Connector Appliance.

References

- Create a TCP/UDP application in the Secure Private Access console
- Assign an access policy to the TCP/UDP application
- Connect an on-premises Citrix Gateway as an identity provider to Citrix Cloud
- Provision Adaptive Authentication

Reserved CIDR addresses for the TCP and UDP servers

Admins can configure reserved CIDR IP addresses for the TCP/UDP servers. These IP addresses are shared in the DNS response instead of the actual IP address during DNS resolution.

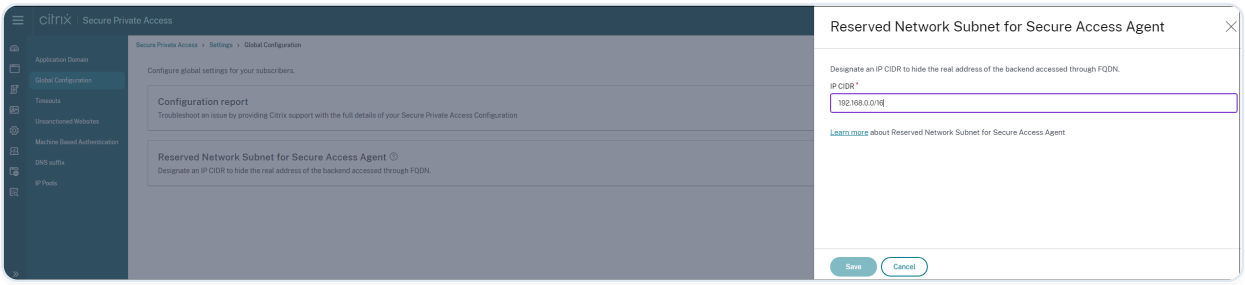
The following are the allowed reserved CIDR IP address ranges:

- 10.0.0.0/8
- 172.16.0.0/12
- 192.168.0.0/16

> **Note:**
>
> Ensure that the reserved IP addresses do not conflict with the following:
>
> - IP address configured for TCP/UDP applications at the customer resource location.
> - Network subnet of the client machines.

Configure reserved CIDR IP addresses

1. Click **Settings**, and then click **Global Configuration**.



2. In **Reserved Network Subnet for Secure Access Agent**, click **Manage**.
3. In **IP CIDR**, enter the private IP address range.
4. Click **Save**.

DNS suffixes to resolve FQDNs to IP addresses

DNS suffix is a global configuration that is applied for all end users. The DNS suffix feature of the Citrix Secure Private Access™ service can be used for the following use cases:

- Enable the Citrix Secure Access™ client to resolve a non-fully qualified domain name (host name) to a fully qualified domain name (FQDN) by adding the DNS suffix domain for the back-end servers.
- Enable admins to configure applications using IP addresses (IP CIDR/IP range), so that the end users can access the applications using the corresponding FQDN under the DNS suffix domain.

For example, while resolving a non-fully qualified domain name "workday", if the DNS suffix "citrix.net" is configured, the operating system appends the suffix "citrix.net" and resolves to "workday.citrix.net".

If multiple DNS suffixes are configured, the DNS suffixes are resolved in a sequence. For example, assume that the following suffixes are added:

- `".citrix.net"`
- `".citrix.com"`
- `".xenserver.com"`

When an end user types "workday", the operating system attempts to resolve the FQDNs in the following sequence. If it succeeds with one suffix, the remaining suffixes are skipped.

1. workday.citrix.net
2. workday.citrix.com
3. workday.xenserver.com

Important:

- DNS suffix configuration can only enable the client to resolve a non-fully qualified domain name by suffixing the domain configured using the DNS suffix feature. For an end user to access an FQDN under the DNS suffix domain, the admin must configure an application with an IP address, FQDN, or a wildcard domain. For details, see point 4 in Use case example.
- If two different applications are configured, one with FQDN and another with IP address, both corresponding to the same back-end server), then the policy of the application with IP address takes higher precedence. For details, see point 5 in Use case example.

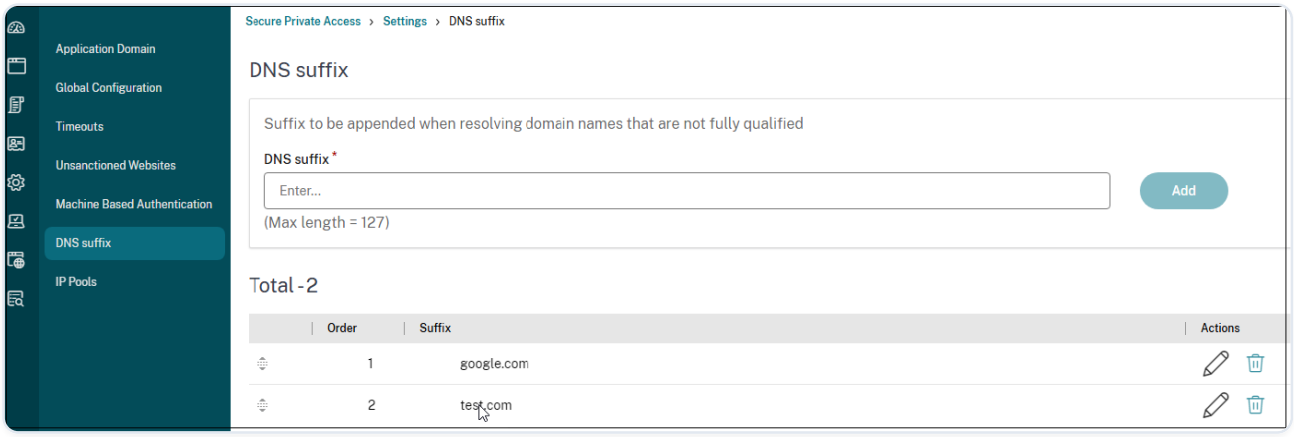
Prerequisites

- Customers must be entitled to the Secure Private Access Advanced edition to use the DNS Suffix feature.
- Contact the Citrix Product Management team to get the DNS suffix feature flags enabled.

How to add DNS suffixes

1. On the Secure Private Access tile, click **Manage**.
2. On the Secure Private Access landing page, click **Settings,** and then click **DNS suffix**.
3. In the **DNS Suffix** field, enter the suffix that must be appended when resolving a non-fully qualified name.
4. Click **Add**.

The suffixes are listed based on the order that they are added. Admins can delete or modify the suffixes.



Example use case

Consider the following:

- An admin has assigned the IP address 192.0.2.1 to a machine in the customer network.
- The FQDNs for the machine (with IP addresses 192.0.2.1) are under the domain “citrix.net” (example, workday.citrix.net).

	DNS SUFFIX AND APP CONFIGURATION	END-USER EXPERIENCE
1	Admin configures the DNS suffix as “citrix.net” and creates an app with IP address 192.0.2.1 with an access policy set to "allow” for user1.	When user1 tries to connect to "workday", the FQDN is suffixed with “citrix.net,” (workday.citrix.net) and the IP address is resolved to 192.0.2.1. Because 192.0.2.1 is allowed for user1 with an app configured, access is granted.
	Note: End user can access the Workday app with 192.0.2.1 or workday.citrix.net or "workday".	
	Without DNS Suffix configuration, access through “workday” and “workday.citrix.net” are denied.	
2	Admin configures the DNS suffix as “citrix.net”, creates an app with FQDN (workday.citrix.net), and sets the access policy to “allow” for user1.	When user1 tries to connect to "workday", "citrix.net" is suffixed to “workday" (workday.citrix.net) . End user can access Workday because an application is configured with “workday.citrix.net” and the access policy is set to “allow” for user1.
	Note: End user can access the Workday app with workday.citrix.net or “workday.”	

	DNS SUFFIX AND APP CONFIGURATION	END-USER EXPERIENCE
	Access to 192.0.2.1 is denied as there is no app configured with this IP address.	
3	Admin configures the DNS suffix as “citrix.net”, creates an app with wildcard domain “*.citrix.net,” and sets the access policy to “allow” for user1.	When user1 tries to connect to “workday”, “citrix.net” is suffixed to “workday” (workday.citrix.net). End user can access Workday because an application is configured with “*.citrix.net” and the access policy is set to “allow” for user1.
	Note: End user can access Workday with workday.citrix.net or “workday”.	
	Access to 192.0.2.1 is denied as there is no app configured with this IP address.	
4	Admin configures the DNS suffix as “citrix.net.” No application is configured for user1 with FQDN (workday.citrix.net) or 192.0.2.1.	When user1 tries to connect to “workday”, “workday” is suffixed with “citrix.net” by the client and resolves “workday.citrix.net” to 192.0.2.1. However, user1 cannot connect to the private server (workday.citrix.net/ 192.0.2.1) because there is no app configured with 192.0.2.1 or workday.citrix.net or *. citrix.net for user1.
5	Admin configures DNS Suffix as “citrix.net." Adds an app with IP address 192.0.2.1,	When user1 tries to connect to “workday”, “citrix.net” is suffixed to Workday

	DNS SUFFIX AND APP CONFIGURATION	END-USER EXPERIENCE
	and sets the access policy to “deny” for user1. Then adds another app with FQDN (workday.citrix.net) that resolves to 192.0.2.1 and sets the access policy to “allow” for user1.	(workday.citrix.net) and the IP address is resolved to 192.0.2.1. However, access to Workday is denied as the policy of the application configured with IP 192.0.2.1 takes precedence over the app configured with FQDN.

Discover related domains using a HAR file

Secure Private Access enables you to upload an HTTP Archive (HAR) file to automatically discover the domains accessed by an application. You can review the discovered domains and select the ones you want to add to the application's related-domain configuration. This simplifies application onboarding by reducing the need to manually identify and configure related domains.

Previously, administrators had to know all of an application's related domains in advance, or discover them reactively as users hit blocked URLs. Because every URL other than the ones configured is blocked by default, this reactive approach leads to a poor user experience. Secure Private Access had no way to identify the internal or embedded URLs within an application.

Example

Suppose you are configuring an application whose primary domain is `example.com`. While using the application, the browser also accesses several additional domains. For example:

- `api.example.com` – Handles the application's backend API calls.
- `auth.example.com` – Manages sign-in and authentication.
- `cdn.example.com` – Serves static content such as images, scripts, and stylesheets.
- `login.microsoftonline.com` – Provides third-party identity authentication.
- `player.vimeo.com` – Loads embedded video content.

Instead of identifying each of these domains manually:

1. Capture a HAR file while using the application.
2. Import the HAR file into Secure Private Access.

3. Review the domains discovered by Secure Private Access. For example, the import might surface `api.example.com`, `auth.example.com`, and `cdn.example.com` as required, along with domains such as `player.vimeo.com` that you can choose to exclude.
4. Select the domains required by the application.
5. Configure routing and resource locations as needed.

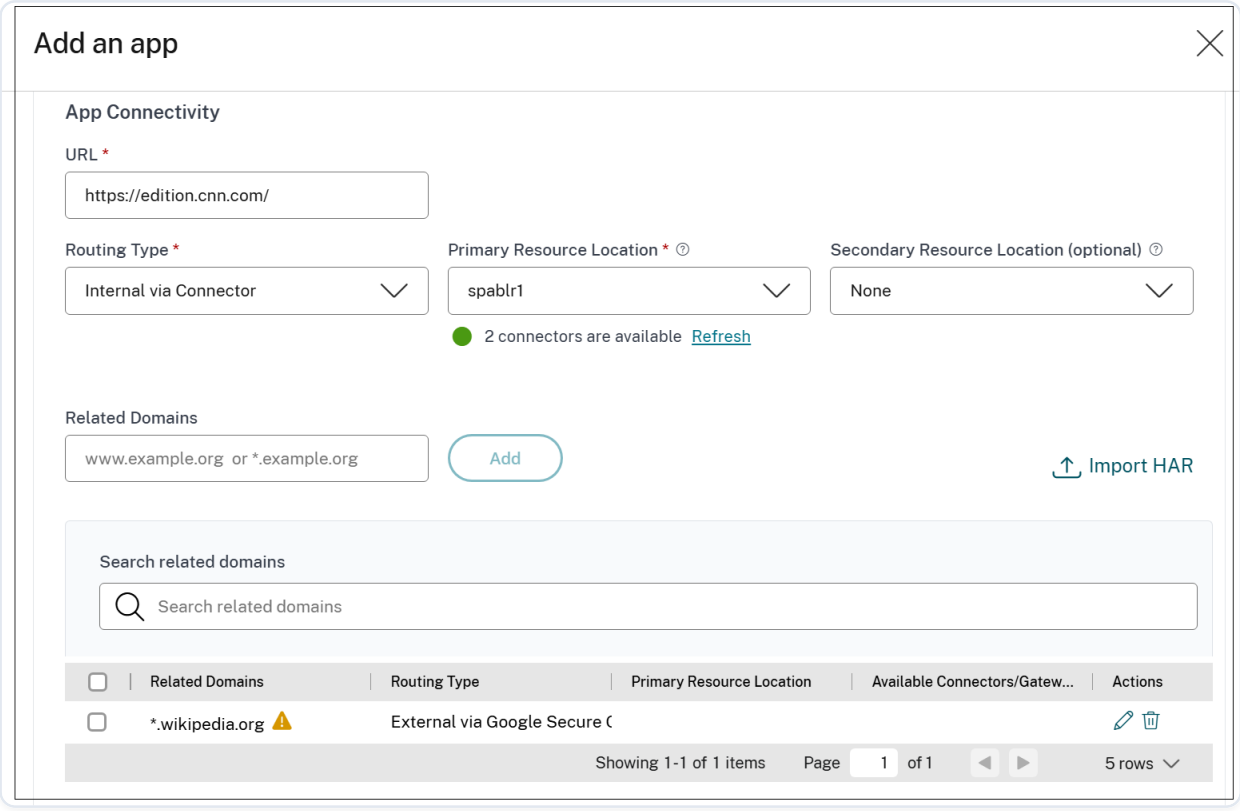
This provides a faster way to identify and configure the domains required for application connectivity.

Prerequisites

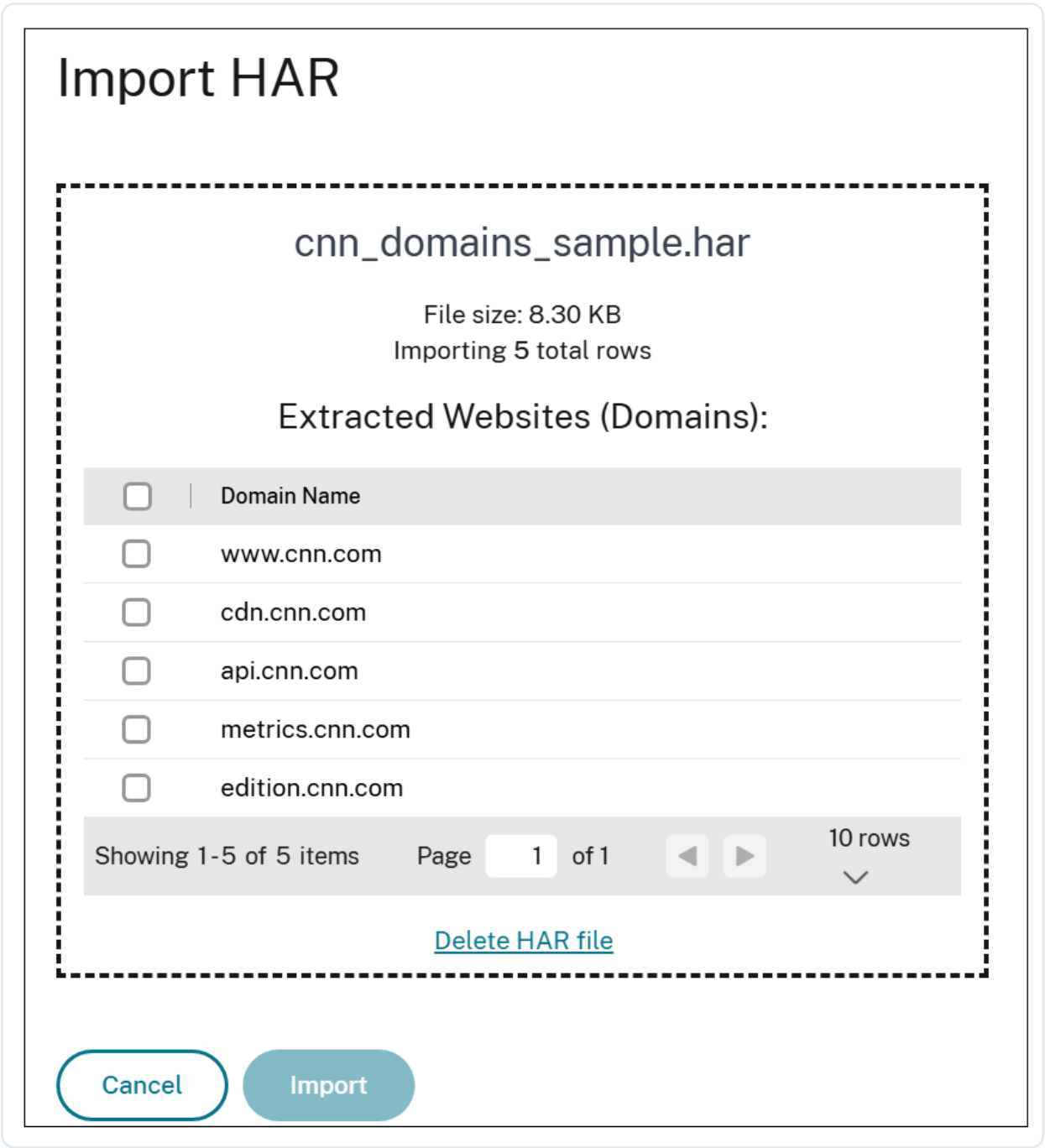
Ensure that you have captured a HAR file while accessing the Web or SaaS application. The HAR file must contain the network request information and must be 50 MB or smaller.

Import a HAR file

1. In the Secure Private Access admin portal, open the Web or SaaS application you want to configure.
2. Go to **App Connectivity** and click **Import HAR**.

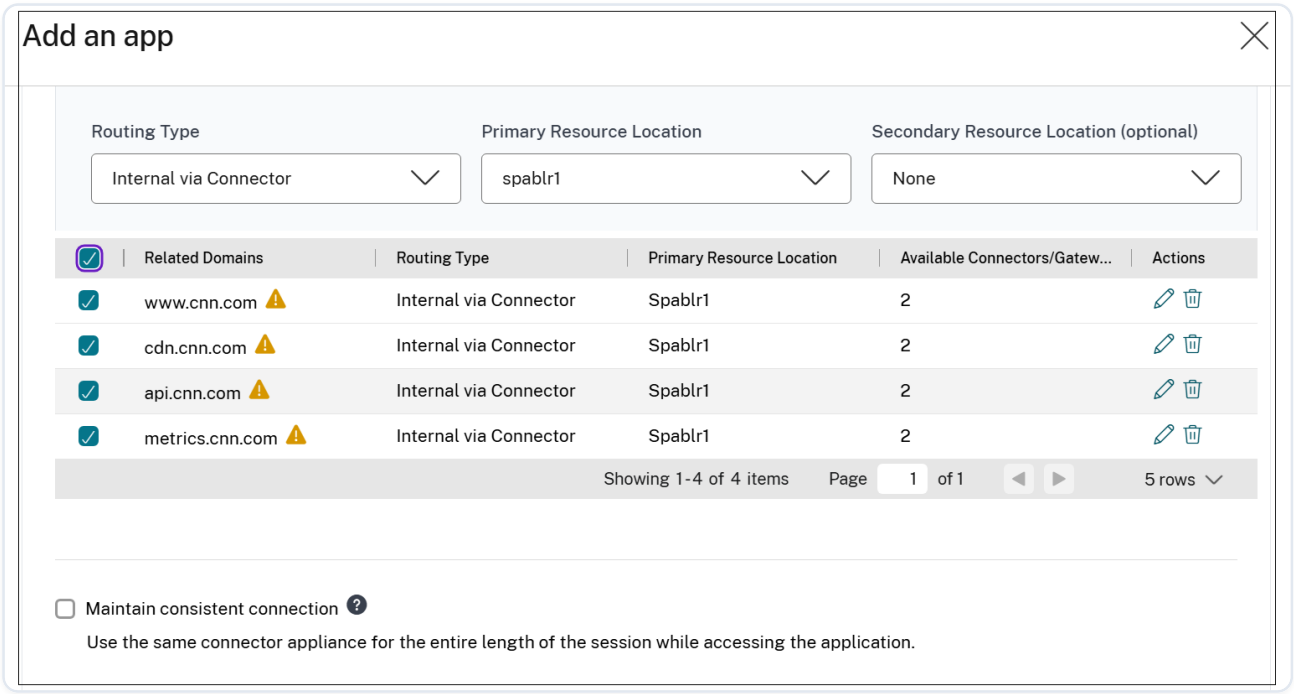


3. Drag and drop the HAR file into the import window, or select the file from your device.
4. Secure Private Access analyzes the HAR file and displays the domains identified from the network requests.



5. Review the discovered domains.
6. Select the domains that you want to add to the application.
7. Select **Import**.

The selected domains are added to the application's **Related Domains** configuration.



Note:

Review the domains discovered before importing them. A HAR file can contain domains that are not required for the application's connectivity.

Manage related domains

After importing the domains, you can manage them from the **Related Domains** table:

- **Search for a domain** – Use the search field to filter the table and quickly find a specific domain.
- **Select domains** – Select individual domains, or use the table header checkbox to select multiple domains. The selection can be used to perform actions on multiple domains at the same time.
- **Edit domain configuration** – Update the configuration of related domains, including the routing type, primary resource location, and secondary resource location.
- **Bulk edit domains** – Select multiple eligible domains and update their routing and resource-location settings at the same time. Bulk editing is available for applicable internal domains. External domains might not support all configuration options.
- **Resource locations** – When configuring a related domain, assign a primary and, where applicable, secondary resource location. Use these settings to define how Secure Private

Access routes traffic for the related domain and which resource locations are used to provide connectivity.

Validation and file requirements

The HAR import feature validates the uploaded file before processing it.

- Only valid HAR files containing network request entries can be imported.
- The maximum supported file size is **50 MB**.
- Domains are automatically extracted from the URLs in the HAR file.
- Duplicate domains are automatically removed.
- Domains are normalized before they are added to the related-domain configuration.

Port-based routing using Routing Exceptions - Preview

The port-based routing feature allows admins to route traffic for different ports of the same destination differently for TCP/UDP apps using routing exceptions. When onboarding applications on Secure Private Access, admins can define how the application traffic is routed using one of the following options:

- **Internal via Connector**: Traffic is securely tunneled via the connector.
- **Internal via Netscaler Gateway**: Traffic is routed via NetScaler Gateway using a hybrid data path.
- **External**: Traffic is routed directly without tunneling it through Secure Private Access.

To route traffic for different ports of the same destination differently, admins must use access policy routing exceptions. Each destination and port combination that requires a distinct routing decision must be configured as a separate application and bound to a separate policy. The UI enforces a uniqueness check, so different routes cannot be configured within different applications with the same destination.

Use cases of port-based routing

Scenario: An admin hosts two applications on the same server (10.102.124.135).

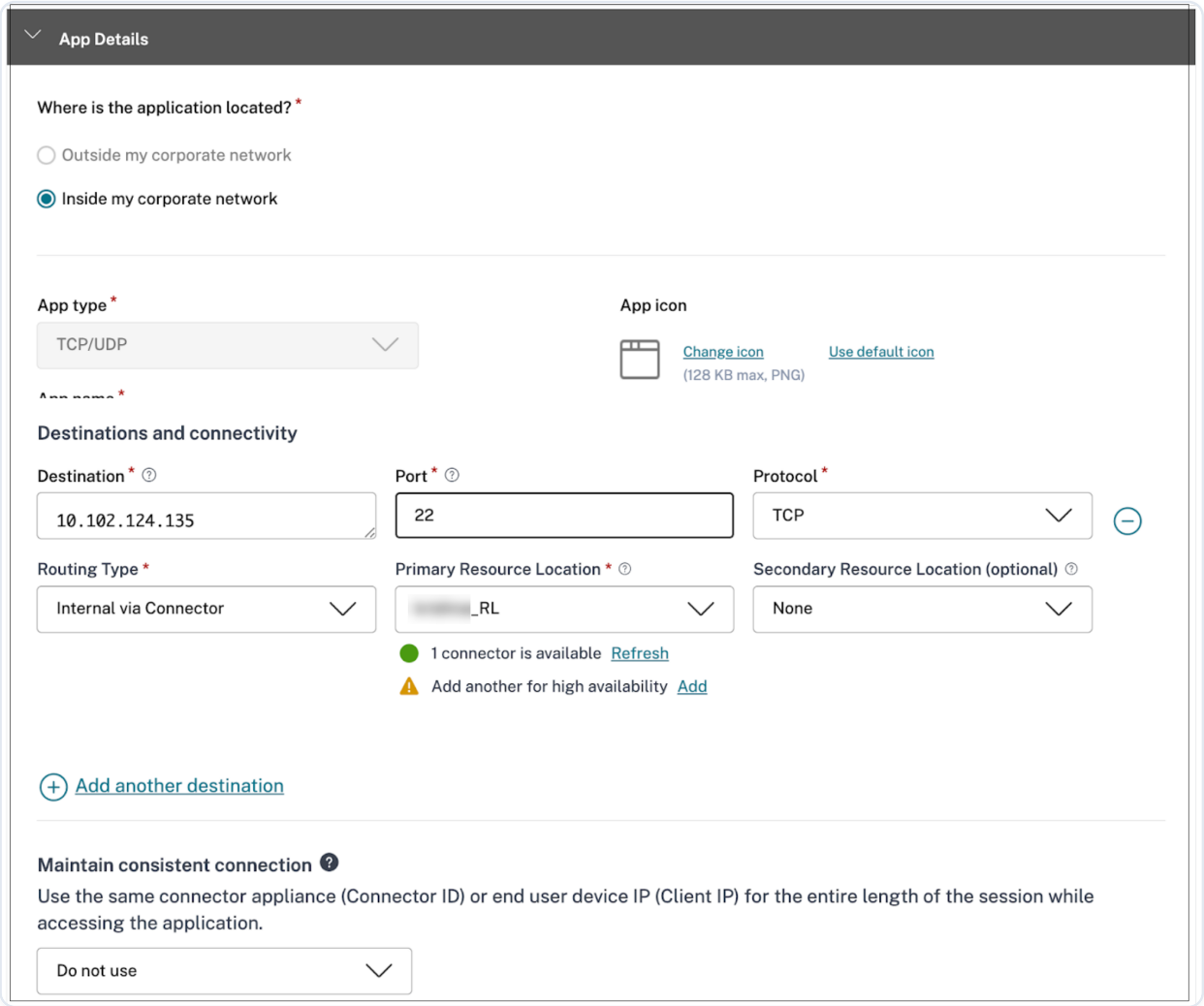
- SSH access on port 22
- Web access on port 80, 443

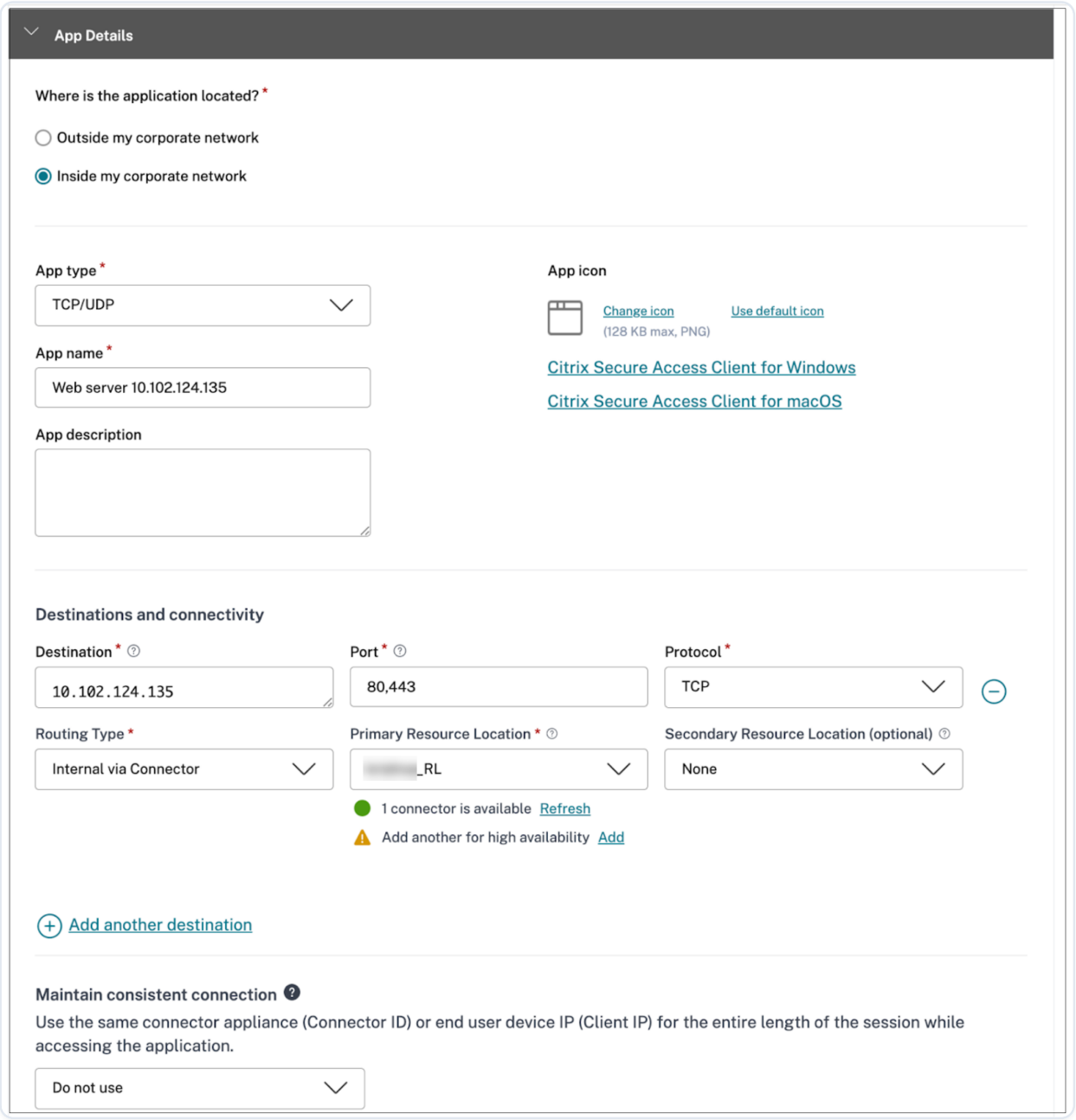
Requirement:

- Allow the developer user group to access SSH internally via a connector.
- Allow the business unit user group to access the web application directly from the corporate network.

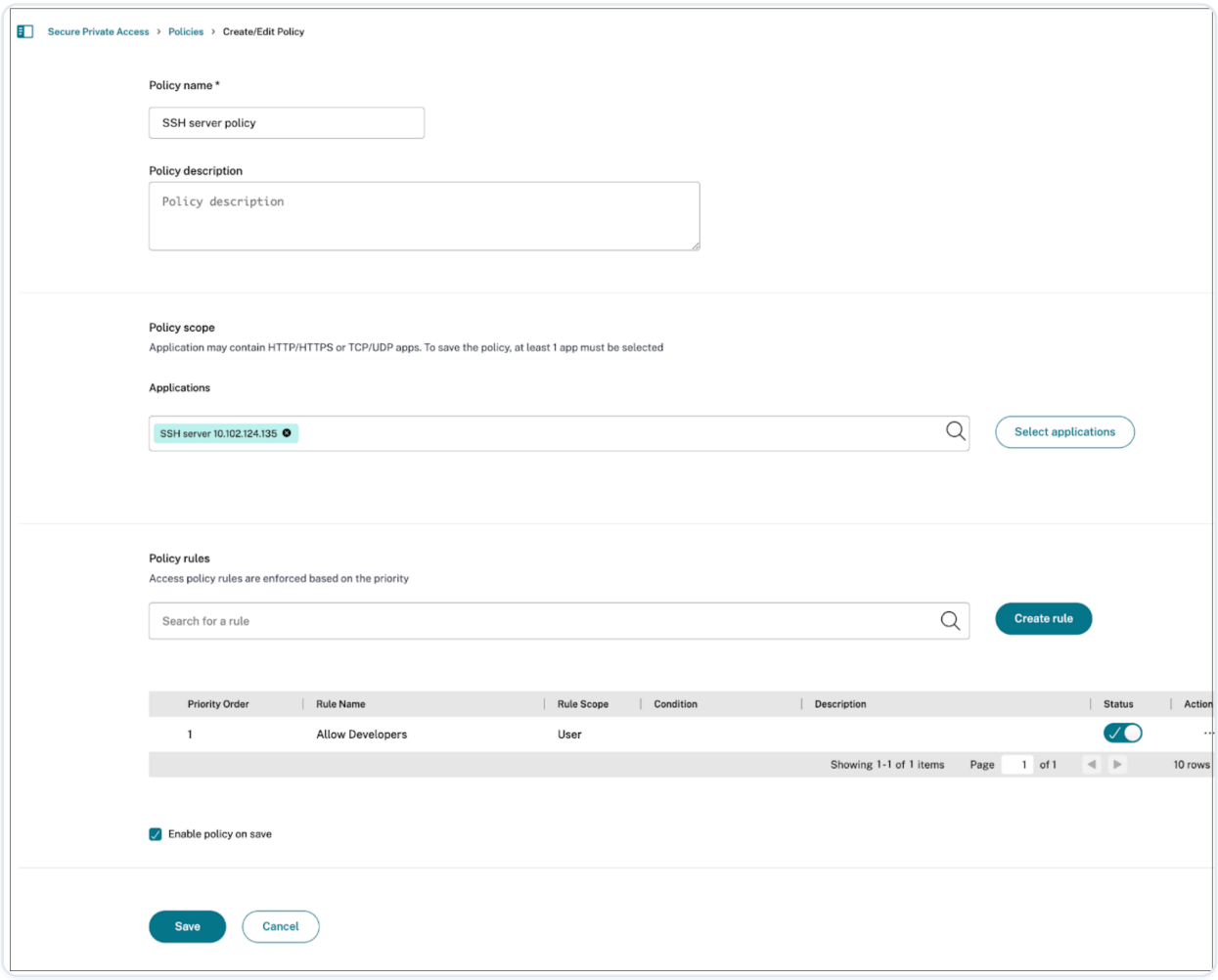
Configuration:

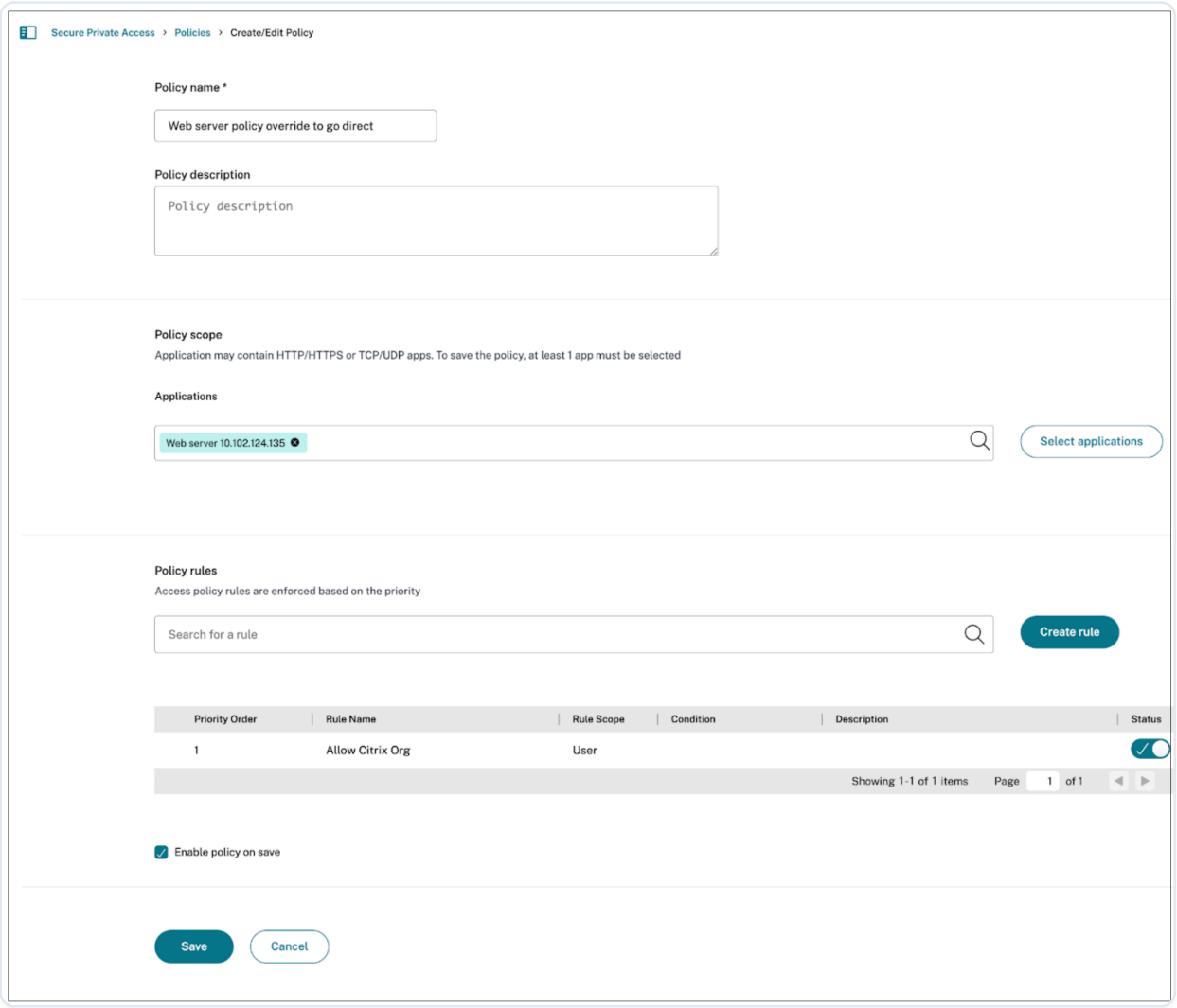
1. Create separate applications for each requirement. For details, see Support for TCP/UDP apps.
    - Create an application for SSH access (destination:10.102.124.135, port 22)
    - Create another application for Web access (destination :10.102.124.135, port 80,443)





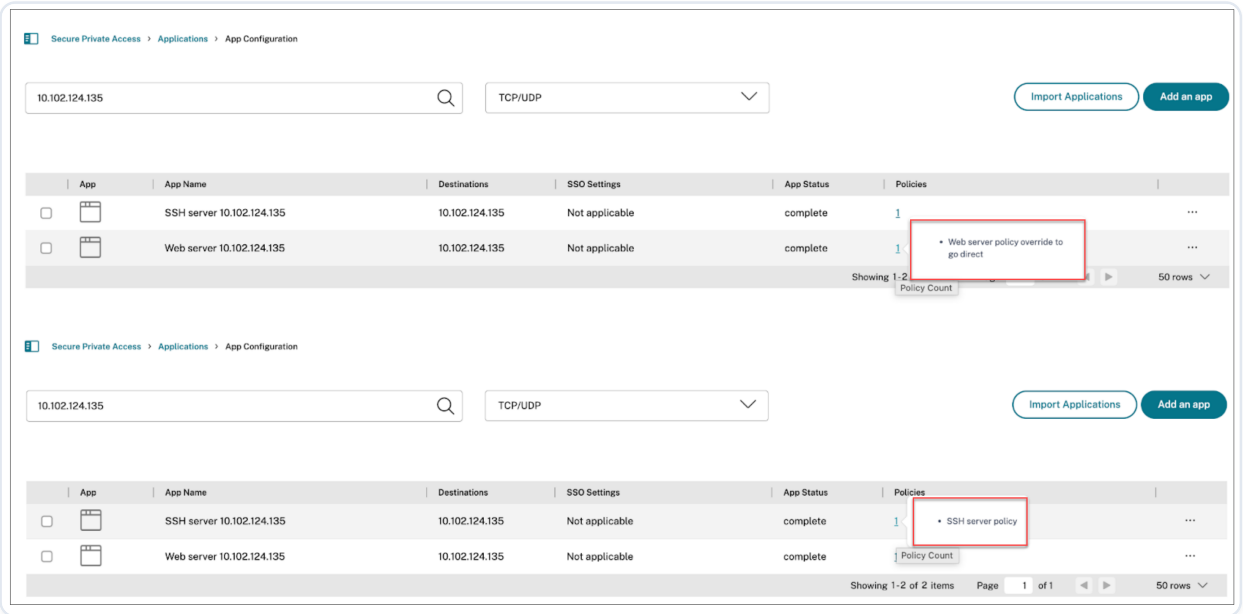
2. Configure the other details for each application as required.
3. Create separate access policies.
    - Define individual policies for each application.
    - Use routing exceptions to specify the desired routing behavior for each configured application.


Secure Private Access › Policies › Create/Edit Policy
Policy name *
SSH server policy
Policy description
Policy description
Policy scope
Application may contain HTTP/HTTPS or TCP/UDP apps. To save the policy, at least 1 app must be selected
Applications
SSH server 10.102.124.135
Select applications
Policy rules
Access policy rules are enforced based on the priority
Search for a rule
Create rule
Priority Order
Rule Name
Rule Scope
Condition
Description
Status
Action
1
Allow Developers
User
Showing 1-1 of 1 items
Page 1 of 1
10 rows
Enable policy on save
Save
Cancel

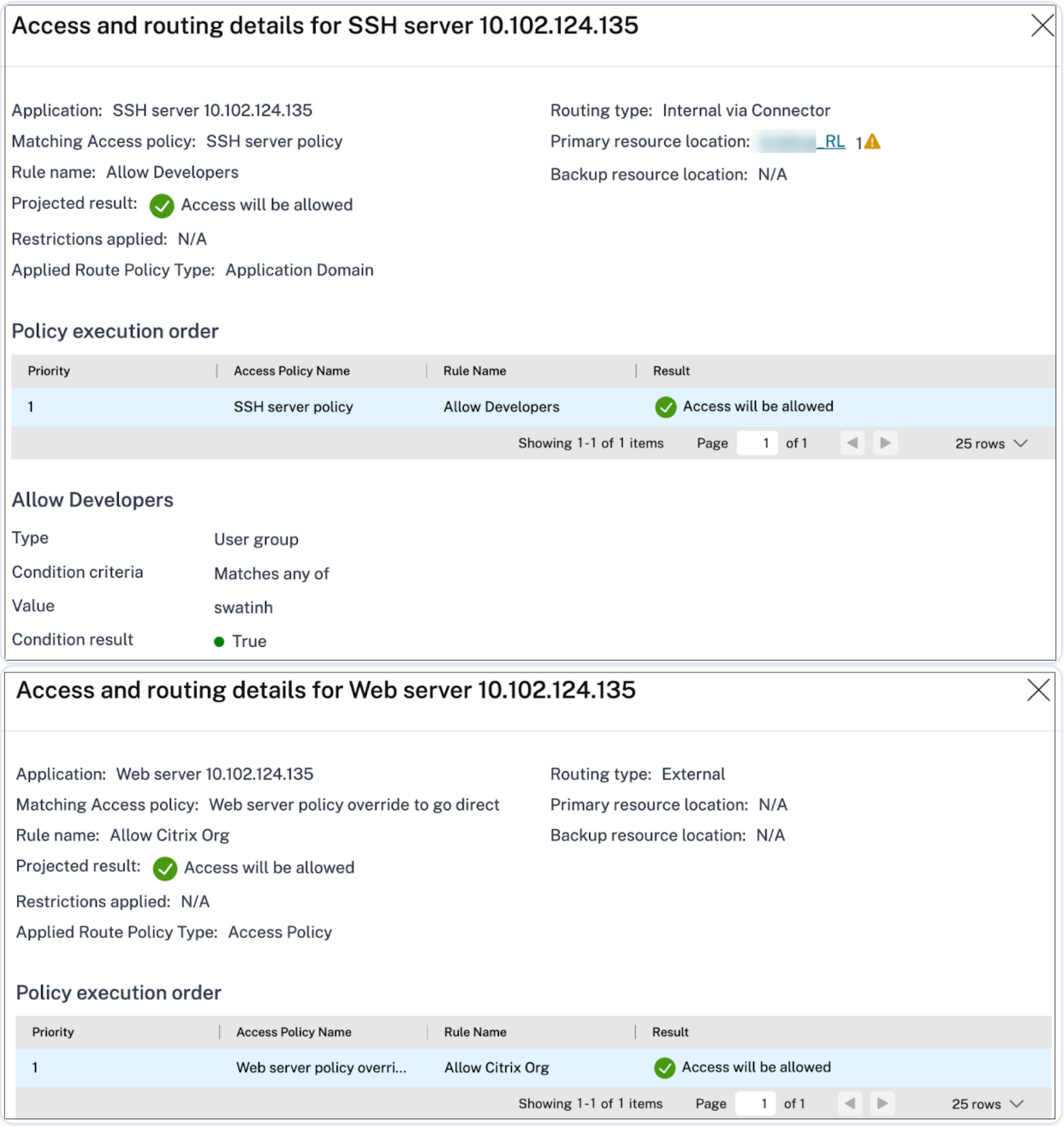


4. Bind policies to applications.

   - Bind the SSH access policy to the SSH application.
   - Bind the Web access policy to the web application.



5. Use the policy modeler to review and validate the applications, policies, and routing confirmations.



Routing options limitations:

- Access policies are evaluated from top-to-bottom, so the first policy that matches the user, context, and application is applied. For hostname-based applications, the route configuration (routing type and Resource Location) defined in the applied policy is used to resolve the destination.

- If no route exceptions are defined in the access policy, then the route configuration in the application configuration is used. Route tunnel and route direct are mutually exclusive. Hence, for hostname-based destinations, we cannot have its route via tunnel (internally) and via direct (external) for different ports.
- Routing internally (via connector or NetScaler Gateway) and direct (external) are mutually exclusive. As a result, the hostname-based destinations cannot be routed both internally and externally. If the requirement is to route traffic for an application both internally and externally, it is recommended to onboard the application using an IP-based destination.

Example to demonstrate port-based routing

The following figure demonstrates how policy priority and routing exceptions affect the end-user experience:

able	Configured applications and policies for a user		Expected behaviour for the user
	App name: LDAP_app Destination URL: example.com Port Number:389 Selected routing in application: 1. Routing Type:Internal via connector 2. Primary resource location: ResourceLocation1 Access policy: LDAP_policy for LDAP_app Routing Exception : None Higher priority	App name: SSH_app Destination URL: example.com Port Number: 22 Pre-selected routing in application (from LDAP_app destination URL) • Routing Type:Internal via connector • Primary resource location: ResourceLocation1 Access policy: SSH_policy for SSH_app Routing Exception: External Lower priority	Both example.com:389 and example.com:22 are resolved via Secure Private Access(Resourcelocation1). example.com:389 is launched successfully. example.com:22 fails to launch as it is supposed to go via External. **Note:** It is not recommended to configure the same domain to go via External and Internal. This limitation is only for FQDN.
	App name: LDAP_app Destination URL: example.com Port Number:389 Selected routing in application: • Routing Type:Internal via connector • Primary resource location: ResourceLocation1 Access Policy :LDAP_policy for LDAP_app Routing Exception : None Lower priority	App name: SSH_app Destination URL: example.com Port Number:22 Pre-selected routing in application (from LDAP_app destination URL) • Routing Type:Internal via connector • Primary resource location: ResourceLocation1 Access Policy:SSH_policy for SSH_app Routing Exception: External Higher priority	Both example.com:389, example.com:22 are launched via External.
	App name: LDAP_app Destination URL: 10.0.0.1 Port Number: 389 Selected routing in application: • Routing Type:Internal via connector • Primary resource Location: ResourceLocation1 Access policy: LDAP_policy for LDAP_app Routing Exception: None Higher priority	App name: SSH_app Destination URL: 10.0.0.1 Port Number: 22 Pre-selected routing in application (from LDAP_app destination URL) • Routing Type:Internal via connector • Primary resource Location: ResourceLocation1 Access policy: SSH_policy for SSH_app Routing Exception: External Lower priority	10.0.0.1:389 is launched via Secure Private Access (ResourceLocation1). 10.0.0.1:22 is launched via External.
	App name: LDAP_app Destination URL: 10.0.0.1 Port Number: 389 Selected routing in application: • Routing Type:Internal via connector • Primary resource Location: ResourceLocation1 Access policy : LDAP_policy for LDAP_app Routing Exception: None Lower priority	App name: SSH_app Destination URL: 10.0.0.1 Port Number: 22 Pre-selected routing in application (from LDAP_app destination URL) • Routing Type:Internal via connector • Primary resource Location: ResourceLocation1 Access policy: SSH_policy for SSH_app Routing Exception: External Higher priority	10.0.0.1:389 is launched via Secure Private Access (ResourceLocation1). 10.0.0.1:22 is launched via External.

Manage certificates in the Secure Private Access console

The Secure Private Access certificate store provides a centralized location for admins to efficiently manage both Certificate Authority (CA) and Secure Sockets Layer (SSL) certificates. This

dedicated store simplifies certificate management by enabling administrators to seamlessly add new certificates, modify existing ones, and remove those that are no longer required.

Previously, Secure Private Access certificates were stored in the NetScaler® Console's certificate store. With the dedicated Secure Private Access certificate store, certificates managed within the NetScaler Console are no longer automatically synchronized or accessible for use within Secure Private Access. Administrators must directly upload the necessary certificates into the Secure Private Access console.

The certificates used in Secure Private Access are organized into two tabs within the Certificates page.

- **Server** - Contains the list of certificates, primarily SSL server certificates related to the direct access (agentless access) operations.
- **Machine authentication** - Contains the list of certificates related to managing machine tunnels initiated from the Citrix Secure Access™ client. These certificates are used when an administrator logs into the Citrix Secure Access client.

  Machine authentication certificates are essential for the Always On feature, utilizing Device Certificates issued by trusted Certificate Authorities (CAs). These CA certificates are securely uploaded and managed within the Machine authentication tab (**Settings > Certificate Store)**, ensuring seamless and robust device authentication for the Always On functionality.

Manage machine authentication certificates

The following sections provide more information about managing machine authentication certificates.

Add a certificate

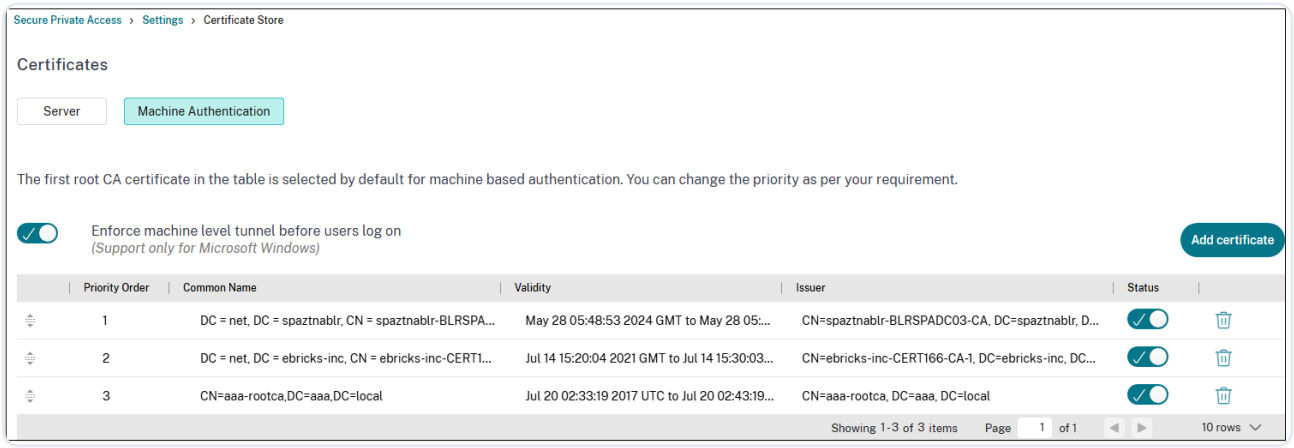
Steps to add a machine authentication certificate.

1. Navigate to **Settings > Certificate Store**.

> **Note:**
>
> We recommend that you use the **Machine Based Authentication** option found under **Settings > Certificate Store** instead of **Settings > Machine Based Authentication**. The option **Settings > Machine Based Authentication** is scheduled for removal in the upcoming service release.

2. Click the **Machine authentication** tab and then click **Add certificate**.
3. In **Name**, enter a name for the certificate.
4. In **Certificate file**, browse to your local drive and upload the certificate file.
    - Certificates for both root CA and intermediate CA are supported.
    - The certificates to be uploaded must be in the PEM format and include the whole chain. The certificate must be generated starting from the intermediate certificate all the way to the root CA.
5. Click **Save**.

The certificate is added to the list of available certificates in the **Machine authentication** tab.



Disable a certificate

You can disable the certificate that is no longer used by sliding the toggle switch OFF in the **Status** column.

Delete a certificate

1. Click the delete icon to delete a certificate.

Set priority for the certificate

If multiple certificates are used for the same machine, you can change the priority of the certificates by using the up-down drag icon in the **Priority Order** column.

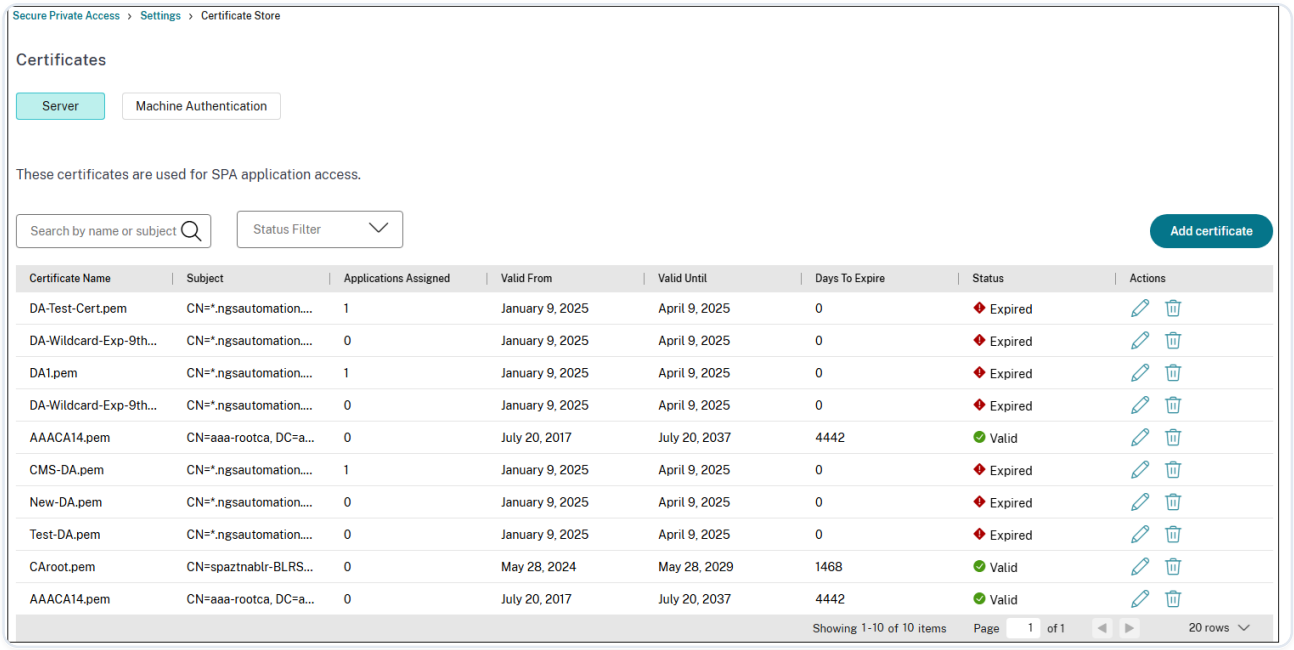
Manage SSL certificates

The following sections provide more information about managing SSL certificates.

Add a certificate

Steps to add an SSL certificate.

1. Navigate to **Settings > Certificate Store**.
2. Click the **Server** tab.
3. Enter a name for the certificate.
4. In **Certificate file**, browse to your local drive and upload the certificate file.
    - Certificates for both root CA and intermediate CA are supported.
    - The certificates to be uploaded must be in the PEM format and include the whole chain. The certificate must be generated starting from the intermediate certificate all the way to the root CA.
5. **Password** (Optional) - Applicable for PFX certificates. If you have an encrypted RSA private key, type the RSA passphrase that was used to encrypt the private key.
6. Click **Save**.

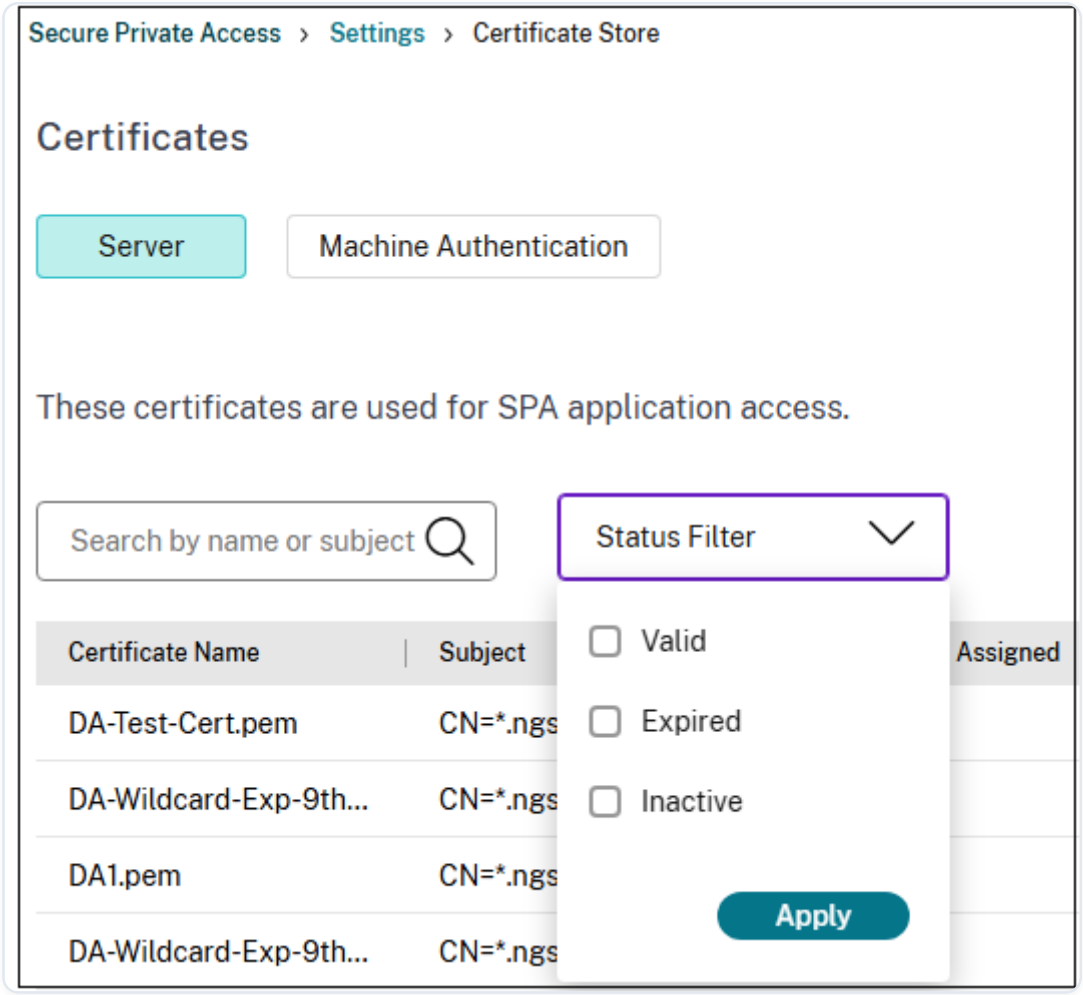


Note:

- The certificate is added to the list of available certificates under the **Server** tab.
- The **Applications assigned** column displays the number of applications for which a certificate is assigned.

Search for a certificate

You can search for an SSL certificate by the certificate name or the subject. You can also search for certificates based on the status of the certificate.



Modify a certificate

Steps to modify an SSL certificate.

1. Click the edit icon next to the certificate.
2. In **Certificate file**, browse to your local drive and upload the modified certificate file.

   Ensure that the updated certificate is for the same domain or the wildcard domain. Otherwise, the upload fails.
3. Click **Save**.

Delete a certificate

Click the delete icon to delete a certificate.

External notification

When a certificate within a customer's account is nearing its expiration date, within the 30-day window leading up to its expiry, an email notification is automatically sent to the specific customer administrators.

Citrix Secure Access™ client

With Citrix Secure Private Access, you can now access all private apps including TCP/UDP and HTTPS apps either using a native browser or a native client application via the Citrix Secure Access client running on your machine. You can now eliminate the dependency on a traditional VPN solution to provide access to all private apps for remote users.

Citrix Secure Access client for Windows

For details on installing the Citrix Secure Access client for Windows, see Install Citrix Secure Access client for Windows.

For more information about the Citrix Secure Access client for Windows, see Citrix Secure Access for Windows.

Citrix Secure Access client for macOS

For details on installing the Citrix Secure Access client for macOS, see Install the Citrix Secure Access client for macOS.

For more information about the Citrix Secure Access client for macOS, see Citrix Secure Access for macOS.

Citrix Secure Access client for iOS

For details on installing up the Citrix Secure Access client for iOS, see Setup Citrix Secure Access for iOS.

For more information about the Citrix Secure Access client for iOS, see Citrix Secure Access for iOS.

Citrix Secure Access client for Android

For details on setting up the Citrix Secure Access client for Android, see Setup Citrix Secure Access for Android.

For more information about the Citrix Secure Access client for Android, see Citrix Secure Access for Android.

Citrix Secure Access client for Linux

For details on installing the Citrix Secure Access client for Linux, see Install Citrix Secure Access client and Citrix EPA client.

For more information about the Citrix Secure Access client for Linux, see Citrix Secure Access for Linux.

Best practices for Web and SaaS application configurations

Application access for published and unpublished apps depends on the applications and access policies configured within the Secure Private Access service.

Application access within Secure Private Access for published and unpublished Apps

- **Access to published web applications and related domains:**
  - When an end user accesses an FQDN that is associated with a published web app, the access is allowed only if an access policy is configured explicitly with the action **Allow** or **Allow with Restrictions** for the user.

    > **Note:**
    >
    > It is recommended not to have multiple applications share the same application URL domain or related domains for an exact match. If multiple apps share the same application URL domain or related domains, the access is provided based on exact FQDN match and policy prioritization. For details, see Access policy matching and prioritization.

  - If no access policy matches with the published app or if an app isn't associated with any access policy, then access to the app is denied, by default. For details on access policies, see Adaptive access policy configuration and management.
- **Access to unpublished internal web applications and external internet URLs:**

To enable zero-trust, Secure Private Access denies access to internal web applications or intranet URLs that are not associated with an application and do not have an access policy configured for the application. To allow access for specific users, ensure that you have an access policy configured for your intranet web applications.

For any URL that is not configured as an application within Secure Private Access, the traffic flows directly to the internet.

- In such cases, access to intranet web application URL domains are routed directly and thus access is denied (unless the user is already inside the intranet).
- For unpublished internet URLs, access is based on the rules configured for unsanctioned apps, if enabled. By default, this access is allowed within Secure Private Access.

Access policy matching and prioritization

Secure Private Access does the following while matching an application for access:

1. Match the domain being accessed to the application URL's domain or related domains for an exact match.
2. If a Secure Private Access application configured with an exact FQDN match is found, then Secure Private Access evaluates all policies configured for that application.
   - Policies are evaluated in a priority order until the user context matches. The action (allow/deny) is applied as per the first policy that matches in the priority order.
   - If no policy matches, then access is denied by default.
3. If an exact FQDN match is not found, then Secure Private Access matches the domain based on the longest match (such as a wildcard match) to find applications and corresponding policies.

   Example 1: Consider the following app and policy configurations:

APPLICATION	APPLICATION URL	RELATED DOMAIN
Intranet	`https://app.intranet.local`	*.cdn.com
Wiki	`https://wiki.intranet.local`	*.intranet.local

POLICY NAME	PRIORITY	USER AND ASSOCIATED APPS
PolicyA	High	Eng-User5 (Intranet)
PolicyB	Low	HR-User4 (Wiki)

If `HR-User4` accesses `app.intranet.local`, then the following happens:

a. Secure Private Access searches all policies for an exact match for the domain being accessed, `app.intranet.local` in this case.

b. Secure Private Access finds `PolicyA`, and checks if the conditions match.

c. As the conditions do not match, Secure Private Access stops here and does not continue to check the wildcard matches, even though `PolicyB` would have matched (since `app.intranet.local` does match on the Wiki app's related domain of `*.intranet.local`) and given access.

d. Hence `HR-User4` is denied access to the Wiki app.

Example 2: Consider the following apps and policy configuration where same domain is used in multiple applications:

APPLICATION	APPLICATION URL	RELATED DOMAIN
App1	xyz.com	app.intranet.local
App2	app.intranet.local	-

POLICY NAME	PRIORITY	USER AND ASSOCIATED APPS
PolicyA	High	Eng-User5 (App1)
PolicyB	Low	HR-User7 (App2)

When user `Eng-User5` accesses `app.intranet.local`, both App1 and App2 will be a match based on the exact FQDN match and hence `Eng-User5` user gets access through `PolicyA`.

However, if App1 had `*.intranet.local` as a related domain instead, then the access for `Eng-User5` would have been denied since `app.intranet.local` would have exact-matched `PolicyB`, for which the user, `Eng-User5`, does not have access.

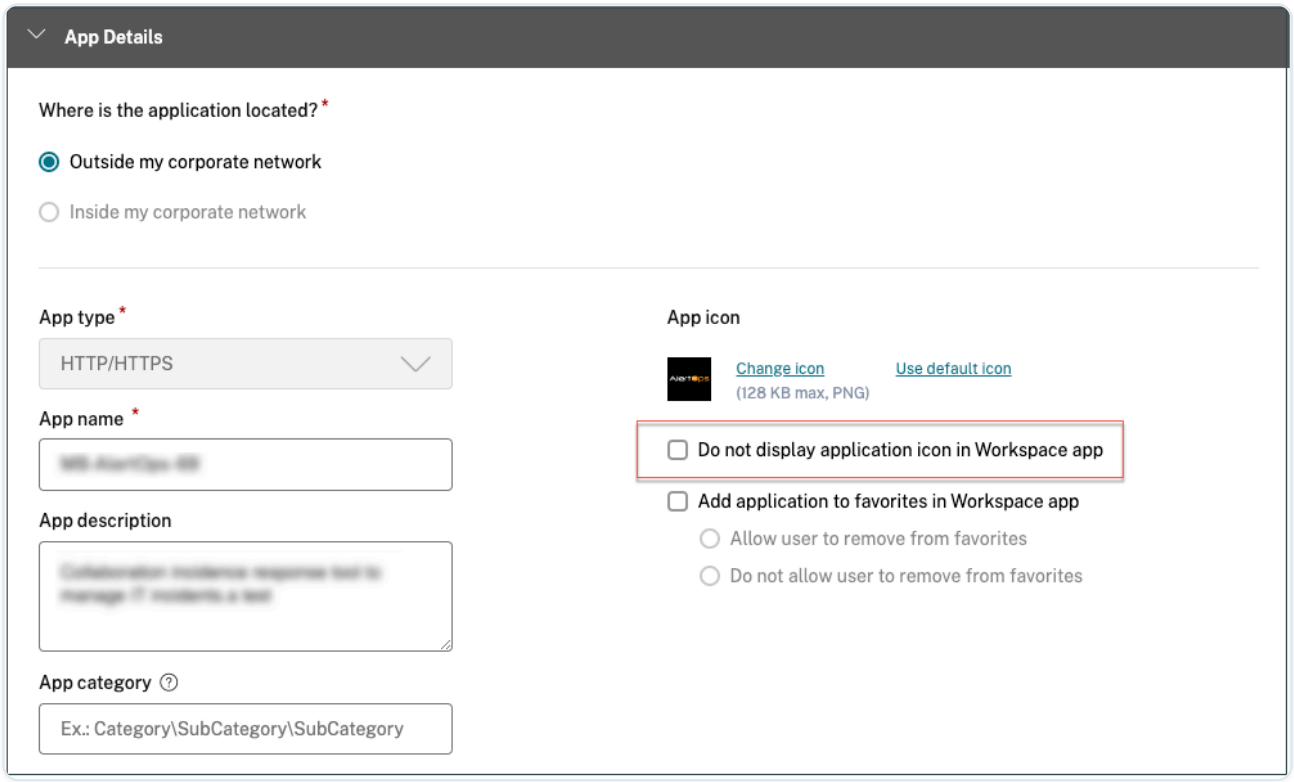
App configuration best practices

The following sections provide more information about the application configuration best practices.

IdP domains must have an application of their own

Instead of adding IdP domains as related domains in your intranet app configurations, we recommend the following:

- Create separate applications for all IdP domains.
- Create a policy to enable access to all users who need access to the IdP authentication page, and keep the policy as the highest priority.
- Hide this app (by selecting the **Do not display application icon to users** option) from the app configuration so that it does not enumerate in the store. For information, see Configure application details.



Note:

> This app configuration only enables access to the IdP authentication page. Further access to individual applications still depends on the individual app configurations and their respective access policies.

> **Example configuration:**

1. Configure all common FQDNs into their own apps, grouping them together where applicable.

   For example, if you have a few apps that use Azure AD as an IdP and you must configure `login.microsoftonline.com` and other related domains (`*.msauth.net`), then do the following:

   - Create a single common application with `https://login.microsoftonline.com` as the application URL and `*.login.microsoftonline.com` and `*.msauth.net` as the related domains.

2. Select the **Do not display application icon to users** option while configuring the app. For details, see Configure application details.
3. Create an access policy for the common application and enable access to all users. For details, see Configure an access policy.
4. Assign highest priority to the access policy. For details, see Priority order.
5. Verify the diagnostic logs to confirm that the FQDN matches the app and that the policy is enforced as expected.

Same related domains must not be a part of multiple applications

Related domain must be unique to an app. Conflicting configurations might result in app access issues. If multiple apps are configured with the same FQDN or some variation of the wildcard FQDN, then you might encounter the following issues:

- The websites stop loading or might display a blank page.
- The **Blocked Access** page might appear when you access a URL.
- The login page might not load.

Thus we recommend having a unique related domain to be configured within a single app.

Incorrect configuration examples:

- **Example: Duplicate related domains across multiple applications**

Assume you have 2 apps where both need access to Okta (example.okta.com):

APP	APPLICATION URL DOMAIN	RELATED DOMAIN
App1	`https://code.example.net`	example.okta.com
App2	`https://info.example.net`	example.okta.com

POLICY NAME	PRIORITY	USER AND ASSOCIATED APPS
Deny App1 to HR	High	User group `HR` for `App1`
Grant Everyone access to App1	Medium	Enable access to user group Everyone to App1
Grant Everyone access to App2	Low	Enable access to user group Everyone" to App2

Problem with the configuration: Although the intent was to give all users access to App2, the user group HR cannot access App2. The user group HR gets redirected to Okta but is stuck based on the first policy that denied access to App1 (which also has the same related domain `example.okta.com` as App2).

This scenario is common for Identity Providers such as Okta, but it can also happen with other tightly integrated apps with common related domains. For details on policy matching and prioritization, see Access policy matching and prioritization.

Recommendation for the above configuration:

a. Remove example.okta.com as a related domain from all apps.
b. Create a new app just for Okta (with the application URL of `https://example.okta.com` and a related domain of `*.okta.com`).
c. Hide this app from the store.
d. Assign the highest priority for the policy to remove any conflict.

Best Practice:

- An app's related domains must not overlap with another app's related domains.
- If this occurs, a new published app must be created to cover the shared related domain and then access must be set accordingly.
- Admins must evaluate if this shared related domain must appear as an actual app in the store.
- If the app must not appear in the store, then while publishing the app, select the **Do not display application icon to users** option to hide it from the store.

Resolve conflicts resulting from same related domains

In scenarios where an app's related domains overlap with another app's domains, admins have the flexibility to route these applications either externally or internally via the Connector Appliances, based on specific requirements. The routing table within the Secure Private Access console (**Settings > Application Domains**) provides a comprehensive list of all configured domains for all applications. This table displays key information about each domain, including the routing type. Admins can easily modify the routing type by clicking the edit icon next to the corresponding domain entry.

The main route table displays the following information for any domain:

- **FQDN/IP:** FQDN or the IP address for which the type of traffic routing is desired to be configured.
- **Type:** App type. **Internal**, **Internal – Bypass Proxy**, or **External** as selected when adding the app.
  - **Internal** - The apps are external but the traffic must flow through the Connector Appliance to the outside network.
  - **Internal – Bypass Proxy** - The domain traffic is routed through Citrix Cloud Connector™, bypassing the customer’s web proxy configured on the Connector Appliance.
  - **External** – The traffic flows directly to the internet.

> **Important:**
>
> If there are conflicts, then an alert icon is displayed for the respective row in the table. To resolve the conflict, admins should click the triangular icon associated with that entry and change the app type.

- **Resource location:** Resource location for routing of type Internal. If a resource location is not allocated, a triangular icon appears in the Resource location column for the respective app. When you hover on the icon, the following message is displayed.

  Missing resource location. Ensure that a resource location is associated with this FQDN.

- **Status:** The toggle switch in the Status column can be used to disable the route for a route entry without deleting the app. When the toggle switch is turned OFF, the route entry does not take effect. Also, if FQDNs of exact match exist, admins can select the route to be enabled or disabled.
- **Comments:** Displays comments, if any.
- **Actions:** The edit icon is used to add a resource location or change the type of route entry. The delete icon is used to delete the route.

> **Note:**
>
> A mini version of the application domains table is available to make the routing decisions during app configuration. The mini route table available in the App Connectivity section in the Citrix Secure Private Access™ service admin console.

Deep-link URLs

For deep-link URLs, the intranet application URL domain must be added as the related domain:

Example:

Intranet app has URL is configured with `https://example.okta.com/deep-link-app-1` as the main application URL domain and the related domain has the intranet application URL domain i.e `*.issues.example.net`.

In this case, separately create an IdP app with URL `https://example.okta.com` and then related domain as `*.example.okta.com`.

App access end-user experience explained

Citrix Secure Private Access™ apps can be accessed in the following ways:

- **Through the Citrix Secure Access™ client:**

- Access Web/SaaS apps: After logging into the Citrix Secure Access client, end users can access Web/SaaS apps using their native browser such as Chrome.
- Access TCP/UDP apps: After logging into the Citrix Secure Access client, end users can access TCP/UDP applications through a client application (for example Remote Desktop Protocol (RDP)).

- **Agentless access:** Allows users to access enterprise web apps without the need for a client. End users can access enterprise web applications without installing a dedicated client on their devices. End users can simply enter the app URLs in their native browser.

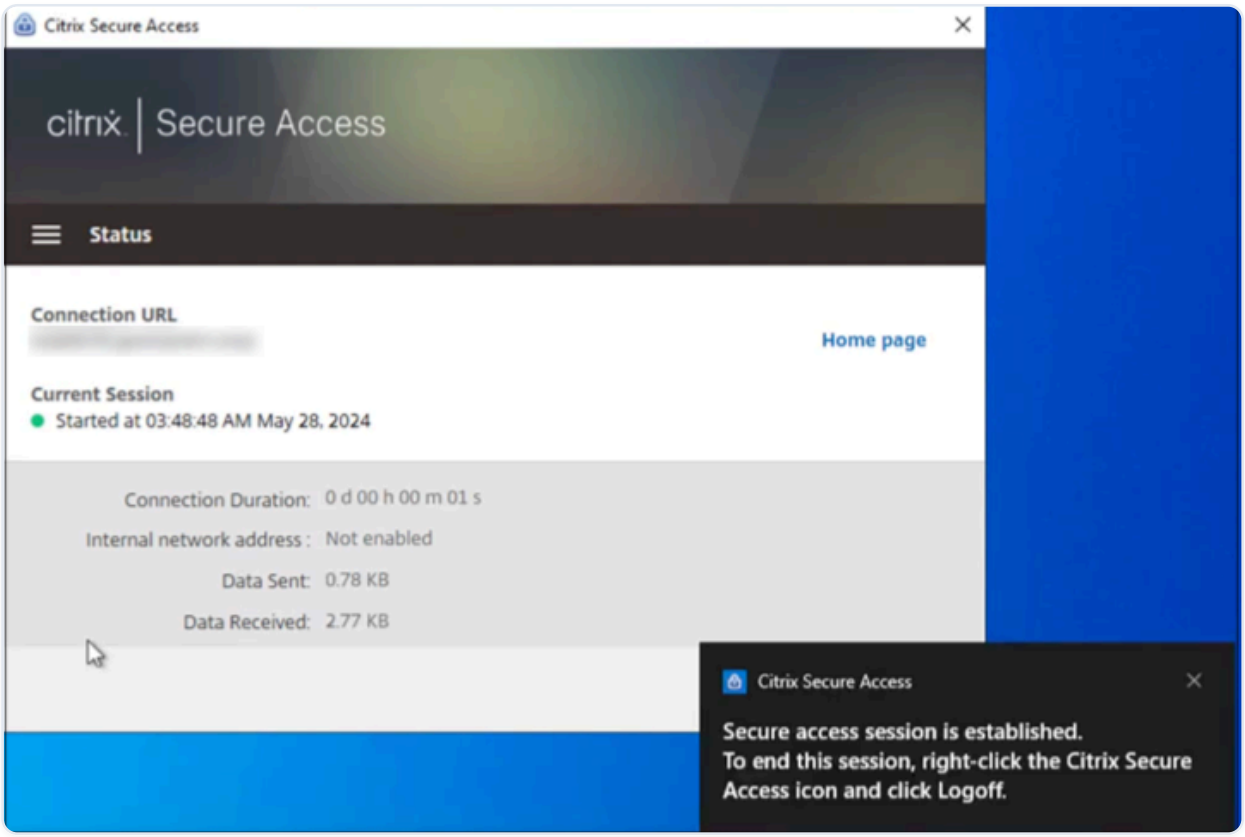
Access a Web app through the Citrix Secure Access client

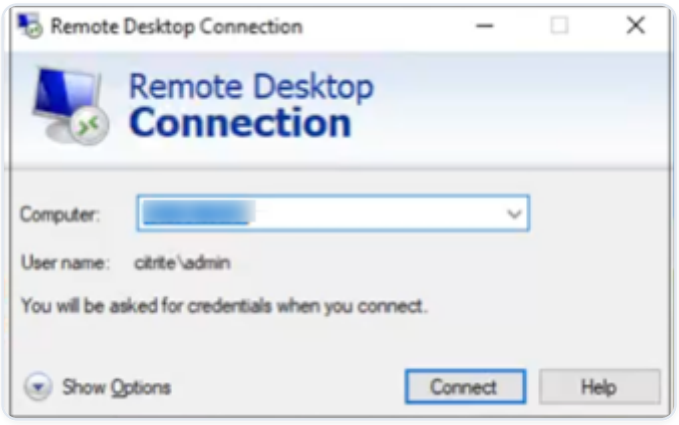
1. Log in to the Citrix Secure Access client.
2. After the secure access session is established, open a native browser (for example Chrome).
3. In the browser, enter the URL of the enterprise web app that you want to access.

Access a TCP/UDP app through the Citrix Secure Access client

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

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





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

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

For more information about the Citrix Secure Access client, see Citrix Secure Access client.

Connector Appliance for Secure Private Access

The Connector Appliance is a Citrix component hosted in your hypervisor. It serves as a channel for communication between Citrix Cloud™ and your resource locations, enabling cloud management without requiring any complex networking or infrastructure configuration. Connector Appliance enables you to manage and focus on the resources that provide value to your users.

All connections are established from the Connector Appliance to the cloud using the standard HTTPS port (443) and the TCP protocol. No incoming connections are accepted. TCP port 443, with the following FQDNs are permitted outbound:

- *.nssvc.net
- *.netscalermgmt.net
- *.citrixworkspacesapi.net
- *.citrixnetworkapi.net
- *.citrix.com
- *.servicebus.windows.net
- *.adm.cloud.com

Configure Secure Private Access with Connector Appliance

1. Install two or more Connector Appliances in your Resource Location.

   For more information about setting up your Connector Appliances, see Connector Appliance for Cloud Services.

2. To configure Secure Private Access to connect to on-premises web apps by using KCD, configure KCD by completing the following steps:

   a. Join your Connector Appliance to an Active Directory domain.

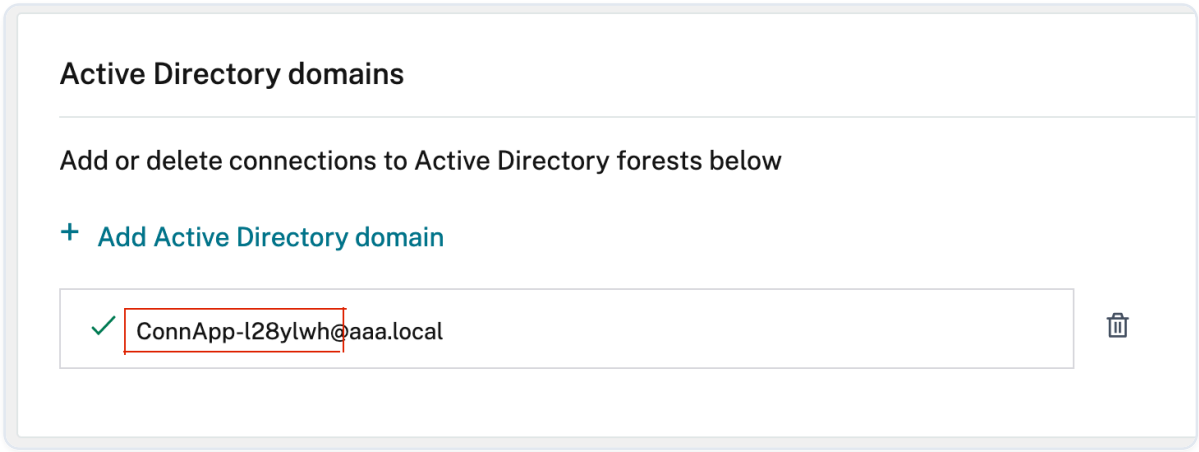
      Joining an Active Directory forest enables you to use Kerberos Constrained Delegation (KCD) when configuring Secure Private Access, but it does not enable identity requests or authentication to use the Connector Appliance.

      - Connect to the Connector Appliance administration webpage in your browser by using the IP address provided in the Connector Appliance console.
      - In the **Active Directory domains** section, click **+ Add Active Directory** domain.

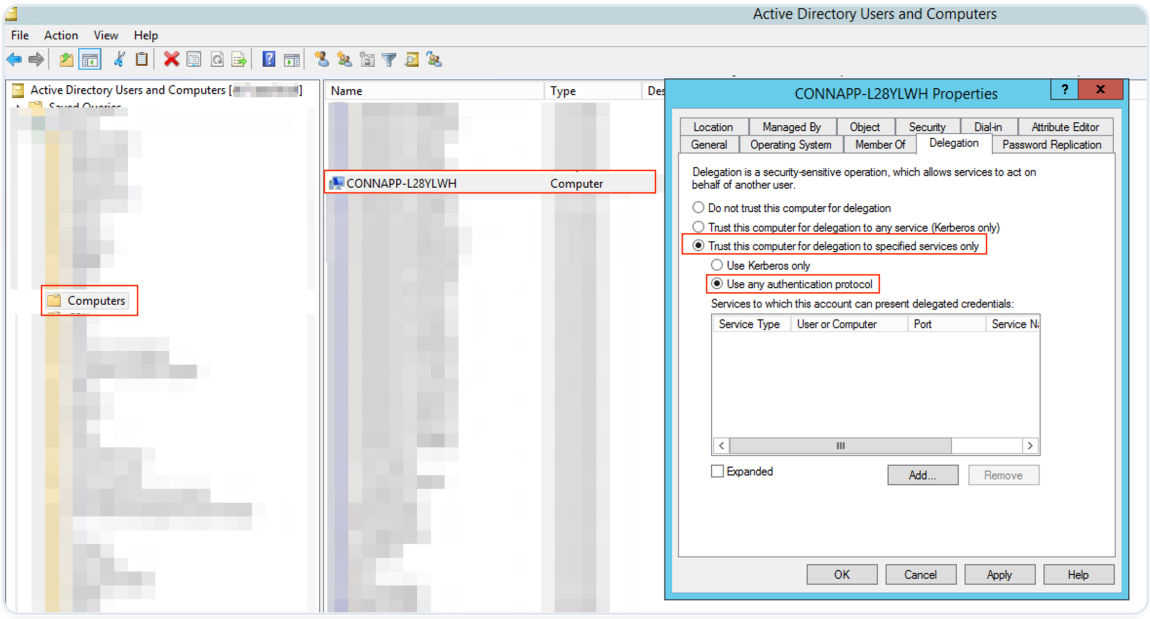
        If you don't have an **Active Directory domains** section in your administration page, contact Citrix® to request enrollment in the preview.
      - Enter the domain name in the **Domain Name** field. Click **Add**.
      - The Connector Appliance checks the domain. If the check is successful, the **Join Active Directory** dialog opens.
      - Enter the user name and password of an Active Directory user that has join permission for this domain.
      - The Connector Appliance suggests a machine name. You can choose to override the suggested name and provide your own machine name that is up to 15 characters in length. Make a note of the machine account name.

        This machine name is created in the Active Directory domain when the Connector Appliance joins it.
      - Click **Join**.

   b. Configure Kerberos Constraint Delegation for web server without a load balancer.

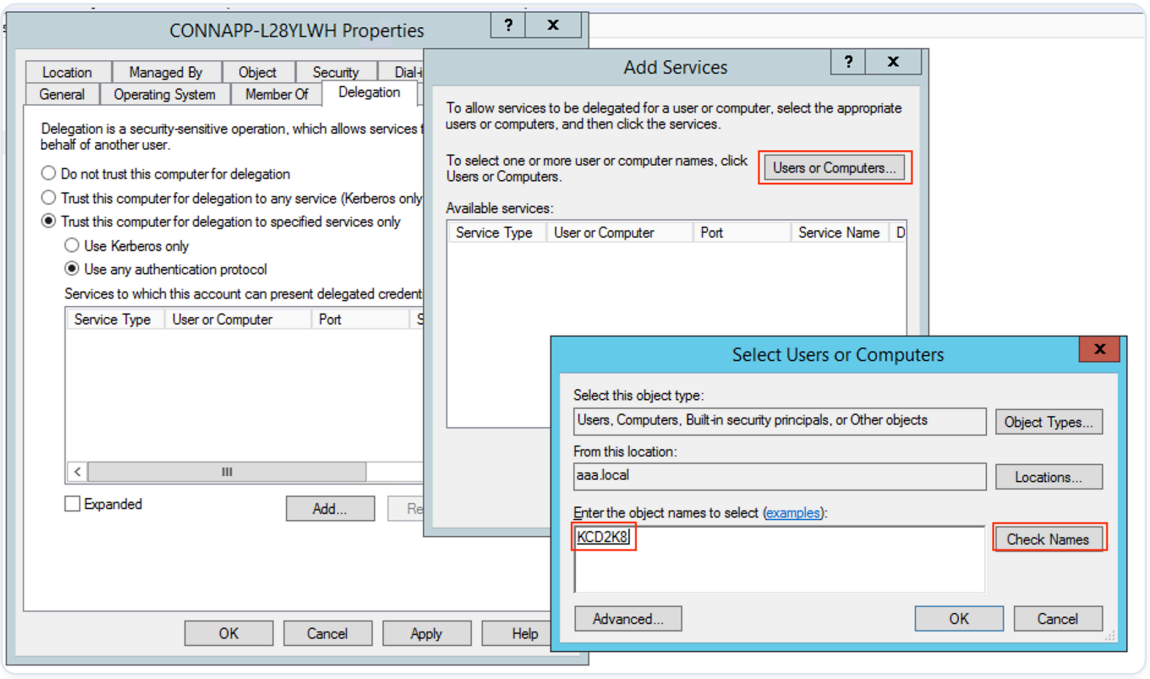


- Identify the connector appliance computer name. You can get this name either from the place where you hosted or simply from the connector UI.
- On your Active Directory controller, look for the connector appliance computer.
- Go to the properties of the Connector Appliance computer account, and navigate to the **Delegation** tab.
- Choose **Trust the computer for delegation to specified services only.** and then select **Use any authentication protocol.**

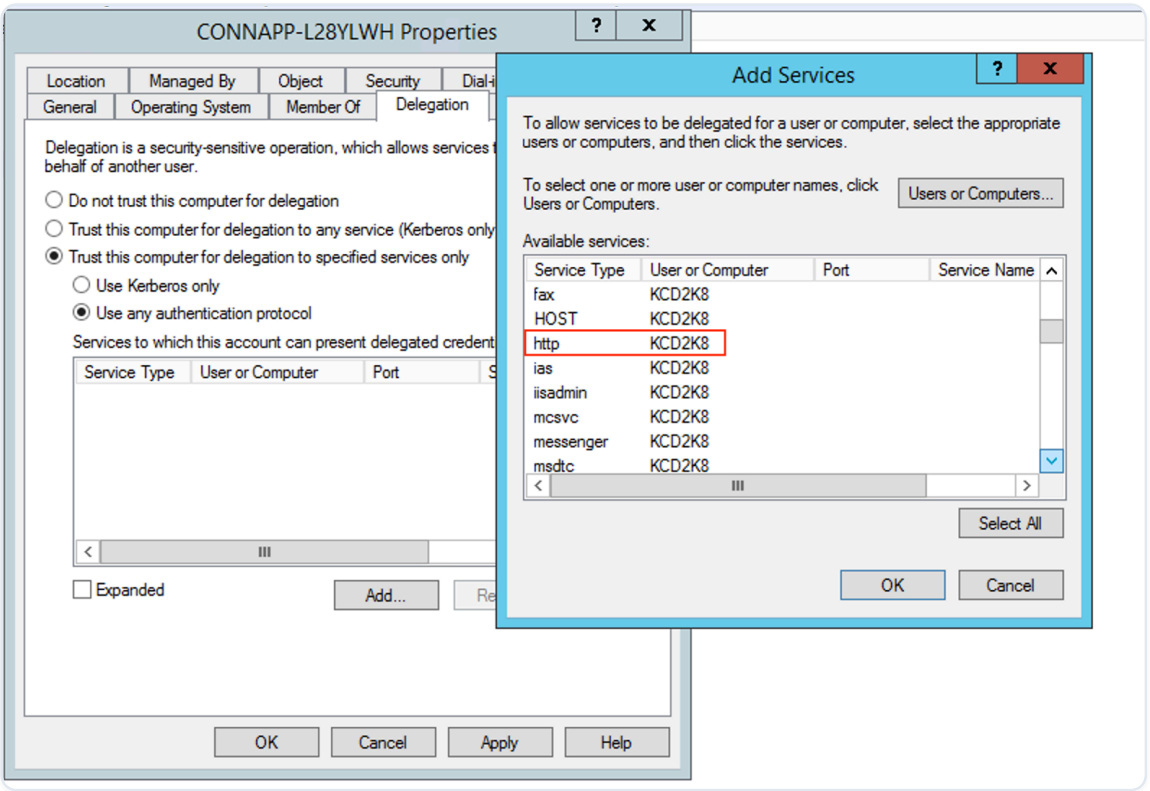


- Click **Add.**
- Click **Users or Computers.**

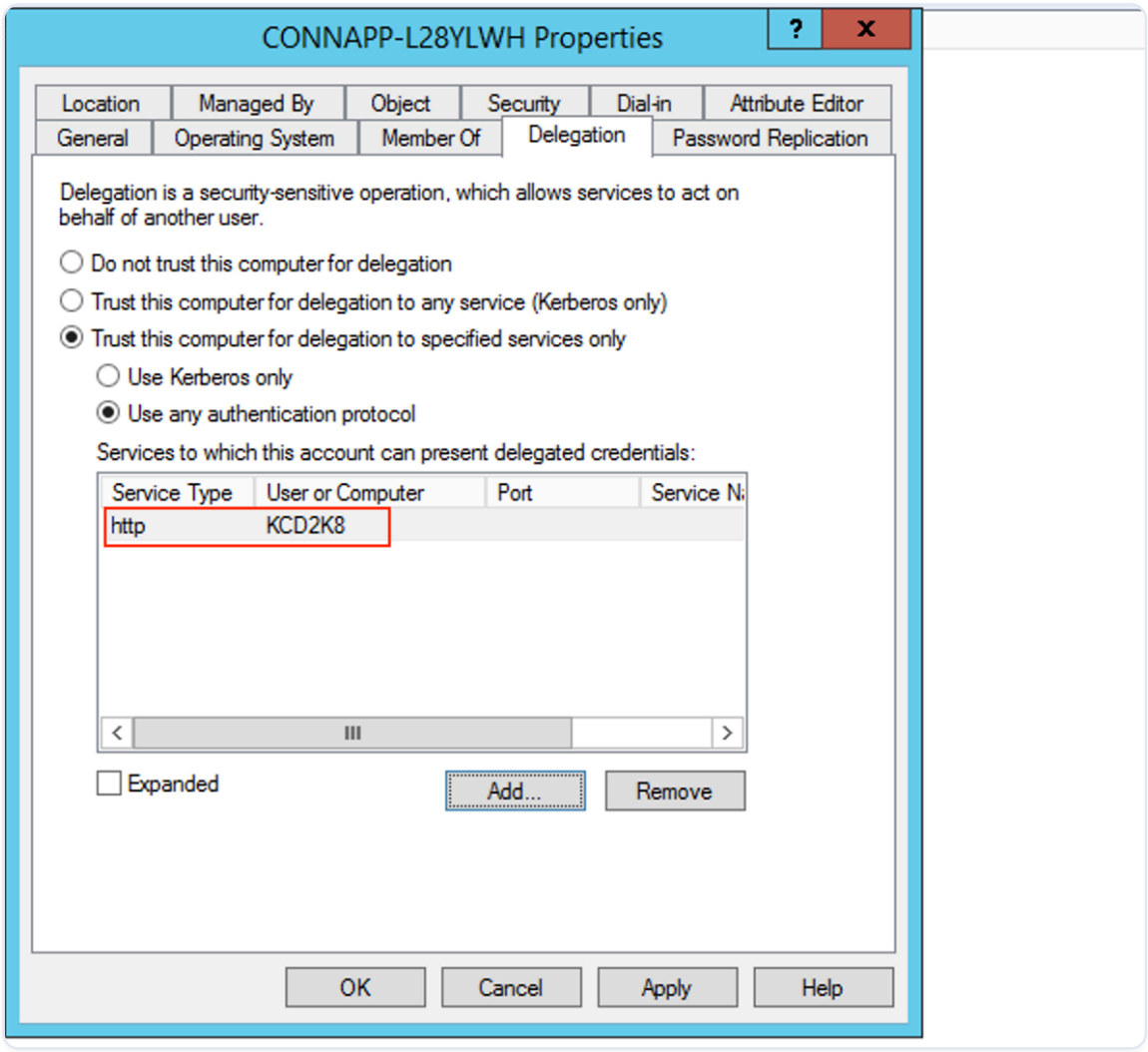
- Enter the target web server computer name, and then click **Check Names.** In the preceding image, **KCD2K8** is the web server.



- click **OK.**
- Select the service type **http.**



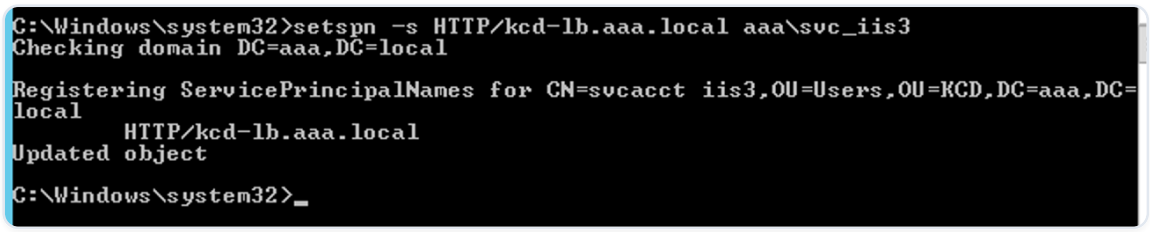
- Click **OK**.
- Click **Apply,** and then click **OK**.



This completes the procedure for adding delegation for a web server.

c. Configure Kerberos Constraint Delegation (KCD) for a web server behind a load balancer.

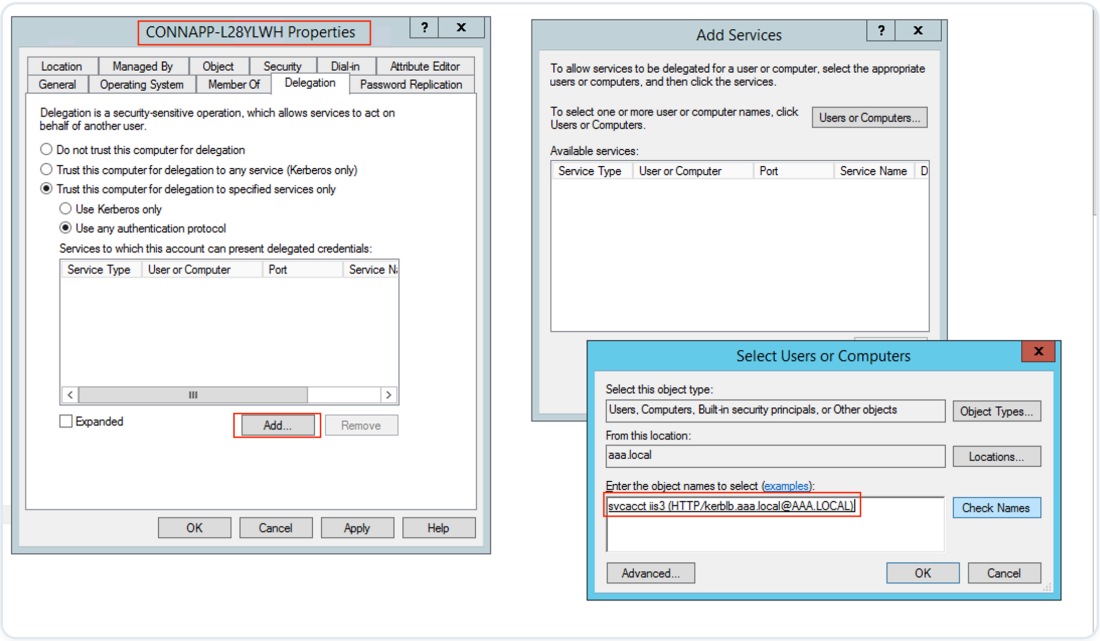
- Add the load balancer SPN to the service account by using the following `setspn` command. `setspn -S HTTP/<web_server_fqdn> <service_account>`



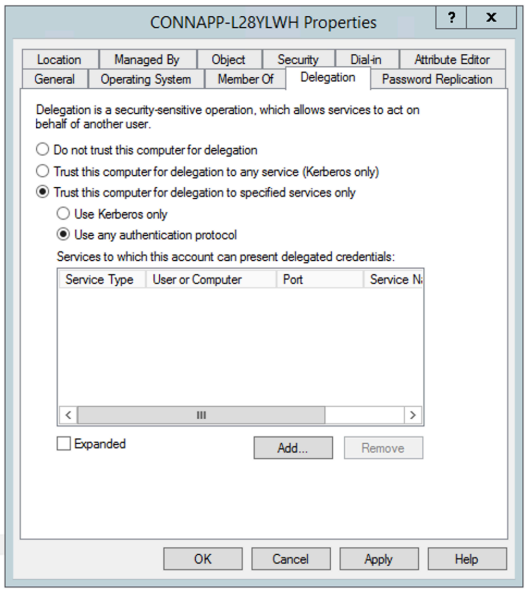
- Confirm the SPNs for the service account using the following command. `setspn -l <service_account>`

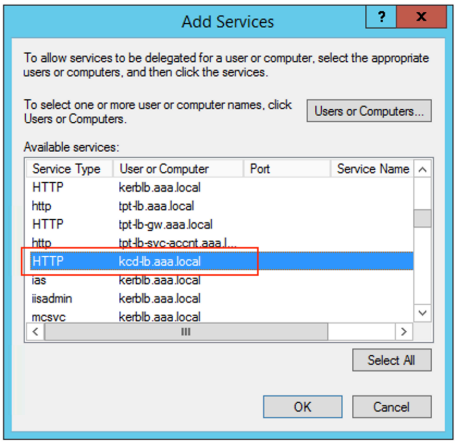


- Create a delegation for the connector appliance computer account.
  - Follow the steps to *Configure Kerberos Constraint Delegation for the webserver* without a load balancer to identify the CA machine and navigate to the Delegation UI.
  - In select **Users and Computers**, select service account (for example, aaa\svc_iis3).



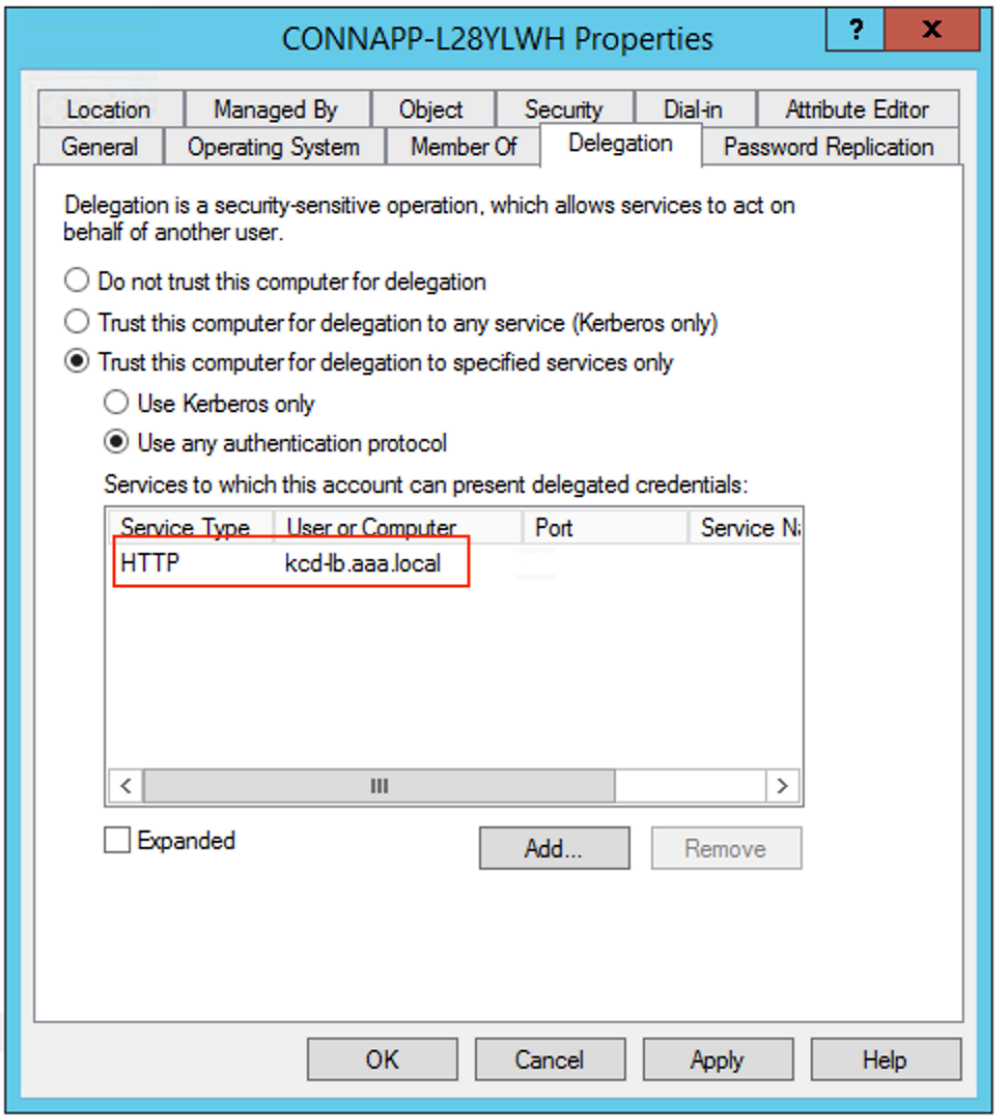
- In the services, select the entry **ServiceType: HTTP** and User or Computer: web server (for example, `kcd-lb.aaa.local`)





- Click **OK**.

- Click **Apply,** and then click **OK**.

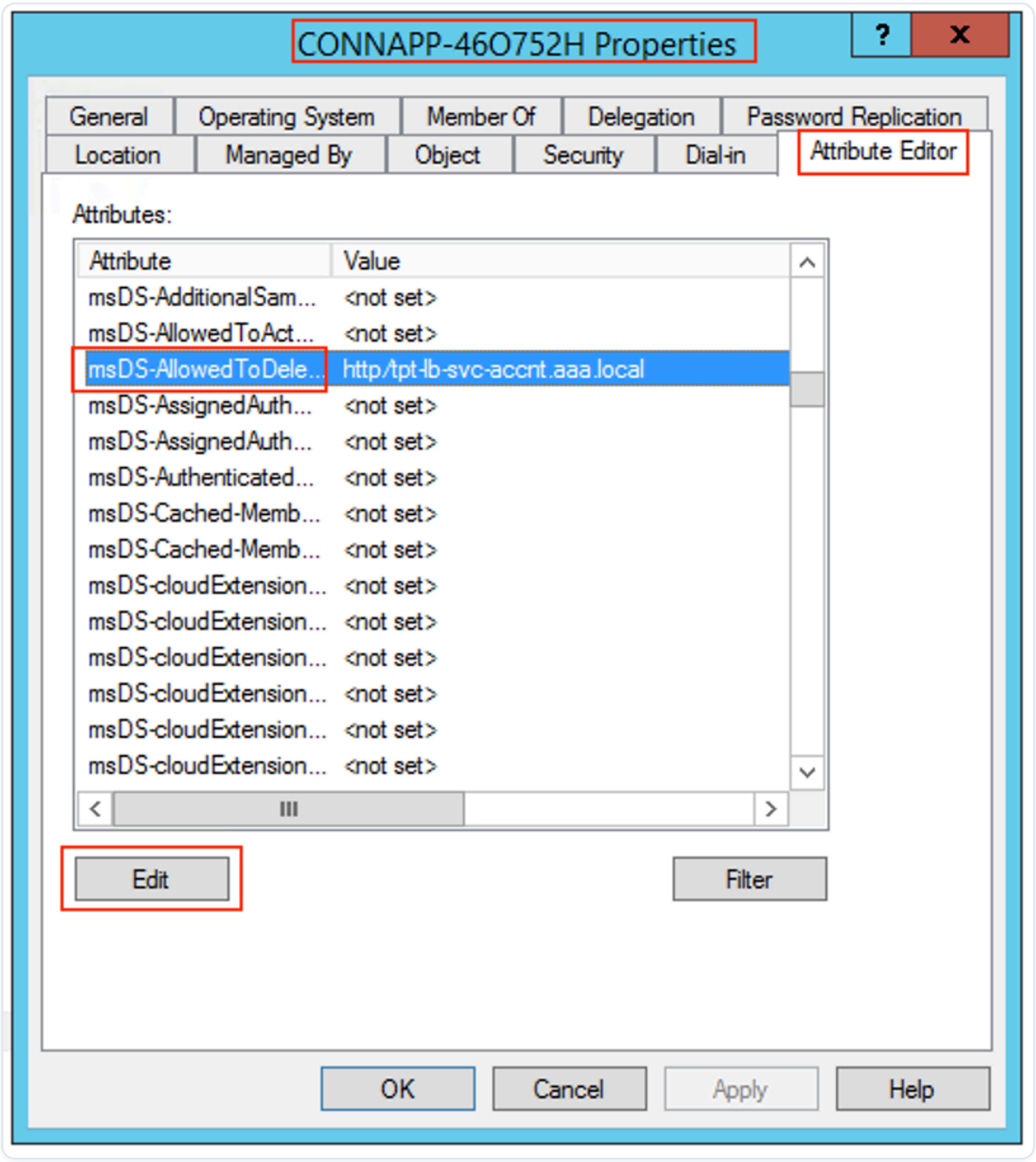


d. Configure Kerberos Constrained Delegation (KCD) for a group managed service account.

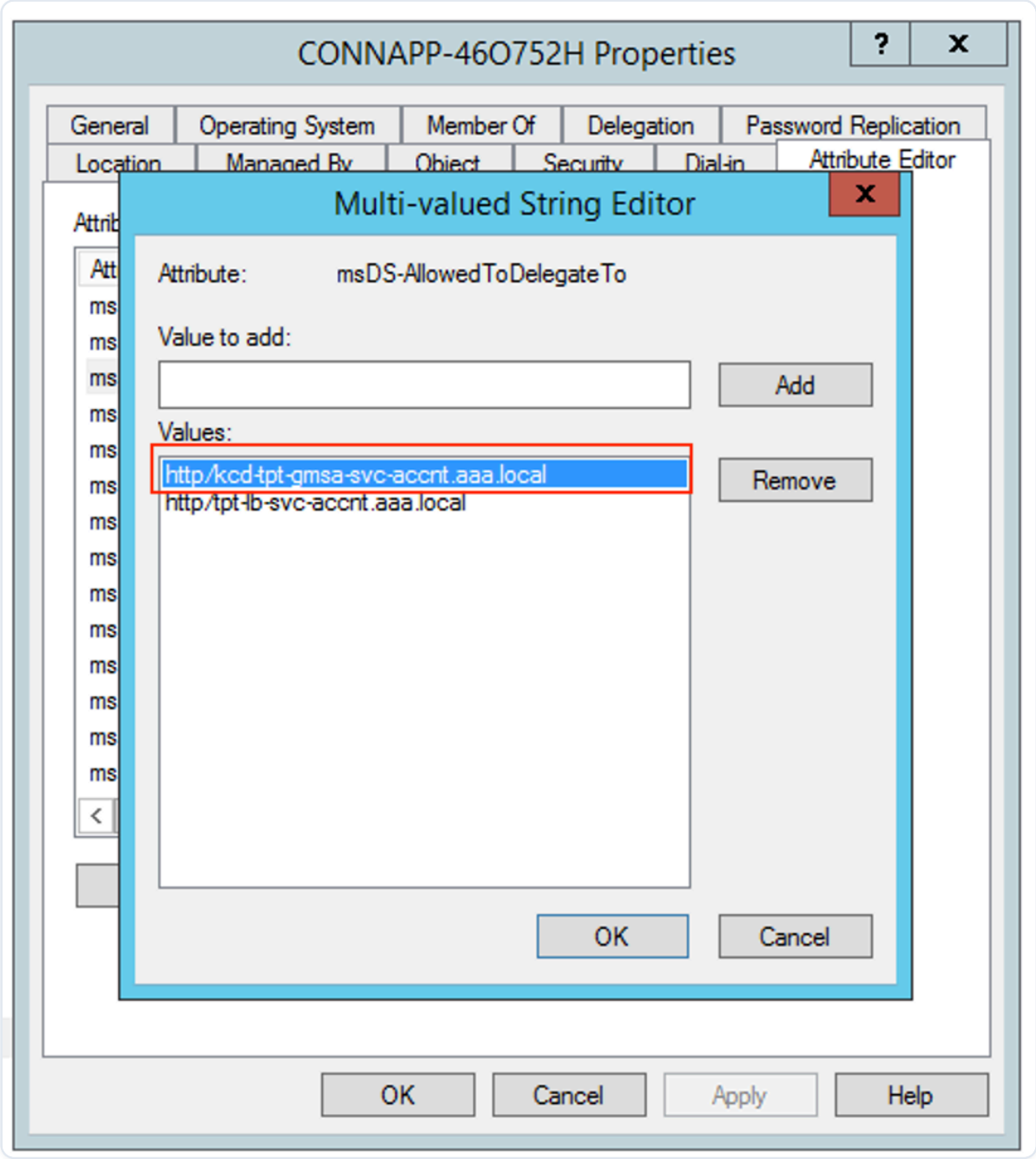
- Add SPN to the group managed service account if not already done. `setspn -S HTTP/<web_server_fqdn> <group_manged_service_account>`
- Confirm the SPN using following command. `setspn -l <group_manged_service_account>`

Because the group managed service account cannot be shown in `Users and Computers` search while adding the delegation entry for the computer account, you cannot add the delegation for a computer account using the usual method. Therefore, you can add this SPN as being delegated entry to the CA computer account by going through the attribute editor

- In the Connector Appliance computer properties, navigate to the **Attribute Editor** tab, and look for the `msDA-AllowedToDeleteTo` attribute.
- Edit the `msDA-AllowedToDeleteTo attribute`, and then add the SPN.



)



)

e. Migrate from Citrix Gateway Connector™ to Citrix Connector Appliance.

- As SPNs is already set to service account while configuring the gateway connector, you do not need to add any more SPNs for the service account if no new kerberos app is configured. You can view the list of all SPNs assigned for the service account by following command and assign them as delegated entries for the CA computer account.

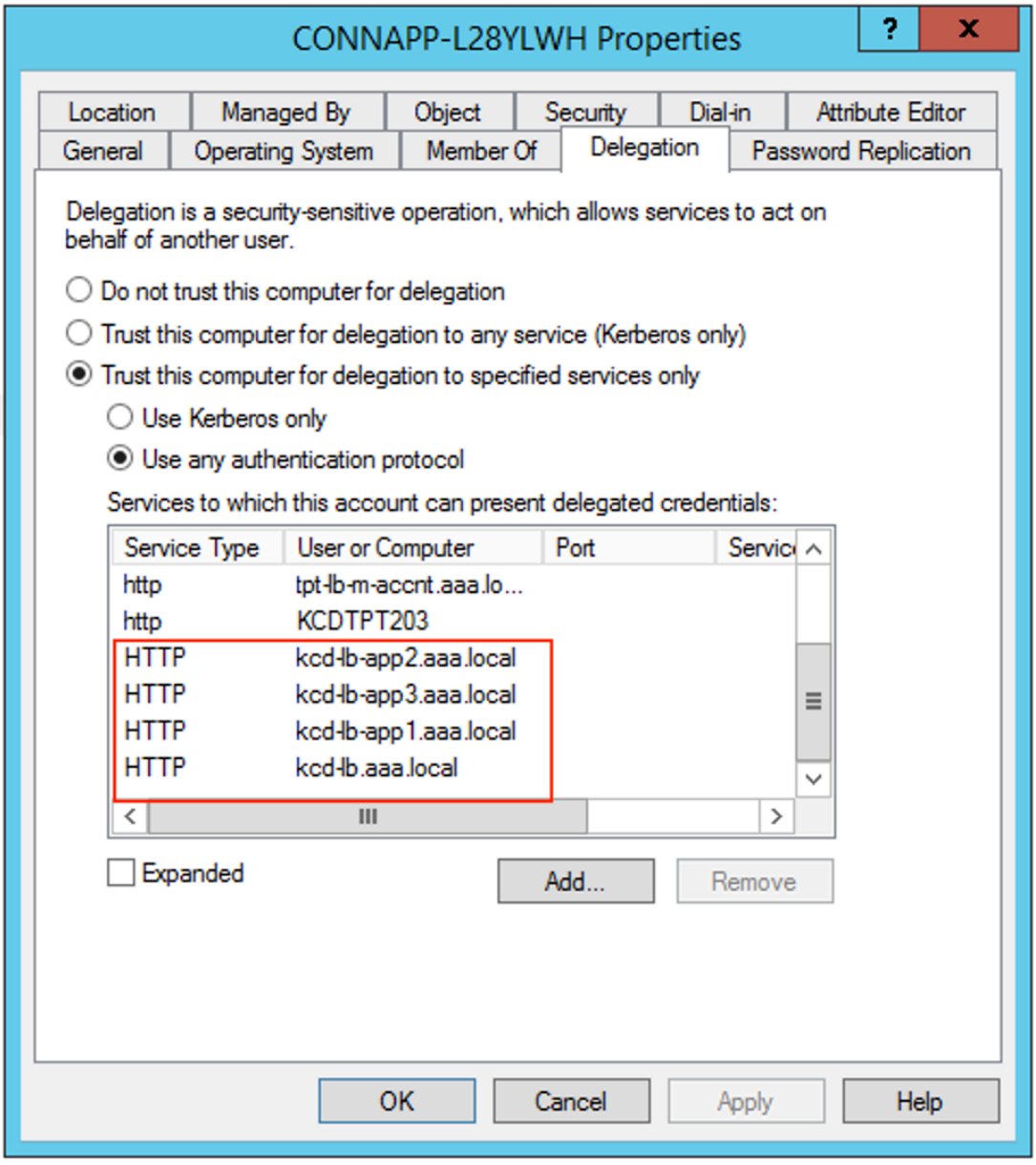
```
setspn -l <service_account>
```

```
C:\Windows\system32>setspn -l aaa\svc_iis3
Registered ServicePrincipalNames for CN=svcacct iis3,OU=Users,OU=KCD,DC=aaa,DC=l
ocal:
        HTTP/kcd-lb-app3.aaa.local
        HTTP/kcd-lb-app2.aaa.local
        HTTP/kcd-lb-app1.aaa.local
        HTTP/kcd-lb.aaa.local
        HTTP/kerblb.aaa.local
        host/kerblb.aaa.local

C:\Windows\system32>_
```

In this example, the SPNs (`kcd-lb.aaa.local, kcd-lb-app1.aaa.local, kcd-lb-app2.aaa.local, kcd-lb-app3.aaa.local`) are configured for KCD.

- Add the required SPNs to the connector appliance computer account as the delegated entry. For details, step *Create a delegation for the connector appliance computer account*.



In this example, the required SPN is added as delegated entires for the CA computer account.

Note: These SPN were added to the service account as delegated entries while configuring the gateway connector. As you are moving away from service account delegation, those entires can be removed from the service account **Delegation** tab.

f. Follow the Citrix Secure Private Access™ documentation to set up the Citrix Secure Private Access service. During the set up, Citrix Cloud recognizes the presence of your Connector Appliances and uses them to connect to your resource location.

- Get started with Citrix Secure Private Access
- Configure Citrix Secure Private Access
- Connector Appliance for Cloud Services
- Internet Connectivity Requirements.
- Support for Enterprise web apps

Validating your Kerberos configuration

If you use Kerberos for single sign-on, you can verify that the configuration on your Active Directory controller is correct from the **Connector Appliance administration page**. The **Kerberos validation** feature enables you to validate a Kerberos realm-only mode configuration or a Kerberos Constrained Delegation (KCD) configuration.

1. Go to the **Connector Appliance administration page**.
   a. From the Connector Appliance console in your hypervisor, copy the IP address to your browser address bar.
   b. Enter the password that you set when you registered your Connector Appliance.
2. From the Admin menu on the top right, select **Kerberos Validation**.
3. In the **Kerberos Validation** dialog, choose the **Kerberos Validation Mode**.
4. Specify or select the **Active Directory Domain**.
   - If you are validating a Kerberos realm-only mode configuration, you can specify any Active Directory domain.
   - If you are validating a Kerberos Constrained Delegation configuration, you must select from a list of domains in the joined forest.

5. Specify the **Service FQDN**. The default service name is assumed to be `http`. If you specify "computer.example.com", this is considered the same as `http/computer.example.com`.
6. Specify the **Username**.
7. If you are validating a Kerberos realm-only mode configuration, specify the **Password** for that user name.
8. Click **Test Kerberos**.

If the Kerberos configuration is correct, you see the message `Successfully validated Kerberos setup`. If the Kerberos configuration is not correct, you see an error message that provides information on the validation failure.

Scale and size considerations

This article details the guidance to determine the concurrent TCP connection limit and concurrent web app request limit of a single Connector Appliance at one resource location.

Web and SaaS applications

The minimum recommended size for a Connector Appliance virtual machine is 2 vCPU and 4 GB RAM. For high availability and resiliency, it is recommended to deploy two Connector Appliances.

Deployment guidance: A Connector Appliance of size 2 vCPU, 4 GB memory, and 10 Gbps NIC can support the following:

- Up to 500 web app requests per second (Secure Browse).
- Data transfer throughput rate of up to 1 Gbps.

These numbers were arrived at 90% CPU utilization and 80% of memory usage.

TCP Applications

The minimum recommended size for a Connector Appliance virtual machine is 2 vCPU and 4 GB RAM.

Deployment guidance: A Connector Appliance of size 2 vCPU, 4 GB memory, and 10 Gbps NIC can support the following:

- Up to 50,000 concurrent TCP connections.
- Data transfer throughput rate of up to 1 Gbps.

These numbers were arrived at 90% CPU utilization and 80% of memory usage.

Mixed traffic (web, SaaS, TCP)

Deployment guidance: A Connector Appliance of size 2 vCPU and 4 GB memory can support the following:

- Up to 300 web app requests per second (Secure Browse).
- Up to 10,000 concurrent TCP connections.
- Overall data transfer throughput rate of up to 1 Gbps.

These numbers were arrived at 90% CPU utilization and 80% of memory usage.

> **Important:**

> To manage your traffic requirements that exceed the recommended limits of web app requests per second (Secure Browse), concurrent TCP connections or the throughput, the Connector Appliance must be scaled horizontally by adding more Connector Appliances.

Connector notifications

The connector generates a notification once it exceeds 80% CPU utilization over a one-hour sample period. For more information, see Connector notifications.

Adaptive access policy configuration and management

In today's ever changing situations, application security is vital for any business. Making context-aware security decisions and then enabling access to the applications reduces the associated risks while enabling access to users.

The Citrix Secure Private Access™ service adaptive access feature offers a comprehensive zero-trust access approach that delivers secure access to the applications. Adaptive access enables admins to provide granular level access to the apps that users can access based on the context. The term "context" here refers to:

- Users and groups (users and user groups)
- Devices (desktop or mobile devices)
- Location (geo-location or network location)
- Device posture (device posture check)

The adaptive access feature applies adaptive policies to the applications that are being accessed. These policies determine the risks based on the context and make dynamic access decisions to grant or deny access to the Enterprise Web, SaaS, TCP, and UDP apps.

How it works

To grant or deny access to applications, admins create policies based on the users, user groups, the devices from which the users access the applications, and the location (country or network location) from where the user is accessing the application.

The adaptive access policies are evaluated in the following scenarios:

- During a Web, SaaS, TCP, or a UDP app enumeration from the Secure Private Access service – If the application access is denied to this user, the user cannot see this application in the store.
- While launching the application – After you have enumerated the app and if the adaptive policy is changed to deny access, users cannot launch the app even though the app was enumerated earlier.

Create an access policy with multiple rules

You can create multiple access rules and configure different access conditions for different users or user groups within a single policy. These rules can be applied separately for both HTTP/HTTPS and TCP/UDP apps, all within a single policy.

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:

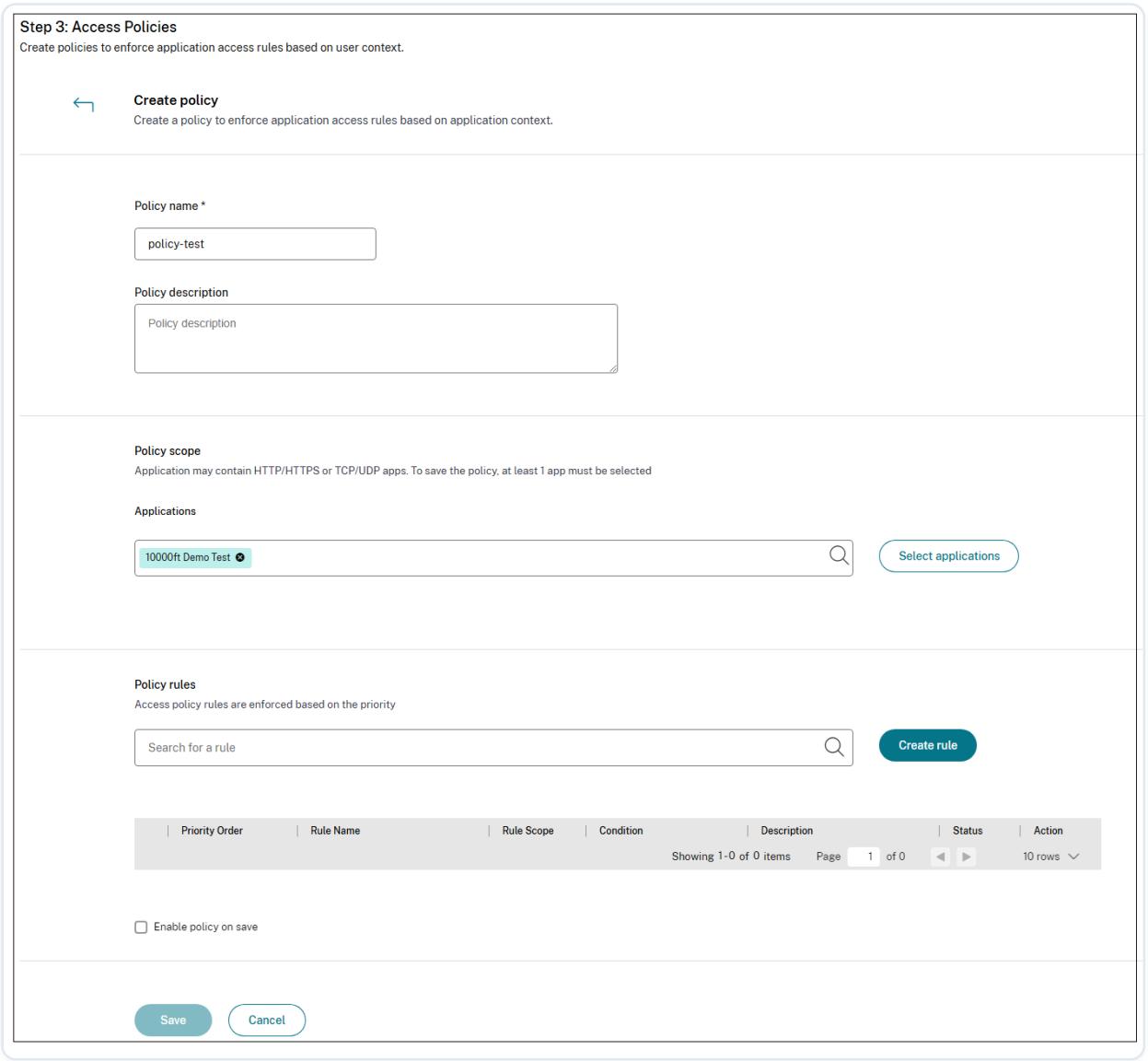
- Set Chrome Enterprise connector policies for Chrome Enterprise
- Data protection rules

Prerequisites

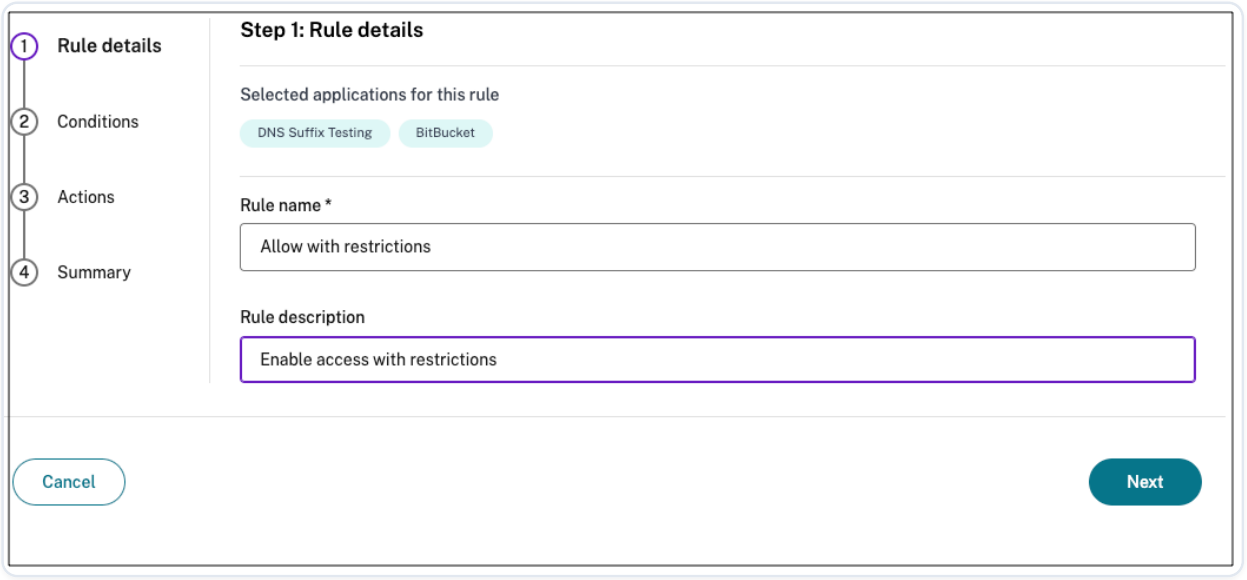
Ensure that you have configured the applications for your users. For details, see Add apps for your users.

Steps to create an access policy:

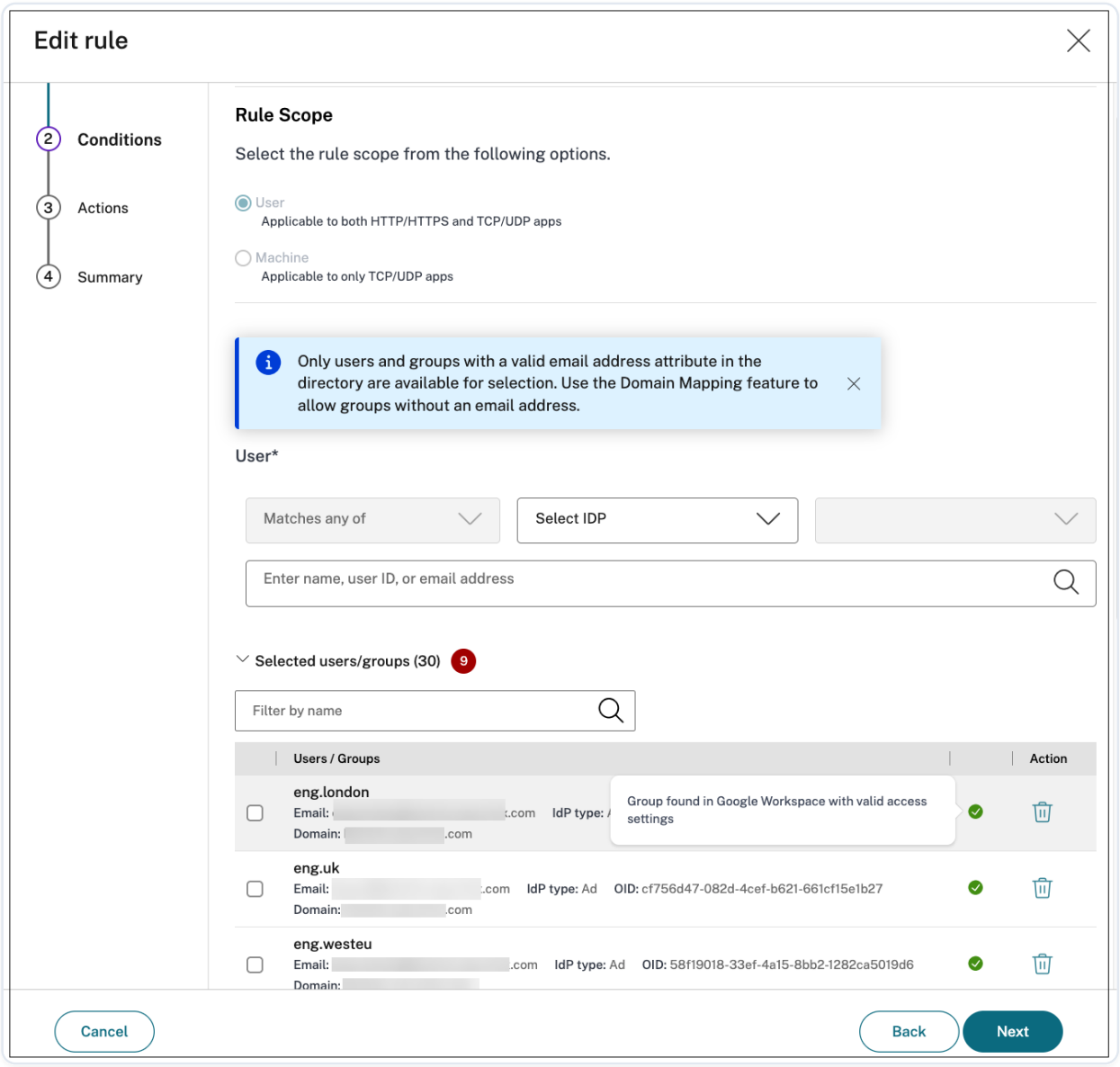
1. Open the **Access Policies** page, and then click **Create policy**.
2. Enter the policy name and description of the policy.
3. In **Applications**, select the app or set of apps on which this policy must be enforced.
4. Click **Create Rule** to create rules for the policy.



5. Enter the rule name and a brief description of the rule, and then click **Next**.



6. Select the users' conditions. The **Users** condition is a mandatory condition to be met to grant access to the apps for the users. You can select the condition, followed by the domain, and then users.



Select one of the following:

- **Matches any of** – Only the users or groups that match any of the names listed in the field and belonging to the selected domain are allowed access.
- **Does not match any** - All users or groups except those listed in the field and belonging to the selected domain are allowed access.

> **Note:**

- You can search for users or groups by display name, email ID, or user principal name. This helps you accurately identify and grant access to the correct user, even when the same user has multiple accounts. For details, see Search for users or groups.
- You must also use synchronized users and groups for Secure Private access policies to evaluate correctly. Else, warning messages are displayed. For details, see Verify user and group synchronization.

7. Add an **Access Mode** condition to restrict application access based on whether users connect through a browser-based client or the Citrix Secure Access client. For details, see Access mode-based policy enforcement.

   Note:

   You can combine access mode with the mandatory **Users** condition and any other conditions.

8. (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.

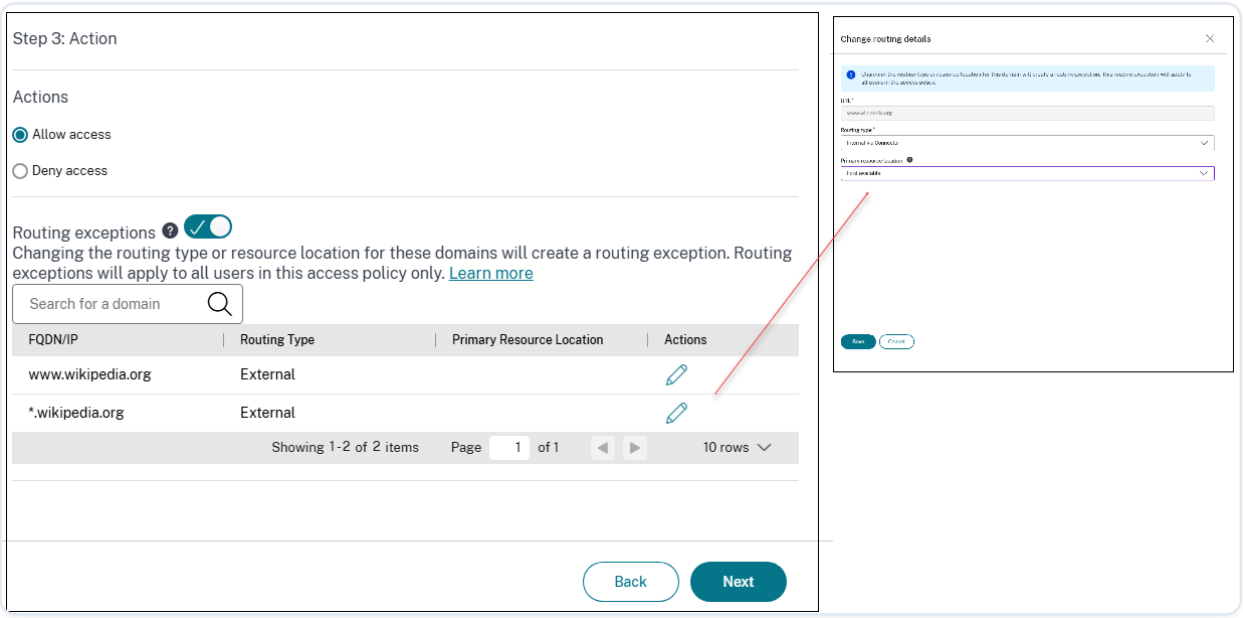
   - **Geo location** – Select the condition and the geographic location from where the users are accessing the apps.
     - **Matches any of:** Only users or user groups accessing the apps from any of the geographic locations listed are enabled for access to the apps.
     - **Does not match any:** All users or user groups other than those from the listed geographic locations are enabled for access.
   - **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 check** – Select the conditions that the user device must fulfill to access the apps.

9. Click **Next**.
10. Select the actions that must be applied based on the condition evaluation.

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



11. (Optional) Modify the routing type or resource location for a specific domain, if required. The **Routing exceptions** toggle allows you to edit the resource locations and routing information for domains of the apps added in the access policy.

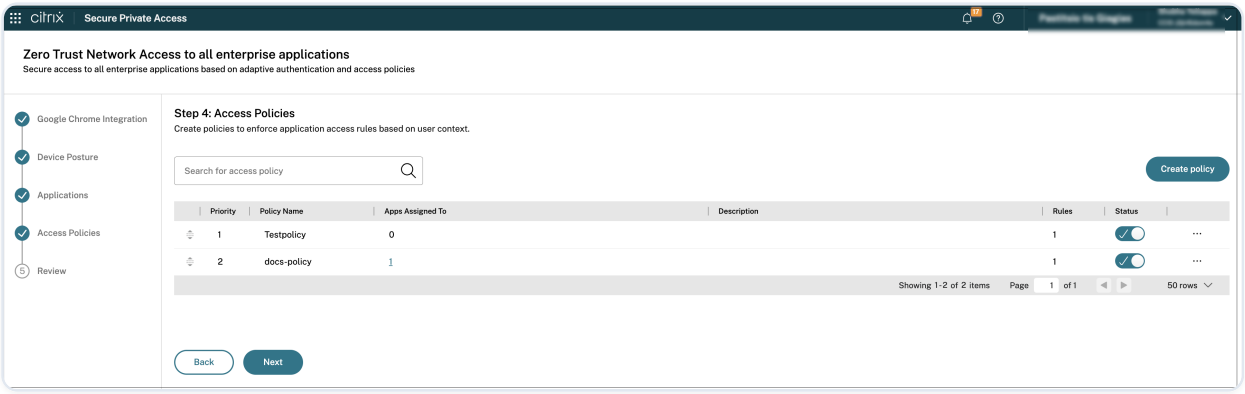
    - In **Routing type**, modify the routing type:

        - **Internal**: The traffic flows through the Connector Appliance. For a web app, the traffic flows within the data center. For a SaaS app, the traffic is routed outside the network through the Connector Appliance.
        - **Internal - Bypass Proxy**: The domain traffic is routed through Citrix Cloud Connector™ appliances, bypassing the customer's web proxy configured on the Connector Appliance.
        - **External**: The traffic flows directly to the internet.

- In **Resource location**, modify the resource location, if necessary. This option is applicable only for the internally routed domains.

For more information about contextual routing, see Context-based app routing and resource locations selection.

After you create the policies, they are listed in the **Access policies** page.



Search for users or groups

The users and groups that you select appear in a grid. Each row in the grid displays the following identity details so that you can clearly distinguish between identically named users or groups across different domains, forests, or identity providers (IdPs):

- **Name** – The display name of the user or group.
- **Email** – The email address associated with the identity.
- **IDP type** – The identity provider, such as Azure AD, Active Directory, Okta, or Google.
- **OID** – The object ID or security identifier of the identity.
- **Domain** – The domain to which the user or group belongs.

You can filter the grid by name, remove individual rows, or select multiple entries and remove them together using **Remove selected**.

Verify user and group synchronization

When selecting users or groups, administrators can verify whether entries from the selected user directory are synchronized with and correctly configured in Google Directory. Secure Private Access policies evaluate correctly only when the users and groups are synchronized. Otherwise, the following warnings might appear:

- **Missing tenant account privileges.**

Workaround:

In the Google Admin console, assign the **Users > Read** and **Groups > Read** privileges to the tenant service account. SPA requires these privileges to verify that a user or group exists.

- **User or group not synchronized.**

  Workaround:

  The searched or selected user or group is not synchronized with Google Directory. Synchronize the directory entity with Google Directory before using it in an SPA policy.

- **Insufficient group access settings.**

  Workaround:

  In the Google Admin console, open the access settings for the selected group and make sure the **Who can view members** has at least the **Group members** option selected.

> **Note:**
>
> This feature is available only after the Google Chrome integration is successfully completed.

Points to remember after a policy is created

- The policy that you created appears under the Policy rules section and is enabled by default. You can disable the rules, if required. However, ensure that at least one rule is enabled for the policy to be active.
- A priority order is assigned to the policy by default. The priority with a lower value has the highest preference. The rule with a lowest priority number is evaluated first. If the rule (n) does not match the conditions defined, the next rule (n+1) is evaluated and so on.

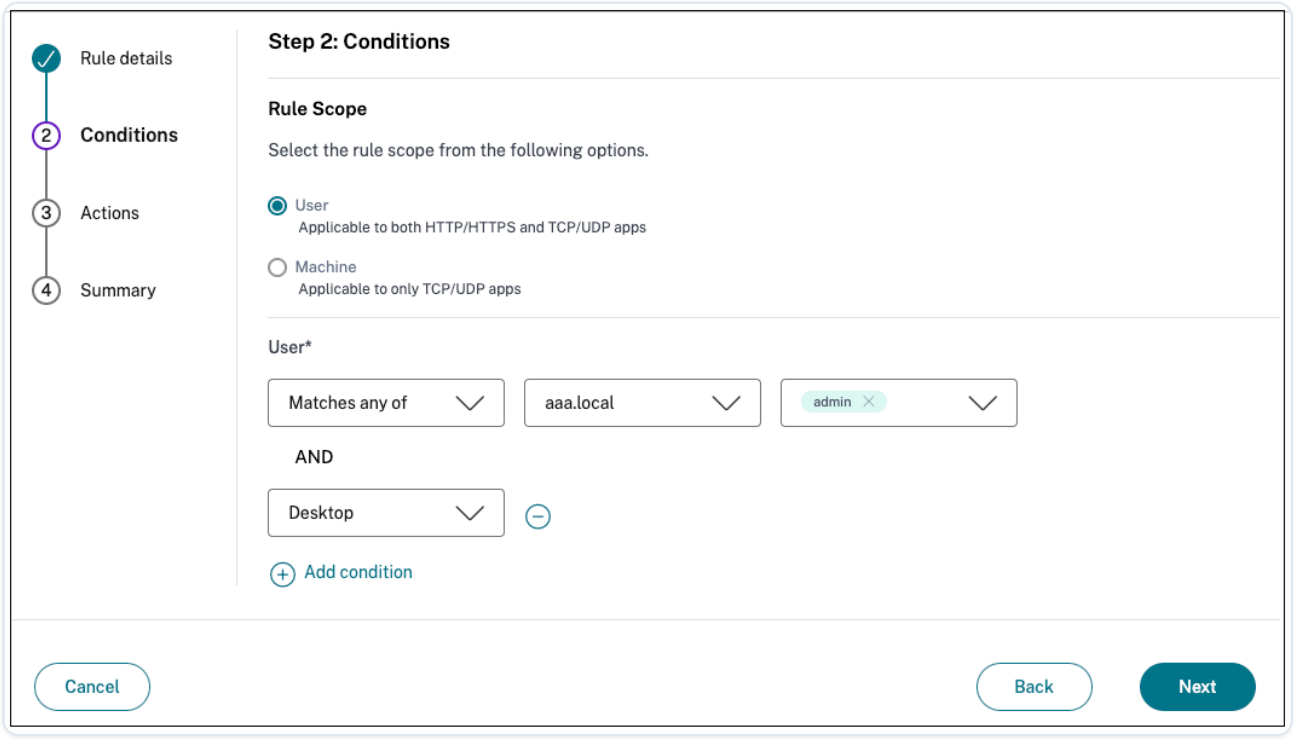
Evaluation of rules with priority order example:

Consider that you have created two rules, Rule 1 and Rule 2. Rule 1 is assigned to user A and Rule 2 is assigned to user B, then both rules are evaluated. Consider that both rules Rule 1 and Rule 2 are assigned to user A. In this case, Rule 1 has the higher priority. If the condition in Rule 1 is met, then Rule 1 is applied and Rule 2 is skipped. Otherwise, if the condition in Rule 1 is not met, then Rule 2 is applied to user A.

Adaptive access based on devices

To configure an adaptive access policy based on the platform (mobile device or a desktop computer) from which the user is accessing the application, see Adaptive access policy configuration and management.

- In **Step2: Conditions** page, click **Add condition.**
- Select **Desktop** or **Mobile device**.
- Complete the policy configuration.



Adaptive access based on the location

An admin can configure the adaptive 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.

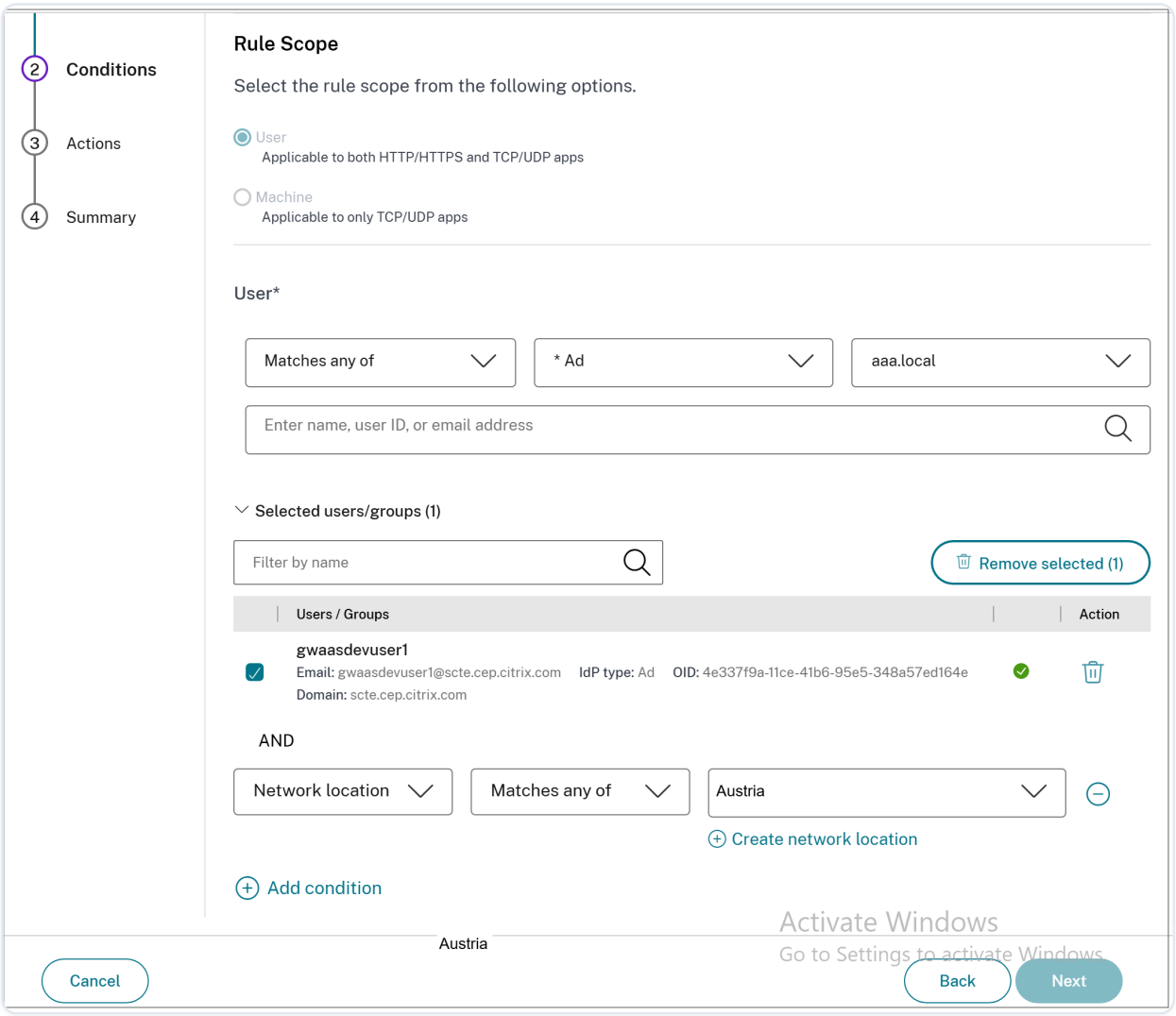
To configure an adaptive access policy based on the location, use the Create an adaptive access policy with multiple rules procedure with the following changes.

- In **Step2: Conditions** page, click **Add condition.**
- Select **Geo-location** or **Network location**.

- If you have configured multiple geo-locations or network locations, then select one of the following as per your requirement.
  - **Matches any of** – The geographic locations or network locations match any of the geographic locations or network locations configured in the database.
  - **Does not match any** – The geographic locations or network locations do not match with the geographic locations or network locations configured in the database.

  Note:

  - If you select **Geo-location**, the source IP address of the user is evaluated with the IP address of the country database. If the IP address of the user maps to the country in the policy, the policy is applied. If the country does not match, this adaptive policy is skipped and the next adaptive policy is evaluated.
  - 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 > StoreFront Cloud > 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.



- Complete the policy configuration.

Adaptive access based on the device posture

You can configure Secure Private Access service to enforce access control using device posture tags. After a device is allowed to log in after the device posture verification, the device can be classified as compliant or non-compliant. This information is available as tags to the Citrix DaaS™ service and Citrix Secure Private Access service and is used to provide contextual access based on device posture.

For complete details on the Device Posture service, see Device Posture.

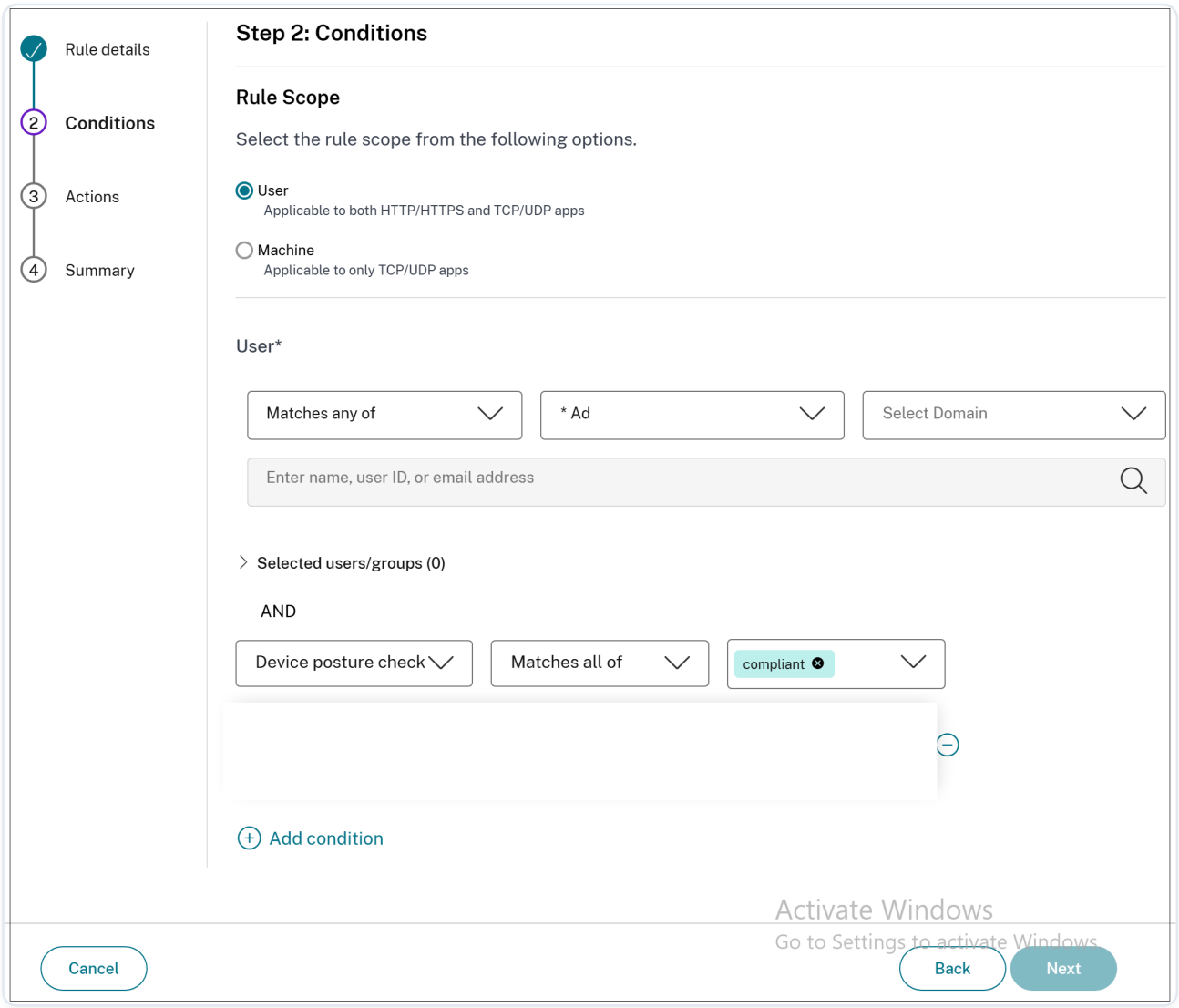
To configure an adaptive access policy based on the device posture, use the Create an adaptive access policy with multiple rules procedure with the following changes.

- In **Step2: Conditions** page, click **Add condition.**
- Select **Device posture check** and the logical expression from the drop-down menu.

- Enter one of the following values in custom tags:
  - **Compliant** - For compliant devices
  - **Non-Compliant** - For non-compliant devices

Note:

The syntax for the device classification tags must be entered in the same manner as captured earlier, that is initial caps (Compliant and Non-Compliant). Else the device posture policies do not work as intended.



Session policies

Admins can configure session policies to route internal corporate users directly to back-end apps without tunneling traffic through Secure Private Access. Session policies offer dynamic routing based on factors, such as network location and device posture.

> **Note:**
>
> - Session policy settings are applied at the session level to all applications rather than being tied to specific applications.
> - Session policies can be assigned to all users or a subset of users.

Routing precedence

Session policies work alongside access policies, with access policies taking precedence if there is a conflict. In such scenarios, access policy routing exceptions override session policies. If neither an access policy nor a session policy is configured, global routing settings (**Settings > Application Domain**) apply.

Supported Citrix Secure Access™ clients

The following versions of Citrix Secure Access client support routing of users directly to back-end applications.

- macOS - 24.11.1 and later
- Windows - 24.11.1.17 and later. Also, the **EnableContextualAccess** VPN client registry must be enabled. For more information, see NetScaler Gateway Windows VPN client registry keys.

Example use case

Scenario:

In an organization, when users are connected to the corporate network “corporate_network1”, then traffic from apps must flow directly to the back-end apps, as these apps are directly reachable on the corporate network. If the users are outside the corporate network, then the app traffic must be tunneled.

Solution:

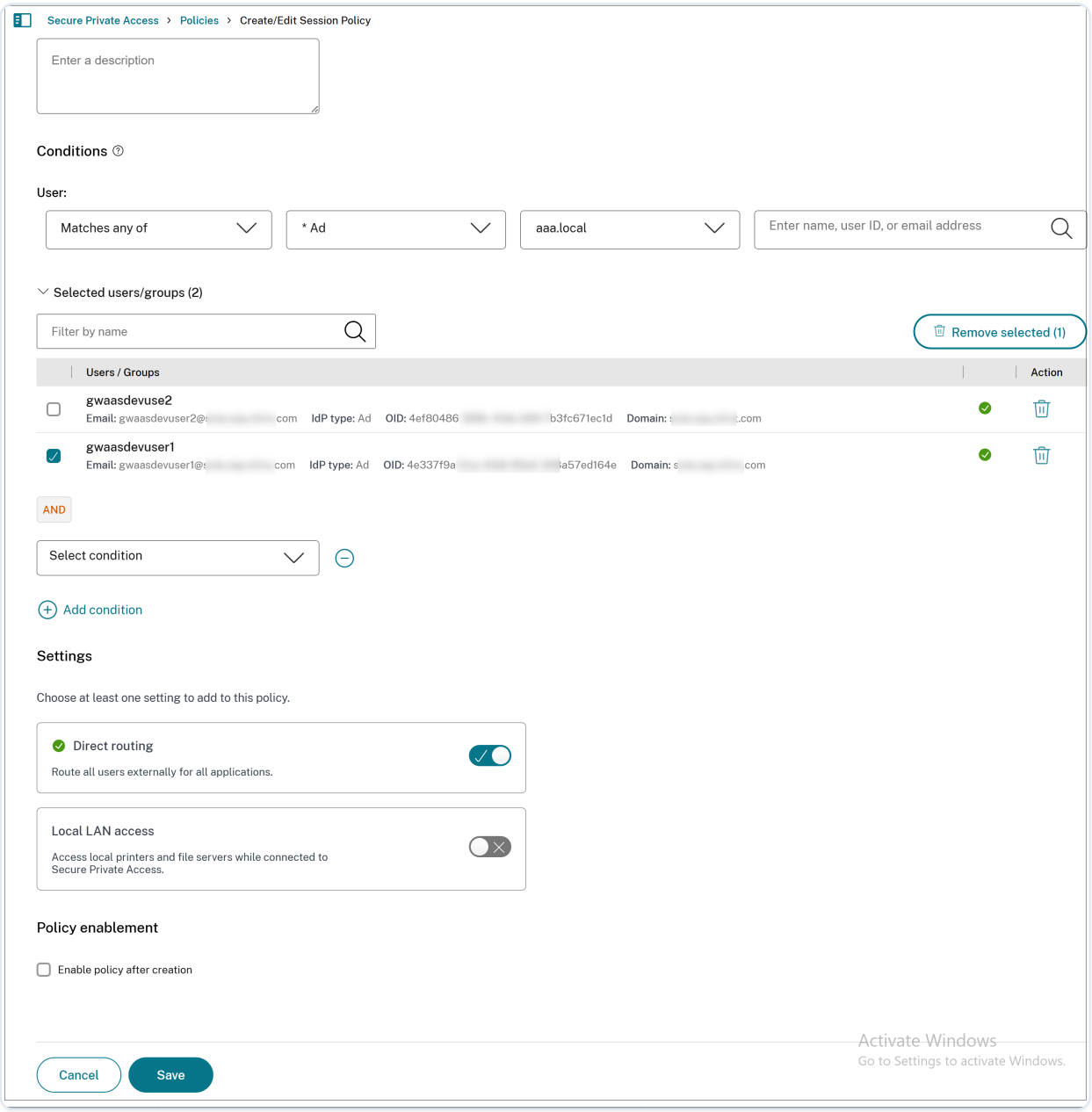
1. Add app1, app2 with routing set to **Internal via Connecto**r.
2. Add an access policy for the apps (app1, app2) to grant access.
3. Add a session policy to configure conditions to specify the user group and network locations that must be considered when granting access.
4. Select the **User** condition and set it to **All users**.
5. Add a **Network Location** condition. Set it to **Matches any of** and specify the network location “corporate_network1”. This ensures that traffic coming from “corporate_network1” flows directly to the back-end apps.

You can also enable routing exceptions for this scenario. For example, if app1 must always be tunneled even on the corporate network, then routing exceptions can be configured for domains of app1 in the access policy. When this is done, the routing exception takes precedence over the session policy.

Configure direct routing within the corporate network using session policies

You must create a session policy to enable users to directly access the back-end applications bypassing the Secure Private Access tunneling. To do this, first, you select the users to which this policy must apply. Second, under ‘Network Location’ select the name of your corporate network. This is an important step to make sure that Direct Routing is only enabled when the user is inside your company's corporate network.

1. Navigate to **Policies > Session Policies** and click **Create Session Policy**.



2. Enter a name for the policy and a description of the policy.
3. Select the users and the conditions for which you want to apply these settings.
4. You can select the condition to apply to all users or specify a subset of users.

Note:

You can search for users or groups by display name, email ID, or user principal name. This helps you accurately identify and grant access to the correct user, even when the same user has multiple accounts.

The users and groups that you select appear in a grid. Each row in the grid displays the following identity details so that you can clearly distinguish between identically named users or groups across different domains, forests, or identity providers (IdPs):

- **Name** – The display name of the user or group.
- **Email** – The email address associated with the identity.
- **IDP type** – The identity provider, such as Azure AD, Active Directory, Okta, or Google.
- **OID** – The object ID or security identifier of the identity.
- **Domain** – The domain to which the user or group belongs. You can filter the grid by name, remove individual rows, or select multiple entries and remove them together using Remove selected.

5. Add an **Access mode** condition to scope the session settings to the intended client type. Session policies evaluated during Secure Private Access routing are treated as CSA access mode. For more information about access modes, see Access mode-based policy enforcement.
6. (Optional) Click + to add multiple conditions based on the context.
7. Define the **Network Location** condition to enable dynamic routing for the entire session. This confirms that direct routing is enabled only when users are inside the company's corporate network.

   When you add conditions based on a context, an AND operation is applied on the conditions wherein the policy is evaluated only if both the users and the optional contextual-based conditions are met. For details on the conditions, see Configure an access policy.
8. Select **Direct routing** to route all users externally to the back-end applications.
9. Select **Local LAN access** to enable seamless access to local LAN resources. For more details, see Seamless access to local LAN resources (printers, file servers).
10. Select **Enable policy after creation**. 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 Session Policies page by using the toggle switch in the Status column.
11. Click **Save**.

Note:

Network location changes trigger session policy refreshes and this might impact the end clients as follows:

- **Citrix Secure Access agent:** Policy refreshes might alter routing configurations and hence impact application access.
- **Citrix Enterprise Browser™:** Policy refreshes occur every 30 minutes. Users must restart the browser or wait for the refresh to access applications.

Citrix Enterprise Browser to Chrome Enterprise Premium migration

The transition from Citrix Enterprise Browser (CEB) to Citrix Enterprise Premium (CEP) marks a significant step forward in Citrix's Secure Private Access evolution to provide secure, adaptive, and high-performance Zero Trust Network Access (ZTNA) to all applications. This topic provides contains detailed information for IT administrators and Citrix professionals to plan and execute a successful gradual migration, ensuring minimal disruption and optimal user experience.

This phased migration approach allows organizations to maintain business continuity during the transition period by running both browser solutions in parallel. With the phased migration, customers can validate compatibility of existing applications and workflows with Chrome Enterprise Premium.

The following key steps are involved in the CEB to CEP migration:

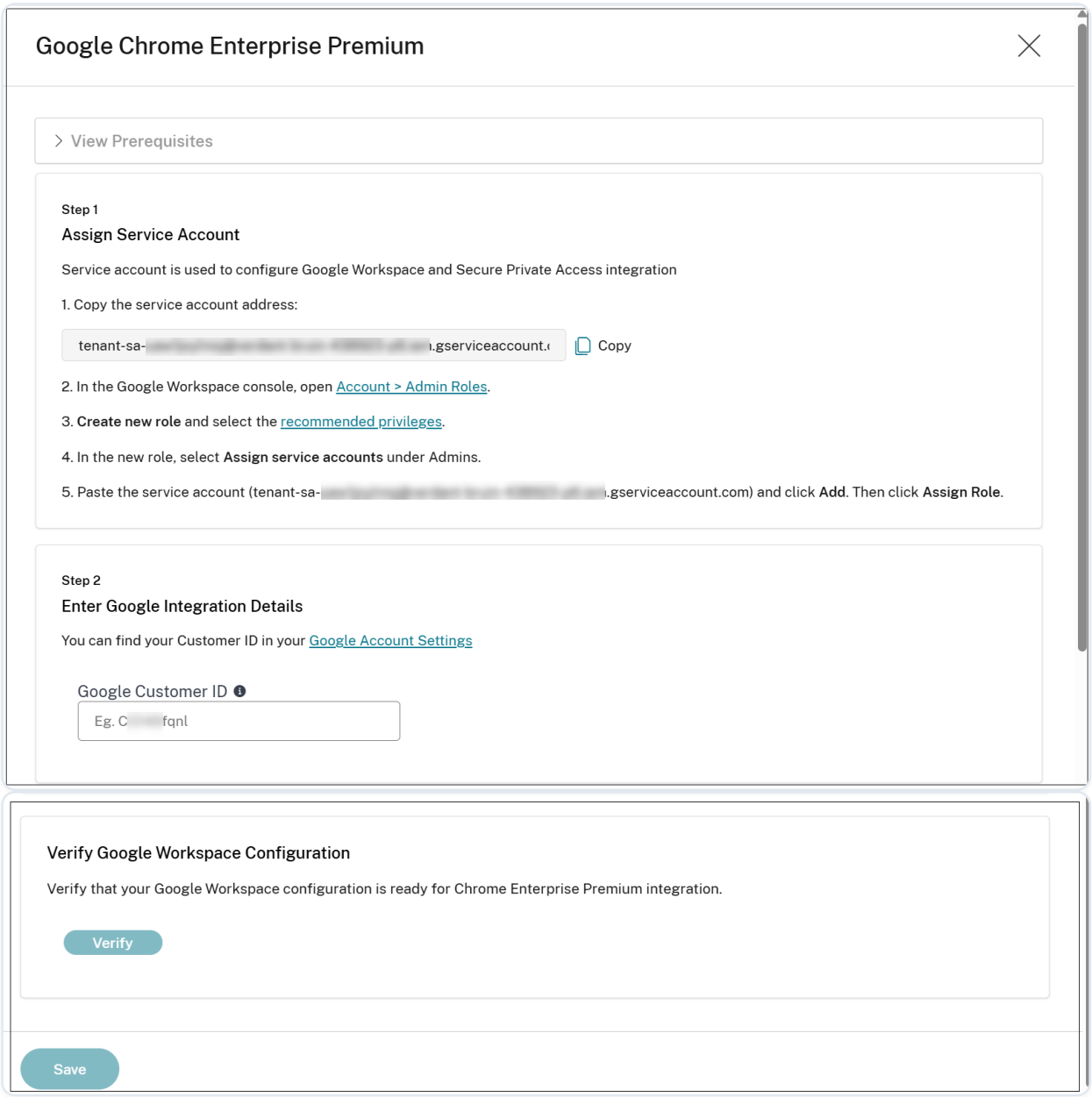
- Configure Chrome Enterprise Premium
- Domain mapping for user groups without email addresses
- Secure Private Access configuration parser for CEP compatibility analysis
- Configuration changes prior to full migration to CEP
- Rollout CEP to the organization (full migration)

Configure Chrome Enterprise Premium

For existing Secure Private Access customers, the migration wizard in the Secure Private Access console facilitates CEP provisioning, extension installation for users, and a path for gradual application and user migration.

1. In the Secure Private Access admin console, navigate to **Chrome Enterprise Premium > Configuration**.

   You can view the Google integration details.



2. Click **Set up Google CEP**.
3. Assign Citrix service account details within the Google WorkSecure Private Access console. For details, see Setup Google Chrome integration.
4. Click **Save** and close.

The Chrome Enterprise Premium provisioning begins.

Policy enrichment for user groups without email

Once the Chrome Enterprise Premium provisioning is successfully completed, a policy update process is automatically triggered for the access policies and session policies.

This update process does the following:

- Review the existing policies (access and session).
- Check for users and user groups without emails in their rules.
- Query the CC Directory service to retrieve their emails, and add them to the policies.

For details, see Domain mapping for user groups without email addresses.

Secure Private Access configuration parser for CEP compatibility analysis

The following key policy elements are not directly supported in CEP:

- Applications
  - Single sign-on
- Access policies
  - Allow access with restrictions
  - Mixed Allow/Deny actions (HTTP/HTTPS vs TCP/UDP)
  - Store URL conditions
  - Desktop/Mobile conditions
- Session policies
  - Store URL conditions
  - Desktop/Mobile conditions
- Security Groups
- Web filtering

These incompatibilities must be resolved before migrating applications from CEB to CEP.

The incompatibility identification process is facilitated by the Secure Private Access configuration parser `<parse_citrix_spa_configuration.py>`. This tool analyzes the Citrix Secure Private Access configuration exports to identify compatibility issues such as the following during the migration to CEP.

- Applications incompatible with CEP
- Access policies incompatible with CEP
- Configured security groups

- Web filtering configuration

> **Note:**

> Security groups and web filtering are not supported in the Citrix Secure Private Access integration with CEP.

> After the analysis, the tool provides different recommendations depending on whether the CEP rollout has been completed across the entire organization (migration of all applications).

How to use the tool

1. Download the script from: Python script to parse the secure private access configuration.
2. In the Secure Private Access admin console, navigate to **Settings > Global Configuration > Create Report** and export the existing Secure Private Access configuration into a JSON format.
3. Download the Python script and run the script using the exported report as input. You must have installed Python 3 to run this script.

   ```
   # python3 parse_citrix_spa_configuration.py <path_to_spa_report>
   ```

   The script can be used either before or after the full migration, providing different recommendation actions.

> **Note:**

> The script does not provide recommendations for the incompatible session policies.

> **Sample report:**

```
% python3 parse_citrix_spa_configuration.py
CitrixSpaConfigurationDump.json



Has the CEP rollout to the entire organization been completed?
```

```
Enter yes/no (default: no): no

CEP INCOMPATIBLE APPLICATIONS (7 out of 185):

1. Application_1 ⚠

   Reason: Has SSO configuration other than 'Don't use SSO'

2. Application_2 ⚠

   Reason: Has SSO configuration other than 'Don't use SSO'

....

--------------------------------------------------

Mitigation guidance:

--------------------------------------------------

Has SSO configuration other than 'Don't use SSO':
```

- Navigate to the application's SSO settings

- Change the SSO setting to 'Don't use SSO'

==========

CEP INCOMPATIBLE POLICIES (15 out of 136):

1. Access_policy_1 ⚠

   Reasons: Contains user(s)/group(s) without email

2. Access_policy_2 ⚠

   Reasons: Mixed actions (HTTP/HTTPS vs TCP/UDP), Contains user(s)/group(s) without email

...

Mitigation guidance:

Platform filter (Desktop/Mobile):

- Remove the unsupported Desktop/Mobile condition

Workspace URL:

- Remove the unsupported Workspace URL rule

Access with restrictions:

- Configure access controls without using restrictions

Mixed actions (HTTP/HTTPS vs TCP/UDP):

- Ensure both actions have the same value

```
  • If that's not possible, create separate policies for HTTP/HTTPS and
TCP/UDP applications




Policy contains user(s)/group(s) without email



  • Add email to the user(s)/group(s) without email and update the policy
```

Configuration changes prior to full migration to CEP

The following configuration changes must be applied manually by the Secure Private Access administrator before initiating the full migration to CEP. These updates ensure compatibility and readiness across all applications and policies.

Single sign-on configuration changes

To ensure compatibility with CEP, it is essential to update the single sign-on (SSO) configuration for all existing applications. The Secure Private Access administrators must perform the following steps:

1. Navigate to the Application Configuration page (**Secure Private Access > App Configuration**).
2. Edit the applications to modify the single sign-on configuration.

   Under the Single Sign On section, in **Which single sign on type would you like to use for your Web app setup?**, select **Don’t use SSO**.

Important:

- This update is mandatory because the SSO step is removed in CEP. By setting the application to **Don’t use SSO**, you ensure continued functionality and alignment with the new migration flow.

- If the single sign-on configuration is not changed as instructed, the application becomes inaccessible after the migration to CEP.

Access policies and session policies updates

To ensure that the access policies are compatible with CEP standards, specific updates are required in the access and session policies. The Secure Private Access administrators must perform the following steps:

1. Navigate to **Secure Private Access > Policies > Access Policies**.
2. Click **Edit** on the relevant policy and modify the action settings.
    a. Within the policy, navigate to the **Policy rules** section, click the ellipsis icon in line with the policy rule and click **Edit**.
    b. Navigate to the **Actions** page and change the **Action** settings.

Standardizing actions across applications

When configuring actions for both HTTP/HTTPS and TCP/UDP applications, ensure the following:

- The same action, either **Allow Access** or **Deny Access** is selected in both sections.
- If the option **Allow access with restrictions** is currently enabled for HTTP/HTTPS applications, it must be removed, as this setting is not supported in CEP.
- Replace **Allow access with restrictions** with either **Allow Access** or **Deny Access**, based on your intended policy behavior.

Application requirement for policy updates

Access policies without assigned applications cannot be updated. To modify these policies, first assign an application to the policy.

Important:

If these updates are not performed, applications associated with access policies containing mixed actions become inaccessible or deny actions setting might be ignored.

Web filtering policy update (optional)

To maintain alignment with the new CEP migration standards, it is necessary to update the web filtering settings within Secure Private Access. Perform the following steps to update web filtering configuration:

1. Navigate to **Secure Private Access > Settings > Unsanctioned Websites**.
2. Delete all websites and Remote Browser Isolation (RBI) entries currently listed under this section.
3. After removing these entries, disable the **Web filtering is enabled** toggle located at the top of the page.

These configurations are no longer relevant following the migration to CEP.

> **Important:**

> If these steps are not completed, there is no impact on the system's operation after the full migration. However, the **Unsanctioned Websites** page will not be visible.

Other policy adjustments (optional)

Review and delete unused conditions:

As part of the migration and policy optimization process, it is recommended to review access and session policies for any conditions that might no longer be applicable. Examples of such conditions include:

- Workspace URL
- Desktop and Mobile options

These conditions can be deleted if they are not relevant to your current environment or business requirements.

> **Note:**

> If these policy adjustments are not made, there is no impact on the system operations.

Security Groups clean-up (optional)

Review the Security Groups configuration within Secure Private Access.

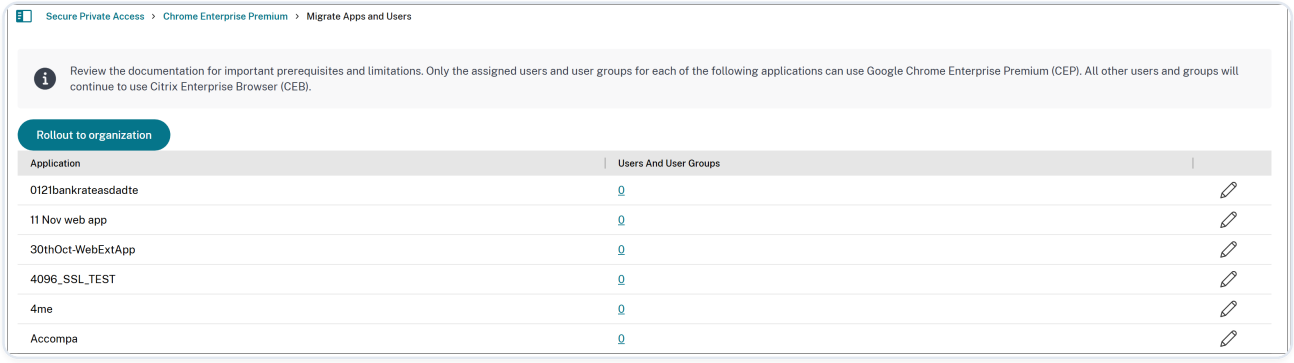
Navigate to **Secure Private Access > Applications > Security Groups** to assess any existing entries.

After migration, the Security Groups configuration will no longer be available. Therefore, any entries currently listed under this tab can be deleted, as they will no longer be relevant to the post-migration environment.

> **Note:**
>
> There is no system impact if this configuration is not updated. Removing these entries is optional and helps maintain a streamlined environment, but it is not required for continued operation.

Rollout CEP to the organization (full migration)

After completing the earlier mentioned steps, click **Rollout to organization** in the **Migrate Apps and Users** page. This is the last stage of the migration process.



> **Important:**
>
> Once the rollout is complete, CEP becomes the default enterprise browser. Reverting to CEB is not possible, and incompatible settings are hidden in the Secure Private Access admin console.

Summary of the migration process

Follow these steps to migrate applications from CEB to CEP:

1. Provision Chrome Enterprise Premium.
2. Migrate one application for a specific group of users.
    a. Enrich the group with email (if not exists).
    b. Fix any incompatibilities.
    c. Migrate the application to CEP.
    d. Verify that the application is accessible via CEP (directly, CWA and WSUI).
3. Enrich the users and user groups with emails.
4. Migrate more applications and users and user groups.
5. Rollout CEP to the organization (full migration).
6. Fix any leftover incompatibilities.
    a. Run the script again, indicating in the prompt that the CEP rollout has been completed.
    b. Fix the incompatibilities.
    c. Verify that the applications are accessible via CEP (directly, CWA and WSUI).

Challenges with the email enrichment process

The email enrichment task can be intricate, as it often involves collaboration among several teams to assign emails to various groups across multiple domains. The Domain Mapping feature facilitates this process. For details, see Domain mapping for user groups without email addresses.

Best practices

1. Start with a pilot migration for a small user group before a full-scale rollout.
2. Leverage Citrix’s official migration tools and documentation.
3. Maintain clear documentation of all changes and configurations.
4. Establish a rollback plan in case of critical issues.

Conclusion

Migration from CEB to CEP modernizes your Citrix environment with enhanced capabilities. Careful planning, thorough testing, and proactive user engagement ensure a smooth transition to CEP.

Advanced Secure Private Access features

The following are some of the advanced features supported by Secure Private Access:

- **Access mode-based policy enforcement:** Access mode-based policy enforcement lets administrators restrict how a user connects to an application. The connection can be through a browser-based client or the Citrix Secure Access client. For more information, see Access mode-based policy enforcement.
- **Local LAN access support:** Secure Private Access supports seamless access to local LAN resources while maintaining a secure connection to corporate resources. For details, see Seamless access to local LAN resources (printers, file servers.
- **Route DNS queries to application-specific resource locations:** Administrators can route DNS queries for specific applications directly to their dedicated resource locations. This enables more accurate DNS resolution, intelligent traffic management, and a better user experience. For details, see Route DNS queries to application-specific resource locations.
- **Hybrid data path for Secure Private Access service:** The hybrid data path for Secure Private Access service leverages both on-premises and cloud infrastructures to provide secure access to applications. Organizations can use the hybrid data path to route all data traffic through an on-premises NetScaler Gateway. This ensures that sensitive data stays within the company's network. Even though the data traffic is routed through the on-premises NetScaler Gateway, Citrix Cloud can still be used for monitoring and managing the applications and users. For details, see Hybrid data path for Secure Private Access service.
- **Discover applications, domains, or IP addresses within your network:** 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 applications, domains, or IP addresses within your network.
- **Context-based app routing and resource locations selection:** Allows admins to edit the internal routing type per URL or resource location based on the user context. For details, see Context-based app routing and resource locations selection.

- **Policy modeling tool:** Provides admins full visibility into the expected app access results (allowed/allowed with restriction/denied) based on their existing configurations. Admins can check the access results for any user based on conditions such as device type, device posture, geo-location, network location, and workspace URL. For details, see Policy modeling tool.
- **Applications import tool:** The Secure Private Access admin console includes a file import tool that allows administrators to bulk import multiple applications into the system using a CSV file or the nsconfig file. This tool is especially useful for organizations shifting from a traditional VPN to a more advanced solution like Secure Private Access. For example, organizations can use this tool to migrate applications that were delivered over a VPN to Secure Private Access and shift to a ZTNA-based architecture. Bulk upload of apps enables the organizations to eliminate the need for manual configuration. For details, see Applications import tool.
- **Terminate active sessions and block users/machines:** - Enables admins to terminate all active sessions immediately and add the users/machines to the block list. Adding a user/machine to the block list terminates all active Secure Private Access application sessions and blocks future application access. For details, see Terminate active sessions and add users/machines to the block list.
- **Timeouts for user sessions:** Allows admins to configure a timeout period for the Web apps and the Citrix Secure Access client to end user sessions if there is no network activity for the specified time period. For details, see Timeouts for user sessions.

Hybrid data path for Secure Private Access service

The hybrid data path for Secure Private Access service leverages both on-premises and cloud infrastructures to provide secure access to applications. Organizations can use the hybrid data path to route all data traffic through an on-premises NetScaler Gateway. This ensures that sensitive data stays within the company's network. Even though the data traffic is routed through the on-premises NetScaler Gateway, Citrix Cloud™ can still be used for monitoring and managing the applications and users.

Key advantages of using hybrid data path

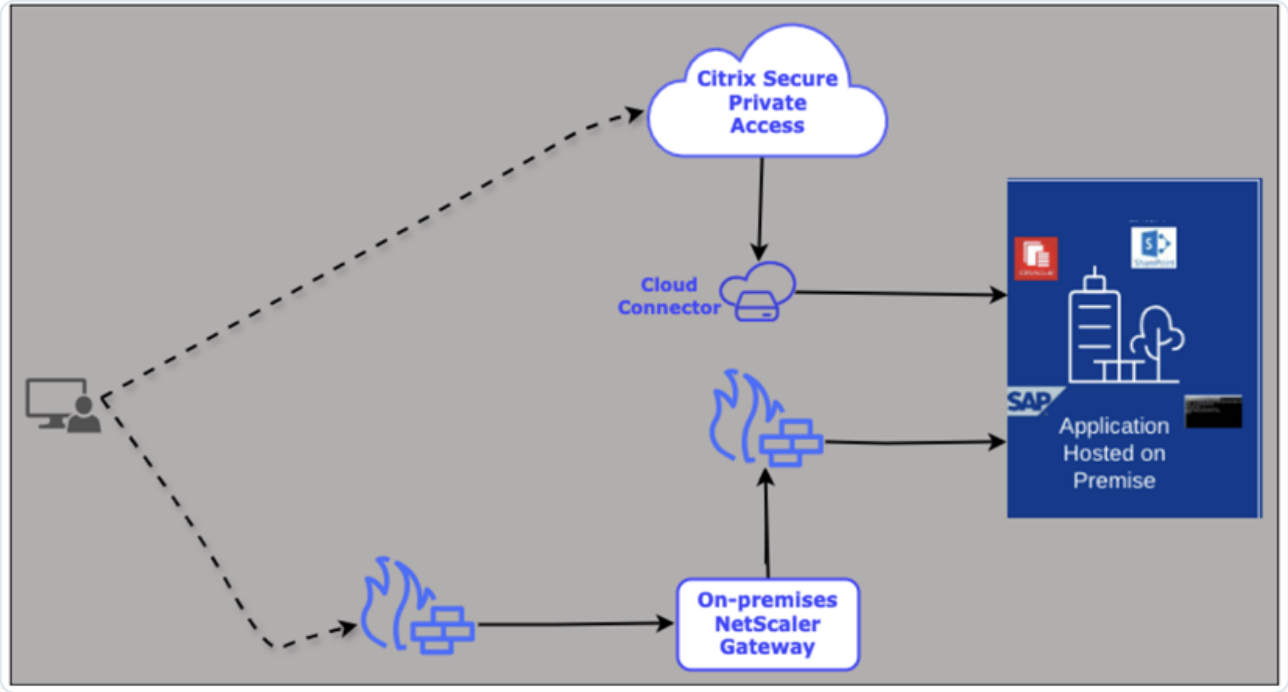
The following are some of the key advantages of using the hybrid data path:

- Extended reach with on-premises gateway:
  - Utilize an on-premises NetScaler® Gateway to provide access to on-premises applications in areas where a cloud PoP is distant.
  - Ensure consistent performance by avoiding routing traffic through distant cloud PoPs.

- Granular security and control:
  - Implement selective routing to direct sensitive applications through secure, on-premises pathways and route less critical applications through the cloud.
  - Enable custom routing for applications to meet data security and compliance requirements based on application data sensitivity
- Direct connectivity for enhanced user experience:
  - Establish direct connections between remote users and required applications, bypassing the cloud PoP.

How hybrid data path works

The following figure displays the hybrid data path work flow.



The following list explains the workflow involved in the hybrid data path:

1. A user logs in to the Citrix Secure Access™ client.
2. After successful authentication, a session is established.
3. The end user attempts to launch an application.
4. The access policies associated with the application are evaluated, and the app is launched.
   - If the application is configured to be routed through the Secure Private Access service, the request is sent to the Cloud Connector and then the specific app is launched.

- If the application is configured to be routed through on-premises NetScaler Gateway, the request is sent to the on-premises NetScaler Gateway and the specific application is launched

Supported clients

The hybrid data path is supported by the following Citrix Secure Access clients:

- Windows - 25.1.1.17 and later
- macOS - 25.02.1 and later

Supported NetScaler Gateway builds

The hybrid data path is supported from NetScaler Gateway version 14.1 build 47.46.

Connectivity requirements

The following sections provide more information about the connectivity requirements.

Allowed list of URLs for outbound connections

The following URLs must be allowed for outbound connections from NetScaler Gateway:

- `https://trust.citrixnetworkapi.net`: For gateway registration with Citrix Cloud.
- `https://trust.citrixworkspacesapi.net`: For gateway registration with Citrix Cloud.
- `https://policy.netscalergateway.net`: For authorizing app launch requests via the gateway.
- `https://cacerts.digicert.com`: For policy service engine certificate validation.

Set up hybrid data path for Secure Private Access applications

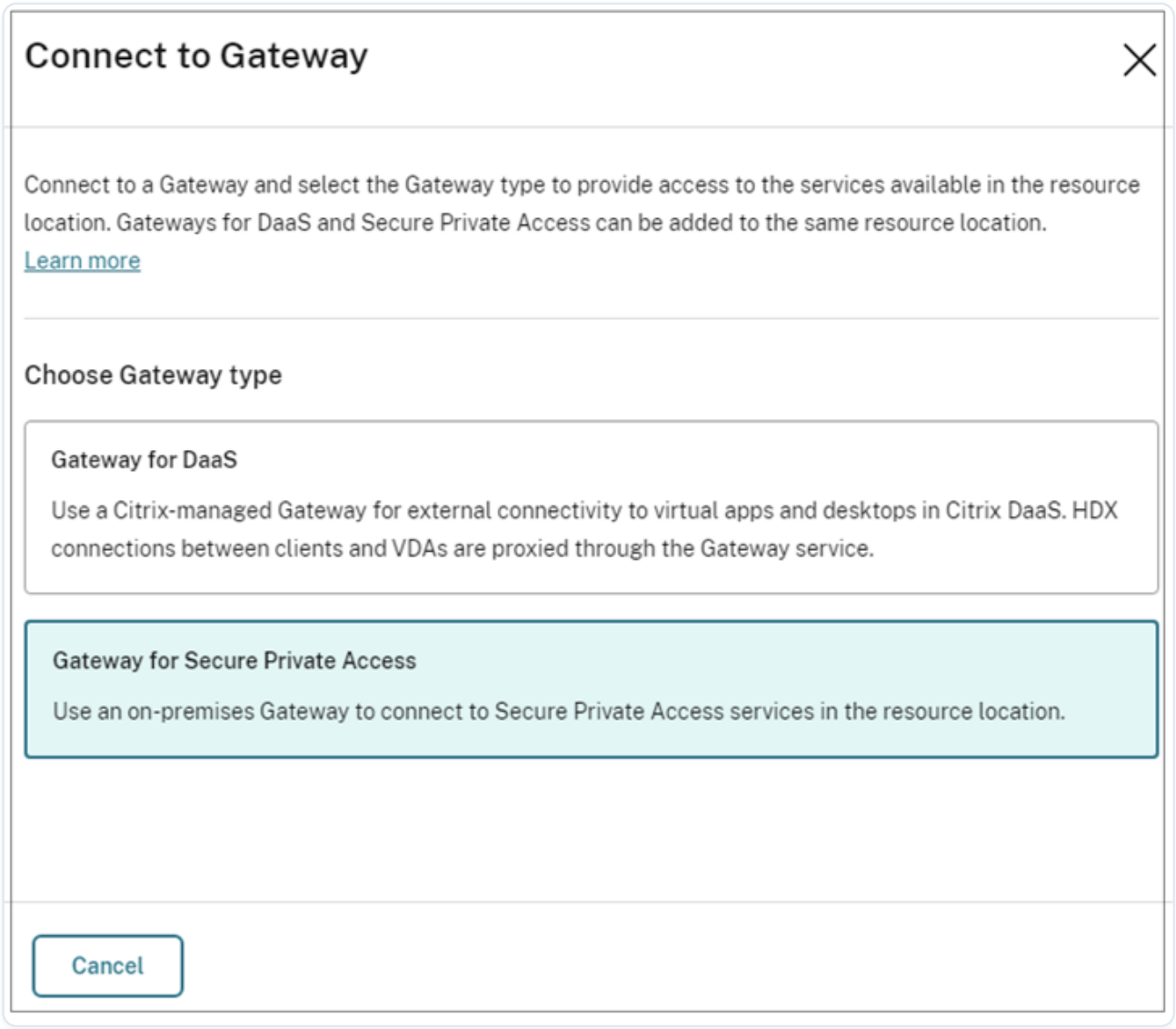
The following high-level steps are involved in setting up the hybrid data path:

1. Connect to a gateway to establish a connection
2. Register NetScaler Gateway with Citrix Cloud
3. Enable routing of data traffic through the on-premises NetScaler Gateway

Connect to a gateway to establish a connection

To establish a connection with the Secure Private Access resources in a specific resource location, you must first connect to a gateway. Citrix Cloud enables you to establish a connection with DaaS and Secure Private Access resources in a specific resource location. The gateway type that you

select determines the services you can access. For enhanced flexibility and to optimize resource utilization, you can add both a DaaS gateway and a Secure Private Access gateway within the same resource location.



- **Gateway for DaaS:** Citrix-managed gateway serves as the external access point for virtual applications and desktops hosted within the Citrix DaaS™ environment. This gateway acts as a secure proxy, mediating and managing the HDX connections between the clients (user devices) and the virtual desktop agents (VDAs) residing in Citrix Cloud.

  You can choose how you want to allow access to virtual apps and desktops based on different business requirements.

- **Gateway for Secure Private Access:** The gateway for Secure Private Access ensures that organizations maintain control over sensitive data by routing all data traffic through an on-premises NetScaler Gateway, ensuring that it remains within the company's network perimeter.

While the on-premises NetScaler Gateway handles the data traffic, Citrix Cloud can be used for centralized management and monitoring capabilities, allowing administrators to oversee and manage applications and users seamlessly.

Perform the following steps to connect to a gateway:

1. Sign into Citrix Cloud.
2. Select **Resource locations > Overview** and then click **Gateway**.
3. In **Choose Gateway type**, select **Gateway for Secure Private Access**.
4. Register your gateway with Citrix Cloud. For details, see Register your NetScaler Gateway with Citrix Cloud.

Register your NetScaler Gateway with Citrix Cloud

You must first select the gateway for Secure Private Access and then register the on-premises NetScaler Gateway with Citrix Cloud. This registration establishes a secure connection between your on-premises NetScaler Gateway and the Citrix Cloud environment for the Secure Private Access service.

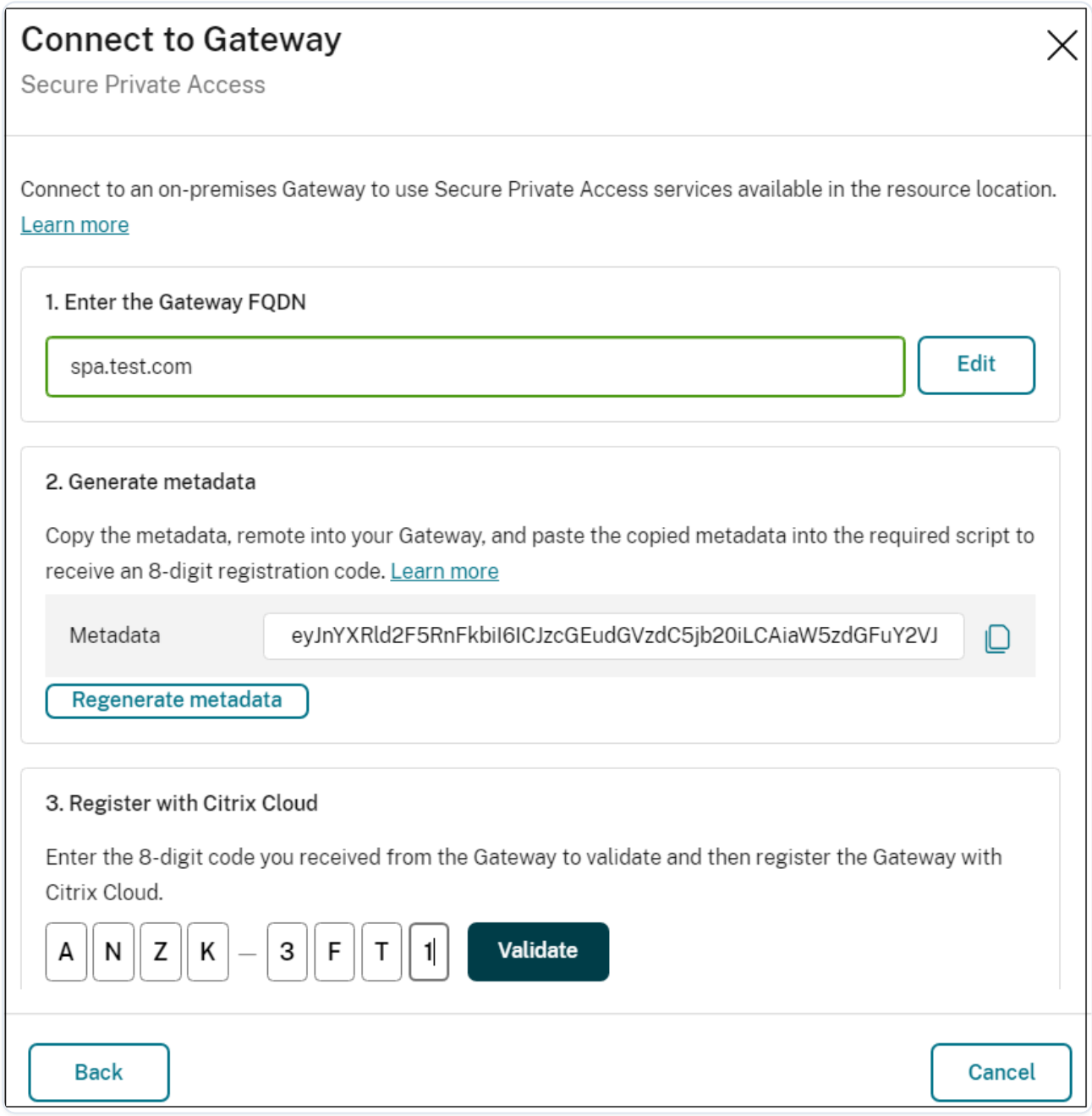
Prerequisites:

Ensure that the following configurations are complete for successful execution of the registration script:

- A subnet IP (SNIP) must be configured on NetScaler.
- A DNS name server must be configured, if not already present.
- An IP address designated for the new VPN virtual server is required.
- The SSL certificate key name for binding to the new VPN virtual server must be specified. This SSL certificate key name must be added to NetScaler before script execution.

Perform the following steps to register your gateway with Citrix Cloud:

1. Sign into Citrix Cloud.
2. Select **Resource locations > Overview** and then click **Gateway**.
3. In **Choose Gateway** type, select **Gateway for Secure Private Access**.



1. Enter the FQDN of the gateway to register with Citrix Cloud.
2. Click **Generate metadata**. You can also regenerate the metadata by clicking **Regenerate metadata**.
   - Copy the metadata into a clipboard.
   - Establish a secure shell (SSH) connection to the NetScaler Gateway located within the on-premises environment. This connection enables you to run the commands and scripts remotely on the NetScaler device.
   - After successfully connecting to the NetScaler Gateway, run the following command:

     ```
     python3 /var/spa/scripts/spa_registration.py <copied metadata>
     ```

- Replace `<copied metadata>` with the actual metadata that you copied earlier.

  The script generates an 8-digit registration code. This code is critical for the registration process.

3. Enter the 8-digit code in the **Register with Citrix Cloud** section.
4. Click **Validate**.

   A warning message appears if the code is invalid. If the validation is successful, the **Register** button appears.

5. Click **Register**.
6. Return to the script execution window. The system must move to the next step and prompt you for the following details for completing the configuration.

   - An IP address designated for the VPN virtual server.
   - The SSL certificate key name to be associated with the VPN virtual server.

You can now configure the routing of applications through the on-premises NetScaler.

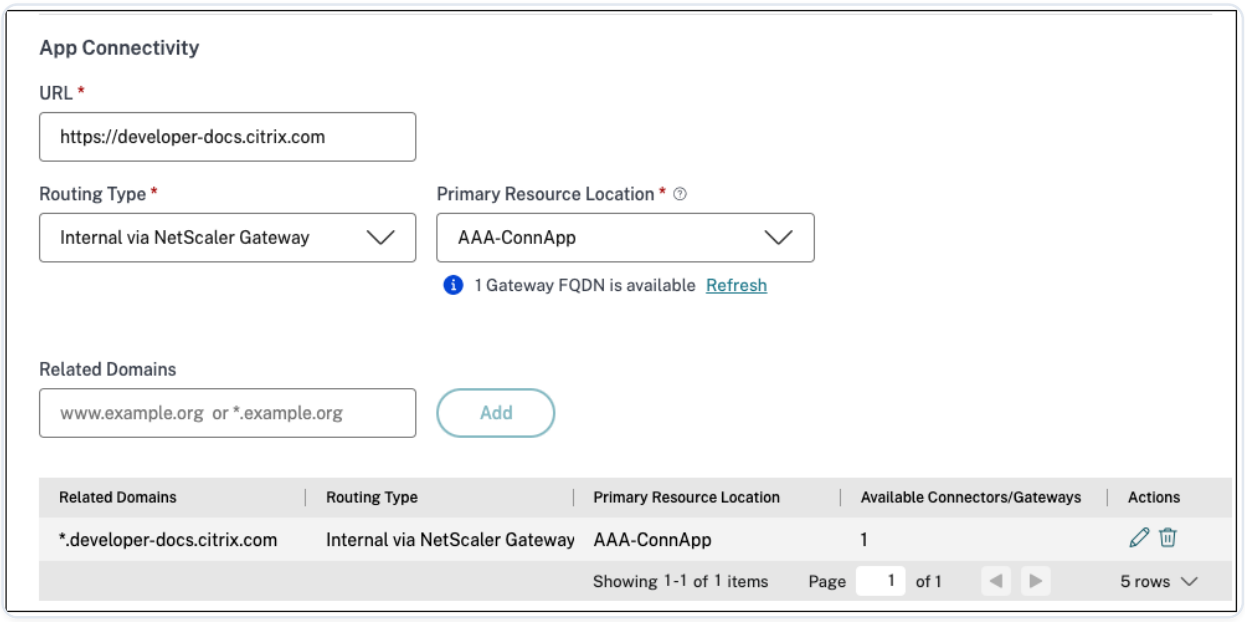
Enable routing of data traffic through the on-premises NetScaler Gateway

Perform the following steps to enable routing of data traffic through on-premises NetScaler Gateway.

1. Configure the app. For details, the following topics:

   - Support for Enterprise web apps
   - Agentless access to Enterprise web apps
   - Support for Software as a Service apps
   - Support for client-server apps

2. In the **App Connectivity** section, you define the routing preferences for the application domains, specifying whether traffic must be routed externally or internally through the Citrix Connector™ Appliance or through the on-premises NetScaler Gateway.



3. In **Routing Type**, select **Internal via NetScaler Gateway**. This ensures that data traffic is routed through the on-premises NetScaler Gateway. You can also update the routing type to **Internal via NetScaler Gateway** for the related domains.

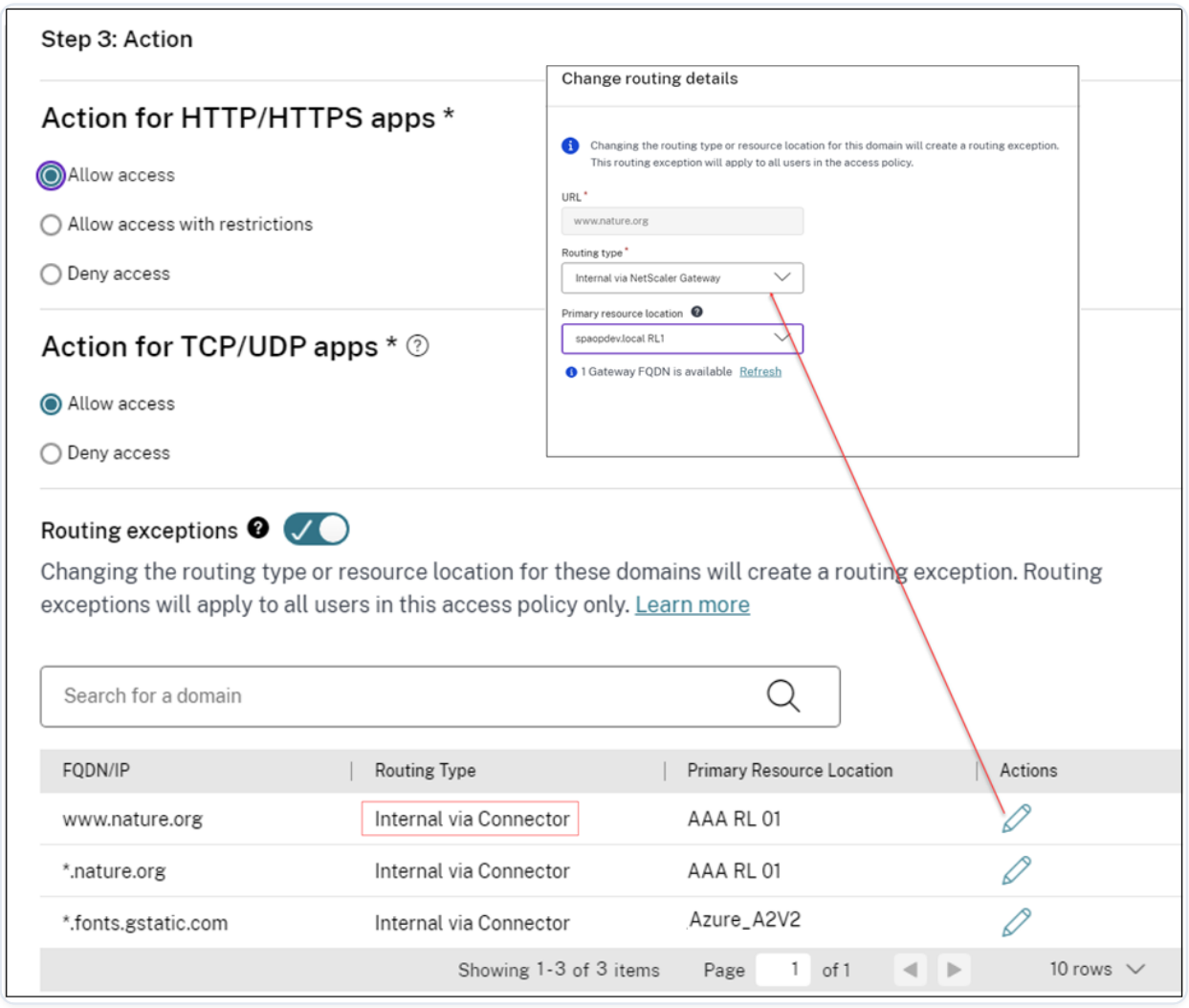
   - Click the edit icon in the **Actions** column of the **Related Domains** table.
   - In **Routing Type**, select **Internal via NetScaler Gateway**.
   - Click **Save**.

Modify the routing details from access policies

You can override the routing behavior to vary based on a specific context. These contexts can include factors such as user groups, geographical location, platform, and other relevant criteria. By modifying the routing behavior based on the context, you can provide an optimized user experience.

Perform the following steps to modify routing of data traffic through on-premises NetScaler Gateway from the access policy.

1. Create or edit an access policy. For details, see Create access policies.



2. In **Step 3: Action** page, enable the **Routing exceptions** toggle. The **Routing exceptions** toggle allows you to edit the resource locations and routing information for domains of the applications added in the access policy.
3. Click the edit icon next to the domain for which you want to modify the routing type.
4. In **Routing type**, select **Internal via NetScaler Gateway**.
5. Click **Save**.

Limitations

- Supported NetScaler Gateway deployment types - The hybrid data path is currently supported only for environments with a high availability setup.
- Fallback mechanism - In the current release, there is no failover or fallback mechanism that automatically redirects traffic to the cloud infrastructure in the event that the on-premises gateway experiences an outage or becomes unavailable.
- The following features are not supported for hybrid data path in the current release:
  - Application discovery

    - Policy modeling
    - Session policies
    - Observability

- The /var/spa/scripts/ folder is created when you run the `installns` script for installing a NetScaler build. This folder is not present on newly deployed NetScaler VPX instances and must be created through the installation process. For more information, see the following topics:
    - Upgrade a NetScaler standalone appliance
    - Upgrade a high availability pair

Issue with Secure Private Access registration script

The Secure Private Access registration script does not run directly on a newly deployed VPX instance on Azure due to a configuration issue with some built-in commands. To resolve this issue, follow these steps:

- Provision a new VPX instance on Azure.
- Don't add any new configuration.
- Set a new password for the nsroot user using the command `set system user nsroot <your-password>`. This step is important as the custom user created during provisioning is deleted after the `clear config` command is run. You can access the NetScaler using nsroot and this new password.
- Save the config using the command `save config`.
- Check the output of `show cache policylabel`. It must be empty.
- Run the command `clear config basic` and type Y.
- Check the output of `show cache policylabel` again. It must show _reqBuiltinDefaults as a label.

```
show cache policylabel



Label Name: _reqBuiltinDefaults

Evaluates: REQ
```

```
Number of bound policies: 3

Number of times invoked: 02)  Label Name: _resBuiltinDefaults

Evaluates: RES

Number of bound policies: 8

Number of times invoked: 03)  Label Name: _httpquicReqBuiltinDefaults

Evaluates: HTTPQUIC_REQ

Number of bound policies: 3

Number of times invoked: 04)  Label Name: _httpquicResBuiltinDefaults

Evaluates: HTTPQUIC_RES

Number of bound policies: 8

Number of times invoked: 0Warning: Feature(s) not enabled [IC]
```

- If you don't see _reqBuiltinDefaults in the command's output, reach out to Citrix support.
- Configure the SNIP, SSL certificate key, and DNS name server.
- Save the config using the command `save config`.
- Run the Secure Private Access registration script again.

Discover applications, domains, or IP addresses within your network

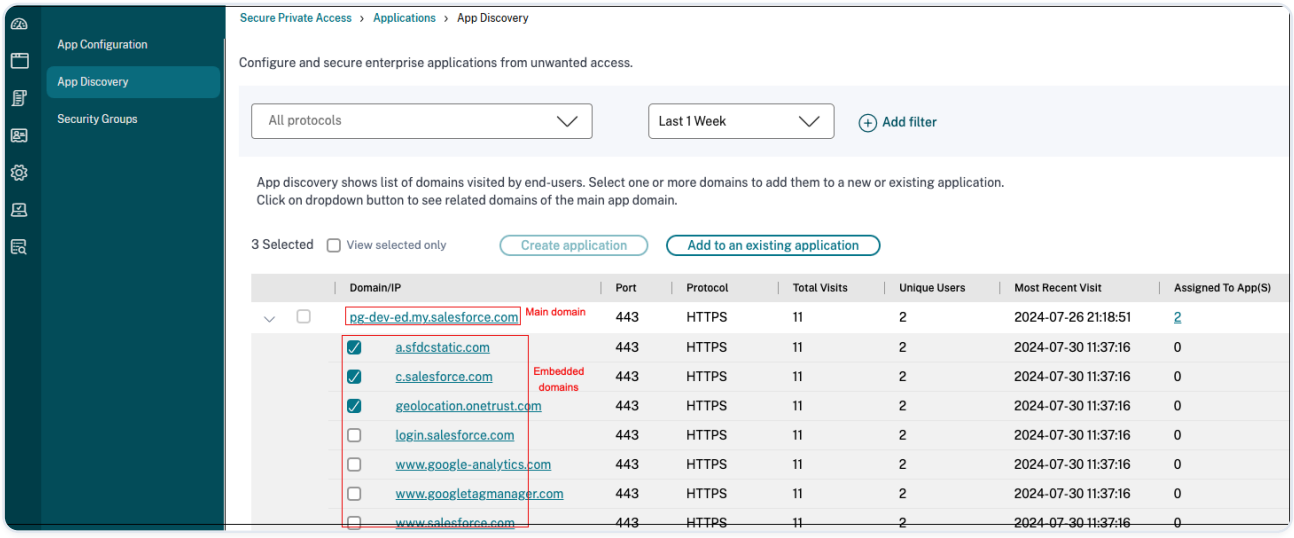
The Application Discovery feature helps an admin get visibility into the external and internal applications (HTTP/HTTPS and TCP/UDP apps) that are being accessed in an organization. This feature discovers and lists all the domains/IPs addresses, published or unpublished. Thus, admins can see what domains/IP 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). All access methods are supported, that is access via Citrix Enterprise Browser™, Secure Access Agent, Direct Access, or from a store.
- Displays both published or unpublished domains/IP addresses accessed by the end users.
- Displays both the main domain and its underlying embedded domains that are required to be configured as related domains while publishing the applications for access made via Citrix Enterprise Browser.
- Displays the embedded domains in a tree structure. Admins can click the expand sign (**>**) in line with the main domain to view the embedded domains.
- Enables admins to create new applications or add those domains to an existing application if a main domain or an embedded domain (HTTP/HTTPS) or the destination IP address (TCP/UDP) is not associated with an application.

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. You can see a main domain with a drop-down list of embedded domains underneath it. These domains must be configured as related domains while publishing the application.



Note:

- Embedded domains are grouped under the main domain only for HTTP/HTTPS apps accessed via Citrix Enterprise Browser. TCP/UDP domains are not grouped under one main domain.

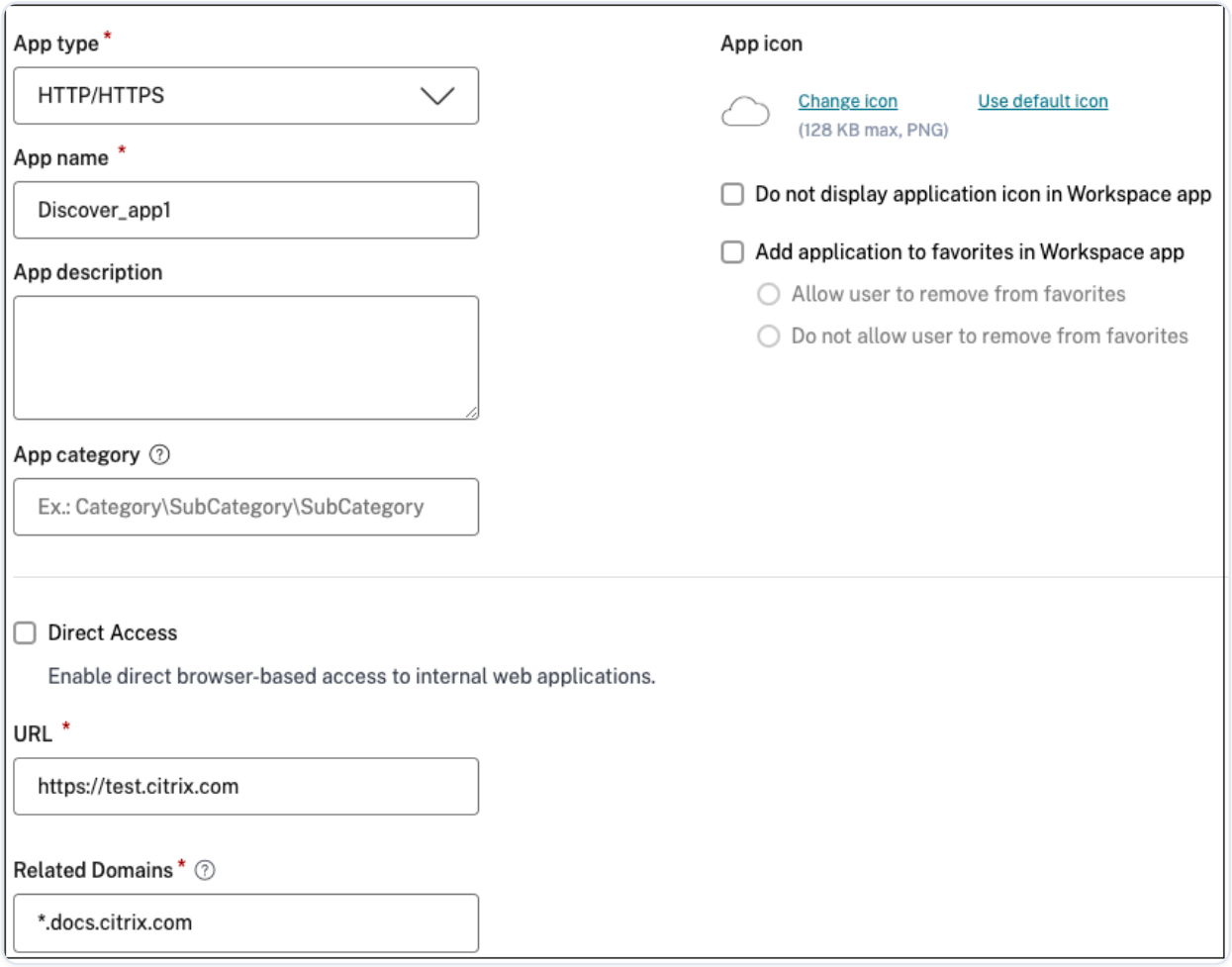
- Grouping of embedded domains is only available for apps accessed from Citrix Enterprise Browser (v119 and later).

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.

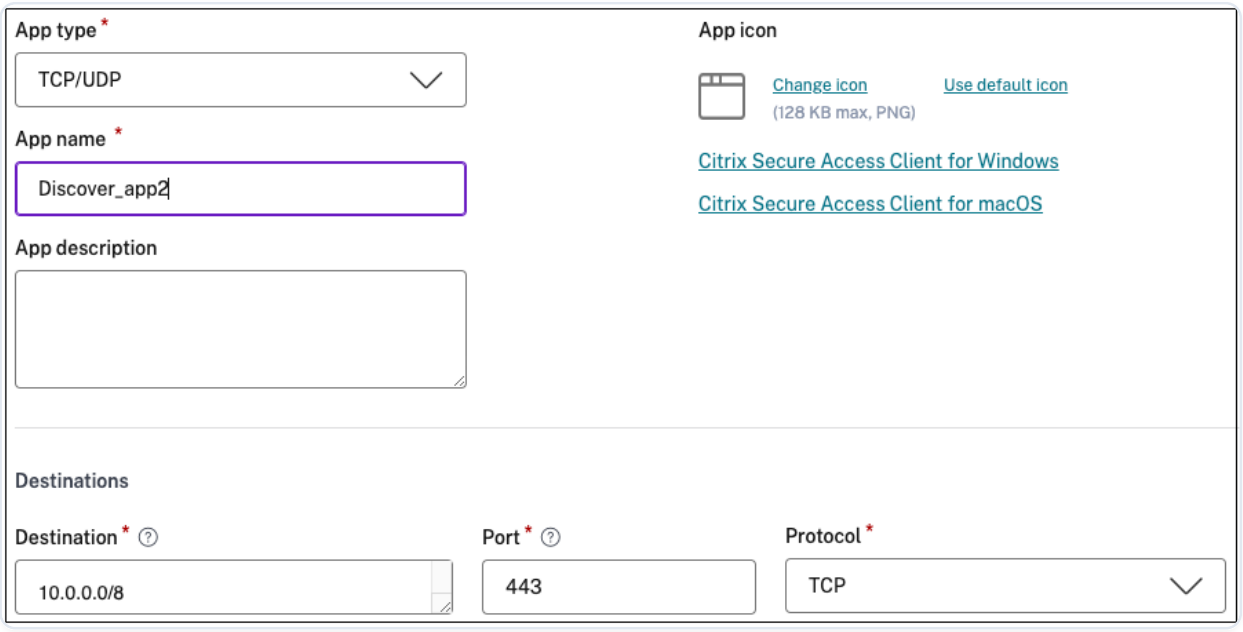


Web app URL: `https://test.citrix.com/` Related domain: `*.citrix.com`

- 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.

- Support for Enterprise web apps
- Support for Software as a Service app
- Support for client-server apps

Create an application from the App discovery page

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

1. Navigate to **Applications > App discovery**.
2. Select a domain from the list. If the domain has embedded domains, then click the expand sign (**>**) in line with the main domain and select the embedded domains.

   Note:

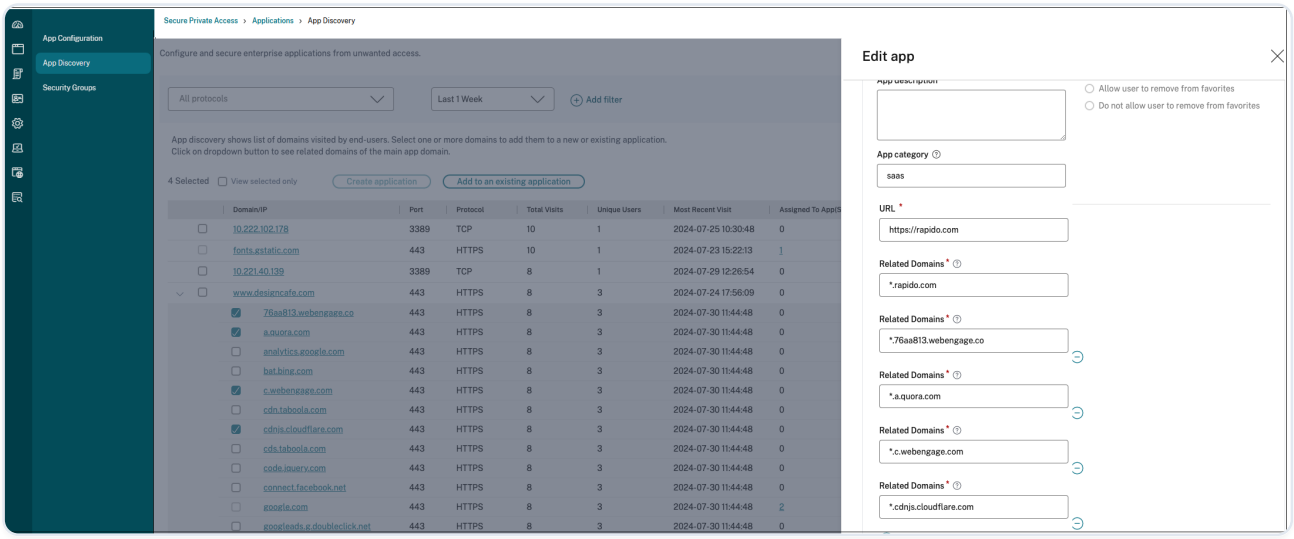
- You cannot select domains belonging to different protocols to create an application. An error message is displayed when you select domains belonging to different protocols.
- If a domain is already associated with an application, you cannot select that domain again to create an application. The checkbox corresponding to that domain appears grayed out and when you hover the mouse over the checkbox and a tooltip appears.
- You cannot select and add embedded domains grouped under different main domains to an application. The Application Discovery feature only allows embedded domains grouped under a single main domain to be added to an app. An error message appears if embedded domains from different main domains are selected and added to the same app.

3. Click **Create application**. For details on creating an application, see Support for Enterprise web apps, Support for Software as a Service app, and Support for client-server apps](/en-us/citrix-secure-private-access/service/spa-support-for-client-server-apps.html).

Update an existing application

To add a domain to an existing application, select the domain from the list. If the domain has embedded domains, then click the expand sign (**>**) in line with the main domain and select the embedded domains.

1. Select the embedded 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 embedded domains that you selected earlier in separate rows.
6. Click **Finish**.

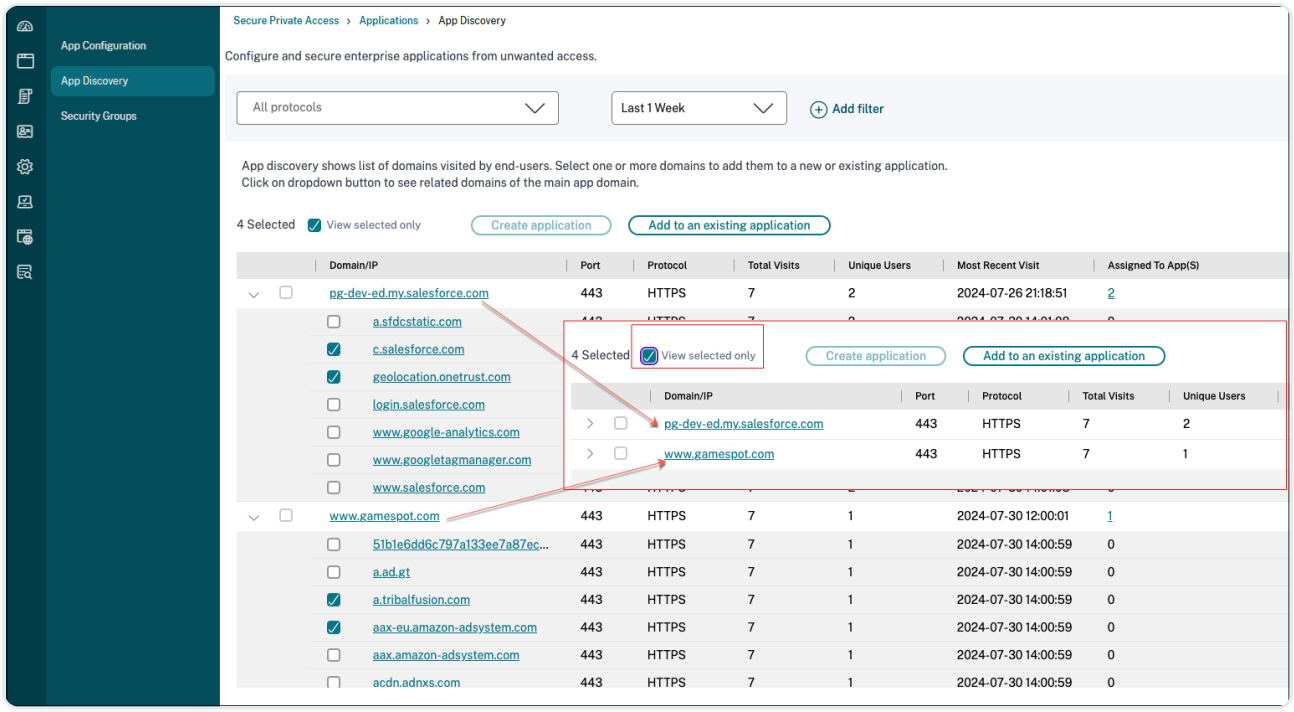


Note:

- 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, single entry, or embedded) whose protocol is HTTP/HTTPS.
- You cannot select a domain that is already associated with an application.

View all selected embedded domains

After you select the domains, you can click the **View selected only** checkbox and proceed with creating or updating the application. Also, If the list of FQDN/IP addresses on the App discovery page spans across multiple pages, you can use the **View selected only** checkbox to view all the main and embedded domains that you have selected to create or update the application. All the main domains of the selected embedded domains are displayed when this checkbox is selected.



Known limitations

- Although the **Create application** and **Add to existing application** options are available in the Secure Private Access dashboard (**Top discovered applications by total visits** chart), it is recommended that you create or update an application from the **App discovery** page (**Applications > App discovery**). This is because, while adding or updating an application from the dashboard and you cancel the operation, the page is reloaded and as a result, all settings are reset.
- Sometimes, you might notice the expand sign (>) against a main domain, but the embedded domains are not fetched for that specific FQDN. This issue can occur in the following cases:
  - Error loading the main webpage due to some access restrictions for the users.
  - An error preventing the loading of the webpage.
  - Caching of the embedded domain resources by Citrix Enterprise Browser, causing the embedded domains not to be fetched from the source.

Context-based app routing and resource location selection

When an app is configured, the app URL and related domains are assigned to a routing type and resource location. This is done during app configuration. This configuration for app routing and resource location then applies to all users who have access to the app. But there might be scenarios such as the following:

- An admin wants to route the same app differently for different users. For example, an internal app URL must be routed externally for a few users to prevent traffic from being routed to the Secure Private Access service.
- There is a need to use different resource locations for different users to route requests to the optimal data center to improve performance.

This can now be done within the access policies using routing exceptions. The routing exceptions configuration in the access policy allows admins to edit the internal routing type per URL or resource location based on the user context. Because this setting is within the access policies, it applies only to the users that are part of that access policy only.

You can also dynamically route entire sessions using **Session Policies**. For details, see Route internal corporate users directly to back-end applications.

> **Note:**
>
> If there is a routing and resource location configuration within an access policy, then it overrides the app configurations.
>
> The following examples demonstrate the routing exception use cases.

- Context-based routing
- User context-based resource location selection
- Route internal corporate users directly to back-end applications

Use case: Context-based routing

Scenario:

- Group A users: Employees of company ABC who access the Outlook app and Microsoft Teams app through Secure Private Access that is routed internally.
- Group B users: Employees of a third-party company working with ABC. They access certain applications (excluding Outlook) through Secure Private Access. They also have their own Outlook application accessed over the internet and do not want to route their Outlook traffic through Secure Private Access.

Problem:

- Group B users log in to the Secure Access Agent to access ABC apps.

- Their requests to access Outlook through their native browser are routed through Secure Private Access, resulting in access denial.
- The destination domain for the Outlook application is the same for both Group A and Group B users.
- The access policy allows access only for Group A users, causing access denial for Group B users when they try to launch Microsoft Teams or Outlook.
- Group B users cannot access their company Outlook because of this routing issue.

Solution:

The ABC company admin can make the following configuration changes to resolve this issue:

1. Define a new access policy specifically for Group B users accessing the Office 365 app.
2. In the access policy, enable the **Routing exceptions** option.

   The admin can view the list of all URLs and related domains of all internal apps associated with the access policy.
3. For all Office365 app URLs, configure the routing to happen externally.

   This ensures that Group B users' requests to access their Outlook application are routed over the internet, bypassing Secure Private Access.

   By implementing these changes, Group B users can access their company Outlook application over the internet without being routed through Secure Private Access, while still maintaining access to other ABC applications as needed.

Use Case: User context-based resource location selection

Scenarios:

- Company XYZ: It has two sets of users located in the US East Coast and the US West Coast.
- Data centers: Two data centers, one on the East Coast and one on the West Coast, both hosting the same Jira application.
- Objective: The admin wants to route the access requests of end users to the selected resource locations based on user context (geo location, network location, user name, and user group) to ensure optimal performance and routing.

Solution:

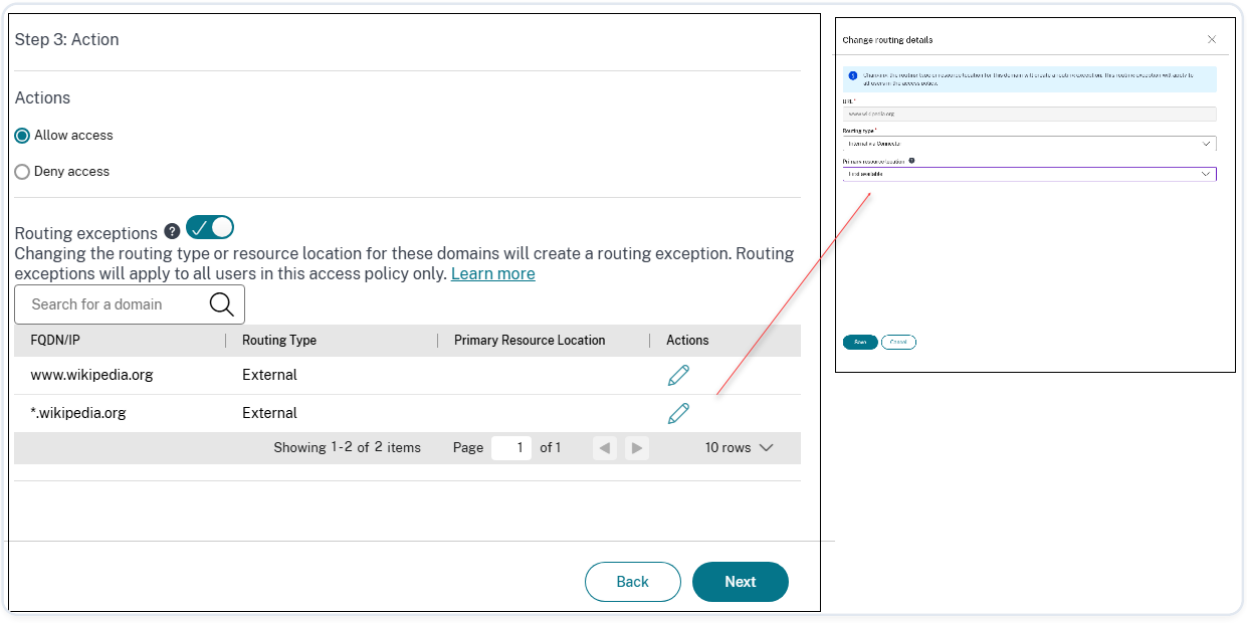
1. Edit the access policy associated with the Jira application to accommodate the new routing requirements.
2. Within the access policy, enable the **Routing exceptions** option.
3. Modify the resource locations per user context.

The admin can ensure that user requests are routed to the optimal data center based on their context, thereby improving performance and managing routing effectively for all users in the company.

Steps to change the routing type or resource location

1. Create or edit an access policy. For details, see Create access policies.
2. In **Step 3: Action** page, enable the contextual routing domain configuration by sliding the **Routing exceptions** toggle switch. The **Routing exceptions** toggle allows you to edit the resource locations and routing information for domains of the applications added in the access policy.

   - **When the toggle is ON:** A list of all the apps' URLs and related domains is displayed in a tabular format along with their global routing and resource location configuration. This list contains the URLs and related domains of all the applications added in the access policy. You can click the edit icon next to a domain to modify its resource location and routing type. This routing exception is applicable to all the users in the access policy only.
   - **When the toggle is OFF:** Existing routing exceptions for the domains are removed and are not applicable. End users are routed based on the global configuration set during the application setup only.

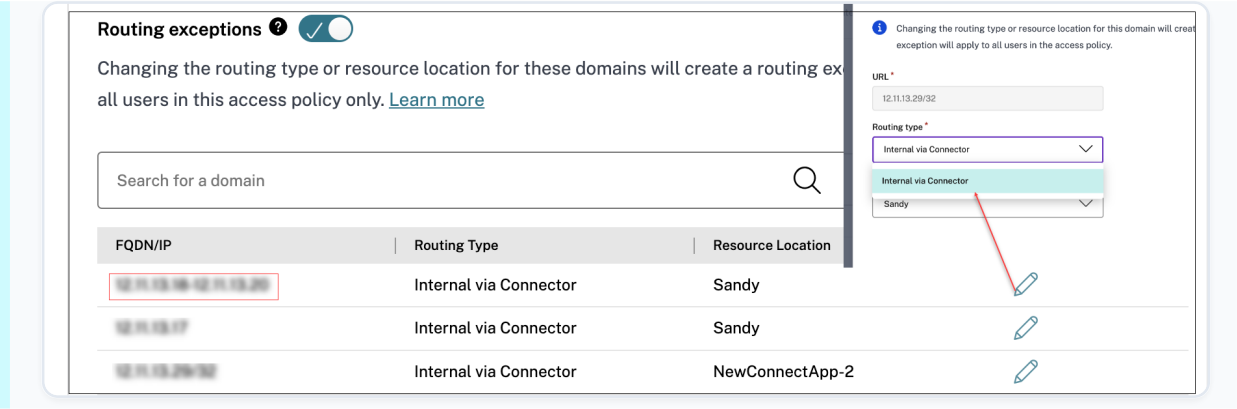


3. Click the edit icon next to the domain for which you want to modify the routing type.
4. In **Routing type**, modify the routing type:
    - **Internal:** The traffic flows via the Connector Appliance.
        - For a web app, the traffic flows within the data center.
        - For a SaaS app, the traffic is routed outside the network through the Connector Appliance.
    - **Internal – Bypass Proxy:** The domain traffic is routed through Citrix Cloud Connector™ appliances, bypassing the customer's web proxy configured on the Connector Appliance.
    - **External:** The traffic flows directly to the internet.
    - **External via Google Secure Gateway:** The traffic flows to the internet through the Google Secure Gateway.

    > **Note:**
    >
    > This routing type applies only to SaaS apps for customers integrated with Google Chrome Enterprise Premium in Secure Private Access cloud and hybrid deployments.

5. In **Resource location**, modify the resource location, if necessary. This option is applicable only for the internally routed domains.

    > **Note:**
    >
    > If an app is created using an IP address, you cannot modify the routing type to **External** as only the **Internal via Connector** option is displayed in the **Routing type** list. You can only modify the resource location. However, this restriction does not apply to apps created using an FQDN.



6. Click **Save**.

Note:

- You can only change the routing and resource location, but cannot add or delete routing domain in the routing table.
- If you delete a domain that has contextual routing enabled from the main routing table, the domain is not deleted from the **Routing exceptions** table within the access policy. This means that the contextual routing configuration for that domain remains intact in the access policy.
- If you delete an app that has contextual routing enabled, then the domain is deleted from the **Routing exceptions** table within the access policy. This means that all contextual routing configurations associated with that app are removed from the access policy.
- The selected related domain overwrites the default setting when the condition meets for the users that are part of this access policy. Otherwise the default routing is applied.
- If the routing is not modified or if the **Routing exceptions** feature is not enabled, the routing happens based on the default settings in the main routing table (**Settings > Application domain**).

Use case: Route internal corporate users directly to back-end applications

Admins can configure session policies to route internal corporate users directly to back-end apps without tunneling traffic through Secure Private Access. Session policies offer dynamic routing based on factors, such as network location and device posture. For details, see Session policies.

Contextual routing insights in Monitor

Contextual routing can lead to dynamic changes in application routes. For instance, an application might be routed through the Secure Private Access service when the user is outside the corporate network, but directly to the app when the user is internal. Providing administrators with visibility into these routing decisions is crucial for troubleshooting routing issues.

The **Application Topology** page in DaaS Monitor provides comprehensive insights into routing decisions and policy details of the Secure Private Access applications accessed through the Citrix Secure Access client. These insights enable the administrators to troubleshoot routing issues efficiently and thus enhance the user experience.

The following details related to application routing are captured in the **Application Topology** page:

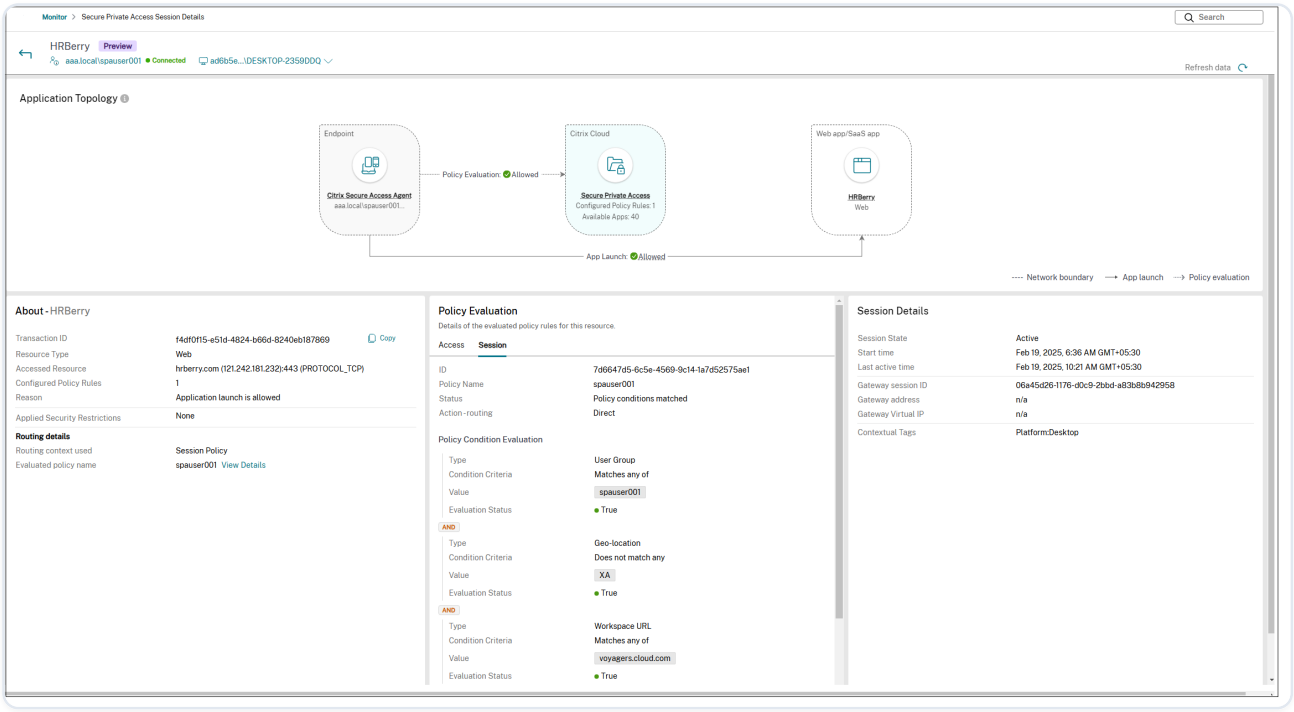
- **Routing context:** The **Routing context** field in the **About** section specifies the policy type (access policy, session policy, or application domain) applied during routing. The routing context helps identify the precedence hierarchy (access policy > session policy > default application configuration) influencing routing decisions.

  For session policy, the **View details** link provides additional details about the session policy.
- **Action-routing:** The **Action-routing** field in the **Policy Evaluation** section displays the routing path (**Direct, Internal via connector, Internal via gateway**) that a user's request takes through the Secure Private Access service.

> **Note:**

> When the default application domain (application configuration) routing is applied, the **Policy Evaluation** section displays the policy details but the **Action-routing** field displays the value **n/a** as no policy is enforced in this scenario.

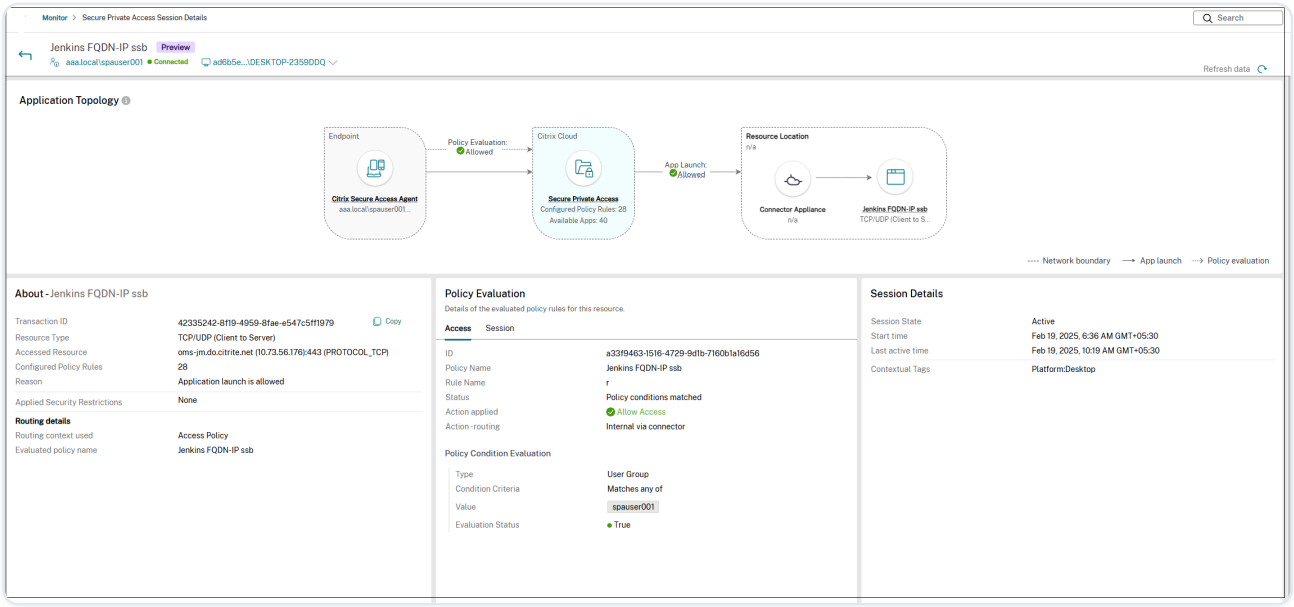
> The following figure displays a topology diagram of an application whose routing type is defined as direct and hence the traffic does not pass through the Secure Private Access service.



Note:

For the Web apps tunneled through the Citrix Secure Access client, the topology diagram displays the resource location name and the connector name.

The following figure displays a topology diagram of an application whose routing type is defined to be internal through the Secure Private Access service using a connector.



For more information, see Integration with DaaS monitor.

Seamless access to local LAN resources (printers, file servers)

When employees are connected through Secure Private Access from their home or remote locations using Citrix Secure Access clients, they might lose the ability to access local network resources if the private IP address range conflicts with published corporate apps. Secure Private Access supports seamless access to local LAN resources while maintaining a secure connection to corporate resources.

For example, if a home printer is configured with IP address 192.0.2.0 and corporate applications are configured with the private IP address 192.0.2.0/30 range, then when a user tries to access the printer, the printer traffic is tunneled through SPA as well which results in an error. By enabling local LAN access, the user can access printers through local LAN without disconnecting the Citrix Secure Access client.

Note:

- Admins can enable the local LAN access feature in session policies for all users or a set of users. For details, see Configure direct routing within the corporate network using session policies.
- If users enable the local LAN access feature when logging in to the Citrix Secure Access client, they can access local LAN resources like home printers, network-attached storage (NAS) devices while connected to Secure Private Access. This helps the user perform basic local tasks with minimal disruption.

Important considerations

- **Enabling local LAN access for all users:** Session policies are evaluated in the order of priority. If local LAN access is required for all users, then the **Local LAN Access** option must be explicitly enabled within each active session policy. When a user matches a session policy, evaluation stops at the first applicable policy. If that policy does not allow Local LAN access, then the user is not evaluated against other subsequent policies, even if those policies have the **Local LAN Access** option enabled.
- **Differences in handling printer traffic by the Citrix Secure Access client for Windows and macOS:** Citrix Secure Access for Windows prioritizes local LAN access. That is, if a printer's IP address conflicts with that of a corporate application, the Citrix Secure Access client for Windows might send the application traffic locally instead of sending it through Secure Private

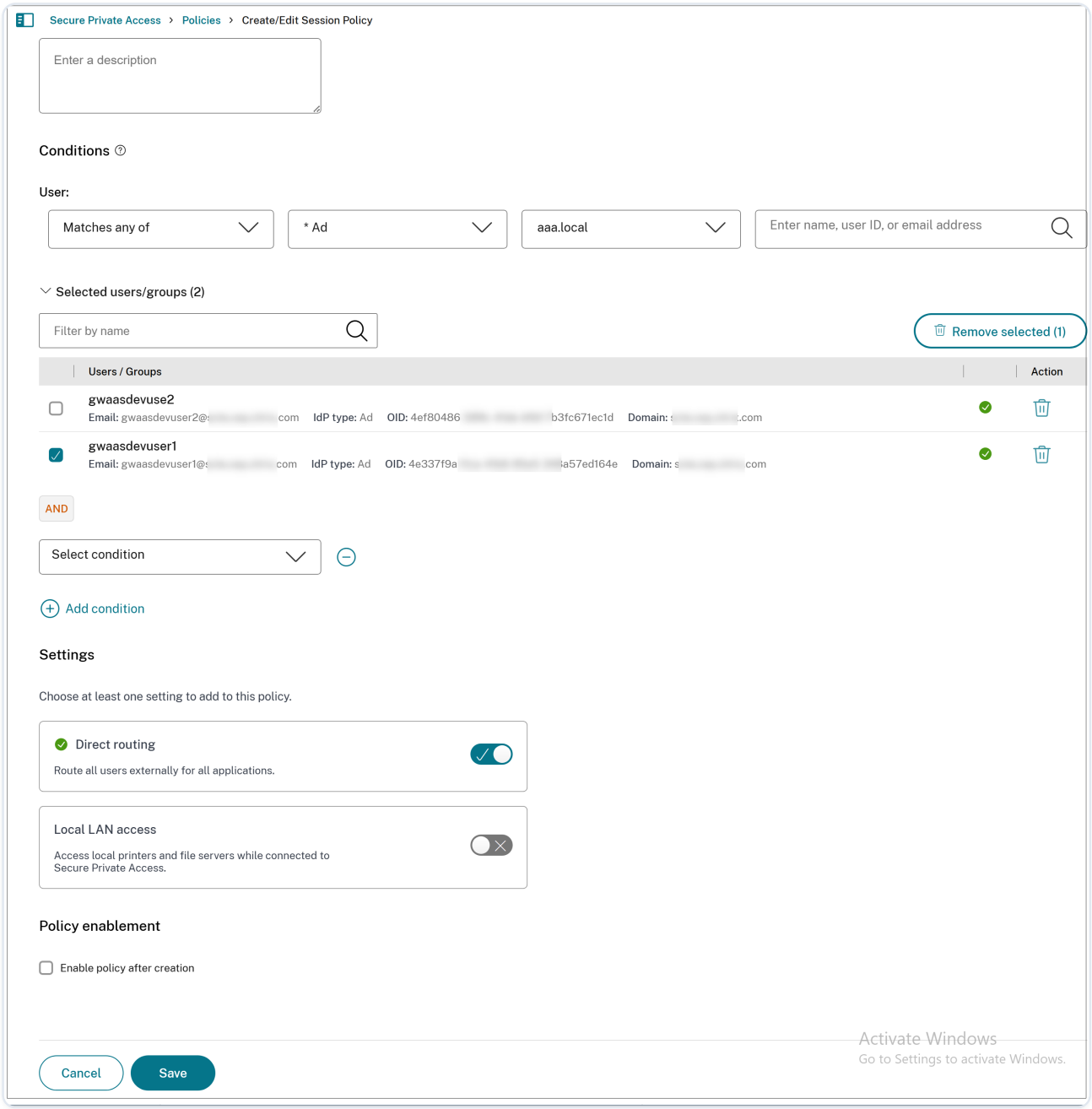
Access. In contrast, the Citrix Secure Access client for macOS can send the printer traffic to the local LAN while simultaneously tunneling application traffic over Secure Private Access.

- **Periodic update:** Because the local LAN access feature is session-specific, any configuration changes to the local LAN setting on the Windows filter (WFP) takes effect upon login and is maintained until logout. Periodic update is not supported.

Enable the local LAN access feature

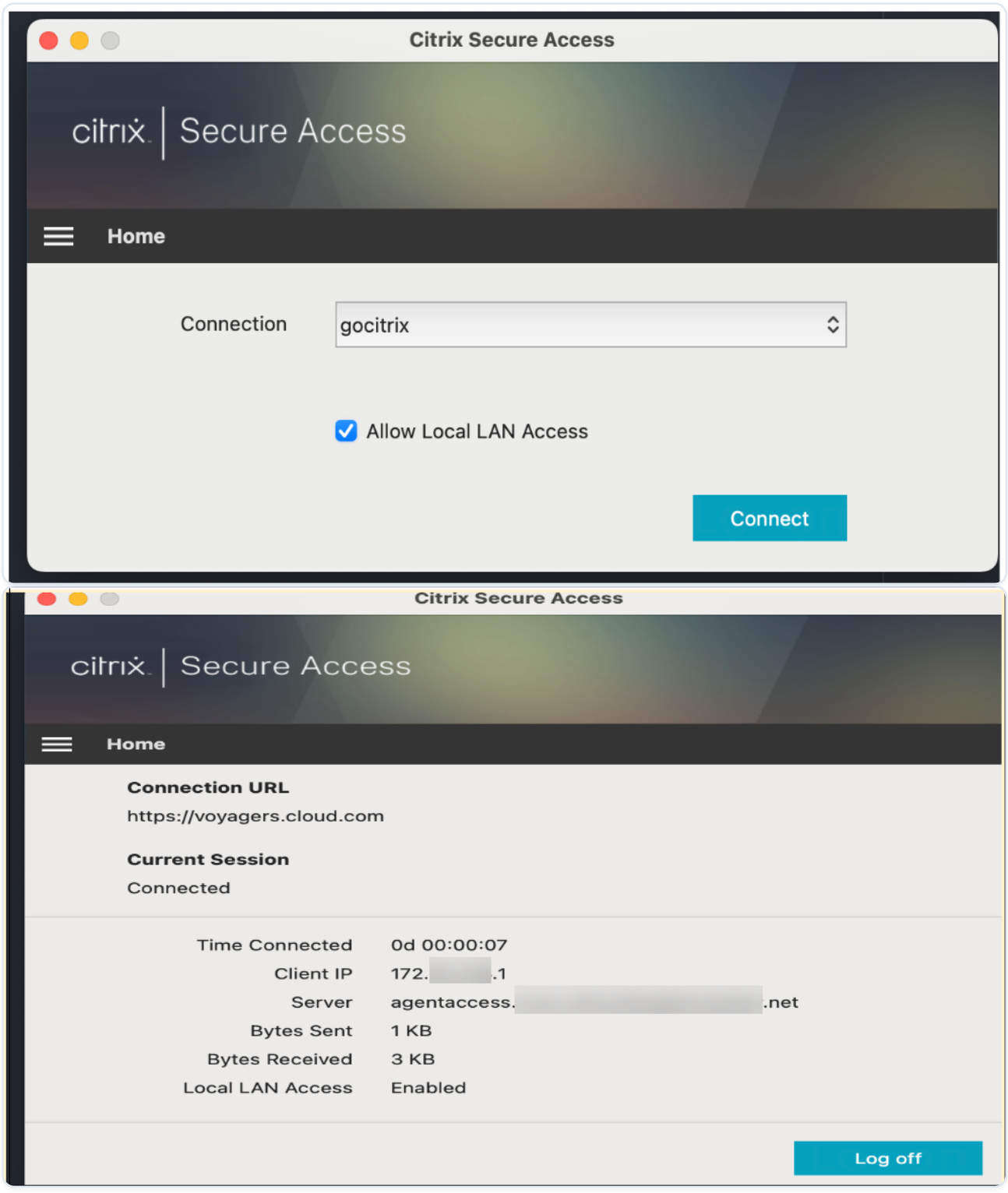
Secure Private Access admin console:

1. Navigate to **Policies > Session Policies** and click Create Session Policy.
2. Create a session policy. For details, see Configure direct routing within the corporate network using session policies.
3. Ensure that you select the **Local LAN access** option.



Citrix Secure Access client:

1. In the Citrix Secure Access client window, select **Allow Local LAN Access**.
2. Click **Connect**.



Policy modeling tool

When managing multiple applications and access policies, it can be challenging for administrators to determine the exact end-user access result. Whether a user is allowed or denied access to an application based on all current configurations.

The policy modeling tool, located under **Access policies > Policy modeling**, provides administrators with comprehensive visibility into expected app access outcomes (allowed, allowed with restriction, or denied) based on current configurations. Admins can check the access results for any user based on conditions such as device type, device posture, geo-location, network location, and store URL. Admins can also evaluate the access policies for specific application destinations.

Access the policy modeling tool

1. In the Secure Private Access console, click **Access Policies** and then click the **Policy modeling** tab.
2. The policy modeling tool user interface appears.
    - The **All Apps** tab is selected by default. This tab can be used for analyzing policies that are applicable across multiple users, user groups, or machines within the environment.
    - To understand how policies are enforced on specific network destinations, such as a specific website domain, an IP address, or a network port, you must use the **URL** or **IP/Port** tabs and enter the destination details.

Analyze policies for a set of users or machines

1. Select the **Users** or the **Machines** tab and enter the following details.
    - **Device type:** Select the device type of the end user. (Desktop is selected by default).
    - **Domain:** Select the domain associated with the user.
    - **Username or user group:** (Applicable only if you have selected the **Users** tab) Select the user name for which you want to analyze the applications and associated policies.
    - **Machine name:** (Applicable only if you have selected the **Machines** tab) Enter the machine name based on which you want to analyze the applications and associated policies.
2. To search for accurate results, add the exact user or machine conditions.
    - Click **Simulate conditions.**
    - Select the condition (Device posture, Geo-location, Network location, User risk score, and store URL) and then select the associated value.
    - Click the + sign to add more conditions.
    - Click **Apply.**

Analyze policies for specific destinations

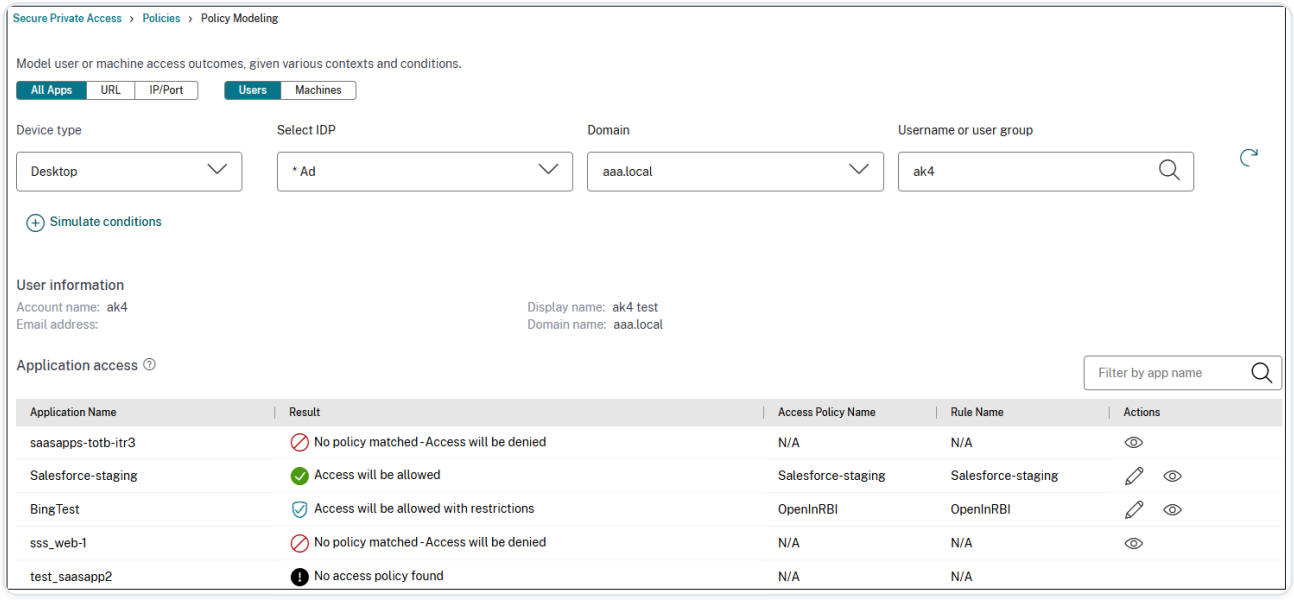
1. Click the **URL** tab for Web/SaaS applications and **IP/Port** tab for the TCP/UDP applications.
2. Enter the following details:

   - **URL:** The URL of the application for which you want to analyze the access policies.
   - **IP:Port:** The IP and port number of the TCP/UDP app for which you want to analyze the access policy. You can also enter the host name followed by the port number.

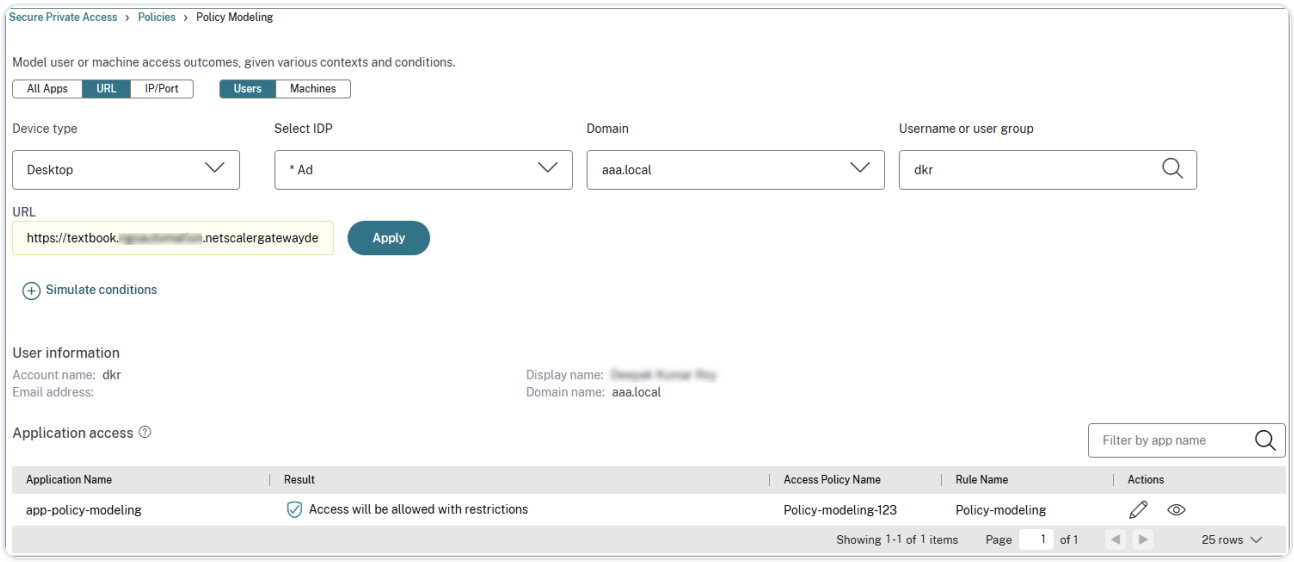
   Examples: 192.0.2.20:443; example.test.net:443
3. Click **Apply.**

The **Application Access** section displays the list of applications and the associated policies based on your search. An eye icon appears alongside the application for which an exact policy match or no policy match has occurred. The admins can also edit a policy for the apps for which access is allowed or access is allowed with restriction.

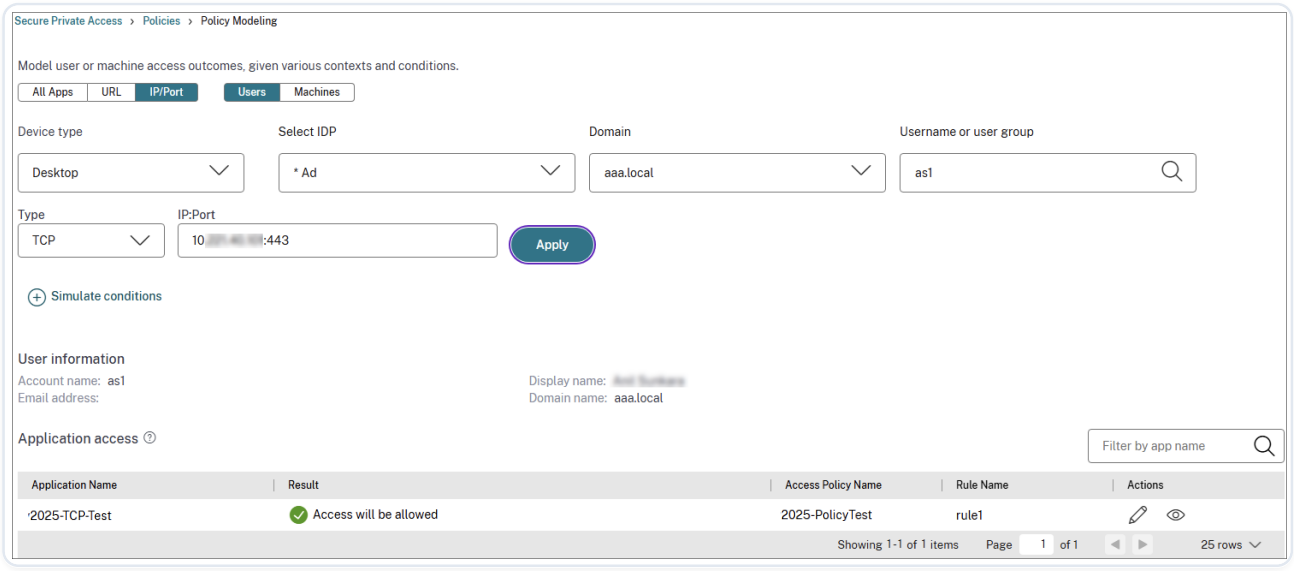
The following figure displays the policy analyzer for all apps:



The following figure displays the policy analyzer for a web app:



The following figure displays the policy analyzer for a TCP app:



Drill down into access policies

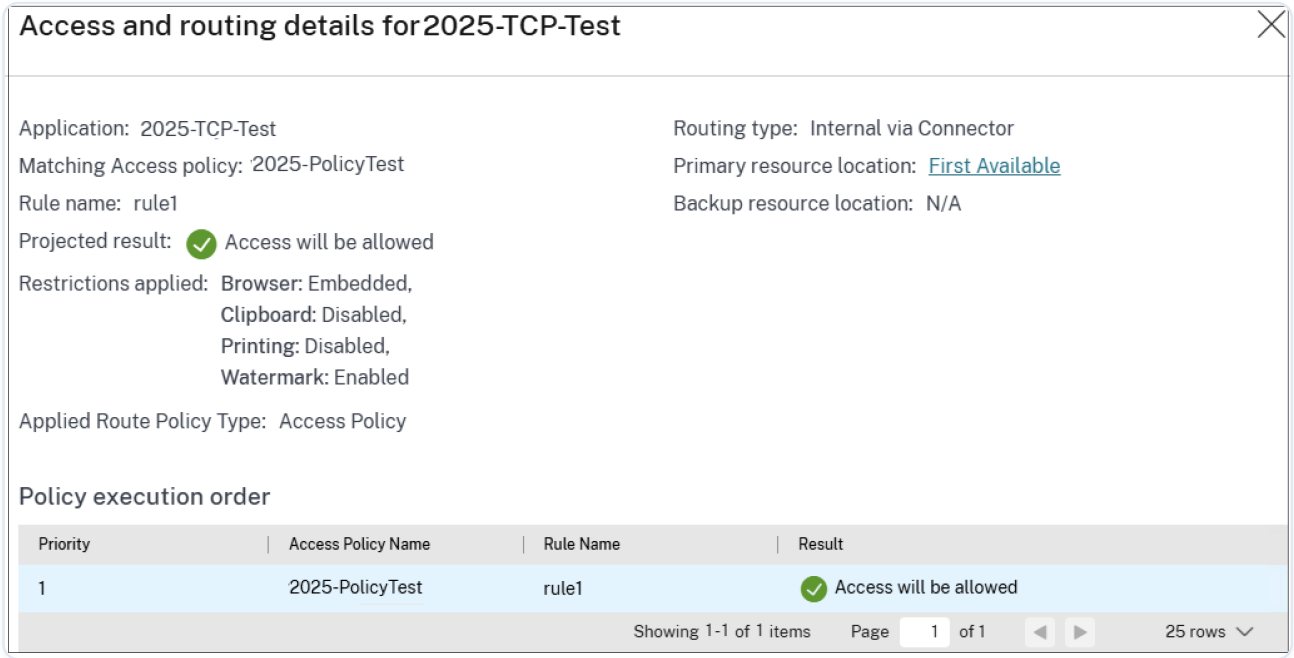
In the **Application Access** section, click the eye icon to view the access and routing details page. The **Access and routing details** page displays a comprehensive list of all relevant policies that influenced the access decisions for that application. This page displays the following information:

FIELD	DESCRIPTION
Application	Name of the application.
Matching Access Policy	The name of the access policy that has an exact match or major match with the application.

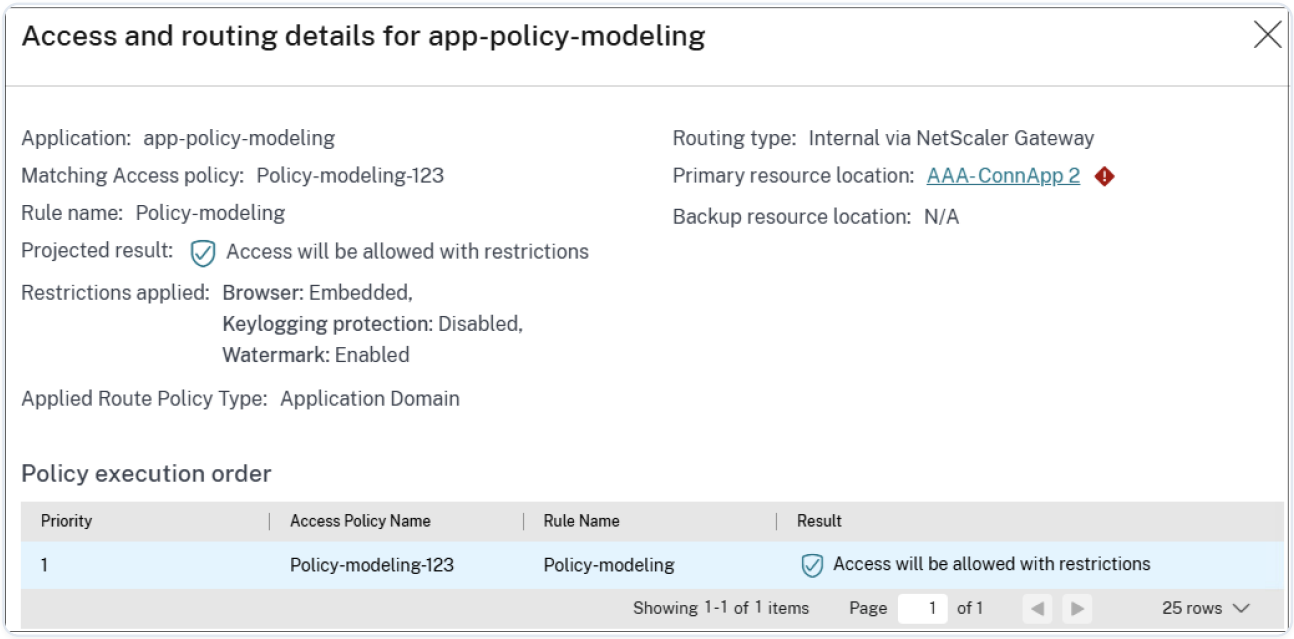
FIELD	DESCRIPTION
Rule Name	The specific rule associated with the matching policy.
Projected Result	The action determined based on the policy evaluation (for example, allow, deny, allow with restriction).
Restrictions Applied	Access restrictions, if any, enforced on the application.
Applied Route Policy Type	Indicates the type of policy that determined the applications routing behavior. The policy type is access policy, session policy, or application domain.
	Identifies the hierarchy in routing decisions. The precedence order being access policy (highest priority), followed by session policy, and then the default application domain (lowest priority).
Routing Type	The routing type details the path a user's request takes through the Secure Private Access service.
	External Requests are routed directly to the intended destination.
	Internal via Connector Requests are routed through a Connector.
	Internal via Gateway Requests are routed through NetScaler Gateway. This routing type is applicable only for hybrid data path that is supported with the Citrix Secure Access client. For details, see Hybrid data path for Secure Private Access services.
Primary Resource Location	Name associated with the primary location of the application.

FIELD	DESCRIPTION
Backup Resource Location	Name of the backup location (if configured).

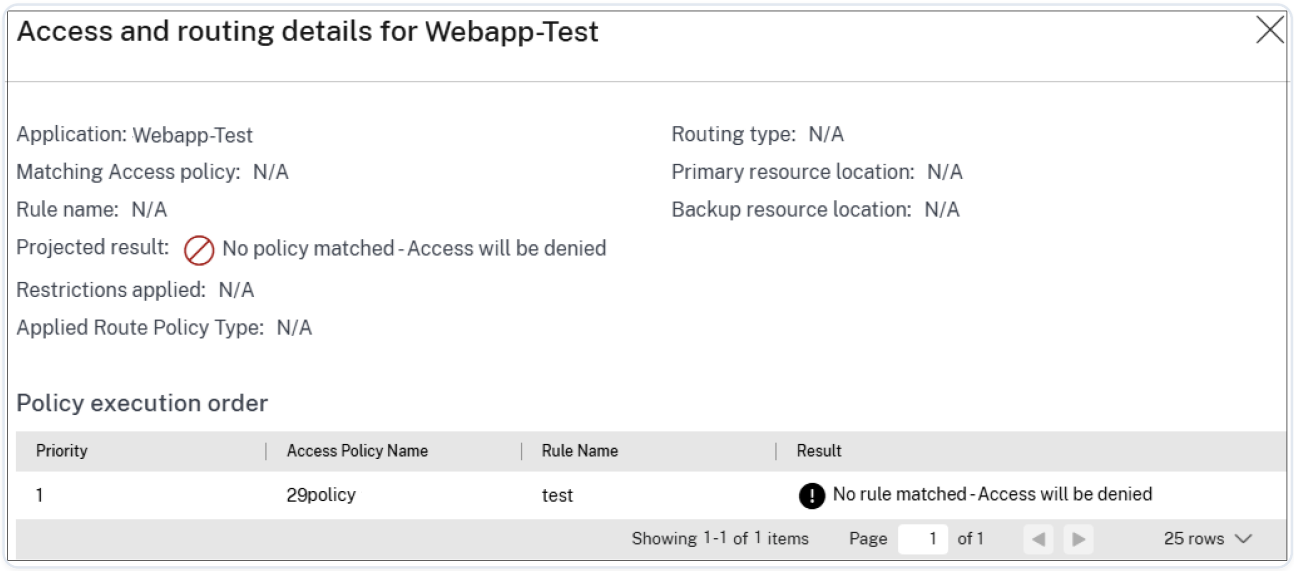
The following figure displays the policy drill-down results for a TCP app for which access is allowed.



The following figure displays the policy drill-down results for a web app for which access is allowed with restrictions.



The following figure displays the policy drill-down results for a web app for which access is denied:



Applications import tool - Preview

The Secure Private Access admin console includes a file import tool that allows administrators to bulk import multiple applications into the system using a CSV file or the nsconfig file. This tool is especially useful for organizations shifting from a traditional VPN to a more advanced solution like Secure Private Access. For example, organizations can use this tool to migrate applications that were delivered over a VPN to Secure Private Access and shift to a ZTNA-based architecture. Bulk upload of apps enables the organizations to eliminate the need for manual configuration.

- **CSV file:** You must ensure that all relevant application details are included within the CSV. These details include the application name, routing type, resource location, and any other necessary configuration parameters.
- **NetScaler files:** You can also import applications by using a pre-generated CSV file. This CSV file is created by a script that parses and extracts relevant application configuration from the ns.conf and ns.log files. The script-generated CSV enables efficient and accurate import of application configurations into the Citrix Secure Private Access console.

How the import works

Here are the high-level steps that an admin must perform when using the CSV-based applications import tool:

1. **Prepare the CSV file:** If you are manually adding the apps, populate the application details in the CSV file. For details, see Preparing the CSV file.
2. **Import the CSV file:** Import the completed CSV file into the Secure Private Access console.
3. **Review the app details:** Review and validate the imported application data.

4. **Update the routing and resource location:** Review and update the routing type and resource location details, if required. Ensure that at least one connector is up in the specified resource location.
5. **View the applications in the Applications page:** View the imported applications in the Applications page. Check if all the applications that you selected for import are imported successfully.

This structured process ensures a thorough migration and proper configuration of applications for secure and seamless access within the Secure Private Access environment.

Preparing the CSV file

Download the CSV file from the Secure Private Access console and add the application details.

1. Navigate to **Applications > App Configuration**.
2. Click **Import Applications**.
3. In **Learn how to import using CSV and NetScaler files**, click **CSV** or **NetScaler**.

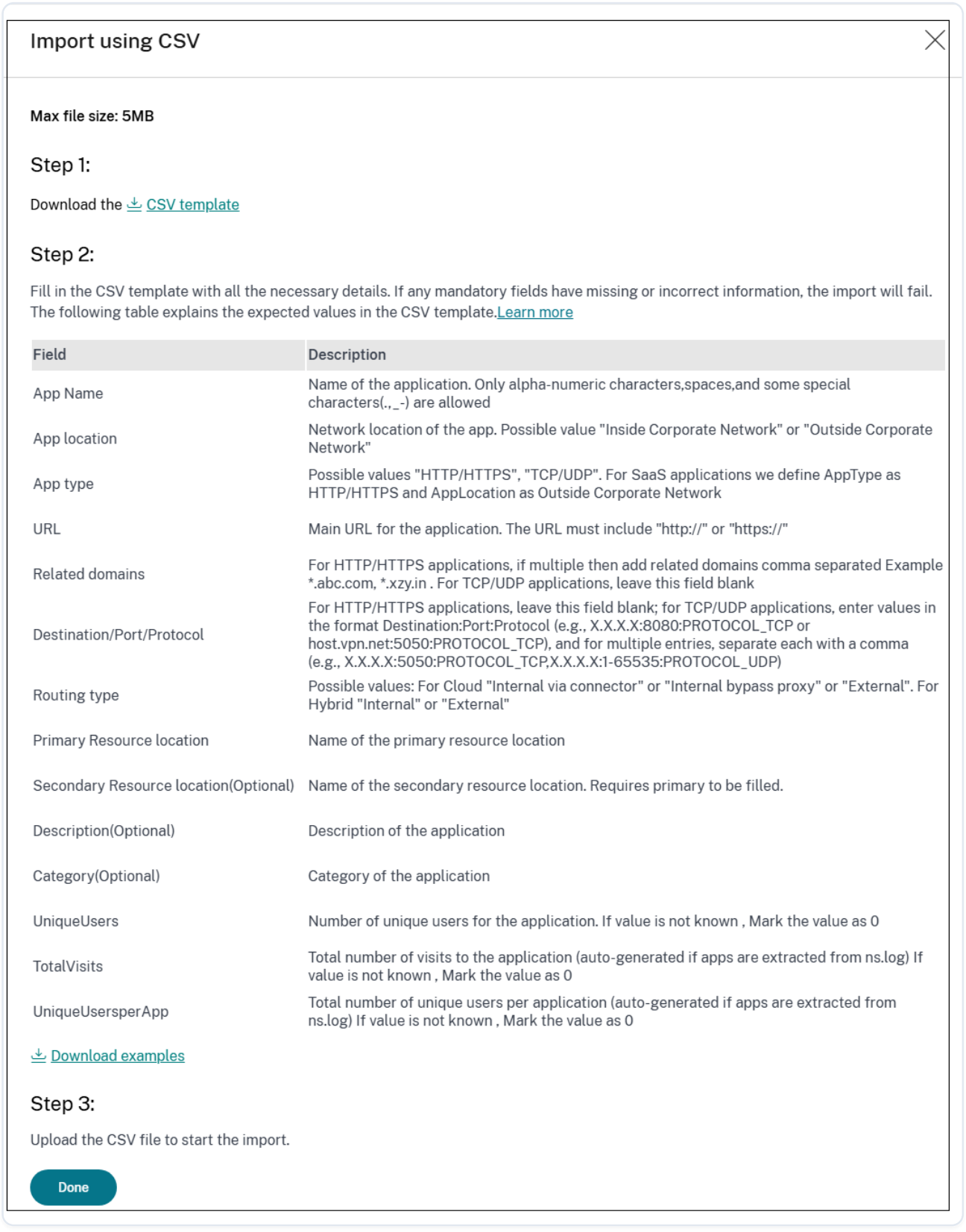
   The **Import using CSV** or the **Import using NetScaler files** page appears accordingly.

   - **CSV** - Download the CSV file (CSV template) and populate the app details. The page also displays sample information on the app data that must be entered.
   - **NetScaler**
     - Download and save the Python script to the designated folder (/var/spa/scripts) in NetScaler.
     - Run the script as `python3 ztna-migration.py` to generate a CSV file from the ns.conf and ns.log files.
     - Once the CSV file is generated, upload it for import.

> **Note:**
>
> When importing a large number of applications from a CSV file, process them in batches of 50. After uploading the CSV, select the first 50 applications and complete the import, then select the next 50 and repeat until all applications are imported.

> Click **Download examples** to view a sample CSV file with the data.

Guidelines for importing applications using the CSV file:



Import using CSV

Max file size: 5MB

Step 1:

Download the CSV template

Step 2:

Fill in the CSV template with all the necessary details. If any mandatory fields have missing or incorrect information, the import will fail. The following table explains the expected values in the CSV template.Learn more

Field	Description
App Name	Name of the application. Only alpha-numeric characters,spaces,and some special characters(.,_-) are allowed
App location	Network location of the app. Possible value "Inside Corporate Network" or "Outside Corporate Network"
App type	Possible values "HTTP/HTTPS", "TCP/UDP". For SaaS applications we define AppType as HTTP/HTTPS and AppLocation as Outside Corporate Network
URL	Main URL for the application. The URL must include "http://" or "https://"
Related domains	For HTTP/HTTPS applications, if multiple then add related domains comma separated Example *.abc.com, *.xzy.in . For TCP/UDP applications, leave this field blank
Destination/Port/Protocol	For HTTP/HTTPS applications, leave this field blank; for TCP/UDP applications, enter values in the format Destination:Port:Protocol (e.g., X.X.X.X:8080:PROTOCOL_TCP or host.vpn.net:5050:PROTOCOL_TCP), and for multiple entries, separate each with a comma (e.g., X.X.X.X:5050:PROTOCOL_TCP,X.X.X.X:1-65535:PROTOCOL_UDP)
Routing type	Possible values: For Cloud "Internal via connector" or "Internal bypass proxy" or "External". For Hybrid "Internal" or "External"
Primary Resource location	Name of the primary resource location
Secondary Resource location(Optional)	Name of the secondary resource location. Requires primary to be filled.
Description(Optional)	Description of the application
Category(Optional)	Category of the application
UniqueUsers	Number of unique users for the application. If value is not known , Mark the value as 0
TotalVisits	Total number of visits to the application (auto-generated if apps are extracted from ns.log) If value is not known , Mark the value as 0
UniqueUsersperApp	Total number of unique users per application (auto-generated if apps are extracted from ns.log) If value is not known , Mark the value as 0

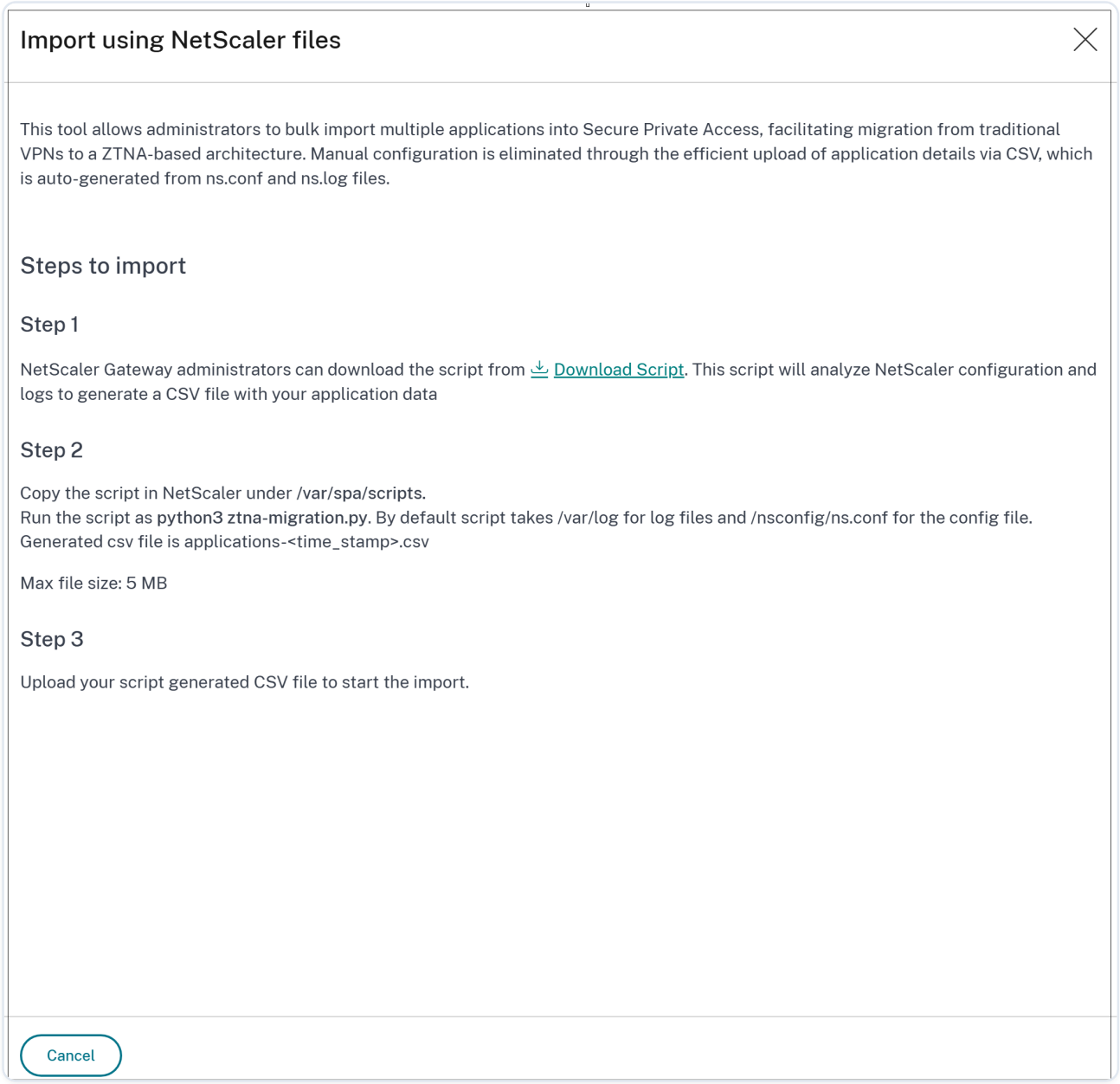
Download examples

Step 3:

Upload the CSV file to start the import.

Done

Guidelines for importing applications using NetScaler files:



Values to be entered in the CSV file

The following table provides guidelines on the values to be entered for each column in the CSV file when manually creating the applications:

COLUMN NAME	VALUE
App Location	Inside Corporate Network (for internal web apps, TCP, UDP apps)
	Outside Corporate Network (for SaaS apps)
App Type	Must be one of the following values.

COLUMN NAME	VALUE
	HTTP/HTTPS
	TCP/UDP
URL	Applicable only for HTTP/HTTPS apps. The URL of the application. The URL must include "http://" or "https:"//
Related Domains	Applicable only for HTTP/HTTPS apps. You can add multiple related domains separated by a comma (,).
	For TCP/UDP apps, leave this field blank.
DestinationPortProtocol	Applicable only For TCP/UDP apps. You must list all IP addresses, IP address range, or IP/CIDR and ports separated by a colon(:).
	For HTTP/HTTPS apps, leave this field blank.
	The destination, port, and protocol must be formatted as follows when entering the data manually.
	Destination:Port:Protocol. Example: 192.0.2.254:5050:PROTOCOL_TCP.
	If there are multiple destinations in the TCP/UDP application, multiple destination entries are separate each with a comma (for example, X.X.X.X:5050:PROTOCOL_TCP,X.X.X.X:1-65535:PROTOCOL_UDP)
	The destination can be an IP address, IP address range, CIDR, host name, domain, or FQDN. The port can be a single port (example 5050) or a port range (example 1–65335).
Routing Type (cloud environment)	Based on the app type, select one of the following values.

COLUMN NAME	VALUE
	Internal – Bypass Proxy - The domain traffic is routed through Citrix Cloud Connector™, bypassing the customer's web proxy configured on the Connector Appliance.
	Internal via Connector - The apps can be external or internal but the traffic must flow through the Connector Appliance.
	External – The traffic flows directly to the internet.
Routing Type (hybrid environment)	**Internal** or **External**.
Primary Resource Location	The name of the primary resource location where the application resides.
	Note: Not applicable for hybrid environments.
Secondary Resource Location (optional)	The name of the secondary resource location where the application resides. The secondary resource location is applicable only if the primary resource location is explicitly specified.
	Note: Not applicable for hybrid environments.
Description	(Optional) Application description.
Category	(Optional) Application category.
UniqueUsers	Number of unique users for the application.
	This value is autogenerated if the apps are extracted from ns.log files.
	If you are updating the CSV file manually, leave it blank.
TotalVisits	Total number of times the application has been accessed.

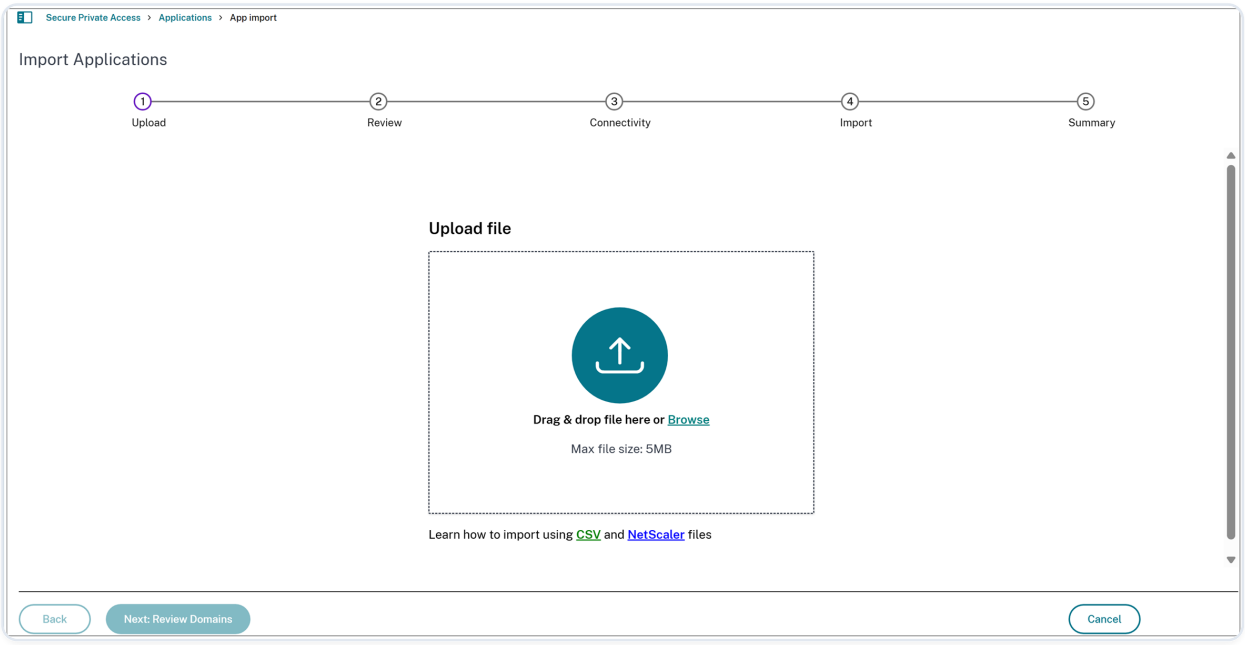
COLUMN NAME	VALUE
	This value is autogenerated if the apps are extracted from ns.log files.
	If you are updating the CSV file manually, leave it blank.
UniqueUsersperApp	Total number of unique users accessing the application.
	This value is autogenerated if the apps are extracted from ns.log files.
	If you are updating the CSV file manually, leave it blank.

Steps to migrate applications using the CSV-based tool

You can import applications while setting up Secure Private Access or after the setup is complete.

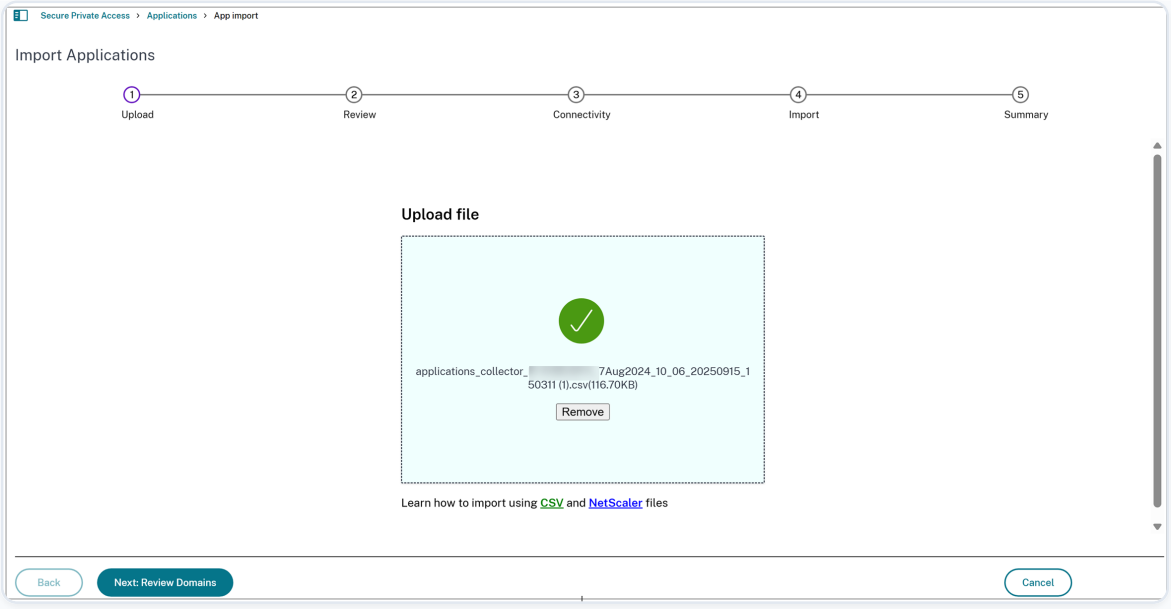
1. On the Secure Private Access service tile, click **Manage**.
2. In the Overview page, click **Continue**.
3. Set up identity and authentication for the users to log in to their stores. For details, see Setup identity and authentication.
4. In **Step2: Applications** page, click **Import application**.

   Alternatively, if your Secure Private Access is already set up, click **Import the application** from the Applications page (**Secure Private Access > Applications**).

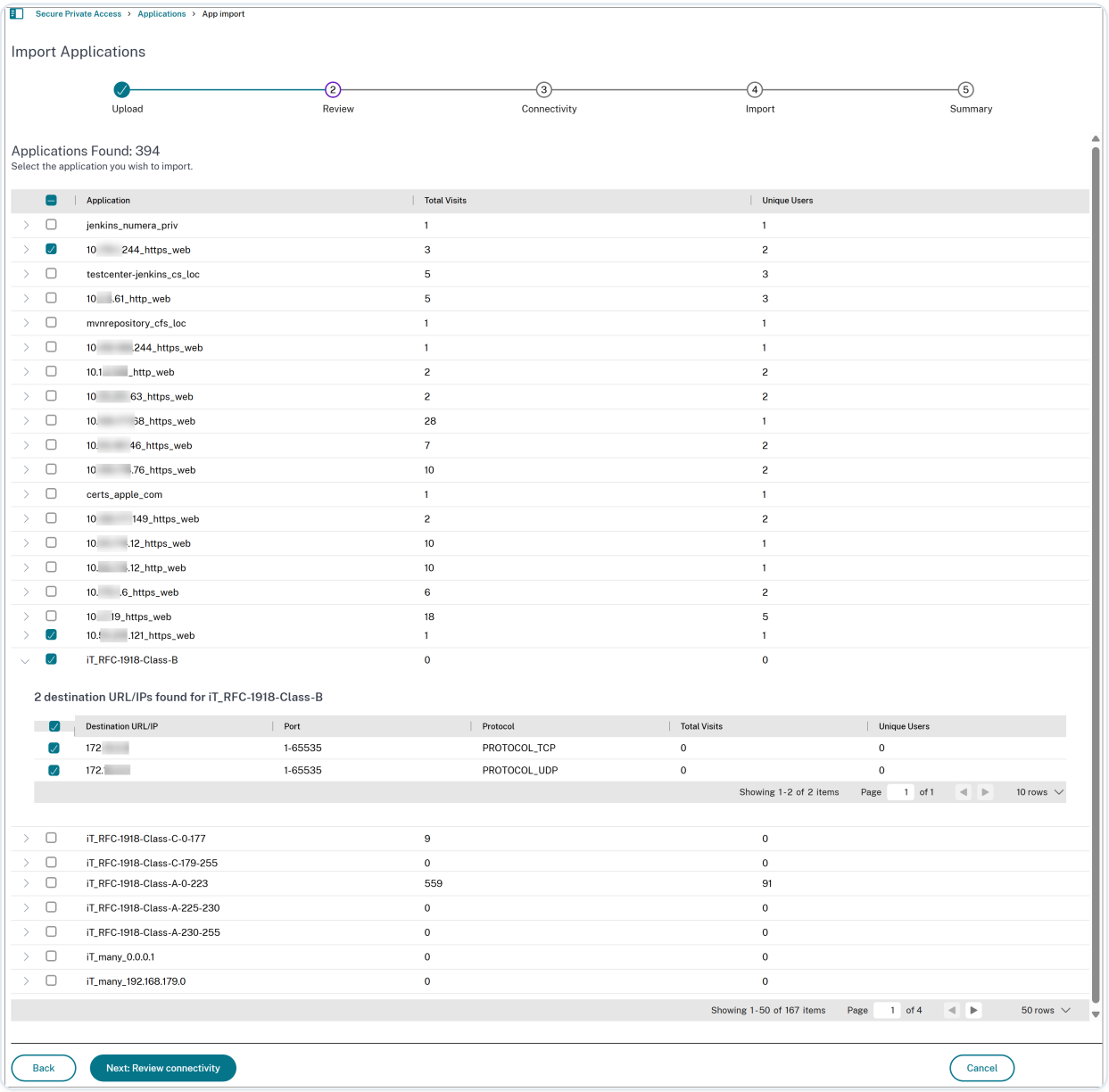


5. Upload the CSV file. You can either drag the CSV file here or browse to select it.
6. Click **Next: Review Domains**.

> **Note:**
>
> - The **Next: Review Domains** button is enabled only if the file contains no errors.
> - If you upload the same CSV/nsconfig file with additional applications, only the diff is imported.



7. Select the applications that you want to import.

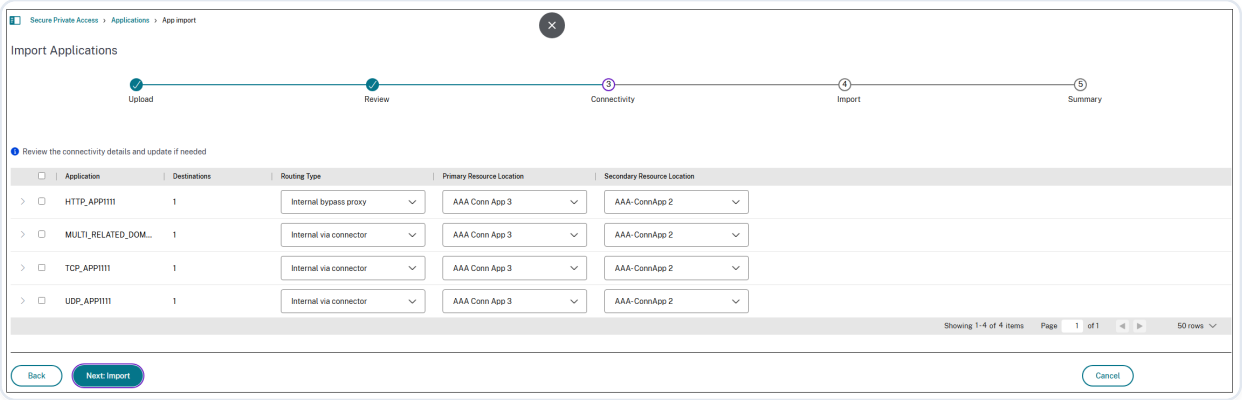


Note:

- If an application with the same domain or wildcard domain already exists, that application is disabled for import. You cannot select those applications.
- The expand icon in line with each application displays additional details regarding the app.
- For SaaS/Web and TCP/UDP applications, the **Import Applications** page displays the total application visits and the count of unique users (distinct users who accessed the application). Use the expand icon to view the application's port and protocol details.

- Manually uploaded SaaS apps (outside the corporate network) via CSV are marked as unpublished and do not appear in the Import Applications UI, despite a successful upload. Therefore, to create a SaaS application by manually adding the entry in the CSV file, you must set **App Location** to **Outside Corporate Network** and **App Type** to **HTTP/HTTPS**.
- For TCP/UDP applications, the tool lists all associated destination URLs and IP addresses. By default, selecting the application automatically selects its related URLs and IP addresses for import. You cannot deselect individual destinations.

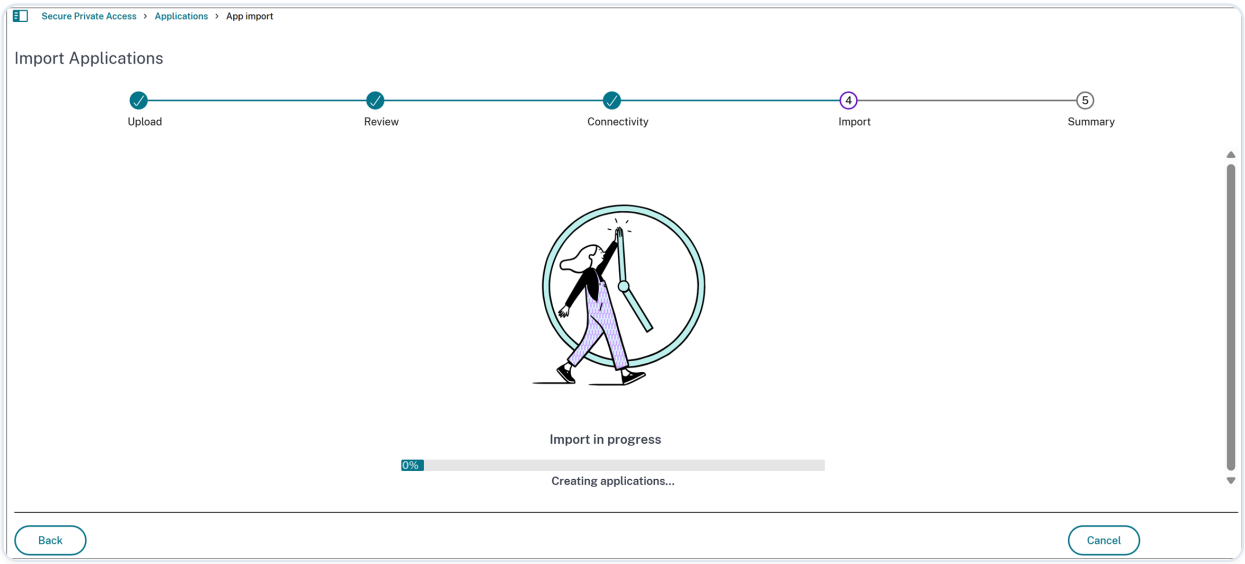
8. Click **Next: Review Connectivity**.
9. The **Next: Review Connectivity** button is enabled only if at least one application is selected.
10. Review and update the connectivity settings. Make necessary changes to routing type and resource locations, if required and then click **Done.**.



Note:

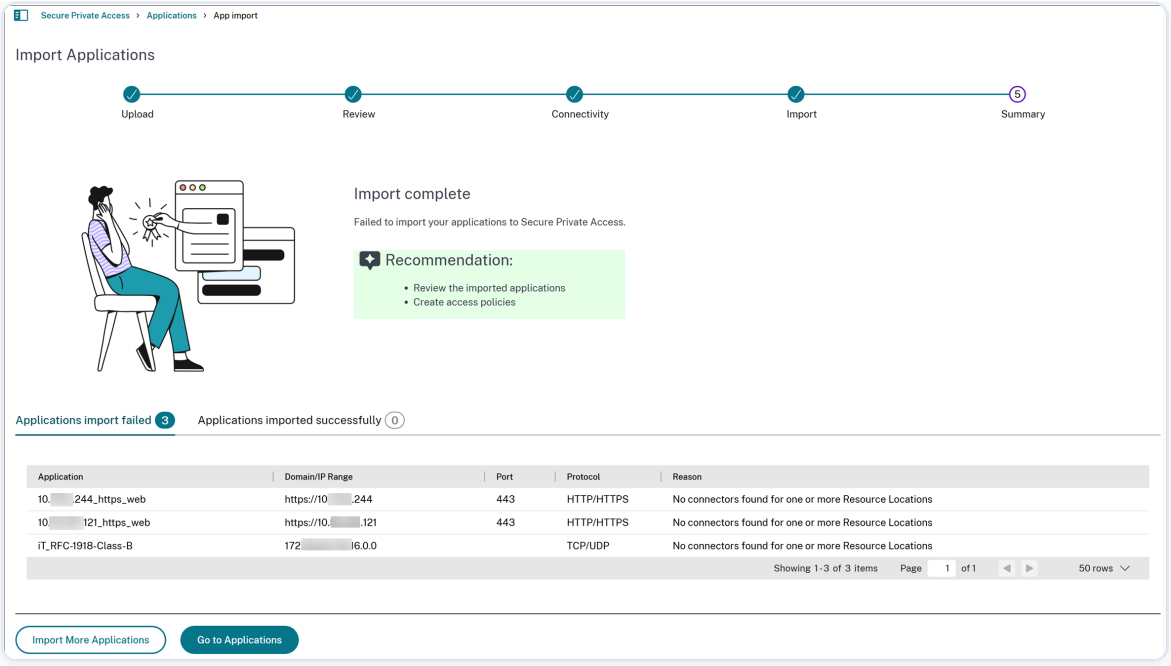
- If the specified resource location does not exist, the first resource location available in the list of resource locations associated with the customer is selected by default. if the Connector Appliance in the specified resource location is not up, the application creation fails.

11. Click: **Next: Import**.



Note:

- The **Import Applications** page displays the imported application details. These applications are also added to the list of applications in the **Applications** page.
- For any failed application imports, the reason for failure is displayed in the **Reason** column. Use this information to correct the CSV file and re-import those applications.



12. Click **Go to Applications** to view the imported applications in the **Applications** page.

Failures to import or create applications when using the CSV file

The following issues can cause import or application creation failures when using the CSV file:

- Modifications or changes to the column names or their casing.
- Deletion or swapping of the columns in the CSV file.
- Missing mandatory application fields in the CSV file.
- An empty CSV file or a CSV file that contains only column names is imported. For an empty file, an error message appears. If the file contains only column names, the **Next** button remains disabled.
- No Connector Appliance is available in the resource location specified in the CSV file.
- A secondary resource location is specified while the primary resource location is missing or empty. The import fails with a validation error indicating that the primary resource location is required.

References

Refer to the following topics for information on creating applications in Secure Private Access.

- Support for Enterprise web apps
- Support for SaaS apps
- Support for TCP/UDP apps

Client internal IP address pools - Preview

The client internal IP address pools contain IP address ranges that are assigned to the logged-in users. Each user and their device receive a unique internal IP address, which is required for identification and session management within Secure Private Access. This internal client IP address is only accessible within the customer's resource location.

Using this internal IP addresses, devices in the customer resource location can tunnel traffic directly to a specific logged-in user's device, enabling server-to-client connections. The client internal IP address also supports source IP stickiness for existing client-to-server tunnel traffic, ensuring stable and consistent connections.

> **Note:**

> Client internal IP address pools feature is in preview. To get this feature enabled, contact Citrix® Support.

Use cases of client internal IP address pools

- **Enable server-to-client connections:** Certain tasks such as pushing configurations, providing remote assistance, or installing software require servers to initiate connections to client devices. Client internal IP address pools make this possible by assigning a defined range of IP addresses used to identify client devices. These internal IP pools are allocated based on user context and location. For example, a specific IP address range can be dedicated to a user group like the HR team.

  To enable server-to-client communication, you must create a server-to-client app and specify the client device's port and protocol details, along with the back-end IP address range that is used to reach the client. For details, see Server-to-client app configuration.

- **Enable client internal IP address stickiness:** To maintain consistent connections, some applications require a continuous session with the same client. For enabling client IP address persistence, see Client IP address stickiness.

  > **Important:**
  >
  > To use the source IP address as the internal IP address or the server-initiated connection functionality, ensure the following:
  >
  > - The switch or the router connected to the Connector Appliance's subnet supports Gratuitous ARP.
  > - The Port security and Dynamic ARP Inspection (DAI) configuration does not affect the source IP address or server-initiated connection functionality.

IP address pool limitations

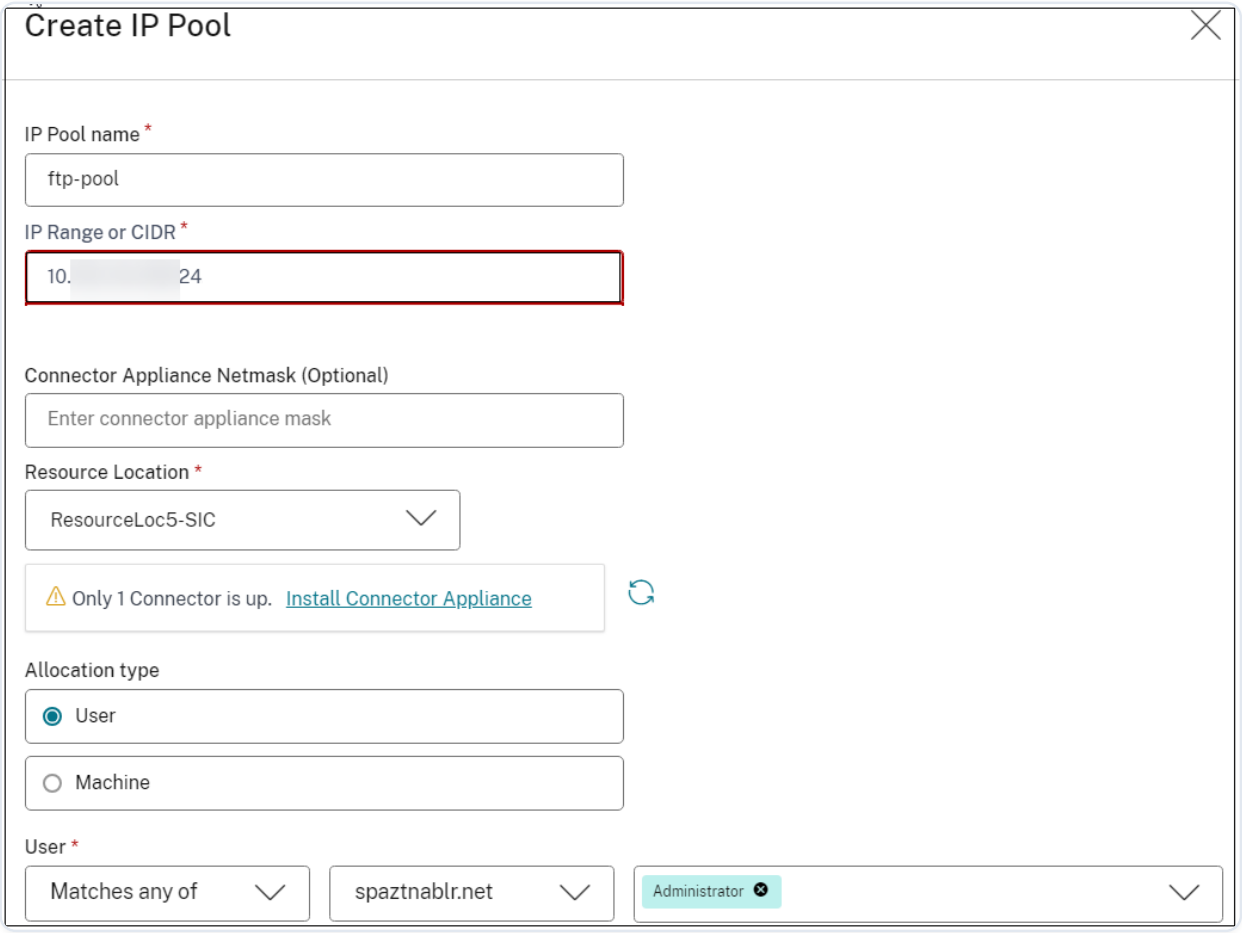
Following are some of the limitations of the IP address pool:

- All Connector Appliances in a resource location must reside within the same IP subnet.
- The internal IP address pools must consist of IP addresses from the Connector Appliance subnet in the same resource location.

- The IP addresses within the internal IP address pools must not overlap with any used IP addresses of the Connector Appliances or other devices within the same subnet.
- If the IP addresses in the pool are exhausted, IP addresses are not assigned to the users and hence server-to-client connections and client internal IP stickiness features cannot be used.
- A maximum of 3 different IP addresses can be assigned to a user, allowing logins from up to 3 different devices. If the same user logs in from a fourth device, no IP address is assigned, preventing the use of server-to-client initiated connections and client internal IP stickiness.
- The assigned internal IP address is sticky and remains the same for daily logins and logouts on the same device. However, if a user is inactive for 15 consecutive days, their sticky internal IP address is released and reassigned to a different user.

Create an intranet IP address pool

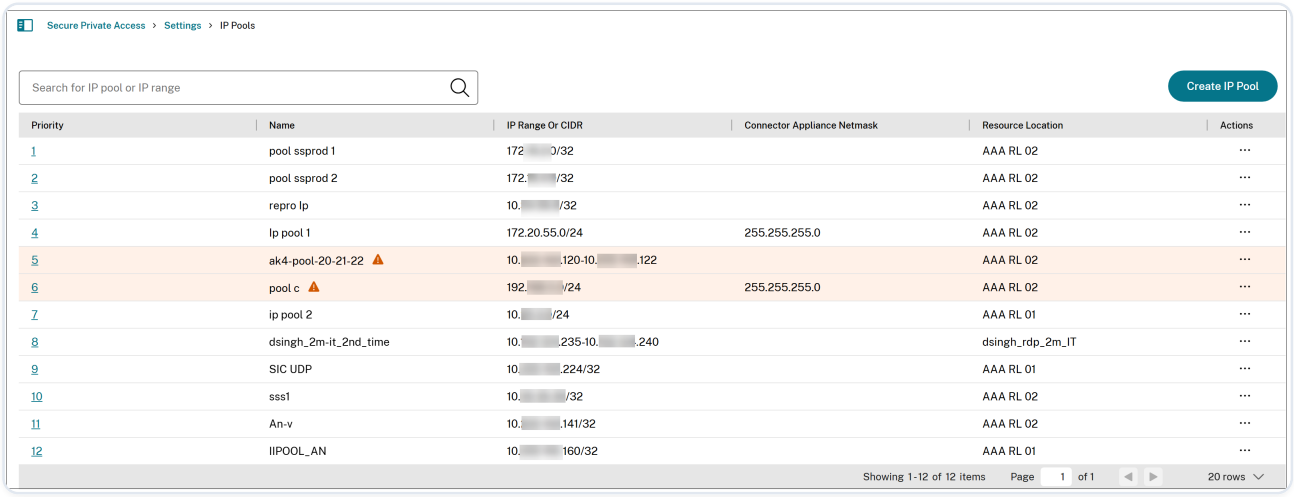
1. Navigate to **Settings > IP Pools** and then click **Create IP Pool**.



2. **IP Pool name**: Enter a name for the IP pool.
3. **IP Range or CIDR**: Enter the range of IP addresses reserved for clients. One of these IP addresses is assigned to the client machines.

4. **Connector Appliance Netmask**: (Optional). In case the Connector Appliance network subnet is different from the Internal IP address subnet, the Connector appliance netmask must be entered.
5. **Resource Location**: Select the resource location where the back-end server is located. Ensure that at least one Connector Appliance is up.
6. **Allocation type**: Select User and select the condition, domain, and the user or user groups to which this pool is applicable.
7. Click **Create**.

The IP address pool that you created is listed in the IP Pools page.



Once the client login is successful, an intranet IP address is assigned to the user from the client internal IP address pool.

As shown in the preceding image, administrators can use the prioritization mechanism to control the priority of the pool. Administrators can define explicit priority levels for each IP pool. The Secure Private Access service allocates IP addresses from highest to lowest priority (top to bottom), ensuring predictable assignment and operational control.

> **Note:**
>
> The priority with a lower value has the highest preference.

Delete an IP address pool

IP address pools can be immediately deleted or over time by using one of the following options.

- **Delete IP Pool by force:** Stops allocating IP addresses to new users and releases unused IP addresses immediately. Active user sessions using the deleted IP addresses might be terminated, resulting in abrupt closures and forced logouts. Users with terminated sessions are allocated new IP addresses only after a different IP address pool is created.
- **Delete IP Pool over time:** Stops allocating IP addresses to new users and releasing unused IP addresses immediately. The system waits for the active sessions to log out or expire before fully deleting the pool. Users with terminated sessions are allocated new IP addresses only after a different IP address pool is created.

Note:

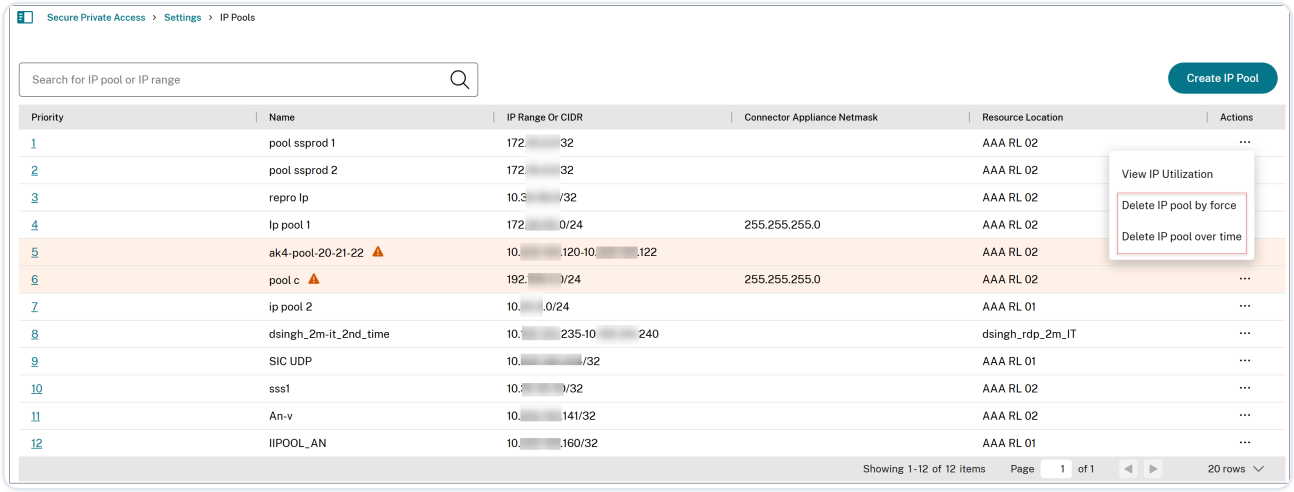
We recommend that you schedule a maintenance window and notify users to log out and then initiate deletion of the IP pool over time. If most IP addresses are freed up after the scheduled time, you can force delete the remaining in-use IP addresses. However, we recommend that you do not force delete large IP address pools.

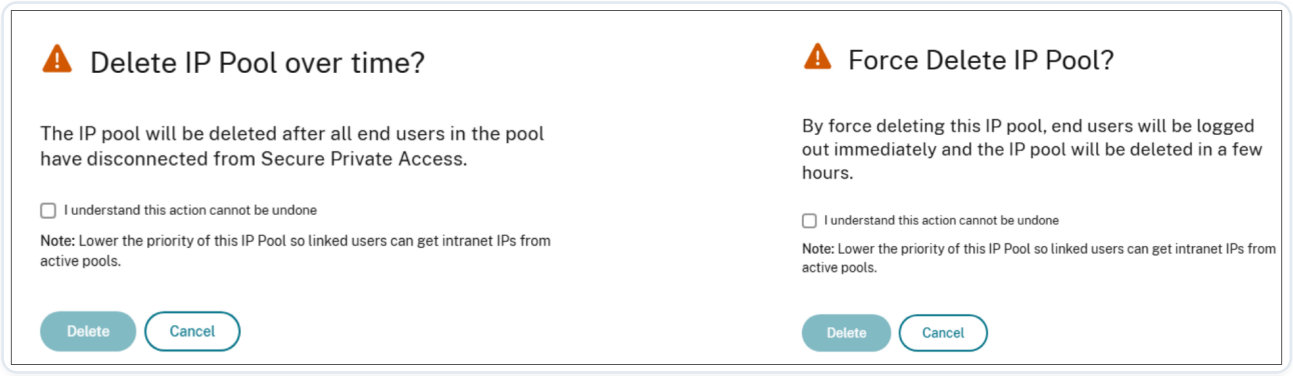
Perform the following steps to delete an IP pool:

1. Navigate to **Settings > IP Pools**.

   The list of IP address pools and their details are displayed.

2. Click the ellipsis (…) next to the address pool that you want to delete, then select either **Delete IP pool by force** or **Delete IP pool over time**.





Note:

When a pool is deleted or scheduled for deletion, the administrator must lower its priority. The priority for this pool must be lower than the other active pools to ensure that Secure Private Access stops allocating new IP addresses from that pool. IP address assignment automatically falls back to the higher priority pools.

View the IP address utilization data

You can monitor the IP address utilization data from the IP Pool Utilization page. This page provides an overview of the status of the IP addresses.

- A list of users and the IP addresses allocated to these users.
- The percentage of available IP addresses that are already allocated and the total number of IP addresses available for allocation.

Administrators can use this data to monitor IP address consumption and ensure that enough IP addresses are available for the users.

Perform the following steps to view the IP address utilization details:

1. Navigate to **Settings > IP Pools**.

   The list of IP address pools along with their details are displayed in a tabular format.
2. Click the ellipsis (...) next to the address pool and then click **View IP Utilization**.

Maintain consistent connections

To ensure persistent and consistent connections for applications that require session continuity, admins can enable either connector stickiness or client IP address stickiness, depending on the

type of application (Web/SaaS or TCP/UDP). Secure Private Access supports both connector stickiness and client IP address stickiness.

- **Connector stickiness** ensures that after a client establishes a connection with the Connector Appliance, all subsequent requests from that client are directed to the same source (Connector Appliance).
- **Client IP address stickiness** ensures that requests from a particular client IP address are consistently routed to the same back-end server.

Connector or client IP address stickiness can be enabled while creating the applications.

- For Web/SaaS applications, admins can enable the **Maintain consistent connections** option.
- For TCP/UDP applications, admins can choose between **Client IP** and **Connector ID** stickiness, depending on their requirement.

For details, see the following sections:

- Connector stickiness
- Client IP address stickiness

> **Important:**
>
> - Client IP address stickiness feature is in Preview.
> - To enable client IP address stickiness, admins must configure client internal IP address pools. The IP address pool is essential for assigning a unique IP address to a user and the associated device. The devices from the customer resource location can tunnel traffic to a specific logged-in user's device using the client's internal IP address. For details, see Client internal IP address pools.

Connector stickiness

Some applications require connector stickiness, which means that all requests for a user session, including the initial login and the following requests come from the same Connector Appliance (the same IP address). If a request is routed through a different Connector Appliance, the application might not function correctly.

- Connector stickiness is specific to a particular user session. If the same user opens the app again, the traffic can be routed to a different Connector Appliance.

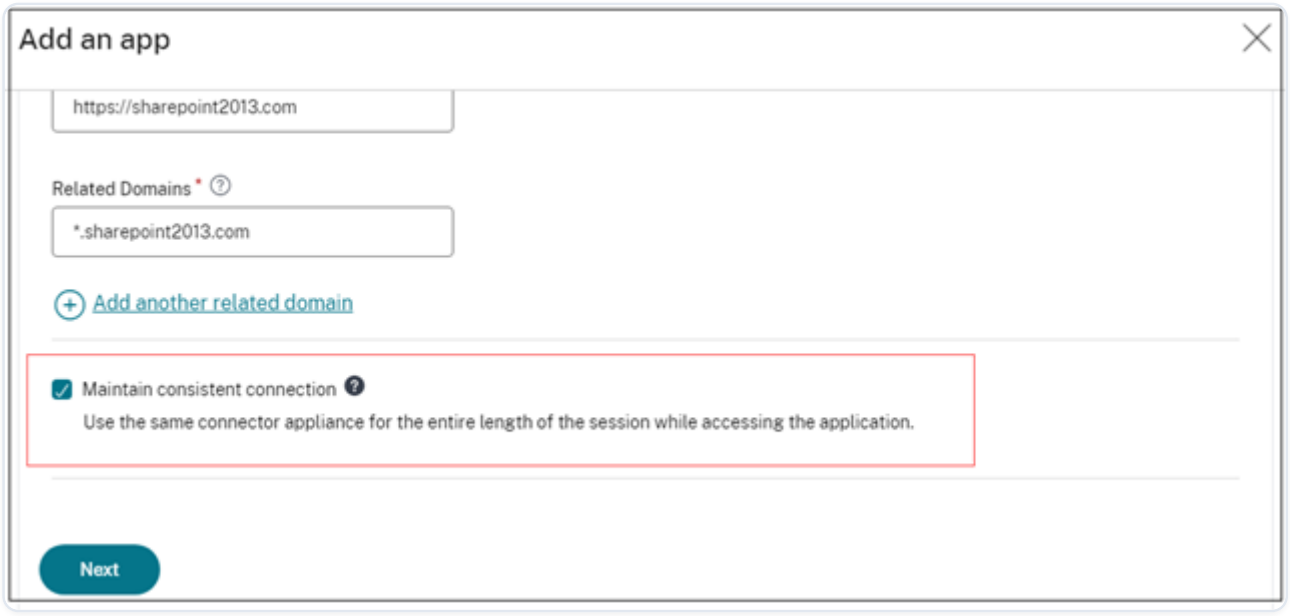
- Connector Appliances are chosen randomly from the available Connector Appliances in a given resource location.
- If a Connector Appliance fails, the connection is redirected to another appliance in the same resource location.

Connector stickiness is important in the following scenarios:

- NTLM protocols, which depend on the IP address to maintain the session state. If a request is routed through a different connector, NTLM authentication may fail, leading to errors or failed logins.
- Applications based on passive FTP, which require connection stickiness to ensure that both the control and data connections are routed to the same back-end server. Without this stickiness, the FTP sessions might fail.

For information on enabling connector stickiness for the applications, see the following topics:

- Configure a web app
- Configure a SaaS app
- Configure a TCP/UDP app



Client IP address stickiness - Preview

When a client connects to the back-end server through load balancing across multiple Connector Appliances in a resource location, the traffic source IP address might appear as a different Connector Appliance IP address. This discrepancy in the IP addresses might lead to issues such as the following:

- **TCP/UDP applications:** Certain applications require a consistent session between a specific client and server. If the source IP address changes, these applications might fail to launch. Applications such as passive FTP, active FTP, and some WebServers rely on IP address affinity (stickiness) to function correctly.
- **Security and monitoring systems:** These systems might find it difficult to track and analyze traffic if the source IP addresses keep changing frequently.

To maintain the source IP address affinity/stickiness, the client internal IP address stickiness can be configured for the TCP/UDP applications (client-to-server). With the client IP address stickiness, a unique internal IP address is assigned to the user session during login. This IP address is used instead of the Connector Appliance IP address in the resource location. This allocation ensures that all the connections from the client to the back-end server use the source IP address as the client internal IP address that is assigned at the time of login. The client IP address stickiness maintains session persistence irrespective of the Connector appliance that is used during the connection.

For enabling client IP address persistence, see Enable client IP address stickiness for TCP/UDP applications.

Prerequisites

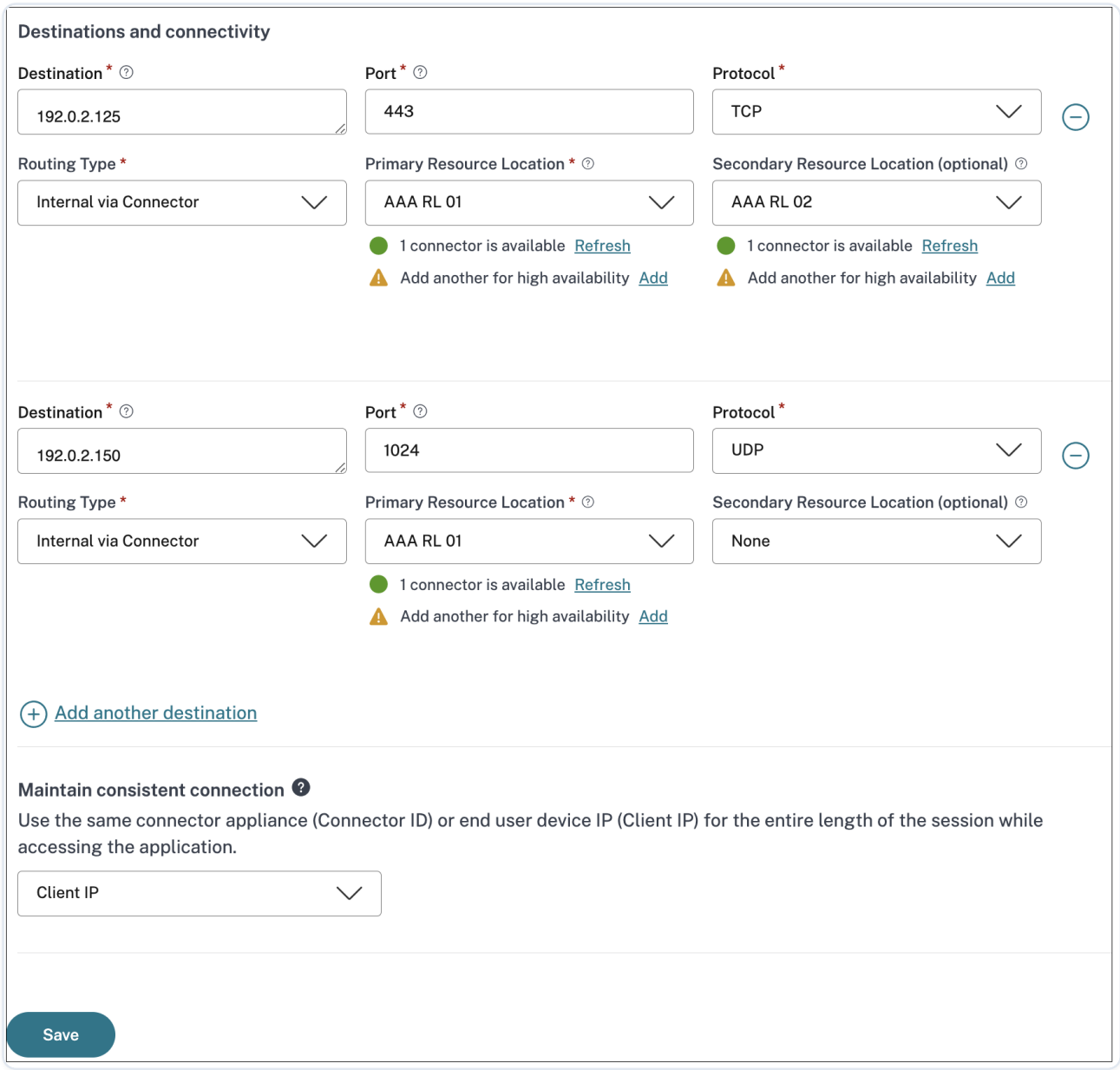
Ensure that the IP address pools are created. The IP address pool is essential for assigning a unique IP address to a user and the associated device. For details, see Client internal IP address pools.

Enable client IP address stickiness for TCP/UDP applications

Perform the steps as outlined in the topic Support for TCP/UDP apps.

In the **App Details** section, enable or disable the client IP stickiness by selecting one of the following values in **Maintain consistent connection**.

- **Do not use:** The application does not require any persistence. The application can work with any source IP address.
- **Client IP:** The application uses the same source IP address for the client with each connection.
- **Connector ID:** The application connects to the same connector appliance with each session.



Note:

To enable client IP address stickiness, select the same resource location that was used when creating the internal IP address pool, and ensure that the same resource location is set in the App Connectivity section.

Terminate active sessions and add users/machines to the block list

Admins can terminate all active sessions immediately and add the users/machines to the block list. Adding a user/machine to the block list terminates all active Secure Private Access application sessions and blocks future application access.

All active application sessions via Chrome Enterprise Premium browser, direct access, Citrix Workspace app for HTML5, and the Secure Access agent are terminated and blocked. All resources connected through the Secure Access agent such as file shares, RDP, SSH sessions are terminated and blocked as well. Users cannot launch any new applications until the users/machines are removed from the blocked list.

When the applications are accessed using the Chrome Enterprise Premium browser, any active browser-based sessions are also terminated, and further access requests from the disabled user are denied according to the Secure Private Access block list policy.

> **Note:**
>
> - Adding a user/machine to the block list does not change or edit the configured Secure Private Access access policy. Access termination and blocking happen despite whatever access policy is configured. Once the user/machine is removed from the list, the existing Secure Private Access access policies for the user are reinstated.
> - Internet access via the Citrix Enterprise Premium browser is allowed even after a user is added to the block list. Only access to published Secure Private Access applications is blocked.

Use cases

You can use this feature in the following scenarios.

- An employee quits the organization or is terminated from the organization. In this case, the admin revokes all Secure Private Access app access by terminating active Secure Private Access sessions and blocking any future app access.
- A device is lost or stolen. In this case, the access is blocked and all current sessions are terminated. The user can be removed from the block list after the situation is under control.

- A user misuses the app access. In this case, access for the user can be immediately revoked. Access is blocked until the user is added to the list.

Prerequisites to block users when using Chrome Enterprise Premium

To block users using Chrome Enterprise Premium with Secure Private Access, ensure that the following prerequisites are met:

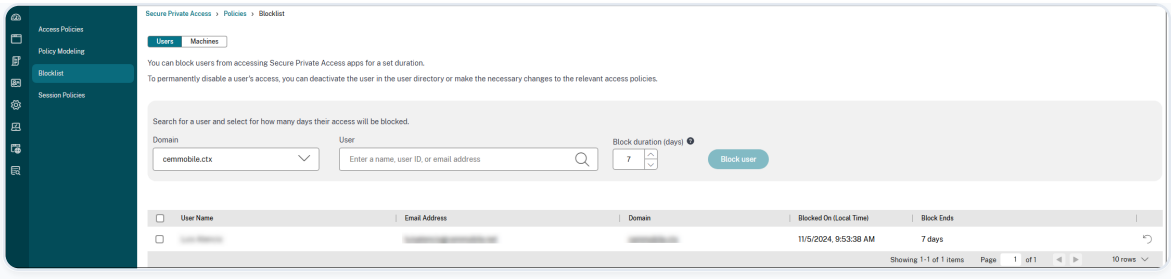
- When synchronizing Microsoft Entra ID users through the Google Cloud / G Suite Connector by Microsoft, ensure that the correct attribute mapping is configured so the user identity matches the Citrix Secure Private Access user records.

If this configuration is not set, the block user policy might not be enforced for users accessing applications through the Chrome Enterprise Premium browser.

Add users/machines to the block list

1. Navigate to **Secure Private Access > Policies > Blocklist**.
2. In **Domain**, select the domain for which the access must be disabled.
3. In **User**, search for the user name that must be added to the block list. All user names that match the search criteria are displayed. If the user is removed from the directory service, then that user name does not appear in the **User** list.

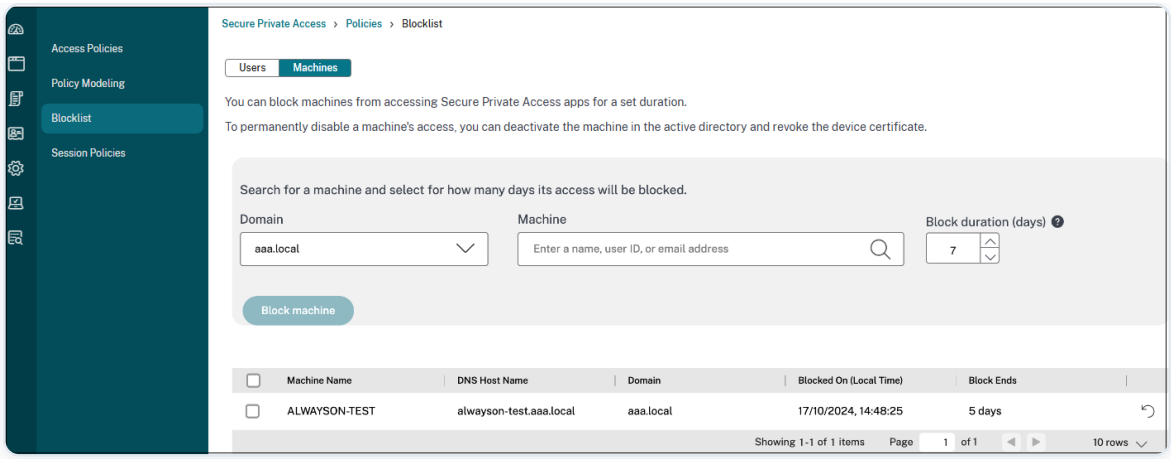
> **Note:**
>
> The **User** field appears only if the **Users** tab is selected.



4. In **Machine**, search for the machine name that must be added to the block list. All machine names that match the search criteria are displayed. If the machine is removed from the directory service, then that machine name does not appear in the **User** list.

> **Note:**

> The **Machine** field appears only if the **Machines** tab is selected.



5. In **Block duration (days)**, enter the number of days for which this user/machine must be blocked. Once you add the user/machine to the blocked list, they are blocked for 7 days by default. However, you can change the duration to anywhere between 1 and 99 days. After the duration ends, the access is restored based on the user directory and policy configuration. Also, this value remains persistent for the user for future additions. For example, if an admin sets the block duration for a user/machine at 30 days, this setting persists for the user/machine for future additions.
6. Click **Block user** or **Block machine** accordingly.

> **Note:**
>
> The **Block user** or the **Block machine**field appears to depend on the tab (**Users** or **Machines**) that is selected.

> The user/machine is added to the block list.

Recommendations:

- You can restore the access even before the block duration ends by doing one of the following steps.
  - Select the access for which you must restore access and then click **Restore access**.
  - Click the restore icon in line with the user for which you want to restore access.

  In both cases, a confirmation dialog appears.

- To revoke access for a user/machine indefinitely, remove the user/machine from your respective directory service, such as Active Directory, and then add them to the block list. This terminates the active Secure Private Access sessions, blocks future app access, and once the user/machine is logged out of the store, the user/machine cannot log in again due to inactive directory credentials.

End user experience after a user/machine is added to the block list

The following sections provide more information about end user experience after a user/machine is added to the block list.

Applications accessed via cloud

When an user is blocked:

- All active Secure Private Access sessions are immediately terminated.
- Future access to all Secure Private Access published applications is blocked.
- Internet access via the Citrix Enterprise Premium browser is allowed even after a user is added to the block list. Only access to published Secure Private Access applications is blocked.

When a machine is blocked:

- Once a machine is added to the block list, the user's access to all currently running applications is blocked.
- Any attempt to access new applications triggers a logout request.

Applications accessed via on-premises NetScaler® Gateway (hybrid data path)

- When a cloud session is terminated (either by user action or due to revocation), the corresponding active NetScaler Gateway sessions are automatically terminated.
- When a blocked user attempts to access new applications through NetScaler Gateway, the system triggers a logout request.

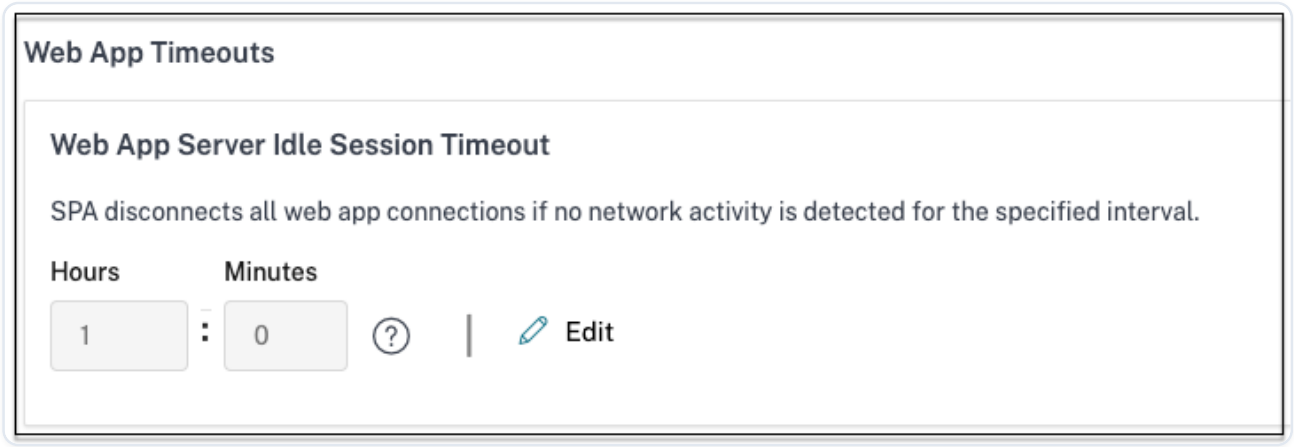
Timeouts for user sessions

You can configure a timeout period for the Web apps and the Citrix Secure Access™ client to end user sessions if there is no network activity for the specified time period. For the Citrix Secure Access client, you can also configure the Citrix Secure Access client to terminate a session if there is no user activity for that specified time period. Also, you can configure a forced disconnection on the Citrix Secure Access client regardless of the user and network activity, once the configured time period expires.

Timeout for the Web app servers

1. Navigate to **Settings > Timeouts**.
2. In **Web App Server Idle Session Timeout**, select the duration, in hours and minutes, for which the Web app session can be idle. The Secure Private Access service terminates the session after this time expires if the session remains idle.

   The minimum duration is 1 hour and the maximum duration can be 168 hours. Default value is 2 hours.

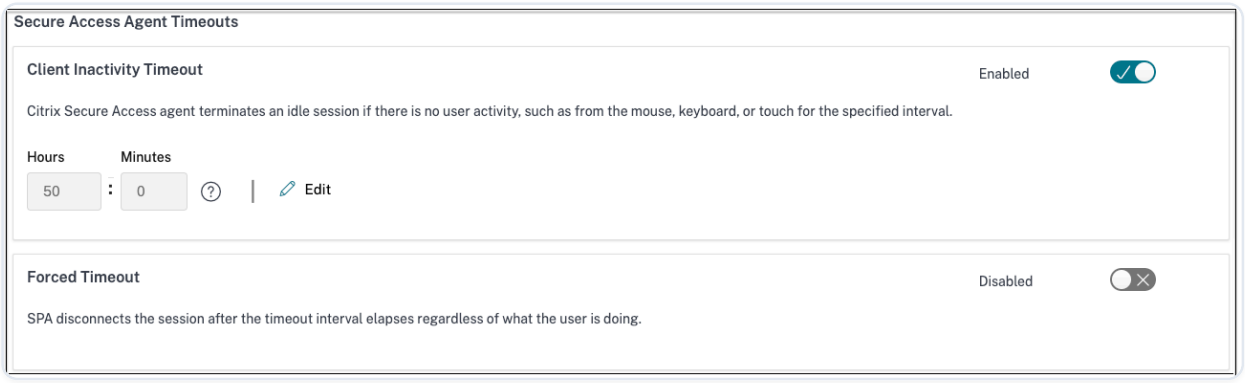


Timeouts for the Citrix Secure Access client

You can configure the following timeouts for the Citrix Secure Access client:

- Client inactivity
- Forced timeout

1. Navigate to **Settings > Timeouts**.



2. In **Secure Access Agent Timeout**, select the duration, in hours and minutes, for the timeout that you want to enforce.

- **Client inactivity timeout**: The duration after which the Citrix Secure Access client terminates a session, if there is no user activity (mouse or keyboard) for the configured period. This option is disabled, by default. You must enable the option by using the toggle switch to enforce the configured timeout period. However, if you disable the toggle switch after the configuration is saved, the client does not initiate a timeout.

  The minimum duration is 5 minutes and the maximum duration can be 168 hours. Default value is 8 hours.

- **Forced timeout**: The duration after which the Citrix Secure Access client terminates a session irrespective of the user or network activity. This option is disabled, by default. You must enable the option by using the toggle switch to enforce the configured timeout period. However, if you disable the toggle switch after the configuration is saved, the client does not initiate a timeout.

  A notification message appears 15 minutes before the session termination.

  The minimum duration is 1 hour and the maximum duration can be 168 hours. Default value is 168 hours.

> **Note:**
>
> If you enable more than one of these settings, the first timeout interval to expire closes the user connection.

Configuration reports

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.
- Authentication domain used for verifying user identities.
- Identity Provider (IdP) used for user identity.
- Customer parameters defined for a specific customer.

- Store configurations related to cloud stores.

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 for new setup or modify existing setup details.

Generate a configuration report

Perform the following steps to generate a configuration report.

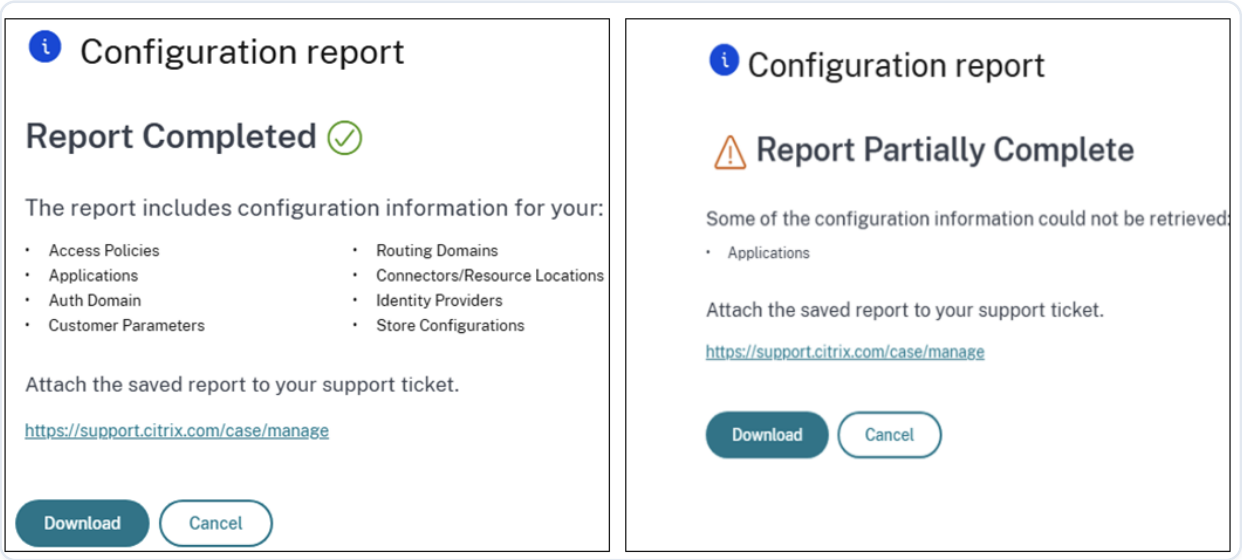
1. In the Secure Private Access admin console, go to **Settings > Global Configuration**.
2. Click **Create report** to initiate the report generation process.

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

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

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

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



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

> **Important:**

> Generating configuration reports is limited to administrators with the following Secure Private Access roles:

> - Full Access Administrator
> - Read Only Administrator
> - Full Monitor Administrator

> Administrators with the Help Desk Administrator role cannot generate configuration reports.

ADFS integration with Secure Private Access

Claim rules are necessary to control the flow of claims through the claims pipeline. Claim rules can also be used to customize the claims flow during the claim rule execution process. For more information about claims, see Microsoft documentation.

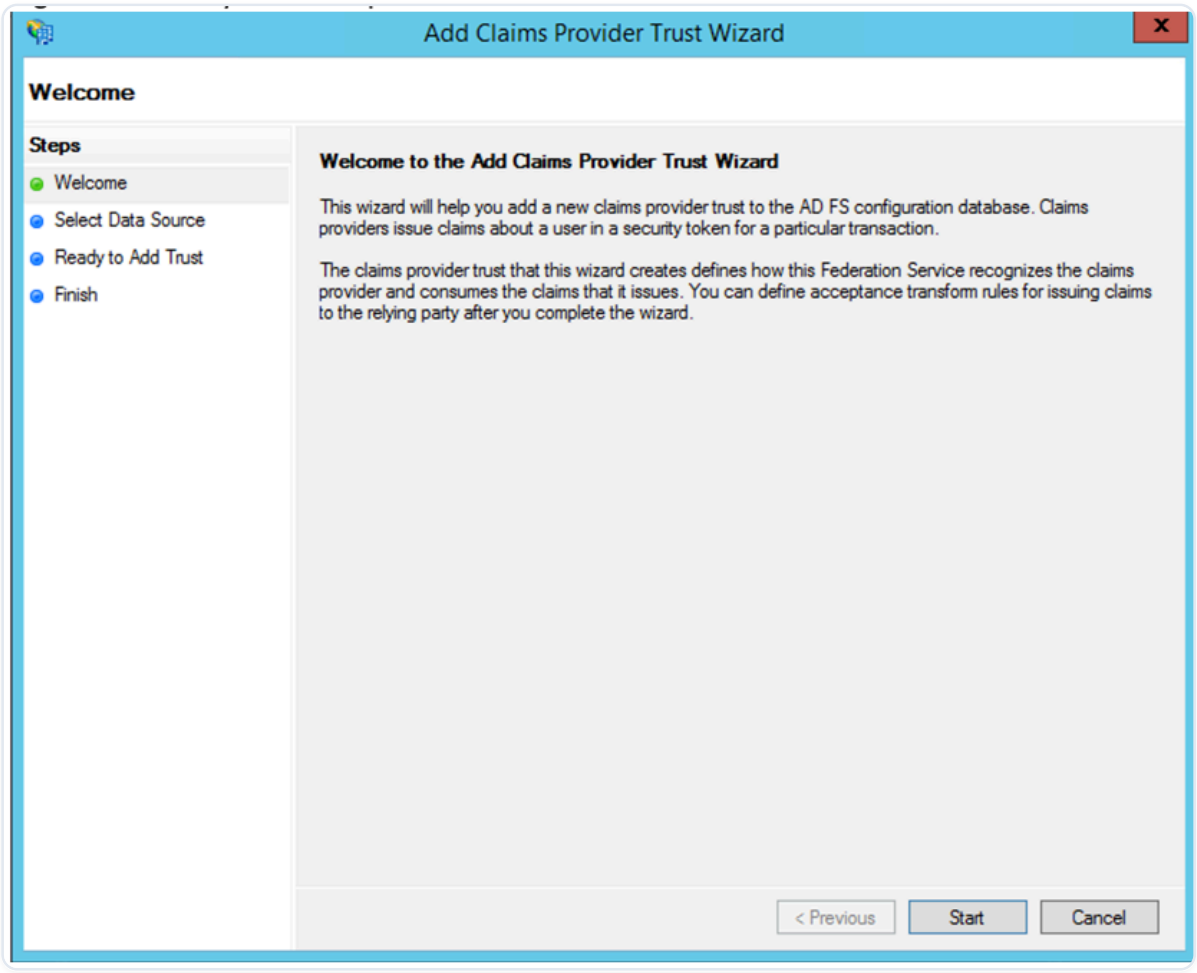
To set up ADFS to accept claims from Citrix Secure Private Access™, you must perform the following steps:

1. Add claim provider trust in ADFS.
2. Complete the app configuration on Citrix Secure Private Access.

Add claim provider trust in ADFS

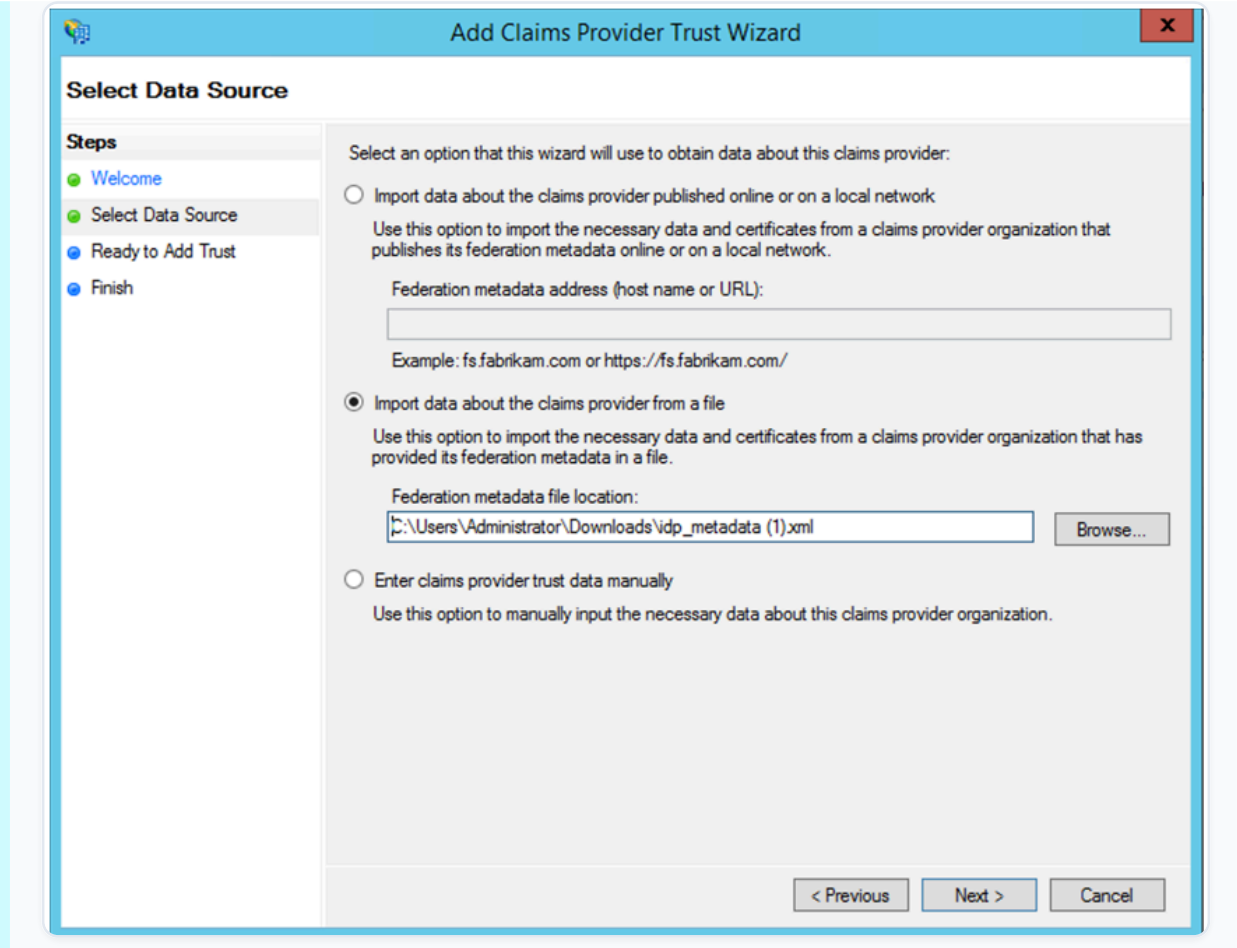
1. Open ADFS management console. Go to **ADFS > Trust relationship > Claim provider Trust**.

a. Right-click and select **Add Claim Provider Trust**.



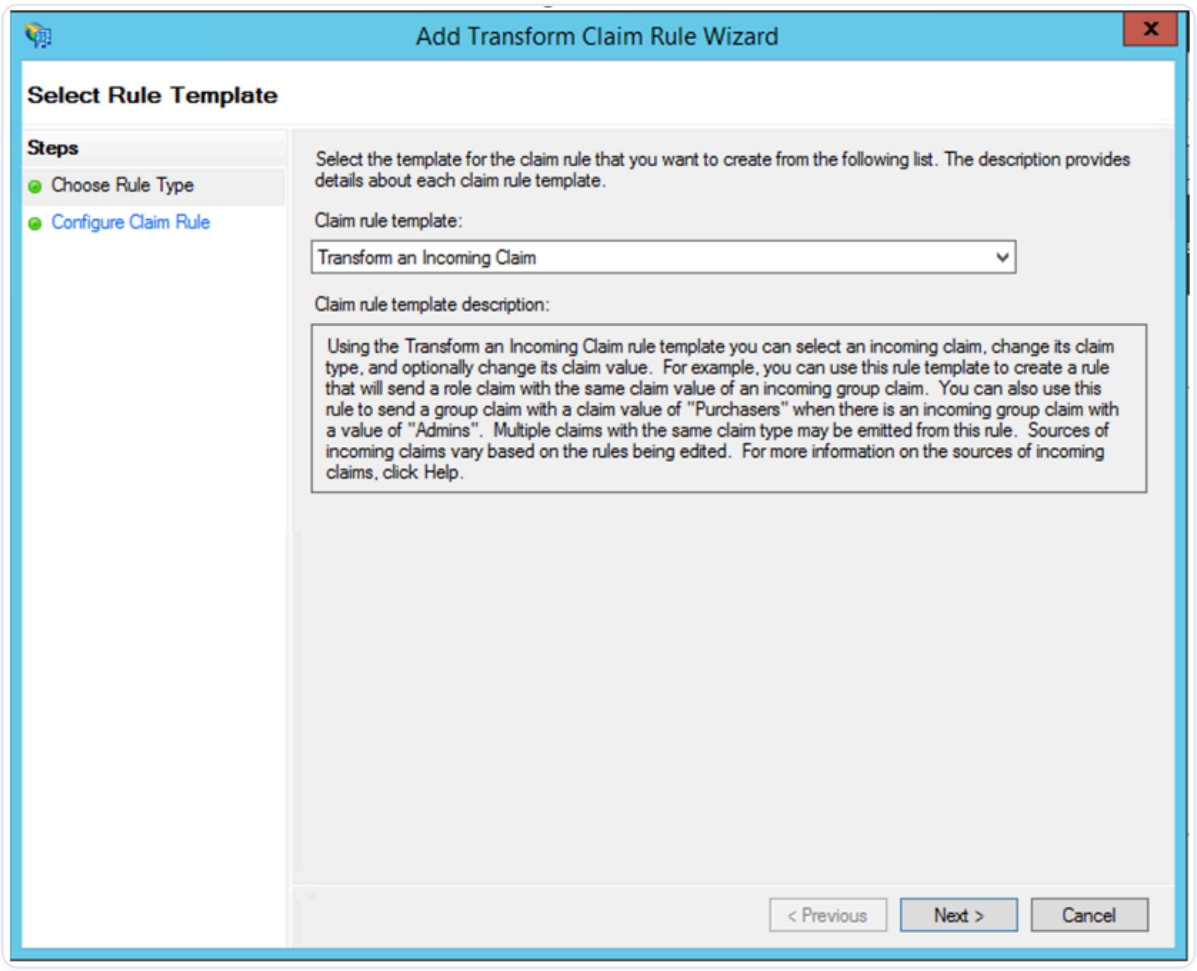
b. Add an app in Secure Private Access that is used to federate to ADFS. For details see, App configuration on Citrix Secure Private Access.

> **Note:**
>
> First add the app and from the app's SSO configuration section, you can download the SAML metadata file, and then import the metadata file into ADFS.

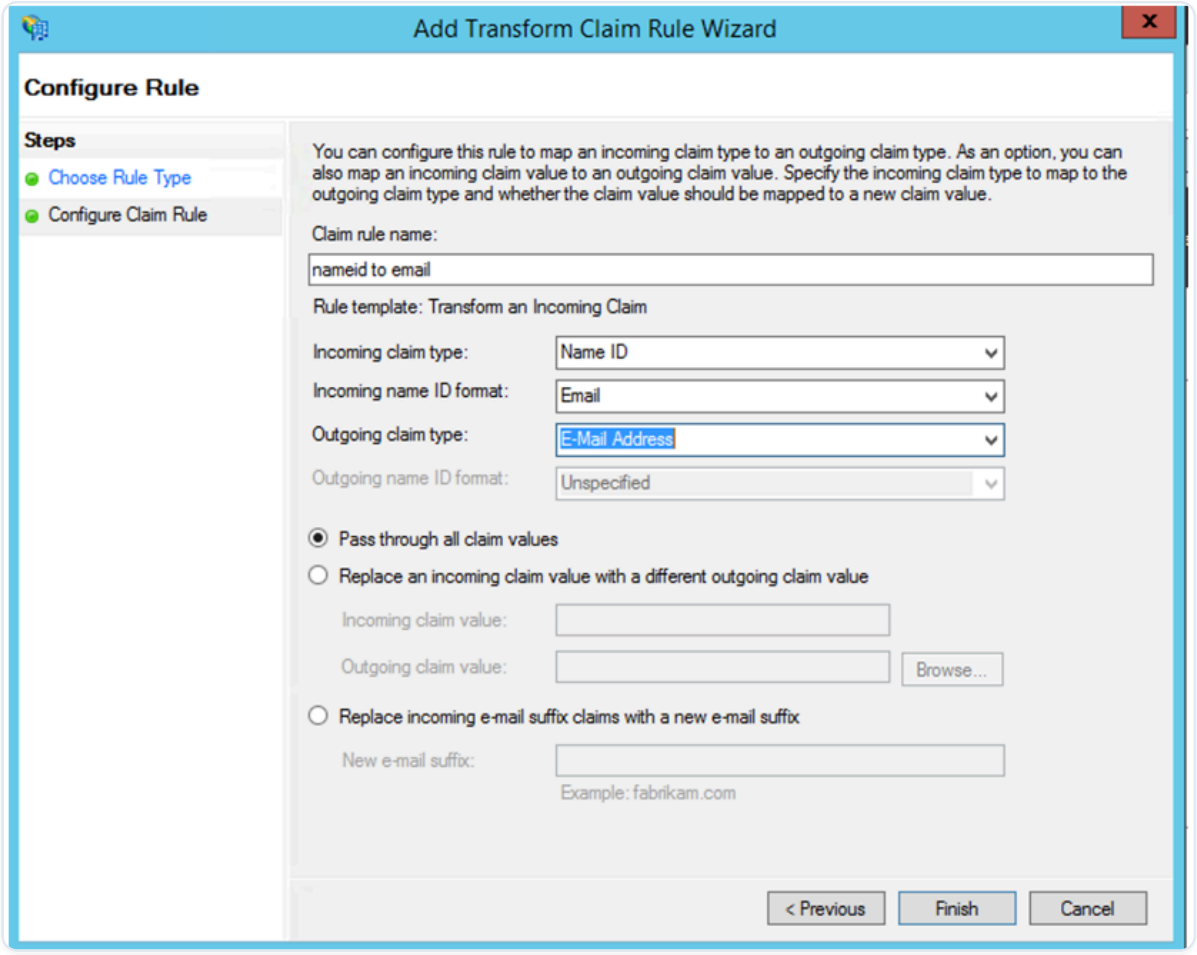


a. Complete the steps to finish adding claim provider trust. After you complete adding the claim provider trust, a window to edit the claim rule appears.

b. Add a claim rule with **Transform An Incoming Claim**.



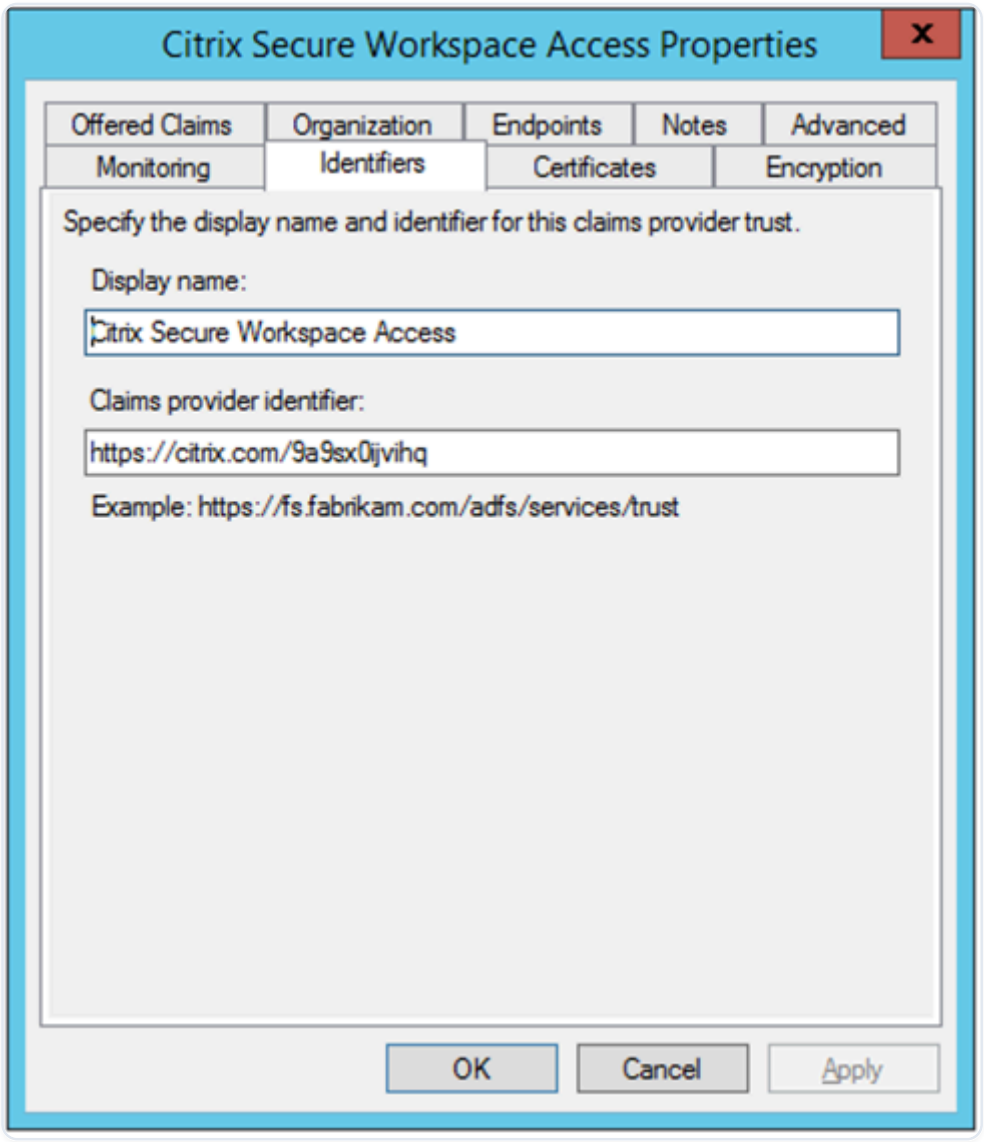
c. Complete the settings as shown in the following figure. If your ADFS accepts other claims, then use those claims and configure SSO in Secure Private Access also accordingly.



You have now configured the claim provider trust that confirms ADFS now trusts Citrix Secure Private Access for SAML.

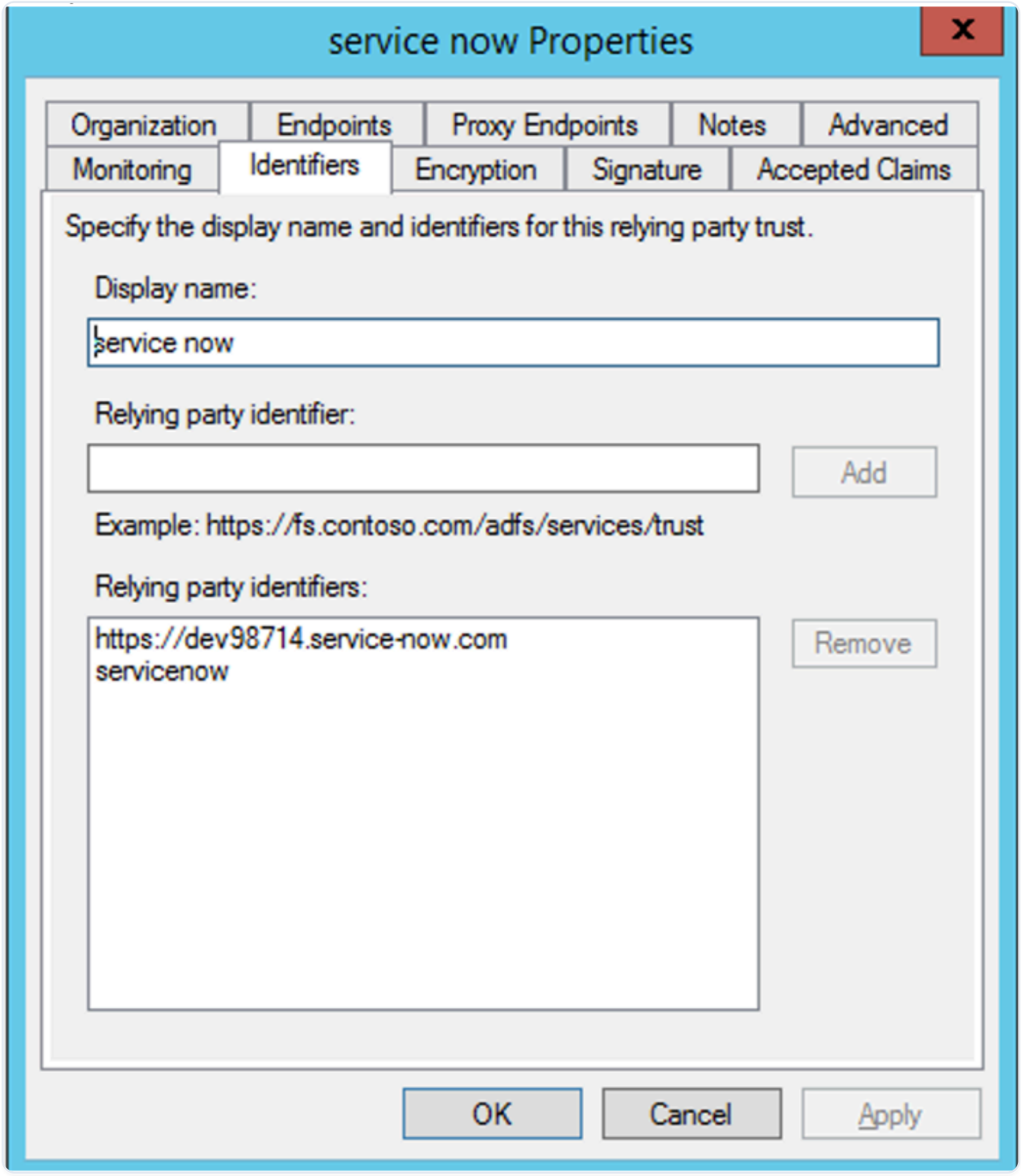
Claim Provider trust ID

Make a note of the claim provider trust id that you added. You need this ID while configuring the app in Citrix Secure Private Access.



Relaying Party Identifier

If your SaaS app is already authenticated using ADFS, then you must already have the Relaying party trust added for that app. You need this ID while configuring the app in Citrix Secure Private Access.



Enable relay state in IdP initiated flow

RelayState is a parameter of the SAML protocol that is used to identify the specific resource the users access after they are signed in and directed to the relying party's federation server. If RelayState is not enabled in ADFS, users see an error after they authenticate to the resource providers that requires it.

For ADFS 2.0, you must install update KB2681584 (Update Rollup 2) or KB2790338 (Update Rollup 3) to provide RelayState support. ADFS 3.0 has RelayState support built in. In both cases RelayState still needs to be enabled.

To enable the RelayState parameter on your ADFS servers

1. Open the file.
    - For ADFS 2.0, enter the following file in Notepad: %systemroot%\inetpub\adfs\ls\web.config
    - For ADFS 3.0, enter the following file in Notepad: %systemroot%\ADFS\Microsoft.IdentityServer.Servicehost.exe.config
2. In the microsoft.identityServer.web section, add a line for useRelyStateForIdpInitiatedSignOn as follows, and save the change: `<microsoft.identityServer.web> ... <useRelayStateForIdpInitiatedSignOn enabled="true" /> ...</microsoft.identityServer.web>`
    - For ADFS 2.0, run `IISReset` to restart IIS.
3. For both platforms, restart the Active Directory Federation Services `(adfssrv) service.` **Note:** If you have windows 2016 or Windows 10 then use the following PowerShell command to enable it. `Set-AdfsProperties -EnableRelayStateForIdpInitiatedSignOn $true`

Link to commands

App configuration on Citrix Secure Private Access

You can either configure the IdP initiated flow or the SP initiated flow. The steps to configure IdP or SP initiated flow in Citrix Secure Private Access are the same except that for SP initiated flow, you must select the **Launch the app using the specified URL (SP initiated)** check box in the UI.

IdP initiated flow

1. While setting up the IdP initiated flow, configure the following.
    - **App URL** – Use the following format for the app URL. `https://<adfs fqdn>/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=<rp id>&RedirectToIdentityProvider=<idp id>`
    - **ADFS FQDN** – FQDN of your ADFS setup.
    - **RP ID** – RP ID is the ID that you can get from your relaying party trust. It is the same as the Relaying Party Identifier. If it is a URL, then URL encoding happens.

- **IDP ID** – IdP ID is the same as the claim provider trust ID. If it is a URL, then URL encoding happens.

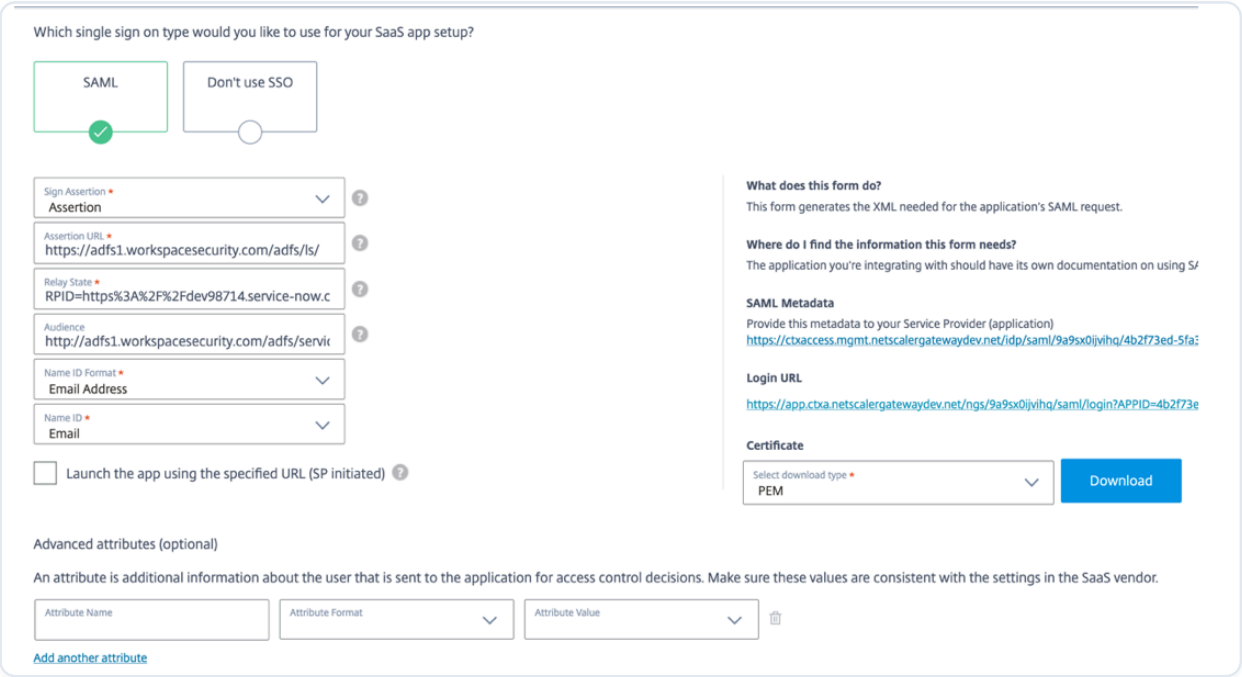
  Example

2. SAML SSO configuration.

   The following are the default values of the ADFS server. If any of the values are changed, get the correct values from the metadata of the ADFS server. Federation metadata of the ADFS server can be downloaded from its federation metadata endpoint, whose endpoint can be known from **ADFS > Service > Endpoints.**

   - **Assertion URL** – `https://<adfs fqdn>/adfs/ls/`
   - **Relay State** – Relay state is important for the IdP initiated flow. Follow this link to construct it properly - Relay State

     Example: RPID=https%3A%2F%2Fdev98714.service-now.com&RelayState=https%3A%2F%2Fdev98714.service-now.com%2F
   - **Audience** – `http://<adfsfqdn>/adfs/services/trust`
   - For the other SAML SSO configuration settings, see to the following image. For more details, Support for SaaS apps.



3. Save and subscribe the app to the user.

SP initiated flow

For SP initiated flow, configure the settings as captured in the **IDP initiated flow** section. In addition, enable the **Launch the app using the specified URL (SP initiated)** check box.

Citrix Secure Private Access Terraform provider

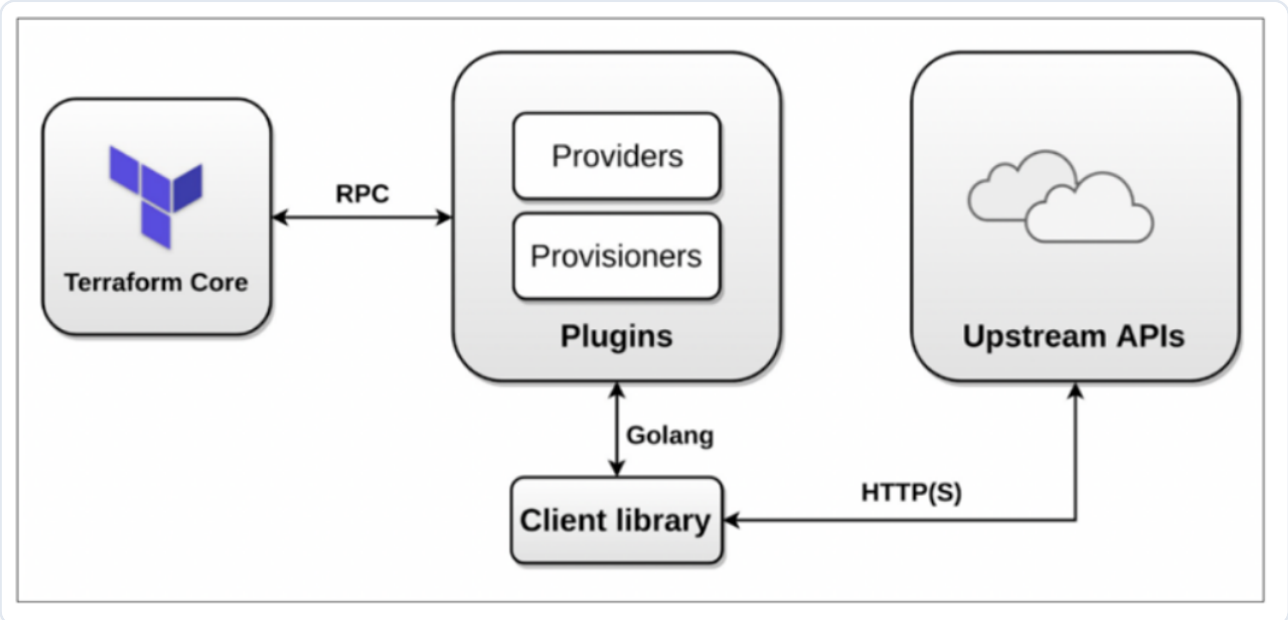
Managing Secure Private Access™ configurations manually through a UI can be time-consuming, error-prone, and difficult to scale across environments. Customers adopting infrastructure-as-code practices need a way to automate Secure Private Access configuration, enforce consistency, and integrate Secure Private Access changes into CI/CD pipelines.

The Citrix Secure Private Access Terraform provider enables customers to provision, configure, and manage Secure Private Access resources programmatically using Terraform. It allows Secure Private Access environments to be managed consistently, repeatedly, and at scale as part of an infrastructure-as-code workflow.

The Citrix Secure Private Access Terraform provider is applicable to:

- Citrix Secure Private Access cloud deployments.
- Customers using Terraform for infrastructure or configuration management.

The following diagram shows the Terraform provider architecture:



Key benefits

The Citrix Secure Private Access Terraform provider exposes Secure Private Access resources as Terraform-managed objects. Customers can define the Secure Private Access configuration declaratively, version it alongside application infrastructure, and apply changes in a predictable manner.

The key benefits of using this solution are:

- Infrastructure-as-code management for Secure Private Access.
- Consistent configuration across environments (dev, test, prod).
- Reduced manual effort and configuration drift.
- Easy integration with CI/CD pipelines and GitOps workflows.
- Faster onboarding and repeatable deployments.

Use case

You can use the Citrix Secure Private Access Terraform provider for the following use cases:

- Automate onboarding of new applications/policies into Secure Private Access.
- Standardize Secure Private Access configuration across multiple environments.
- Recreate or recover Secure Private Access environments using versioned Terraform state.
- Integrate Secure Private Access configuration changes into existing Terraform workflows.
- Enable DevOps teams to manage access policies alongside infrastructure.
- Migrate Secure Private Access configuration from trial tenant to production tenant.
- Merge Secure Private Access configuration of 2 customers for acquisition scenarios.

System requirements

Ensure that the following system requirements are met:

- Terraform v1.3 or later.
- Access to a Citrix Secure Private Access tenant.
- Network connectivity to Citrix Cloud™ APIs.

Prerequisites

Before using the Citrix Secure Private Access Terraform Provider, ensure that the following prerequisites are met:

- You have an active Citrix Secure Private Access subscription.
- You have permissions to manage Secure Private Access resources in your Citrix tenant.
- Terraform is installed and available in your environment.
- API credentials or authentication method for Citrix Cloud is configured.

Permissions

The Service Principal Authentication account used by Terraform must have permissions to:

- Create, update, and delete Secure Private Access resources.
- Read the existing Secure Private Access configuration for state reconciliation.

Installation

See Installing Terraform and Configuring the Citrix Terraform Provider.

Terraform configuration

With the Terraform provider, Secure Private Access configuration can be managed outside the Citrix UI. Customers can continue using the UI if needed, but Terraform is the recommended approach for automated and large-scale deployments.

To use the Terraform provider for Secure Private Access, you must define the provider in your Terraform configuration as follows:

```
terraform {

  required_providers {

    citrixspa = {

      source = "citrix/citrixspa"

      version = `<version>`
```

```
    }

  }

}



provider "citrixspa" {

  base_url      = "<https://api.cloud.com/accessSecurity>"  # for
commercial deployment

  customer_id   = "xxxxxxxxxxxx" # the CC customer id

  client_id     = "xxxxxxxxxxxx" # client id of service principal

  client_secret = "xxxxxxxxxxxx" # client secret of service principal

}
```

Once the provider is configured, you can define Secure Private Access resources using Terraform resource blocks and apply them using standard Terraform commands, such as:

- `terraform plan`
- `terraform apply`

> **Note:**
>
> The Terraform provider is enabled by default after it is declared in the Terraform configuration and initialized.

Troubleshooting issues

- **The `terraform apply` operation fails with authentication errors.**

  Cause: Invalid or missing Citrix Cloud credentials.

  Solution: Verify provider authentication configuration and permissions.

- **Unexpected changes detected in `terraform plan`.**

  Cause: Configuration drifts due to manual UI changes.

  Solution: Align changes through Terraform and refresh state if needed.

Limitations

- Not all Secure Private Access features might be available in the initial provider release.
- Changes made directly in the UI might cause Terraform state drift.
- The `terraform destroy` operations might not remove all dependent resources automatically.

Important considerations

- Terraform state files might contain sensitive configuration data and must be stored securely (for example, remote backends).
- We recommend that you manage Secure Private Access resources using Terraform exclusively after adoption.
- We strongly recommend pinning the provider version to avoid unexpected changes.
- Always review `terraform plan` output before applying changes.

References

- Terraform Registry documentation
- Terraform documentation

Visibility and monitoring

Admins can use the following features/resources for visibility and monitoring Secure Private Access.

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, in addition to the Secure Private Access dashboard. For details, see Integration with DaaS Monitor.

Secure Private Access usage dashboard

Visibility in to the Secure Private Access users, applications, policies, connector status is available in the Secure Private Access dashboard. Admins can use the dashboard to monitor these events. For details, see Dashboard.

Secure Private Access application and session monitoring

Monitor your Secure Private Access sessions and application trends across your organization by using Citrix Monitor. For details see the following topics:

- Monitor provides filtering functionalities for the sessions and applications making it easier to analyze user activities and address application performance issues. For details, see Sessions and application monitoring.
- Admins can view the session and error trends in Monitor that help identify patterns and troubleshoot issues. For details, see Error and session trends.

Connector Appliance health monitoring

The Connector Appliance component is automatically added as part of Infrastructure monitoring when you deploy Secure Private Access. Any Connector Appliance that is connected to the Citrix

DaaS site is automatically onboarded for comprehensive monitoring, providing administrators with real-time visibility into the health and performance of these critical infrastructure components.

For more information on Connector Appliance health monitoring, see Connector Appliance health metrics.

Secure Private Access usage dashboard

The Secure Private Access service dashboard displays the diagnostics and usage data of the SaaS, Web, TCP, and UDP apps. The dashboard provides admins full visibility into their apps, users, connectors health status, and bandwidth usage in a single place for consumption. This data is fetched from Citrix Analytics. The data for the various entities can be viewed for the preset time or for a custom timeline. For some of the entities, you can drilldown to view further details.

The metrics are broadly classified into the following categories.

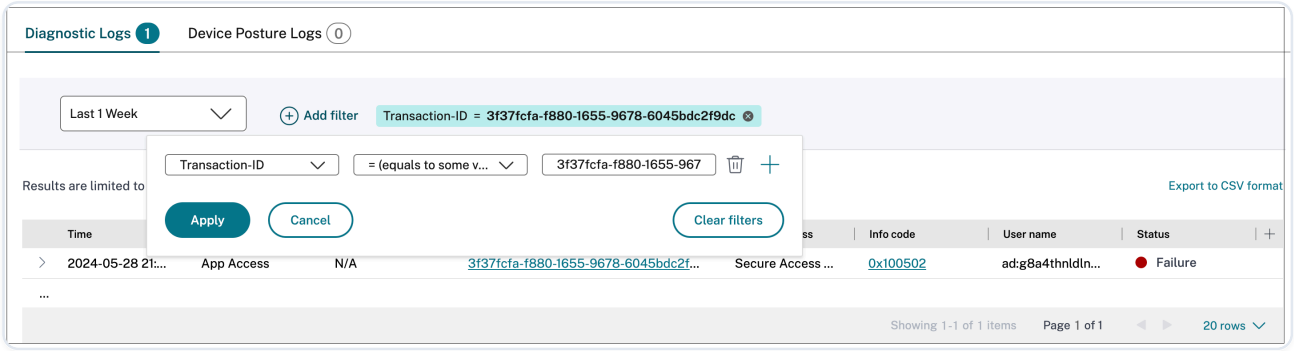
- **Logging and Troubleshooting**
  - Diagnostic logs: Logs related to authentication, application launch, app enumeration, and device posture checks.
- **Users**
  - Active users: Total number of unique users accessing the applications (SaaS, Web, and TCP) for the selected time interval.
  - Uploads: Total volume data uploaded through the Secure Private Access service for the selected time interval.
  - Downloads: Total volume of data downloaded through the Secure Private Access service for the selected time interval.
- **Applications:**
  - Applications: Total number of applications (independent of the time interval) configured currently.
  - Application launch count: Total number of applications (app sessions) launched by each user for the selected time interval.
  - Domains configured: Total number of domains configured for the selected time interval.
  - Applications discovered: Total number of unique, individual domains that have been accessed but are not associated with any apps

- **Access policies**
  - Access policies: Total number of access policies (independent of the time interval) configured currently.

Diagnostic logs

Use the **Diagnostics Logs** chart to view the logs related to authentication, application launch, app enumeration, and also logs related to device posture. You can click the **See more** link to view the details of the logs. The details are presented in a tabular format. You can view the logs for the pre-set time or for a custom timeline. You can add columns to the chart by clicking the + sign depending on what information you want to see in the dashboard. You can export the user logs into CSV format.

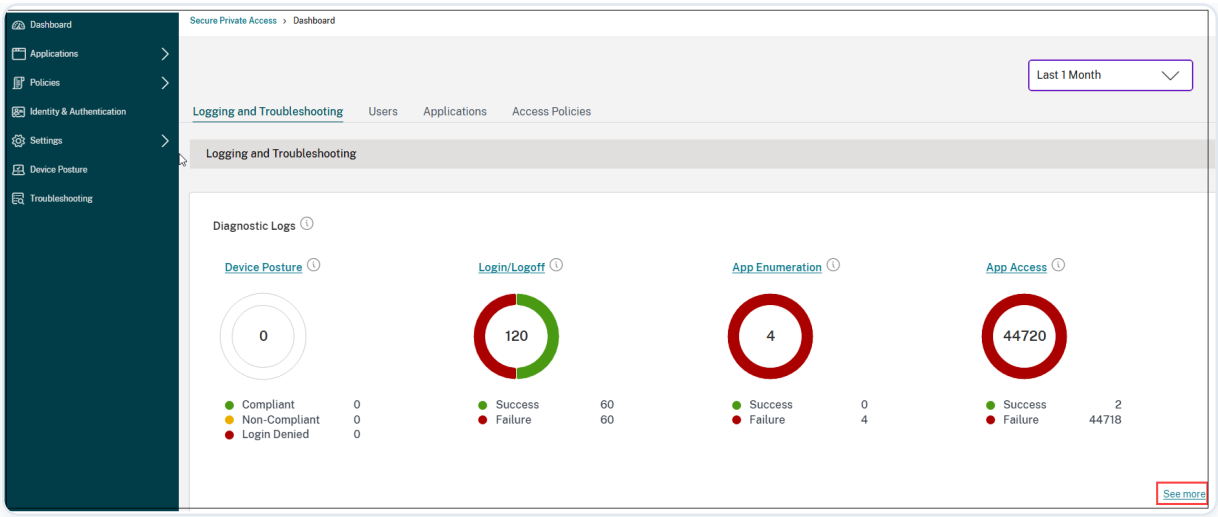
- You can use the **Add Filter** option to refine you search based on the various criteria such as app type, category, description. For example, in the search fields, you can select `Transaction ID`, `= (equals to some value)`, and enter `7456c0fb-a60d-4bb9-a2a2-edab8340bb15` in this sequence, to search for all logs related to this transaction ID. For details on search operators that can be used with the filter option, see Search operators.



- **Device posture logs:** You can refine your search based on the policy results (**Compliant, Non-compliant, and login Denied**). For details on device posture, see Device Posture.

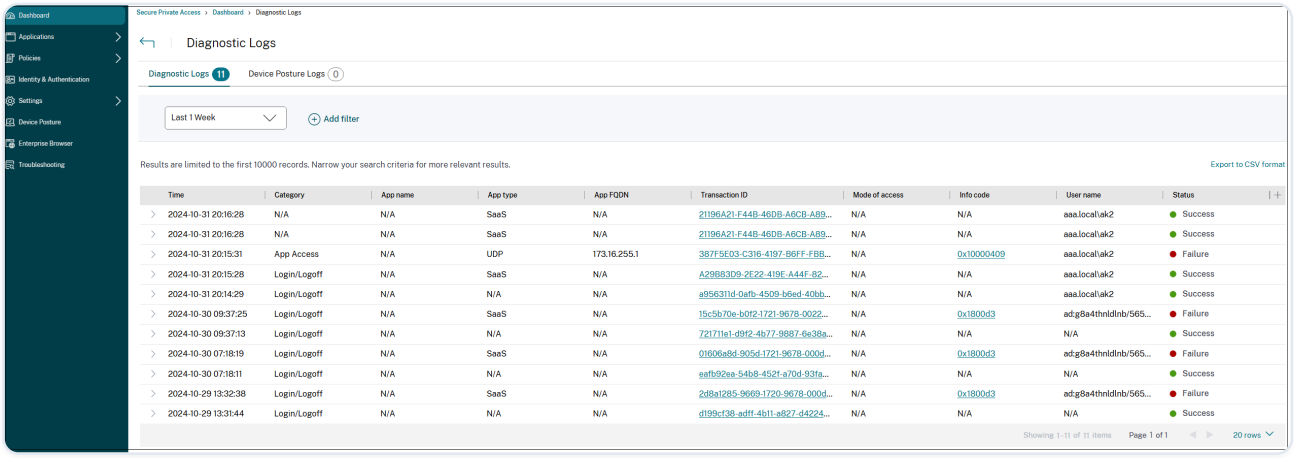
Note:

- Every failure event within the Secure Private Access diagnostic logs dashboard has an associated info code. For details, see Info code.
- Transaction ID correlates all Secure Private Access logs for an access request. For details, see Transaction ID.



- You can click the expand icon (>) to view the complete details of the logs.
- The **Diagnostic Logs** page displays the embedded domains for each of the main URLs that are accessed. Admins can view the embedded domains by clicking the expand icon (>) from the main URL. Admins can use the embedded domains list to address issues related to app access or app rendering. For example, if a domain was missed in the application configuration, then the specific app cannot be accessed by the end user. In this case, the admin can view the list of embedded domains, identify the missing domain, and then update the app configuration with the missing domain.

By default, the **Diagnostic Logs** page displays the current week's data and only the recent 10000 records. Use the custom date search and filters to refine your search results further.

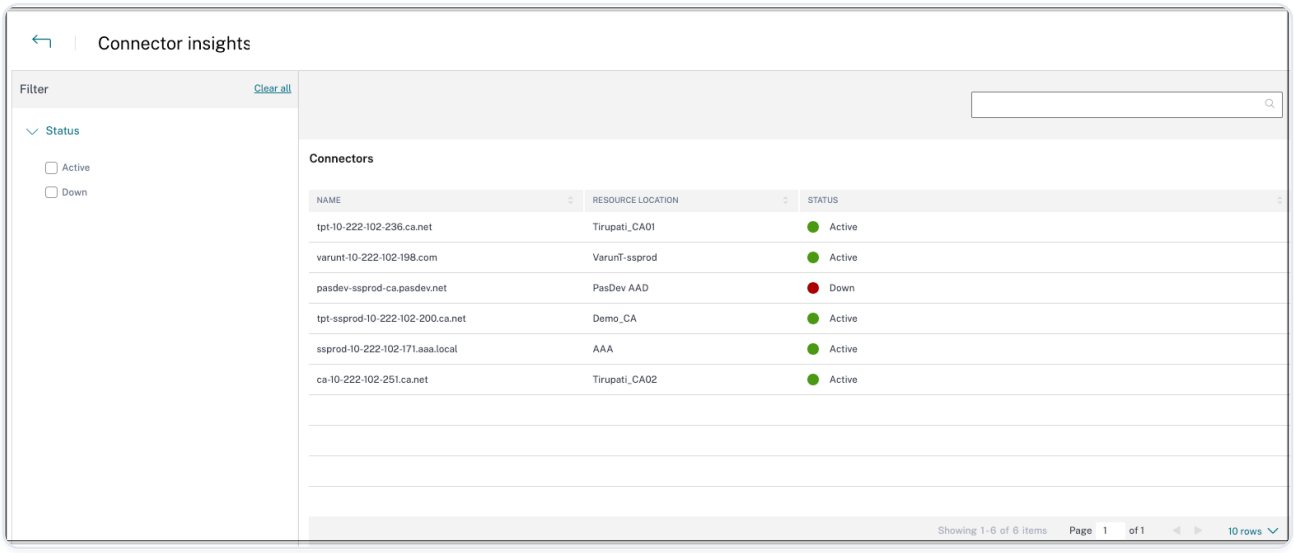


Important:

For a comprehensive list of errors that users might encounter when using the Secure Private Access service, see Info code lookup table.

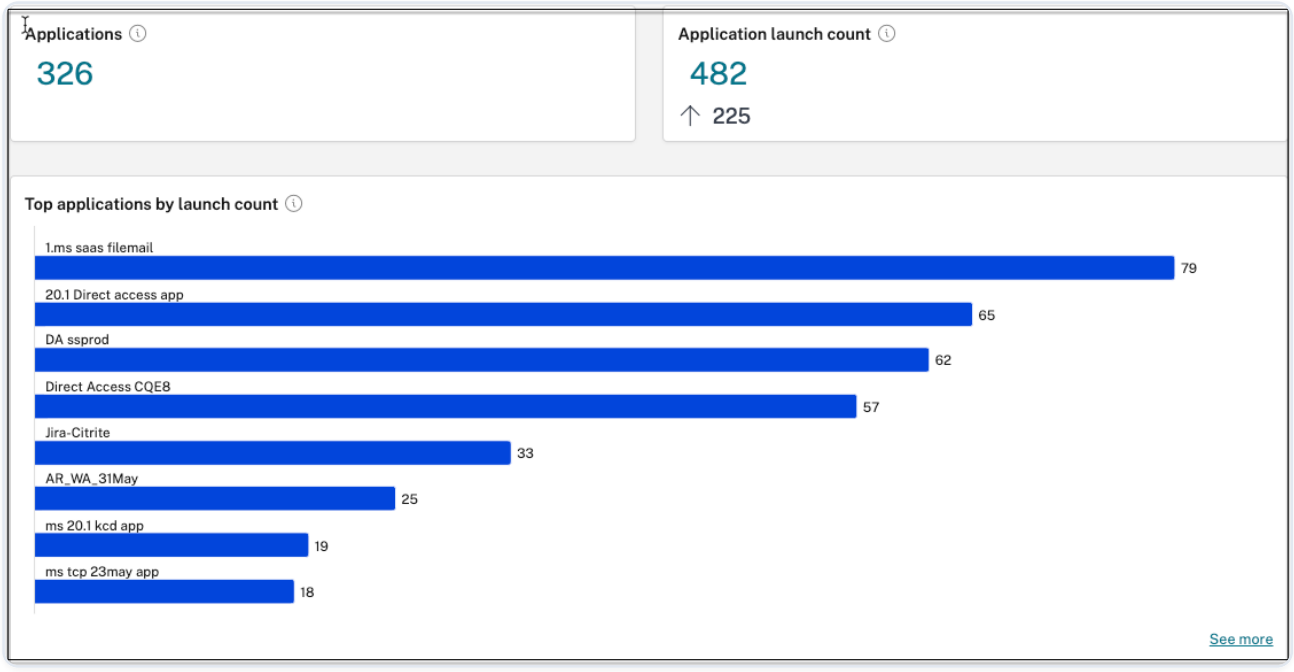
Connector status

Use the **Connector status** chart to view the status of the connectors and the resource locations where the connectors are deployed. Click the **See more** link to view the details. In the **Connector insights** page, you can use the filters **Active** or **Inactive** to filter the connectors based on their status.



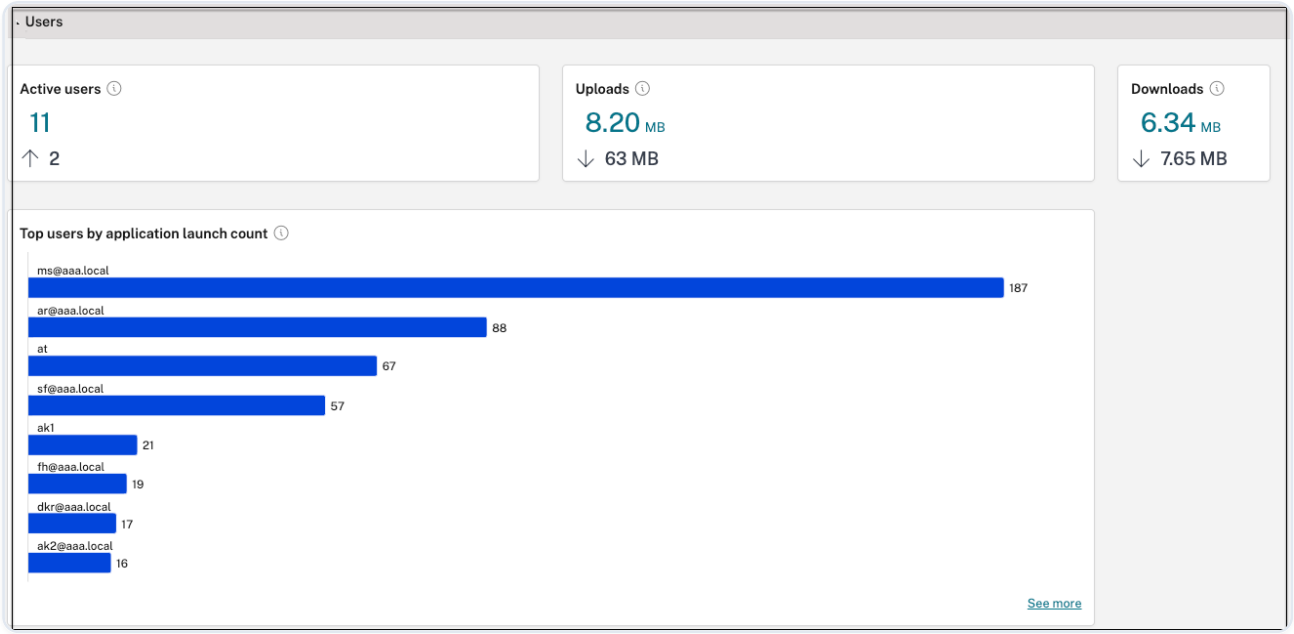
Top applications by launch count

Use the **Top applications by launch count** chart to view the list of top applications based on the number of the times the app was launched, the total volume of data uploaded to the app server, and the total volume of data downloaded from the app server. You can apply the filters **SaaS Apps**, **Web Apps**, or **TCP/UDP Apps** to narrow down your search to specific apps. You can filter the data for a pre-set timeline or for a custom timeline.



Top users by applications launch count

Use the **Top users by applications launch count** chart to view the data per user. For example, the number of times a user has launched the TCP app, the total volume of data uploaded to the app server, and the total volume of data downloaded from the app server. You can filter the data for a pre-set timeline or for a custom timeline.

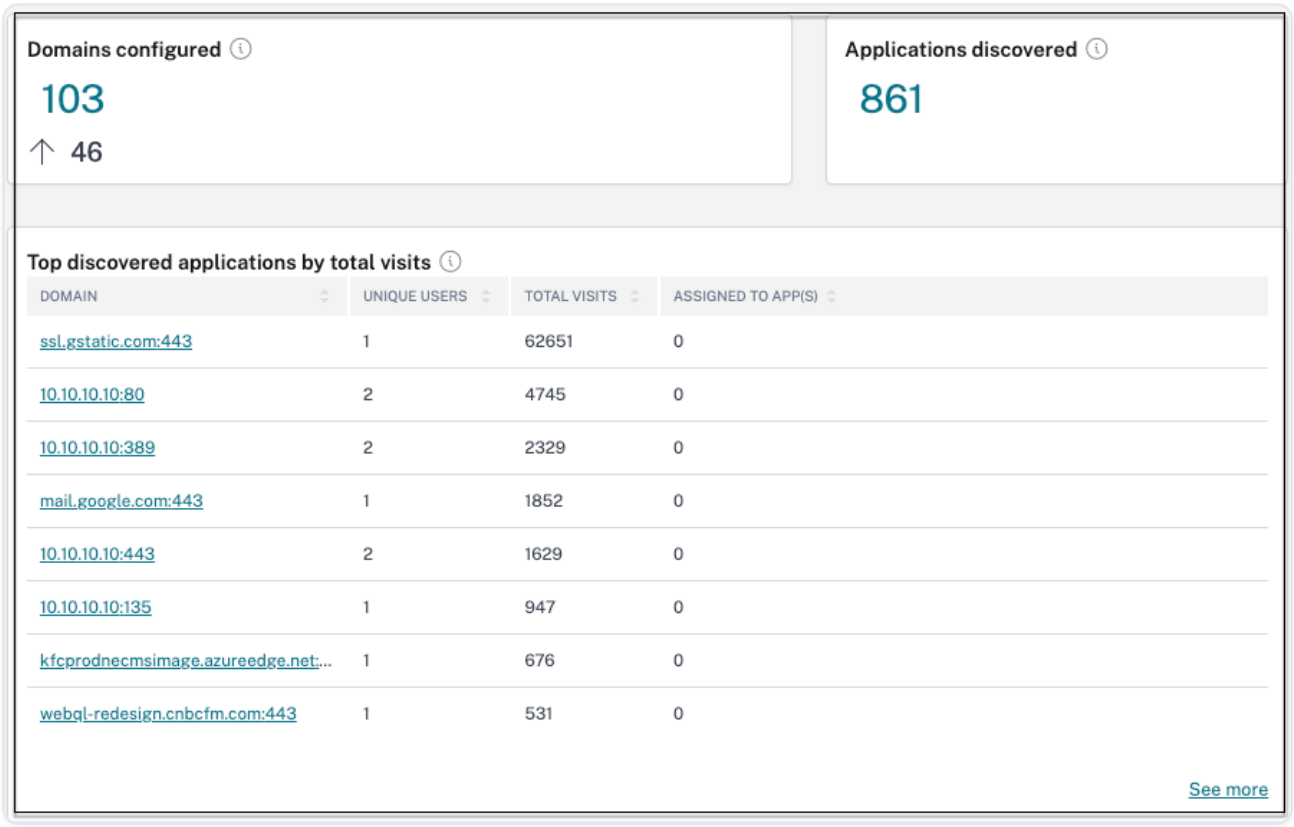


Top access policies by enforcement

Use the **Top access policies by enforcement** chart to view the list of access policies that are enforced on the apps. Click the **See more** link to view the list of policies that are associated with the apps and the number of times the policies are enforced. You can also use the **Search** option in the Access policies page to filter the policies based on the policy name. You can also search for specific policies using the search operators to further refine your search. For details, see Search operators.

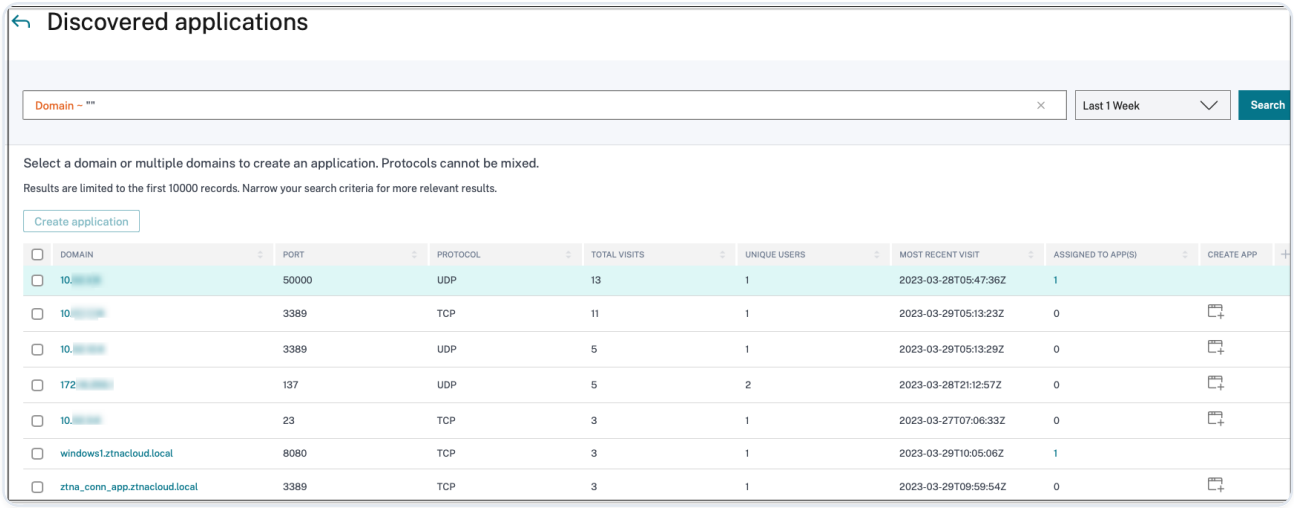
Top discovered applications

Use the **Top discovered applications by total visits** to view the list of unique, individual domains that have been accessed at some point but are not associated with any apps. These domains are listed based on the number of total visits to those domains. Admins can use this chart to see if any domain of particular interest is accessed by many users. In such cases, admins can create an app with that domain for easy accessibility.



In the chart, the **ASSIGNED TO APPs** column displays the total number of applications that have this domain configured as a part of their related URL or Destination URL values. Clicking the number displays the apps that are assigned to this domain.

You can click the **See more** link to view more details about all the domains.



The **Discovered applications** page displays the details of the domains such as domain name, port, protocol, total visits, unique users, and the most recent visit date. All the columns in the chart are sortable. You can use the search bar to search based on domain.

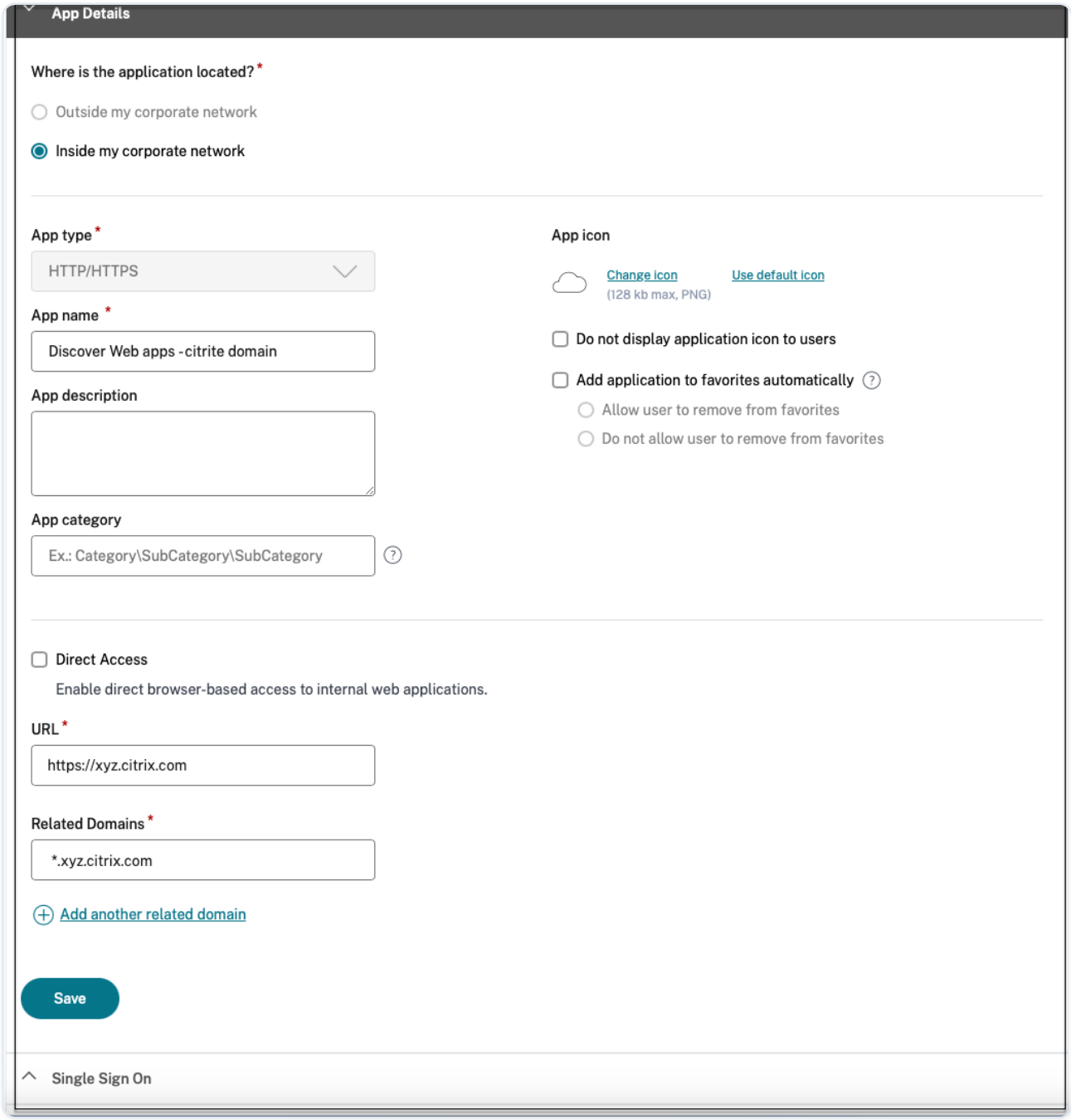
Note:

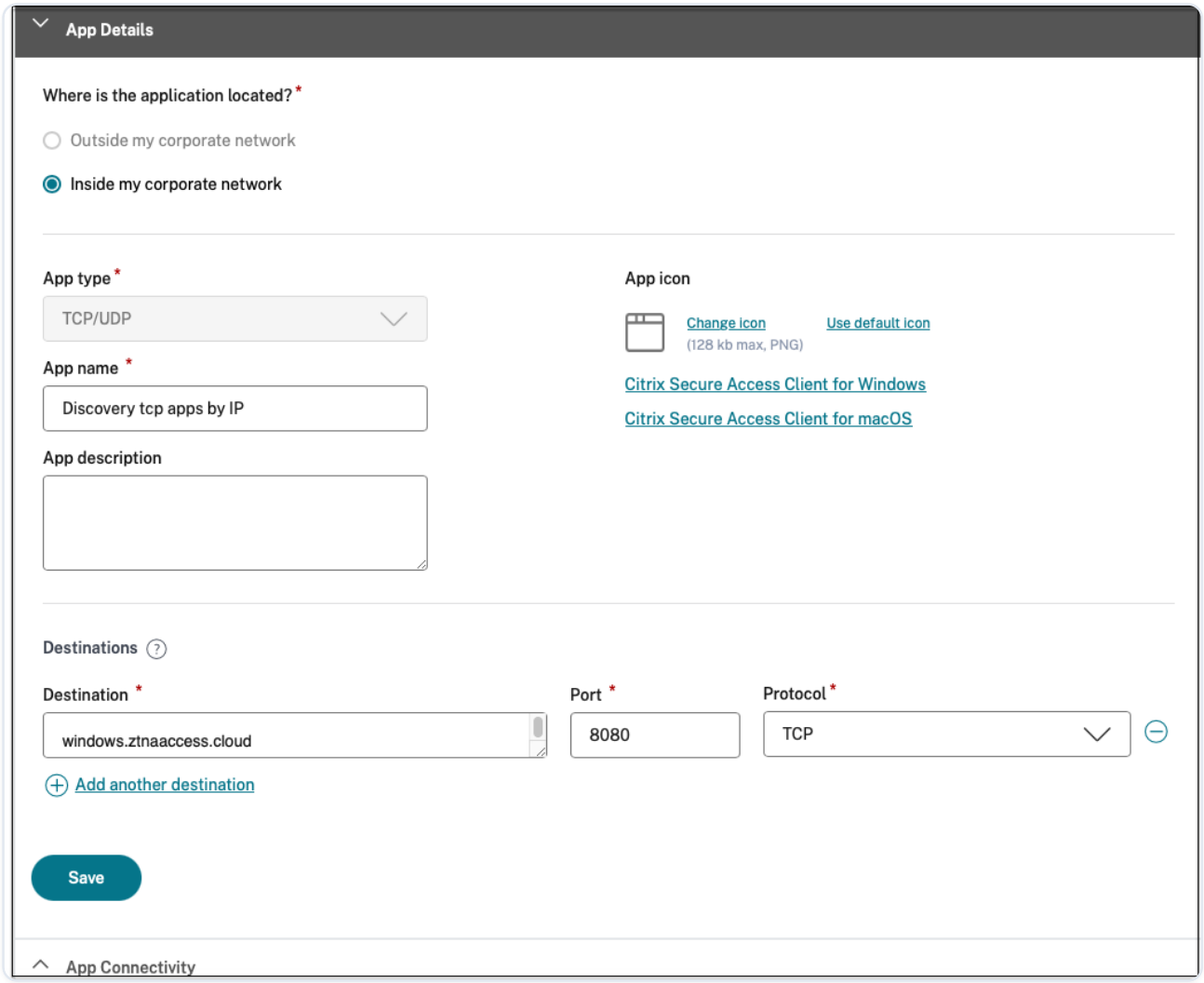
- The protocols are derived based on the standard ports used by customers.
- The list of discovered domains is limited to 10000 records.

Creating an app from the chart

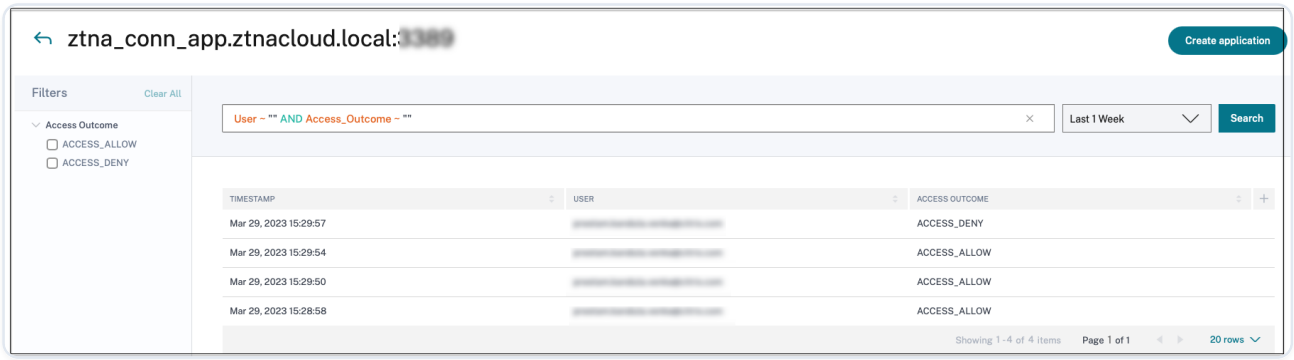
Click the **+** icon in line with the respective domain to create an app. The app configuration wizard pops up. The create app icon does not appear for the rows in which an app is already created with the same domain, port, and protocol combination, and is in complete state.

- The app type is auto populated based on the app's protocol that you have selected. However, you can change the type, if necessary.
- The values in the **URL, Related Domains, Destination, Port, Protocol** fields are all auto-populated. Complete the steps for adding an app. For details, see Admin-guided workflow for easy onboarding and set up.


App Details
Where is the application located? *
Outside my corporate network
Inside my corporate network
App type *
HTTP/HTTPS
App name *
Discover Web apps - citrite domain
App description
App category
Ex.: Category\SubCategory\SubCategory
App icon
Change icon
Use default icon
(128 kb max, PNG)
Do not display application icon to users
Add application to favorites automatically
Allow user to remove from favorites
Do not allow user to remove from favorites
Direct Access
Enable direct browser-based access to internal web applications.
URL *
https://xyz.citrix.com
Related Domains *
*.xyz.citrix.com
Add another related domain
Save
Single Sign On



You can also click the unique domain link to see more details and create an application for that domain. When you click a domain link, the user authentication logs for the domain are displayed. Click the **Create application** button. Complete the steps for adding an app.



Search operators

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

- **= (equals to some value)**: To search for the logs/policies that exactly match the search criteria.

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

Secure Private Access applications, seesions and trends

Secure Private Access is integrated with Monitor, the monitoring and troubleshooting console for Citrix DaaS. Administrators and help-desk personnel can use this integration to monitor and troubleshoot Web/SaaS and TCP/UDP application sessions and events from the DaaS Monitor console. This provides additional monitoring capabilities that complement the Secure Private Access dashboard.

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

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

To know more about the integration with Monitor, see Secure Private Access.

Applications, sessions, and trends

Monitor provides enhanced visibility into Secure Private Access sessions and their associated trends. This comprehensive monitoring capability offers granular insights into how applications are being accessed and used, as well as detailed information about individual user activity within these sessions. This allows administrators to gain a deeper understanding of user behavior, application performance, enabling proactive management and optimization of the Secure Private Access environment.

To understand the session definitions in the context of secure private access, see Session definitions.

To view a Secure Private Access session by user, see View a user session.

To view the session details, see Visibility for Secure Private Access service.



Health monitoring

The following sections provide more information about health monitoring.

Connector Appliance

Connector Appliance is a Citrix component hosted in your hypervisor. It serves as a channel for communication between Citrix Cloud and your resource locations, enabling cloud management without requiring any complex networking or infrastructure configuration. Connector Appliance enables you to manage and focus on the resources that provide value to your users. For details, see Connector Appliance for Secure Private Access.

The Connector Appliance health metrics feature provides an essential capability for monitoring the health and performance of the Connector Appliance component within the Citrix infrastructure. This component is automatically onboarded for monitoring when connected to a Citrix DaaS site, ensuring seamless integration into the Infrastructure monitoring dashboard.

The health metrics are displayed in the Infrastructure monitoring dashboard, providing a centralized view of the Connector Appliance's status. Administrators can access detailed metrics and trends to proactively identify and resolve issues.

The following figure displays a sample of the Connector Appliance health in Monitor.



Session and application trends

Administrators can monitor sessions and application trends across their organizations from the DaaS Monitor. This includes tracking rollouts, understanding how policies and configurations are functioning, and analyzing potential issues.

For details, see Visibility for Secure Private Access Service.

Sessions and application trends

Monitor your Secure Private Access sessions and application trends across your organization using Citrix Monitor. Track rollout progress, understand how your policies and configurations are performing, and identify if they are causing widespread user issues. Citrix Monitor provides comprehensive visibility into user activities and application usage patterns to optimize your deployment.

Citrix Monitor delivers real-time and historical insights into your Secure Private Access environment, enabling administrators to make data-driven decisions about resource allocation, policy adjustments, and user experience improvements. The monitoring capabilities help you maintain optimal performance while ensuring security compliance.

Session monitoring

Admins can monitor active user sessions in real-time using Monitor. You can monitor app failures for web/SaaS and TCP/UDP apps and view active sessions for web/SaaS apps in the Dashboard. For details see Visibility for Secure Private Access Service.

Application trends

Monitor Secure Private Access application access trends, view active application sessions, and identify applications experiencing issues or failures. Citrix Monitor provides comprehensive analytics to help you understand application usage patterns, optimize performance, and ensure reliable access to your organization's critical applications.

For detailed information about accessing these monitoring capabilities and interpreting the data, see Visibility for Secure Private Access Service.

Triage and troubleshoot

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.

Refer to the following topics for detailed information:

Troubleshoot app related issues

View the issues related to device posture status, login/logoff statuses, app enumeration, and app access. For details, see Troubleshoot app related issues.

Secure Private Access sessions codes in DaaS Monitor

View the list of error codes related to application enumeration, application launch, and sessions in Citrix Monitor. For details, see Secure Private Access sessions codes in DaaS Monitor.

Troubleshoot sessions related issues in Monitor

Use the Monitor's Help Desk view (Activity Manager page) to view information about the user or endpoint. For details, see Troubleshoot sessions related issues in Monitor.

Troubleshoot device posture related issues

You can troubleshoot the Device Posture issues/errors in DaaS Monitor using the transaction ID that is generated for each session when a user connects through Secure Private Access or DaaS. When you locate the transaction ID, the DaaS Monitor displays information about the session and the associated Device Posture policy that was applied. Monitor also displays the policy results, including whether the device passed or failed the posture checks. For details, see Device Posture service troubleshooting.

Troubleshoot authentication related issues

Whenever any conditional authentication fails, you can use the transaction ID available in the failure message and search in the Monitor for the failure details. Monitor helps you to troubleshoot conditional authentication failure events by displaying failure reasons and conditional policies on the Monitor UI. For details, see Authentication Troubleshooting.

Troubleshooting using logs

The Secure Private Access and Device Posture logs help administrators identify configuration issues, connectivity problems, policy misconfigurations, and device compliance issues enabling faster identification and resolution of issues.

Secure Private Access logs

You can view the Secure Private Access logs from the Secure Private Access dashboard. For information on the various events captured in diagnostic logs, see Events.

For more information on the Secure Private Access diagnostic logs, see Diagnostic logs.

For the various error codes associated with each event, see Diagnostic log info codes.

Device Posture logs

The diagnostic logs in the Device Posture dashboard offer insights into to device compliance (Compliant, Non-compliant, and Login Denied). These logs enable administrators to monitor endpoint security, ensure adherence to organizational policies, and identify devices that might present environmental risks.

You can view the Device Posture logs and events in the Secure Private Access dashboard and in the Identity and Access Management console.

For more information, see Device Posture logs and events.

Real-time session troubleshooting using Monitor

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.

Diagnostic logs error codes

The following table provides a comprehensive list of the various errors that users can possibly run into when using the Secure Private Access service and the corresponding resolution.

INFO CODE	DESCRIPTION	RESOLUTION
0x180022	App launch failed as authentication service is down	App launch failed as the authentication service is down
0x1800B7	App launch failed because App FQDN length exceeded	App launch failed because App FQDN length exceeded
0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7	Web app launch failed as unable to connect to back end web app	Web app launch failed as unable to connect to back end web app
0x18001A, 0x18001B	User details not found	User details not found
0x1800AA	Web/SaaS app launch has failed due to user attributes not found while preparing the SAML token	Web/SaaS app launch has failed
0x180010	Web/SaaS app launch has failed due to inability to identify the application FQDN	Web/SaaS app launch has failed due to inability to identify the application FQDN
0x180040	Web/SaaS app launch has failed due to invalid appId provided by the SAML service provider	App launch failed due to invalid appId provided by the SAML service provider

INFO CODE	DESCRIPTION	RESOLUTION
0x180011, 0x180012, 0x180013, 0x180017, 0x180032, 0x180033, 0x180034, 0x180035, 0x180048	Web/SaaS app launch has failed due to invalid app access request	Web/SaaS app launch has failed due to invalid app access request
0x1800D4, 0x1800E1, 0x180106, 0x180107, 0x1800EB, 0x1800EC	App launch has failed during policy evaluation due to internal error	App launch has failed during policy evaluation due to internal error
0x1800D9	App launch has failed while parsing policy evaluation response	App launch has failed while parsing policy evaluation response
0x1800DA	App launch has failed with invalid result during policy evaluation	App launch has failed with invalid result during policy evaluation
0x1800DB	App launch has failed with invalid resource location configuration	App launch has failed with invalid resource location configuration
0x1800E0	App launch failed as the length of the app name is too long	App launch failed as the length of app name is too long
0x1800EE	App launch has failed during connection establishment to the private TCP server due to invalid app ID	App launch has failed during connection establishment to the private TCP server due to invalid app ID
0x1800E3	App launch has been denied during policy evaluation	App launch has been denied during policy evaluation
0x1800EA	App launch has failed due to destination FQDN being too long	App launch has failed due to destination FQDN being too long
0x1800ED	App launch has failed due to invalid destination IP	App launch has failed due to invalid destination IP

INFO CODE	DESCRIPTION	RESOLUTION
0x180102	App launch failed as no response was received from the Connector Appliance	App launch failed as no response was received from the Connector Appliance
0x10000005	Web/SaaS application launch failed due to a failure to establish a connection with the back-end app server	Web/SaaS application launch failed due to a failure to establish a connection with the back-end app server
0x10000101, 0x10000102, 0x10000103, 0x10000104	Web/SaaS FormFill SSO failed due to invalid application configuration	Web/SaaS FormFill SSO failed due to invalid application configuration
0x10000202	Kerberos SSO for Web/SaaS failed	Kerberos SSO for Web/SaaS failed
0x10000203	Web/SaaS SSO failed due to internal server error	Web/SaaS SSO failed due to internal server error
0x10000303, 0x10000304	Web/SaaS app launch failed due to the configured proxy being unreachable	Web/SaaS app launch failed due to the configured proxy being unreachable
0x10000305	Web/SaaS app launch failed due to a failure to authenticate with the configured proxy	Web/SaaS app launch failed due to a failure to authenticate with the configured proxy
0x10000414	Application launch failed due to a request coming on an invalid IP/hostname or port	Application launch failed due to a request coming on an invalid IP/hostname or port
0x10000415	Application launch failed as the destination server refused the connection	Application launch failed as the destination server refused the connection
0x10000416	Application launch failed as the destination was not found	Application launch failed as the destination was not found

INFO CODE	DESCRIPTION	RESOLUTION
0x10000417	Application launch failed as the destination network was not reachable	Application launch failed as the destination network was not reachable
0x10000405	Application launch failed due to the inability to connect to the destination	Application launch failed due to the inability to connect to the destination
0x10000301	Connector to SPA service connection failed	Connector to Secure Private Access service connection failed
0x10000302	Connector failed to read the proxy details	Connector failed to read the proxy details
0x10000306	Configured proxies are not reachable	Configured proxies are not reachable
0x10000401	Connector Appliance not able to reach to FR	Connector Appliance not able to reach FR (Edge node)
0x10000403, 0x10000404, 0x10000407	Application launch failed due to the internal connection error	Application launch failed due to the internal connection error
6003, 6007	Citrix Secure Access client failed to do SSO	Citrix Secure Access client failed to do SSO

App launch failed as authentication service is down

Info code: 0x180022

Secure Private Access allows admins to configure a third-party authentication service such as the traditional Active Directory, AAD, Okta, or SAML. Outages in these authentication services can this issue.

Check if the third-party servers are up and reachable.

App launch failed because app FQDN length exceeded

Info code: 0x1800B7

App FQDNs must not exceed 512 characters. Check the application FQDN in the app configuration page to ensure that it does not exceed this limit.

1. Go to the **Applications** tab in the admin console.
2. Look for the application whose FQDN exceeds 512 characters.
3. Edit the application and fix the app FQDN length.

Web app launch failed as unable to connect to back end web app

Info code: 0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7

Broken browsing experience of web applications running inside the corporate network.

1. Filter through the diagnostic logs for the FQDNs that are not resolvable.
2. Check for reachability of the back-end server from inside the corporate network.
3. Check the proxy settings to see if the connector is blocked from reaching the back-end server.

User details not found

Info code: 0x18001A, 0x18001B

Domain user details are not found while the Secure Private Access service is processing the request. This issue might occur when the necessary domain user attributes are from Citrix Cloud™ are missing.

1. Ensure that the Citrix Cloud Connector™ has no issues in syncing the users to Citrix Cloud.
2. Ensure that the domains in **Citrix Cloud > Identity and Access Management** are reachable.
3. Log out and log in again to Citrix Workspace.

Web/SaaS app launch has failed due to user attributes not found while preparing the SAML token

Info code: 0x1800AA

Necessary user attributes are not found while the Secure Private Access service is preparing the SAML token. This issue might occur when the necessary domain user attributes from Citrix Cloud are missing.

1. Ensure that the Citrix Cloud Connector has no issues in syncing the users to Citrix Cloud.
2. Ensure that the domains in **Citrix Cloud > Identity and Access Management** are reachable.
3. Log out and log in again to Citrix Workspace.

Web/SaaS app launch has failed due to inability to identify the application FQDN

Info code: 0x180010

No application found for the given domain name.

Ensure that the domain name length doesn't exceed the configuration limit.

Web/SaaS app launch has failed due to invalid appId provided by the SAML service provider

Info code: 0x180040

The AppId provided by the SAML service provider is invalid. Not able to find the app with given app ID by the SAML service provider.

1. Check the SAML service provider configuration.
2. Ensure that the IdP URL configured at the SAML service provider is appropriate.
3. This app ID must map with the app configured at the Secure Private Access service.

Web/SaaS app launch has failed due to invalid app access request

Info code: 0x180011, 0x180012, 0x180013, 0x180017, 0x180032, 0x180033, 0x180034, 0x180035, 0x180048

App access failed due to an invalid request received by the Secure Private Access service.

Cannot identify the application received by the Secure Private Access service. Received request parameters might be invalid.

1. Re-launch the application or log out and log in again to Citrix Workspace.
2. If the issue persists, contact Citrix Support.

App launch has failed during policy evaluation due to internal error

Info code: 0x1800D4, 0x1800E1, 0x180106, 0x180107, 0x1800EB, 0x1800EC

Contact Citrix Support with the transaction ID and client collected debug logs.

App launch has failed while parsing policy evaluation response

Info code: 0x1800D9

Application configuration might possibly have special characters or there might be an issue in the policy configuration.

Ensure that the TCP/UDP/HTTP apps configuration does not contain unsupported characters.

1. Click **Applications** in the Secure Private Access admin console.
2. Check if the application name or destinations contain any special characters.

Check if the policies are configured correctly and are assigned to the correct applications.

1. Click **Access Policies** in the Secure Private Access admin portal.
2. Review the policy configuration, policy name, and conditions.
3. Check if the policy is assigned to the correct application.

If the configurations are good, contact Citrix Support with the transaction ID and client debug logs.

App launch has failed with invalid result during policy evaluation

Info code: 0x1800DA

There might be an application or policy configuration issue. Ensure that the TCP/UDP/HTTP apps configuration does not contain unsupported characters.

1. Click **Applications** in the Secure Private Access admin console.
2. Check if the application name or destination domain/FQDN contains any special characters.
3. Also check if the destination IP/IP range/IP CIDRs are valid.

Ensure that the **Application Domain** table (**Secure Private Access > Settings > Application Domain**) has application destination entry enabled.

Check if the policies are configured correctly and are assigned to the correct applications.

1. Click **Access Policies** in the Secure Private Access admin portal.
2. Review the policy configuration, policy name, and conditions.
3. Check if the policy is assigned to the correct application.

App launch has failed with invalid resource location configuration

Info code: 0x1800DB

There might be an issue with the resource location and configuration

Ensure that the resource location is configured.

1. Log in to the Citrix Cloud portal and click **Resource Locations** from the menu.
2. Check if the expected resource location is configured.

Ensure that the resource location is healthy and active.

1. Log in to the Citrix Cloud portal and click **Resource Locations** from the menu.
2. Check if the expected resource location is active and healthy.

Ensure that the correct resource location is selected for the destination in the **Application Domain** table (**Secure Private Access > Settings > Application Domain**).

1. Click **Settings** in the Secure Private Access admin console.
2. Click the **Application Domain** tab.
3. Check if the accessed destination has the correct resource location configured.
4. Check if the accessed destination entry is active in the **Application Domain** table.

   The destinations configured in the TCP/UDP/HTTP application are automatically added to the **Application Domain** table. It is recommended not to delete/disable active TCP/UDP/HTTP application's destinations/URL.

App launch failed as the length of app name is too long

Info code: 0x1800E0

Contact Citrix support with the transaction ID and client collected debug logs.

App launch has failed during connection establishment to the private TCP server due to invalid app ID

Info code: 0x1800EE

Contact Citrix support with the transaction ID and client collected debug logs.

App launch has been denied during policy evaluation

Info code: 0x1800E3

Contact Citrix support with the transaction ID and client collected debug logs.

App launch has failed due to destination FQDN being too long

Info code: 0x1800EA

Ensure that the FQDN length is under 256 characters.

App launch has failed due to invalid destination IP

Info code: 0x1800ED

Access only valid private IP addresses from the clients.

App launch failed as no response was received from the Connector Appliance

Info code: 0x180102

Check the reachability of Connector Appliance.

Application launch failed due to a request coming on an invalid IP/hostname or port

Info code: 0x10000414

Check the validity of the host name, IP address, or port number.

Application launch failed as the destination server refused the connection

Info code: 0x10000415

Check the status of the destination server.

Application launch failed as the destination was not found

Info code: 0x10000416

Check the destination server host name.

Application launch failed as the destination network was not reachable

Info code: 0x10000417

Connector Appliance has connectivity issue with the back end Private TCP/UDP servers. Check the Network settings for your Connector Appliance.

- Check if the back end server that the end user is trying to connect is up and running and is able to receive the requests.
- Check for the reachability of the back-end servers from inside the corporate network.
- Check the proxy settings to see if the connector is blocked from reaching the back-end server.
- If the request for an FQDN based app, check the DNS entry for the respective app in the DNS server.

Application launch failed due to the inability to connect to the destination

Info code: 0x10000405

Connector Appliance has connectivity issue with the back end Private TCP/UDP servers. Check the Network settings for your Connector Appliance.

- Check if the back end server that the end user is trying to connect is up and running and is able to receive the requests.
- Check for the reachability of the back-end servers from inside the corporate network.
- Check the proxy settings to see if the connector is blocked from reaching the back-end server.
- If the request for an FQDN based app, check the DNS entry for the respective app in the DNS server.

Connector to Secure Private Access service connection failed

Info code: 0x10000301

- Look up the transaction ID for the error code.
- Filter all events matching the transaction ID in the Secure Private Access dashboard.
- Check if any error occurred in the other component matching the transaction ID if found do the respective workaround matching to that error code.
- If no error is found in other components, then do the following:
  - Go to the Connector Appliances admin page.
  - Download the diagnostic report. For details, see Generating a diagnostic report.
  - Capture the packet trace. For details, see Verify your network connection.
- Contact Citrix support with this diagnostic report and packet trace along with the error code and transaction ID.

Connector failed to read the proxy details

Info code: 0x10000302

Connector Appliance has connectivity issue with the back-end private TCP/UDP servers. Check the Network settings for your Connector Appliance.

- Check if the back-end server that the end user is trying to connect is up and running and is able to receive the requests.
- Check for the reachability of the back-end servers from inside the corporate network.
- Check the proxy settings to see if the connector is blocked from reaching the back-end server.

- If the request for an FQDN based app, check the DNS entry for the respective app in the DNS server.

Configured proxies are not reachable

Info code: 0x10000306

Connector Appliance has connectivity issue with the back-end private TCP/UDP servers. Check the Network settings for your Connector Appliance.

- Check if the back-end server that the end user is trying to connect is up and running and is able to receive the requests.
- Check for the reachability of the back-end servers from inside the corporate network.
- Check the proxy settings to see if the connector is blocked from reaching the back-end server.
- If the request for an FQDN based app, check the DNS entry for the respective app in the DNS server.

Connector Appliance not able to reach FR (Edge node)

Info code: 0x10000401

Check the network connectivity with the Citrix Secure Private Access service.

For more information, see Network settings for your Connector Appliance.

Application launch failed due to the internal connection error

Info code: 0x10000403, 0x10000404, 0x10000407

- Look up the transaction ID for the error code.
- Filter all events matching the transaction ID in the Secure Private Access dashboard.
- Check if any error occurred in the other component matching the transaction ID. If an error is found, do the respective workaround matching to that error code.
- If no error is found in other components, then do the following:
  - Go to the Connector Appliances admin page.
  - Download the diagnostic report. For details, see Generating a diagnostic report.
  - Capture the packet trace. For details, see Verify your network connection.
- Contact Citrix support with this diagnostic report and packet trace along with the error code and transaction ID.

Web/SaaS application launch failed

Web/SaaS application launch failed due to a failure to establish a connection with the back-end app server.

Info code: 0x10000005

Check the target URL or check the Connector Appliance network settings. For details, see Network settings for your Connector Appliance.

Web/SaaS FormFill SSO failed due to invalid application configuration

Info code: 0x10000101, 0x10000102, 0x10000103, 0x10000104

Check the SSO form app configuration and make sure that the user name, password, action, and login URL fields are correctly configured on the app settings.

Kerberos SSO for Web/SaaS failed

Info code: 0x10000202

Kerberos SSO for Web/SaaS failed due to either an internal server error with Connector Appliance or an inability to fetch the token from the Domain Controller.

Check the Kerberos SSO settings on the back-end server and the domain controller. Also check the fallback NTLM authentication settings.

For details, see Validating your Kerberos configuration.

Web/SaaS SSO failed due to internal server error

Info code: 0x10000203

Check the SSO settings in the Secure Private Access service and the back-end server. For Secure Private Access service, see Set the preferred sign-on method.

Web/SaaS app launch failed due to the configured proxy being unreachable

Info code: 0x10000303, 0x10000304

Check the proxy server settings and make sure that it is reachable to Connector Appliance. For details, see Register your Connector Appliance with Citrix Cloud.

Web/SaaS app launch failed due to a failure to authenticate with the configured proxy

Info code: 0x10000305

Check the proxy server credentials and make sure that they are configured correctly in Connector Appliance. For details, see After registering your Connector Appliance.

Citrix Secure Access™ client failed to do SSO

Info code: 6003

Error retrieving the Secure Private Access single sign-on handle from the Broker Agent service.

Check if the Secure Private Access SSO flag is enabled on the delivery group. For details, see Seamless log in from Citrix Secure Access Client on VDA.

Info code: 6007

Failed to log in to Secure Private Access.

Re-launch the VDA if the Citrix Secure Access client session is timed out.

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
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

CODE	STATUS	DESCRIPTION
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
4002	Deny	Application launch was denied because no policy matched

CODE	STATUS	DESCRIPTION
4101	Failure	Application launch error - An internal error occurred during application launch
4102	Failure	Application launch error (internal)
4103	Allow/deny/failure	Error retrieving policy details for the app
4104	Failure	Application Launch Error - No application configuration found

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.

CODE	DESCRIPTION	RESOLUTION/WORKAROUD
5016	Destination server connection failed	Verify network reachability to the destination (ping -S `<SNIP>` from NetScaler Gateway).
5017	Destination server DNS resolution failed	Make sure the hostname your application uses is resolved by the intended DNS servers (internal vs public).
5018	Gateway internal error	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).

Secure Private Access logs and events

The logs and events are crucial for monitoring, troubleshooting, and ensuring compliance. The Citrix Secure Private Access service-related logs and events can be accessed from the following sources:

Diagnostic dashboard

The diagnostic dashboard provides a centralized interface for viewing and analyzing logs and events. Admins can use this dashboard for monitoring and troubleshooting issues related to Secure Private Access. For details, see Secure Private Access dashboard.

List of errors

For a comprehensive list of errors that users might encounter when using the Secure Private Access service, see Diagnostic log info codes.

Audit logs

Audit logs capture detailed records of user activities and system changes. These logs are essential for compliance and security purposes, as they help track who accessed the system, what changes were made, and when these actions occurred. For details, see Audit and System Logs.

System logs

System Logs contain information about the internal operations of the Secure Private Access service. These logs are useful for diagnosing system-level issues, such as performance issues or errors in service functionality. For details, see System Log.

Device posture logs

Device posture logs provide insights into the security posture of devices accessing the Secure Private Access service. These logs help ensure that devices meet the required security standards before granting access, thus enhancing overall security. For details, see Device Posture logs.

Diagnostic logs

The following sections provide more information about the diagnostic logs.

FAQ

The following sections provide more information about the frequently asked questions.

What are Secure Private Access diagnostic logs?

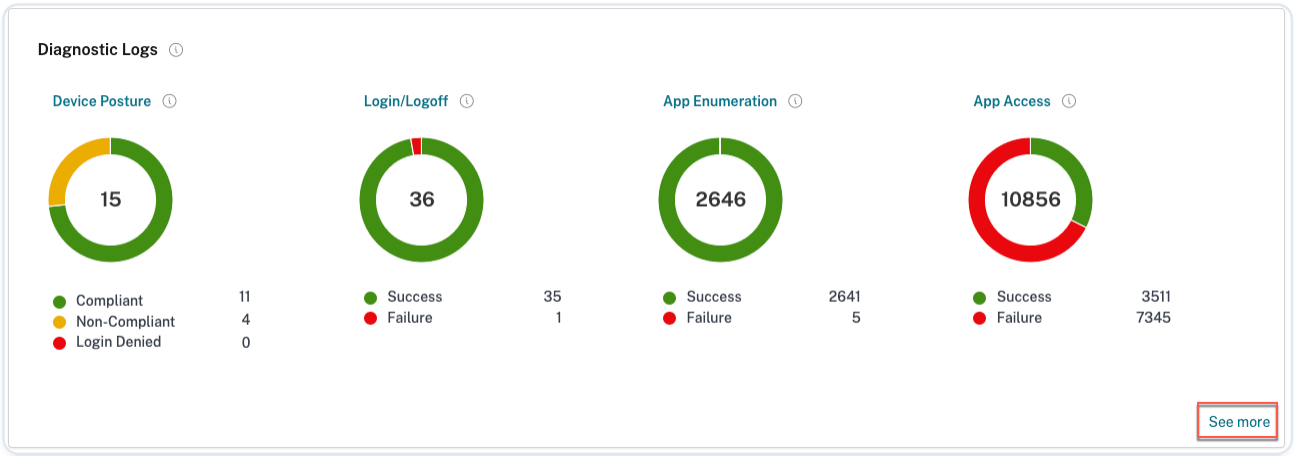
Secure Private Access diagnostic logs capture all events that occur when a user accesses any application (Web/SaaS/TCP/UDP). These logs capture device posture, app authentication, app enumeration, and app access logs. The details are presented in a tabular format. You can view the logs for the pre-set time or for a custom timeline. You can add columns to the chart by clicking the + sign depending on what information you want to see in the dashboard. You can export the user logs into CSV format.

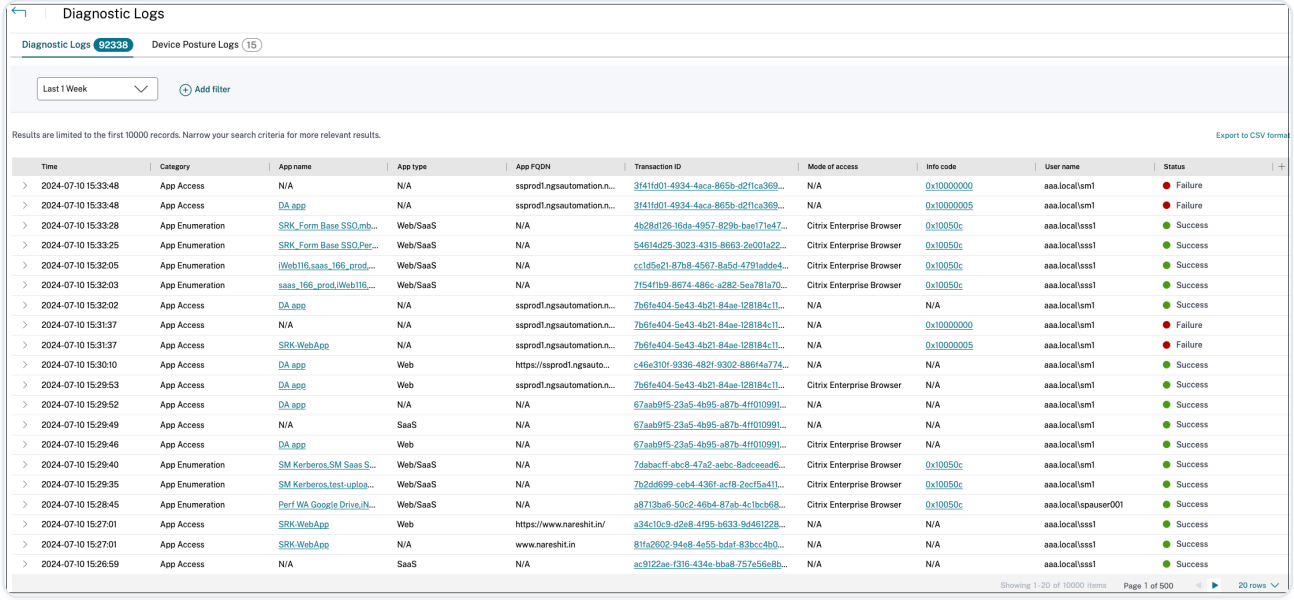
Where do I find Secure Private Access logs?

1. Log on to Citrix Cloud.
2. On the Secure Private Access service tile, click **Manage**.
3. Click **Dashboard** on the left navigation in the admin user interface.
4. In the **Diagnostic Logs** chart, click the **See more** link.

Which widget displays the Secure Private Access diagnostic logs?

The **Diagnostics Logs** widget in the **Logging and Troubleshooting** section displays a pie chart view of all Secure Private Access events related to authentication, application launch, app enumeration, and also logs related to device posture. The Secure Private Access diagnostic logs fetch events from multiple internal components, each sending an event when an end user accesses an application. These events are divided in categories; **Login/Logoff**, **App Enumeration**, and **App Access**. The pie chart displays the overall success/failures ratio of each category. Clicking the colored pie on any chart takes you to the diagnostic logs where you can find the appropriate events. There are also device posture logs if you have Device Posture service enabled. You can also click the **See more** link to view the complete diagnostic logs.





What details can I find in the Secure Private Access diagnostic logs?

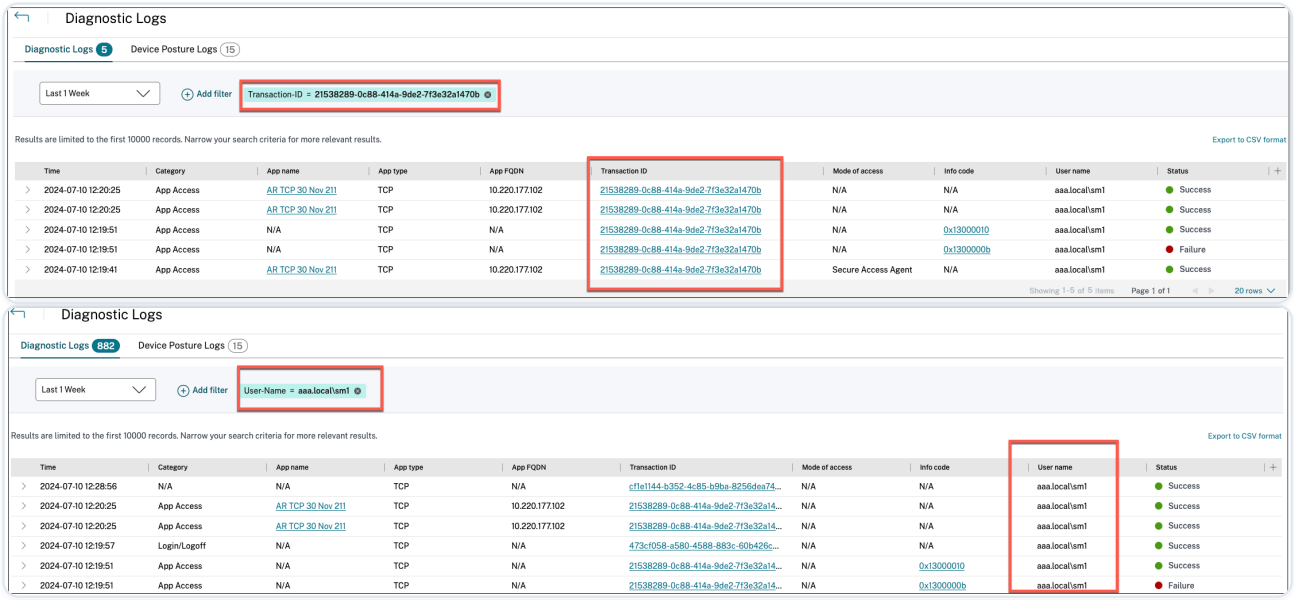
The Secure Private Access user logs dashboard provides the following details, by default.

- **Timestamp** - Time of the event in UTC.
- **Username** - User name of the end-user accessing the app.
- **App Name** - Name of the app/apps that were accessed.
- **Policy Info** - Name of the access policy or policies that were triggered during the event.
- **Status** - Status of the event, success, or failure.
- **Info Code** - Code associated with each failure event within the Secure Private Access diagnostic logs dashboard. See more information on info code.
- **Description** - Reason for the failure or more details about the event.
- **APP FQDN**: FQDN of the application accessed.
- **Event type** - Event type associated with the operation performed.
- **Operation type** - Operation for which the log is generated.

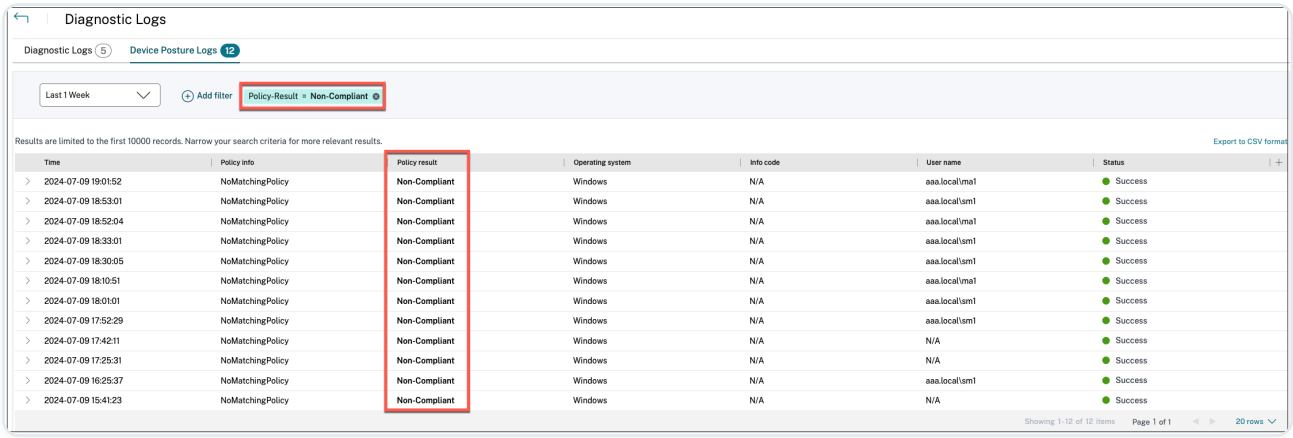
- **Category** - Category available, depending on the type of event. Available options are: app authentication, app enumeration, or app access. These options are also available as filter options. You can use these options to filter logs depending on the type of issue that you are facing.
- **Transaction ID** - Transaction ID correlates all Secure Private Access logs for an access request. Learn how to use a transaction ID. The following details can be fetched by clicking the + button on the rightmost side of the dashboard:
- **SPA PoP Location** - Name/ID of the Secure Private Access service PoP location that was used during app access. See Secure Private Access PoP Locations.

How do I filter the diagnostic logs?

You can use the **Add Filter** option to refine you search based on the various criteria, such as app type, category, description. For example, in the **Search** field, you can click **Transaction ID, = (equals to some value), and enter 21538289-0c88-414a-9de2-7f3e32a1470b**, to search for all logs related to this transaction ID. For details on search operators that can be used with the filter option, see Search operators.



You can also use the various filter options to refine your search on the Device Posture logs.



What events are captured in the Secure Private Access diagnostic logs?

The Secure Private Access diagnostic logs capture the following events:

- **Device Posture:** End-user device status. These logs capture information about the device posture results, whether the device was deemed compliant, non-compliant, or denied access based on your device posture policy.
- **Login/Logoff**: Events related end-user logon or logoff status to the Citrix Secure Access client and authentication to stores (internal or external providers).
- **App Enumeration**: In the Secure Private Access service, access policies configured by admins decide which user gets to access which app. Denied applications are not visible (not enumerated) to end-users within Citrix Workspace App. These events help you know which applications were allowed or denied Access to a user based on the access policies configured within the Secure Private Access service.
- **App Access**: Events of end-user application/endpoint access, allow/deny status, single sign-on status, and connectivity status as per the configured access policies for the selected time interval.

List of errors

For a comprehensive list of errors that users might encounter when using the Secure Private Access service, see Diagnostic log info codes.

Diagnostic log info codes

Use this topic to troubleshoot some of the app configuration, authentication and SSO, or app access-related issues. Copy the info code from the 'Info Code' column within the Secure Private Access diagnostic logs and then search for that code on this page to find the corresponding troubleshooting steps. The following are some FAQs to help you use this topic better.

For more information on the diagnostic logs, see Diagnostic logs.

The following error lookup table provides a comprehensive overview of the various errors that users can possibly run into when using the Secure Private Access service.

INFO CODE	DESCRIPTION	RESOLUTION
0x180006, 0x1800B7	App launch failed because App FQDN length exceeded	App launch failed because app FQDN length exceeded
0x180022	App launch failed as Authentication Service is down	App launch failed as authentication service is down
0x180001, 0x18001A, 0x18001B, 0x18008A	Single sign-on errors, Connection establishment failure between Citrix Cloud and on-premises connectors, SAML SSO failure, Invalid app FQDN	App access is denied
0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC		
0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0		
0x1800B1, 0x1800B2, 0x1800B3, 0x180048		
0x1800EF	Problem connecting to Connector Appliance	Problem connecting to Connector Appliance
0x18009D	DNS lookup/Connection failed	Secure Browser Service - DNS lookup/connection errors
0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5	Web app launch failed as unable to connect to back end web app	Web app launch failed as unable to connect to back-end web app
0x1800A6, 0x1800A7		
0x1800BC, 0x1800BF	User is not entitled to access the Web/SaaS app	User is not entitled to access the Web/SaaS app
0x1800BD	User is not entitled to access the Web/SaaS app for DirectAccess	User is not entitled to access the Web/SaaS app for DirectAccess

INFO CODE	DESCRIPTION	RESOLUTION
0x1800D0	Citrix Secure Access agent Session launch has failed while fetching the application configuration	Citrix Secure Access agent Session launch has failed while fetching the application configuration
0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA	Citrix Secure Access agent Session launch has failed while fetching the application configuration, Citrix Secure Access agent App launch has failed during policy evaluation, Citrix Secure Access agent App launch has failed	Malformed client requests
0x1800DE	Citrix Secure Access agent App launch has failed during Policy evaluation	Citrix Secure Access agent App launch has failed during Policy evaluation
0x180055, 0x1800DF, 0x1800E3	Apps restricted by contextual policy, Access denied due to policy configuration	One or more apps not listed in the user dashboard
0x1800EB	Citrix Secure Access agent app launch has failed as IPv6 is not supported	Citrix Secure Access agent app launch has failed as IPv6 is not supported
0x1800EC, 0x1800ED	Citrix Secure Access agent App launch has failed due to invalid IP address	Citrix Secure Access agent App launch has failed due to invalid IP address
0x10000001, 0x10000002, 0x10000003, 0x10000004	Citrix Secure Access client login failure due to network issue	Network connectivity reachability issue with Citrix Secure Access client
0x10000006	Citrix Secure Access client login failure due to proxy in the middle	Proxy server interfering client connectivity with service

INFO CODE	DESCRIPTION	RESOLUTION
0x10000007	Citrix Secure Access client login failure due to untrusted certificate authority	Untrusted server certificate issue is observed
0x10000008	Citrix Secure Access client login failure due to invalid certificate	Invalid server certificate issue is observed
0x1000000A	Citrix Secure Access client login failure due to configuration issue	Login failed as configuration is empty for the user
0x1000000B	Citrix Secure Access client login failure due to connection failure	Connection terminated by the network or end user
0x10000010	Citrix Secure Access client login failure due to expired session	Configuration download failed as session is expired
0x10000013	Citrix Secure Access client login failure due huge configuration list	Citrix Secure Access client failed to log in
0x11000003	Citrix Secure Access client login failure due to control channel creation failure	Control channel establishment failed as the session expired
0x11000004	Citrix Secure Access client login failure due control channel creation failure	Control channel establishment failed
0x11000005	Citrix Secure Access client login failure due control channel creation failure	Control channel establishment failed
0x11000006	Citrix Secure Access client login failure due control channel creation failure	Control channel establishment failed because of network issue

INFO CODE	DESCRIPTION	RESOLUTION
0x12000001	Citrix Secure Access client logout failure as session already expired	Unable to logoff as session is terminated
0x12000002	Citrix Secure Access client logout failure as session already timed out	Session is forcefully terminated
0x13000001	App access failed as the session expired	Application launch failed as session is expired
0x13000002	App access failed as inadequate license	Application Launch failed because of license issue
0x13000003, 0x13000008, 0x001800DF	App access failed as access forbidden, TCP/UDP app launch is denied as per Policy	Application launch failed as access is denied by service
0x13000004, 0x13000005	App access failed as the server is unavailable	Application launch failed as the client is unable to reach the service
0x13000007	App access failed as the access policy is disabled or the user is not subscribed	Application launch failed as policy evaluation and config validation failed
0x13000009	App access failed as the routing entry is missing	Application launch failed because of issues in application domain table
0x1300000B	The client closed the connection	Client closed the connection with Secure Private Access service
0x1300000C	The FQDN resolution over ZTNA failed	Unable to resolve FQDN by the DNS server
0x1300000E	App launch failed due to use of non-Chrome browser	App launch failed due to use of a non-Chrome browser

INFO CODE	DESCRIPTION	RESOLUTION
0x001800D3	Applications configuration download failure while login	Failed to fetch configured application destinations list
0x001800D9, 0x001800DA	TCP/UDP app launch has failed during parsing policy evaluation response, TCP/UDP app launch has failed with invalid result during policy evaluation	Application configuration issue
0x001800DB	TCP/UDP app launch has failed with invalid resource location configuration	Issue with resource location
0x13000006, 0x001800DC, 0x001800DD	TCP app launch has failed due to unsupported Enhanced Security policy configured for the app, TCP app launch has failed due to unsupported Secure Browser Service redirection configured for TCP App	Enhanced security policy is bound to the HTTP application
0x001800DE	TCP/UDP app launch has failed as there is no application configuration found for the destination	Unable to locate the application
0x001800EA	TCP app launch has failed due to destination FQDN is too long	Host name length exceeds 256 characters
0x001800ED	TCP app launch has failed because of invalid destination IP	Invalid IP address
0x001800EF	TCP app launch has failed during connection establishment to private TCP server	Unable to establish end-to-end connection

INFO CODE	DESCRIPTION	RESOLUTION
0x001800F5	UDP app launch failed because of IPV6 address	IPv6 received in the app request
0x001800F9	UDP Traffic failed to deliver as client connection is lost	UDP traffic failed to deliver
0x001800FF	UDP Data traffic delivery failed	UDP data traffic delivery failed
0x10000401	Citrix rendezvous server dial failed	Application launch failed because of network connectivity issues
0x10000402, 0x1000040C	Unable to register the Connector Appliance, UDP network connection initialization failure	Connector appliance failed to register to Secure Private Access service
0x10000403, 0x10000404, 0x10000407, 0x1000040A	Connection error, Control packet transmission failure, Error on reading Gateway service, Control packet parsing failure, Error on writing gateway service	Connectivity issue with Connector Appliance
0x1000040B, 0x1000040F, 0x10000410		
0x10000405, 0x10000408, 0x10000409, 0x1000040D	Back-end Unreachable, UDP packet transmission failure, UDP packet receiving failure, Error on writing back-end, back-end closed the connection	Connectivity issues with Connector Appliance and back-end private TCP/UDP servers
0x1000040E, 0x10000412		
0x10000406	DNS resolution failed	Connector appliance fails to resolve DNS for FQDNs
0x10000411	Gateway service closed the connection	Private server connection terminated
0x10000413	Error in determining connection teardown reason	Failed to connect or send data to the private service IP or FQDN

INFO CODE	DESCRIPTION	RESOLUTION
0x100508	User context does not match the access rule conditions	No matching policy condition
0x100509	Access policy not associated with the application	No access policy associated with the application
0x10050C	Policy evaluation results of multiple applications that the user might be entitled to	App enumeration information
0x00180101	TCP/UDP app launch failed as routing entry is missing in application domain table	TCP/UDP app launch failed as routing entry is missing in application domain table
0x00180102	TCP/UDP app launch failed as connectors are not healthy	TCP/UDP app launch failed as connectors are not healthy
0x00180103	UDP/DNS request failed, as Connector is unreachable	UDP/DNS request failed, as Connector is unreachable
0x20580001	Failed to load the page as NGS Cookie is expired	Failed to load the page as NGS Cookie is expired
0x20580002	Access policy fetch failed because of network failure	Access policy fetch failed because of network failure
0x20580003	Access policy fetch failed while parsing the JSON web token	Access policy fetch failed while parsing the JSON web token
0x20580004	Network failure to fetch Access Policy details	Network failure to fetch Access Policy details
0x20580005	Policy fetch failed while fetching public certificate	Policy fetch failed while fetching public certificate
0x20580007	Policy fetch failed while validating signature of JWT	Policy fetch failed while validating signature of JWT

INFO CODE	DESCRIPTION	RESOLUTION
0x20580008	Policy fetch failed while validating the public certificate	Policy fetch failed while validating the public certificate
0x2058000A	Failed to determine store environment to form a policy URL	Failed to determine store environment to form a policy URL
0x2058000B	Failed to get response of access policy fetch request	Failed to get response of access policy fetch request
0x2058000C	Access policy fetch failed due to an expired secondary DS auth token	Access Policy fetch failed due to an expired secondary DS auth token
0x10200002	Connector appliance is not registered	Connector appliance is not registered
0x10200003	Unable to connect to connector appliance	Unable to connect to connector appliance
0x10000301	Connection to Citrix SPA service failed	Connection to Citrix Secure Private Access service failed
0x10000303, 0x10000304	The proxy server is not reachable	Proxy server is not reachable
0x10000305	Proxy server authentication failed	Proxy server authentication failed
0x10000306	Configured proxy servers are not reachable	Configured proxy servers are not reachable
0x10000307	Received error response from backend server	Received error response from backend server
0x10000005	Unable to send request to the target URL	Unable to send request to the target URL
0x10000107	Failed to process SSO	Failed to process SSO

INFO CODE	DESCRIPTION	RESOLUTION
0x10000108, 0x1000010B	Failed to process SSO, unable to determine SSO settings	Failed to process SSO, unable to determine SSO settings
0x10000101, 0x10000102, 0x10000103, 0x10000104	FormFill SSO failed, incorrect form app configuration	FormFill SSO failed, incorrect form app configuration
0x1000010A	FormFill SSO failed, incorrect form app configuration	FormFill SSO failed, incorrect form app configuration
0x10000202	Kerberos SSO failed	Kerberos SSO failed
0x10000203	Failed to process SSO for auth type	Failed to process SSO for auth type
0x10000204	Kerberos SSO failed but falling back to NTLM	Kerberos SSO failed but falling back to NTLM
0x14000001	Multiple ZTNA entitled accounts configured in the Citrix Workspace application	Multiple ZTNA entitled accounts configured in Citrix Workspace application

Resolution steps

The following sections provide resolution steps for most of the info codes. For the codes that do not have the resolution steps captured, contact Citrix Support.

One or more apps not listed in the user dashboard

Info code: 0x180055, 0x1800DF, 0x1800E3

Due to the contextual policy settings, apps might not be seen for some users or devices. Parameters like trust factors (device posture or risk score) can affect the accessibility of the applications.

1. Copy the transaction ID from the `reasons` column for error code `0x18005C` in the Diagnostic Logs csv file.
2. Modify the `prod` column filter in the csv file to show events from the component called `SWA.PSE` or `SWA.PSE.EVENTS`. This filter shows logs related to policy evaluation only.
3. Search for the evaluated policy payload in the `reason` column. This payload shows the evaluated policy for the user's context for all apps that the user is subscribed to.

4. If the policy evaluation indicates as app denied for the user, the possible reasons can be:
    - Incorrect matching conditions in policy - check App policy configuration in Citrix Cloud™
    - Incorrect matching rules in policy - check App policy configuration in Citrix Cloud
    - Incorrect matching default rule in policy - this is a fall-through case. Adjust the conditions accordingly.

User is not entitled to access the Web/SaaS app

Info code: 0x1800BC, 0x1800BF

The user might have clicked the app link for which the user might not have a subscription.

Ensure that the user has a subscription to the applications.

1. Go to the application in the management portal.
2. Edit the app and go to the **Subscription** tab.
3. Ensure that the targeted user has an entry in the subscription list.

Slow back-end app performance

Info code:0x18000F

There are cases where the customer network is flaky due to the connectors in a resource location that can be down or the back-end server itself might not be responding.

1. Ensure that the connector appliance is positioned geographically close to the back-end server to rule out network latencies.
2. Check if the back-end server's firewall is not blocking the connector appliance.
3. Check if the client is connecting to the nearest cloud POP.

    For example, `nslookup nssvc.dnsdiag.net` on the client, the canonical name in the answer indicates the geo-specific server such as `aws-us-w.g.nssvc.net.`

App launch failed because App FQDN length exceeded

Info code: 0x180006, 0x1800B7

App FQDNs must not exceed 512 characters in length. Check the application FQDN in the app configuration page. Ensure that the length does not exceed 512 bytes in size.

1. Go to the **Applications** tab on the management console.
2. Look for the application whose FQDN exceeds 512 characters.

3. Edit the application and fix the app FQDN length.

App details length exceeded

Info code: 0x18000E

Check the policies if they are blocking the app access.

1. Go to **Access Policies**.
2. Look for the policies where the app has entitlement.
3. Review the policy rules and conditions for the end user.

App access is denied

Info code: 0x180001, 0x18001A, 0x18001B, 0x18008A, 0x1800A9, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3, 0x180048

This is related to contextual policies, where policies are denying the app for a given user.

Check the policies if they are blocking the app access

1. Go to **Access Policies**.
2. Look for the policies where the app has entitlement.
3. Review the policy rules and conditions for the end user.

Applications not enumerated

Applications can be missing from the enumerated list because of policy denials or if the Secure Private Access integration is not enabled.

- If access must be enabled for some of the apps but you see zero apps, try enabling the Secure Private Access integration.
    - Sign into Citrix Cloud.
    - Select **StoreFront Cloud** from the hamburger menu, and then click **Service Integrations**.
    - Click the ellipsis button in Secure Private Access, and then click **Enable**.
- If the Secure Private Access integration is already enabled, disable it, and then enable it again to see if you have any apps.

Problem connecting to Connector Appliance

Info code: 0x1800EF

App routing fails because of non-availability of TCP connections with on-premises connectors.

REVIEW EVENTS FROM THE CONTROLLER COMPONENT

1. Look up the `transaction ID` for error code `0x1800EF` in the diagnostic logs csv file.
2. Filter all events matching the transaction ID in the csv file.
3. Also, filter the `prod` column in the csv file that match `SWA.GOCTRL`.

   If you see events with the `connectType` message `multiconnect::success`? then;

   - This indicates that the tunnel establishment request was relayed to the controller successfully.
   - Check if the `Resource Location` in the log message is correct. If it is incorrect, fix the resource location in the app configuration section on the Citrix management portal.
   - Check if the `VDA Ip and Port` in the log message is correct. The VDA IP and port indicates the back-end application IP and port. If it is incorrect, fix the app FQDN or IP address in the app configuration section on the Citrix management portal.
   - Proceed to review the Connector events if you don't find any earlier mentioned issues.

   If you see events with the `connectType` message `connect::failure` or `multiconnect::success`, then;

   - Check if the recommended fix for this log message states - `Check if connector is still connected to same pop`. This indicates that the connector at the resource location might have gone down. Proceed to review the Connector events.
   - Contact Citrix Customer support if the earlier mentioned messages are not seen.

   If you see events with the `connectType` message `IntraAll::failure`, then contact Citrix customer support.

REVIEW EVENTS FROM THE CONNECTOR COMPONENT

1. Look up the `transaction ID` for error code `0x1800EF` in the Diagnostic Logs csv file.
2. Filter all events matching the transaction ID in the csv file.
3. Also filter the `prod` column in the csv file that match `SWA.ConnectorAppliance.WebApps`.
4. If you see events with `status` as `failure`, then;

   - Review the `reason` message for each of these failure events.
   - `UnableToRegister` indicates that the connector wasn't able to register to Citrix Cloud successfully. Contact Citrix Support.

- `IsProxyRequiredCheckError` or `ProxyDialFailed` or `ProxyConnectionFailed` or `ProxyAuthenticationFailure` or `ProxiesUnReachable` indicates that the connector wasn't able to resolve the back-end URL through the proxy configuration. Check the proxy configuration for correctness.
- For further debugging see Connector SSO events.

Single sign-on errors

For single sign-on, different SSO attributes from the app configuration are extracted and applied during app launch. If that particular user doesn't have the attributes or if the attributes are incorrect, the single sign-on might fail. Ensure that the configuration looks correct.

1. Go to **Access Policies.**
2. Look for the policies where the app has entitlement.
3. Review the policy rules and conditions for the end user.

SSO methods such as Form SSO, Kerberos, and NTLM are performed by the on-premises connector. Review the following diagnostic logs from the connector.

REVIEW SSO EVENTS FROM THE CONNECTOR COMPONENT

1. Filter the `component name` in the csv file that match `SWA.ConnectorAppliance.WebApps`.
2. Do you see events with status as "failure"?

    - Review the message for each of these failure events.
    - `IsProxyRequiredCheckError` or `ProxyDialFailed` or `ProxyConnectionFailed` or `ProxyAuthenticationFailure` or `ProxiesUnReachable` indicates that the connector wasn't able to resolve the back-end URL through the proxy configuration. Check the proxy configuration for correctness.
    - `FailedToReadRequest` or `RequestReceivedForNonSecureBrowse` or `UnableToRetrieveUserCredentials` or `CCSPolicyIsNotLoaded` or `FailedToLoadBaseClient` or `ProcessConnectionFailure` or `WebAppUnSupportedAuthType` indicates tunneling failure. Contact Citrix Support.
    - `UnableToConnectTargetServer` indicates that the back-end server is unreachable from the connector. Check the back-end configuration again.
    - `IncorrectFormAppConfiguration` or `NoLoginFormFound` or `FailedToConstructForLoginActionURL` or `FailedToLoginViaFormBasedAuth` indicates form-based authentication failure. Check the form SSO configuration section in App configuration in the Citrix management portal.

- `NTLMAuthNotFound` indicates NTLM based authentication failure. Check the NTLM SSO configuration section in the app configuration in the Citrix management portal.
- For further debugging, see Connector events.

App launch failed as authentication service is down

Info code: 0x180022

Secure Private Access allows admins to configure a third-party authentication service such as the traditional active directory, AAD, Okta, or SAML. Outages in these authentication services can this issue.

Check if the third-party servers are up and reachable.

SAML SSO failure

Info code: 0x18008A, 0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3

Users face an authentication failure during app launch when it is IdP initiated or might see inaccessible links when it is SP initiated. Check the SAML app configuration at the Secure Private Access service side and service provider configuration as well.

Secure Private Access configuration:

1. Go to the **Applications** tab.
2. Look for the problematic SAML app.
3. Edit the application and go to the **Single Sign On** tab.
4. Check the following fields.
    - Assertion URL
    - Relay State
    - Audience
    - Name Id format, Name Id, and other attributes

Service provider configuration:

1. Log in to the service provider.
2. Go to **SAML settings.**
3. Check the IdP certificate, audience, and IdP login URL.

If the configuration looks correct, contact Citrix support.

Invalid app FQDN

Info code: 0x180048

Customer admin might have provided an invalid FQDN or an FQDN where DNS resolve fails at the back-end server.

In this case, the end user sees an error on the webpage. Check the application settings.

SAAS APP VALIDATION

Check if the app can be accessed from the network.

WEB APP VALIDATION

1. Go to the **Applications** tab.
2. Edit the problematic application.
3. Go to **App Details** page.
4. Check the URL. The URL must be accessible either in intranet or internet.

Secure Browser Service - DNS lookup/connection failed

Info code: 0x18009D

Broken browsing experience via Remote Browser Isolation service. Check the back-end server that the end user is trying to connect.

1. Go to the back-end server and check if it is up and running, and is able to receive the requests.
2. Check for proxy settings if it is stopping the connection to the back-end server.

> **Note:**
>
> The Citrix Remote Browser Isolation™ service was formerly known as the Secure Browser service.

CWA Web - DNS lookup/connection errors for Web apps

Info code: 0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7

Broken browsing experience of web applications running inside a corporate network.

1. Filter through the diagnostic logs for the FQDNs that are not resolvable.

2. Check for reachability of the back-end server from inside the corporate network.
3. Check the proxy settings to see if the connector is blocked from reaching the back-end server.

Direct Access - Misconfigured as Web app

Because Web app traffic is always routed via the connector, configuring direct access on them results in an app access error.

Check for the conflicting configuration between the routing domain table and the app configuration.

1. Go to the application in the management portal.
2. Edit the app and check if direct access is enabled.
3. Check the app FQDN inside the routing domain table if it has been marked as internal.

User is not entitled to access the Web/SaaS app for DirectAccess

Info code: 0x1800BD

App configuration disables direct access for traffic that originates from browser-based clients.

Ensure that the user has a subscription to the applications.

1. Go to the application in the management portal.
2. Edit the app and check the agentless access configuration.

Enhanced security policies - Secure Browser Service misconfiguration

Info code: 0x1800C3

Incorrect behavior seen than what was intended by the policy rules. Check contextual access policies.

1. Go to the **Policies** tab.
2. Check the policies associated with the application.
3. Check the rules for those policies.

Enhanced security policies - policy misconfiguration

Incorrect behavior seen than what was intended by the policy rules. Check the enhanced security settings.

1. Go to the application.
2. Click the **Access Policies** tab.
3. Check the settings in the **Available security restrictions:** section.

Citrix Secure Access™ agent session launch has failed while fetching the application configuration

Info code: 0x1800D0

Citrix Secure Access app fails to successfully establish a full tunnel to Citrix Cloud.

1. Review the routing domain configuration for the TCP/UDP apps.
2. Ensure that the maximum number of entries is well within the 16k limit.

TCP/UDP apps - Malformed client requests

Info code: 0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA

Either the VPN tunnel is not established or certain FQDNs might not be tunneled.

1. Ensure that the requests are not being fabricated or reconstructed by proxies in the middle.
2. Suspected man-in-middle attacks.

TCP/UDP Apps - Secure Browser Service redirect misconfiguration

Info code: 0x1800DD

Remote Browser Isolation service redirects can only be applied for Web apps and not TCP/UDP apps. Review the app configuration in the Secure Private Access service GUI.

> **Note:**
>
> The Citrix Remote Browser Isolation service was formerly known as the Secure Browser service.

Citrix Secure Access agent app launch has failed during the policy evaluation

Info code: 0x1800DE

Ensure that all the internal FQDNs that are to be tunneled by the Citrix Secure Access client have a corresponding entry in the routing domain table.

Citrix Secure Access agent app launch has failed as IPv6 is not supported

Info code: 0x1800EB

Review the routing domain entries. Ensure that there are no IPV6 entries in the table.

Citrix Secure Access agent app launch has failed due to invalid IP address

Info code:0x1800EC, 0x1800ED

Review the routing domain entries. Ensure that the IP addresses are valid and are pointing to the correct back end.

Network connectivity reachability issue with Citrix Secure Access client

Info code: 0x10000001, 0x10000002, 0x10000003, 0x10000004

1. Check if the client machine network is reachable. If the network is reachable, contact Citrix Support with the client debug logs.
2. Check if the proxy or firewall is blocking the network.

To collect client debug logs, see How to collect client logs.

Proxy server interfering client connectivity with service

Info code: 0x10000006

1. Check if the client machine network is reachable.
2. Check if the proxy is configured correctly in the client.
3. If there are no issues with both, contact Citrix Support with the client debug logs.

To collect client debug logs, see How to collect client logs.

Untrusted server certificate issue is observed

Info code: 0x10000007

Contact Citrix Support to check whether the server certificate is correctly generated by a valid CA.

Invalid server certificate issue is observed

Info code: 0x10000008

Contact Citrix Support to check whether the server certificate is self-signed, expired, or from an untrusted source.

Login failed as configuration is empty for the user

Info code: 0x1000000A

1. Ensure that at least one TCP/UDP/HTTP app is configured. For details, see Add and manage applications.

2. Ensure that the Application Domain table (**Secure Private Access > Settings > Application Domain**) is not empty or all entries are not disabled. The destinations configured in the TCP/UDP/HTTP application are automatically added to this table.

It is recommended that you do not delete or disable an active TCP/UDP/HTTP application's destinations or URL.

Connection terminated by the network and or end user

Info code: 0x1000000B

Check if the network is interrupted or if the end-user canceled the connection during the ZTNA session connection.

Configuration download failed as session is expired

Info code: 0x10000010

The VPN session might have expired during the ZTNA session config download request. Try to relogin to the Citrix Secure Access client.

Citrix Secure Access client failed to log in

Info code: 0x10000013

The Citrix Secure Access client failed to login as the configuration size exceeds the maximum configuration limit.

1. Review the routing domain configuration for the TCP/UDP apps in **Secure Private Access > Settings > Application Domain**
2. Ensure that the number of entries are not huge. If the entries list is huge, disable or remove unused destinations.

   If the destination list is expected to be more than 1000s, try increasing the max configuration download size by updating the ConfigSize registry key. For details, see Citrix Gateway VPN client registry keys.

Control channel establishment failed as the session expired

Info code: 0x11000003

The control channel for the DNS request establishment has failed as the session is expired.

The ZTNA session might have expired during the control channel setup.

Try to relogin to the Citrix Secure Access client.

Control channel establishment failed

Info code: 0x11000004

The control channel for DNS request establishment has failed.

- **Maintain the resource location healthy:**

1. Log on to Citrix Cloud.
2. Click **Resource Location** from the hamburger menu.
3. Run a health check for the connector appliances on the respective resource location.
4. If this does not fix the issue, try restarting the connector virtual machine.

- **Maintain HA connector appliance:**

1. Log on to Citrix Cloud.
2. Click **Resource Location** from the hamburger menu.
3. Ensure that the expected resource location has at least two Connector Appliances.

Ensure the following:

- The resource location LAN is in working condition.
- No firewall or proxy is in the middle blocking Connector Appliance to the service or the back-end servers.
- The client network is healthy.
- The back-end private servers are up and running.
- The DNS servers are up and running.
- FQDNs are resolvable.

If you meet the preceding recommendations, then do the following.

1. Fetch the transaction ID from the diagnostic log for this error.
2. Filter all events matching the transaction ID in the Secure Private Access dashboard.
3. Check if any error occurred in the client or Connector Appliance or Service diagnostic logs, matching to the transaction ID. Then take the appropriate actions accordingly.
4. Check if the resource location is chosen correctly for the destination in the application domain table (**Secure Private Access > Settings > Application Domain**).
5. Check if the application is configured with the correct port, IP ranges, domains. For details, see Add and manage applications.

If you are still not able to resolve the issue, Contact Citrix Support with the error code respective to the transaction ID and client logs.

To collect client debug logs, see How to collect client logs.

Control channel establishment failed

Info code: 0x11000005

Control channel (for DNS request) establishment failed.

1. Check the Secure Private Access service license entitlement.
2. If not entitled, Contact Citrix Support to check the license.

For details, see `<https://www.citrix.com/buy/licensing/product.html>`.

Control channel establishment failed due to network issue

Info code: 0x11000006

Control channel (for DNS request) establishment failed due to network issue.

1. Check if the Secure Private Access service is reachable.
2. If not reachable, Contact Citrix Support with the error code and the client Logs.

To collect client debug logs, see How to collect client logs.

Control channel establishment failed due to insufficient IIPs

Info code: 0x11000007

Control channel (for DNS request) establishment failed due to insufficient IIPs.

Contact Citrix Support with the error code and the client Logs.

To collect client debug logs, see How to collect client logs.

Unable to logoff as session is terminated

This issue might have occurred because the client machine (keyboard or mouse) was idle for more than the configured timeout period.

Info code: 0x12000001

Try to relogin to the Citrix Secure Access client.

Session is forcefully terminated

The session is forcefully terminated as the configured force timeout is reached.

Info code: 0x12000002

Try to relogin to the Citrix Secure Access client.

Application Launch failed as session is expired

Info code: 0x13000001

1. The ZTNA session has expired during the app launch.
2. Try to relogin to the Citrix Secure Access client.

Application Launch failed because of license issue

Info code: 0x13000002

1. Check for the Secure Private Access service license is entitlement.
2. If not entitled, Contact Citrix Support to check the license.

For details, see `<https://www.citrix.com/buy/licensing/product.html>`.

Application launch failed as access is denied by service

Info code: 0x13000003, 0x13000008, 0x001800DF

Application launch is denied as per the policy configuration for the user and application.

Ensure the following.

- Same destinations are not used in multiple applications (HTTP, HTTPS, TCP, UDP)
- There are no overlapping destinations on multiple applications.
- Access policies are bound to the applications.

Also check the conditions and actions of the policies configured for the denied application. Then review the policy conditions and actions.

For details see, Access policies.

Application launch failed as the client is unable to reach the service

Info code: 0x13000004, 0x13000005

1. Check if the Secure Private Access Service is reachable.
2. Launch the app again.

3. If the app is not reachable for a long time, Contact Citrix Support with the error code and client logs.

To collect client debug logs, see How to collect client logs.

Application launch failed as policy evaluation and config validation failed

Info code: 0x13000007

Application launch failed as policy evaluation and config validation is failed by the Secure Private Access service.

Unable to spot application for accessed destination.

Application launch failed as access is denied by service.

Application launch failed because of issues in application domain table

Info code: 0x13000009

Application launch failed as the Application domain table does not have an entry for the accessed destination.

Check that the route entry is correctly configured for the application in **Secure Private Access > Settings > Application Domain**.

Client closed the connection with Secure Private Access service

Info code: 0x1300000B

1. Check if the end-user manually closed the connection.
2. If not, contact Citrix Support with the error code and client logs.

To collect client debug logs, see How to collect client logs.

Unable to resolve FQDN by the DNS server

Info code: 0x1300000C

This issue occurs when the Connector Appliance fails to resolve DNS for FQDNs.

1. Check the DNS entry for the respective app FQDN in the DNS server.
2. Ensure that an appropriate DNS server is configured in the Connector Appliances. For details, see Configuring network settings on the Connector Appliance administration page.

App launch failed due to use of non-Chrome browser

Info code: 0x1300000E

Application launch fails because browser mode is set to Google Chrome Enterprise Premium, and a non-chrome browser is used.

Use Chrome Browser to launch the application.

- Check that the default system browser in the user's system is set to Chrome.
- Check that the user is not trying to manually launch the app using a non-Chrome browser.

Unable to locate the application

Info code: 0x001800DE

You might be unable to locate the application for the accessed destination for the user. This might occur if the destination to resource location mapping missing in the Application Domain table.

- Ensure that the TCP/UDP or HTTP application is configured for the accessed destination.
- Ensure that the user has a subscription to the application for the accessed destination.

1. Go to the application in the management portal.
2. Edit the app and go to the **Subscription** tab.
3. Ensure that the targeted user has an entry in the subscription list.
4. Ensure that the **Application Domain** table has the destination and the appropriate resource location.

Failed to fetch configured application destinations list

Info code: 0x001800D3

- Ensure that at least one TCP/UDP/HTTP app is configured. For details, see Add and manage applications.
- Ensure that the Application Domain table (**Secure Private Access > Settings > Application Domain**) page is not empty or not all entries are disabled. The destinations configured in the TCP/UDP/HTTP application are automatically added to this table. It is recommended not to delete or the disable the active TCP/UDP/HTTP application's destinations or URLs in the Application Domain table.

Application configuration issue

The application configuration contains a special character or some policy configuration issue.

Info code: 0x001800D9, 0x001800DA

Ensure the following:

- The app configuration does not contain unsupported characters.
- The destination IP address or IP address range or the IP CIDR are valid.
- The application destination is enabled in the Application Domain table (**Secure Private Access > Settings > Application Domain**).
- The policies are configured and bound to the respective application.
- The access policy configuration is correct.

Issue with resource location

Info code: 0x001800DB

- Ensure that a resource location is configured.
    a. In the Citrix Cloud hamburger menu, select **Resource Location**.
    b. Ensure that the expected resource location is configured and the resource location is in active status.
- Ensure that a correct resource location is selected for the destination in the Application Domain table (**Secure Private Access > Settings > Application Domain**).

The destinations configured in the TCP/UDP/HTTP application are automatically added to this table. It is recommended not to delete or disable the active TCP/UDP/HTTP application's destinations or URLs in the Application Domain table.

Enhanced security policy is bound to the HTTP application

Info code: 0x001800DC, 0x001800DD, 0x13000006

HTTP Application which has an enhanced security policy bound is accessed through the Citrix Secure Access client.

- Ensure that the same destination is not used for both TCP/UDP and HTTP applications.
- If enhanced security policy is enabled for HTTP/HTTPS application, it is recommended to access the app only through Citrix Workspace app or Citrix Remote Browser Isolation service.
- Disable enhanced security control for HTTP/HTTPS applications to access the app through the Citrix Secure Access client.
    - Go to the Secure Private Access admin portal.

- Click the **Applications** tab and search for the policy name for the accessed destination HTTP/HTTPS application.
- Click the **Access Policies** tab and search for the policy name identified earlier.
- Select the policy and click **Edit**.
- Change the action from **Allow access with restriction** to **Allow access.**

For details on configuration, see Add and manage applications.

> **Note:**
>
> The Citrix Remote Browser Isolation service was formerly known as the Secure Browser service.

Host name length exceeds 256 characters

Info code: 0x001800EA

The host name received in the application launch request exceeds 256 characters.

It is recommended that the FDQN characters do not exceed 256 characters.

Invalid IP address

Info code: 0x001800ED

The IP address received in the application launch request is invalid.

It is recommended to access only a valid private IP address from the clients.

Unable to establish end-to-end connection

Info code: 0x001800EF

Unable to establish end-to-end connection between the client and the server configured in resource location.

- Ensure that the resource location is in active status.
  - In the Citrix Cloud hamburger menu, select **Resource Location**.
  - Run a health check for the Connector Appliances on the respective resource location.
  - If this does not fix the issue, restart the connector virtual machine.

- Maintain a high availability Connector Appliance
  - In the Citrix Cloud hamburger menu, select **Resource Location**.
  - Ensure that the resource location has at least two Connector Appliances.
- Ensure the following:
  - Resource location LAN is in working condition.
  - No firewalls or proxies in the middle blocking Connector Appliance to the service or back-end servers.
  - Client Network is healthy.
  - Back-end private servers are healthy.
  - DNS servers are healthy.
  - FQDNs are resolvable.

If there are no issues with these, then do the following:

1. Fetch the transaction ID from the diagnostic logs for this error.
2. Filter all events matching the transaction ID in the Secure Private Access service dashboard.
3. Check the diagnostic logs corresponding to the transaction ID from the Secure Private Access service dashboard and then take appropriate actions accordingly.
4. Check that a correct resource location is selected as the destination in the Application Domain table (**Secure Private Access > Settings > Application Domain**).
5. Check if the application is configured (**Secure Private Access > Applications**) with the correct IP address, port, and FQDN.

If none of these steps resolve the issue, then contact Citrix Support with the error code respective to the transaction ID and collect client logs.

To collect client debug logs, see How to collect client logs.

IPv6 received in the app request

Info code: 0x001800F5

An IPv6 is received in the app request that is not supported. Currently, only IPv4 is supported.

Edit the application to fix the application IP address issue.

1. Go to the Secure Private Access admin portal.

2. Click the **Applications** tab.
3. Search for the app and click **Edit**.

For details, see Add and manage apps.

UDP traffic failed to deliver

Info code: 0x001800F9

UDP traffic failed to deliver as the client connection is lost

1. Check if the client session is active.
2. Log out and then relogin.

UDP data traffic delivery failed

Info code: 0x001800FF

- Look up the transaction ID for the error code and filter all events matching to the transaction ID in the Secure Private Access service dashboard.
- Check if any error occurred in the other component matching the transaction ID. If an issue is found in other components, then take appropriate actions accordingly.
- If this does not solve the issue, contact Citrix Support with the error code along with the respective transaction ID.

Application launch failed due to network connectivity issues

Info code: 0x10000401

Application launch failure because of network connectivity issues between Connector Appliance and Secure Private Access service

1. Check the public internet connectivity of the Connector Appliance.
2. Check if any proxy or firewall rules are blocking the connection.
3. If any proxy is causing the issue, bypass the proxy and try the app launch again.
4. Check the health status of the Connector Appliance (**Citrix Cloud > Resource Location**).

For details on network settings, see Network settings for your Connector Appliance.

Connector Appliance failed to register to Secure Private Access service

Info code: 0x10000402, 0x1000040C

1. Go to the Connector Appliances admin page and check the Connector Summary.

2. If the connector status is not good, then go to the resource location in the management portal.
3. Run a health check for the Connector Appliances on the respective resource location.
4. If the health check fails, restart the connector virtual machine.
5. Check the connector summary and run the health check again.

For details on network settings, see Network settings for your Connector Appliance.

Connectivity issue with Connector Appliance

Info code: 0x10000403, 0x10000404, 0x10000407, 0x1000040A, 0x1000040B, 0x1000040F, 0x10000410

- Look up the transaction ID for the error code.
- Filter all events matching the transaction ID in the Secure Private Access dashboard.
- Check if any error occurred in the other component matching the transaction ID if found do the respective workaround matching to that error code.
- If no error is found in other components, then do the following:
  - Go to the Connector Appliances admin page.
  - Download the diagnostic report. For details, see Generating a diagnostic report.
  - Capture the packet trace. For details, see Verify your network connection.
- Contact Citrix support with this diagnostic report and packet trace along with the error code and transaction ID.

Connectivity issues with Connector Appliance and back-end private TCP/UDP servers

Info code: 0x10000405, 0x10000408, 0x10000409, 0x1000040D, 0x1000040E, 0x10000412

Connector Appliance has connectivity issue with the back end Private TCP/UDP servers.

- Check if the back end server that the end user is trying to connect is up and running and is able to receive the requests.
- Check for the reachability of the back-end servers from inside the corporate network.
- Check the proxy settings to see if the connector is blocked from reaching the back-end server.
- If the request for an FQDN based app, check the DNS entry for the respective app in the DNS server.

Connector Appliance fails to resolve DNS for FQDNs

Info code: 0x10000406

- Check the DNS entry for the respective app FQDN in the DNS server.
- Ensure that an appropriate DNS server is configured in the Connector Appliances. For details, see Configuring network settings on the Connector Appliance administration page.

Private server connection terminated

Info code: 0x10000411

Connection to the private server is terminated by the client or Secure Private Access service.

1. Check if the end user has closed the application.
2. Check other diagnostic logs matching to this log's transaction ID and take appropriate actions accordingly.
3. Launch the app again.
4. If this does not resolve the issue, contact Citrix Support with the error code and the transaction ID.

Failed to connect or send data to the private service IP or FQDN

Info code: 0x10000413

- Private server connection terminated
- Connectivity issues with Connector Appliance and backend private TCP/UDP servers. Review the routing domain entries. Make sure that the IP addresses are valid and are pointing to the correct back end.

No matching policy condition

Info code: 0x100508

The user context does not match the access rule conditions defined in the policies assigned to the app.

Update the policy configuration to match the user's context.

No access policy associated with the application

Info code: 0x100509

1. In the Citrix Secure Private Access™ service GUI, click **Access Policies** on left navigation.
2. Ensure that an access policy is associated with the respective app.
3. If an access policy is not associated with the app, create an access policy for the app. For details, see Create access policies.

4. If this does not resolve the issue, contact Citrix Support.

No application configuration found for the FQDN or the IP address

Info code: 0x10050A

No matching application was found for the incoming FQDN or the IP address request. Hence, the app is classified as an unpublished application. If this is not expected, do the following.

1. Go to the Secure Private Access service admin portal.
2. Click **Applications** on left navigation.
3. Search for the app, and click **Edit**.
4. Add an FQDN or the IP address to the application. You can add the exact domain, IP address, or a wildcard domain.

   Note: Adding an FQDN or an IP address in **Secure Private Access > Settings > Application Domain** does not solve this issue. It must be added as part of the application configuration.

App enumeration information

Info code: 0x10050C

This code captures the policy evaluation results of multiple applications that the user might be entitled to. App access might be denied for the following reasons:

- The user context does not match the access rule conditions defined in the policies assigned to the app – For details, see No matching policy condition.
- No access policy is associated with the application – For details, see No access policy associated with the application.
- A policy associated with the application is configured to deny access – In this case, no action required as this is intended.
- Unexpected Internal error in enforcing access policy. For details, contact Citrix Support.

TCP/UDP app launch failed as routing entry is missing in application domain table

Info code: 0x00180101

This issue can occur if the application configuration is present but the routing entry is missing or was previously deleted.

Add a routing entry (**Secure Private Access > Settings > Application Domain**) for the destination that is accessed.

TCP/UDP app launch failed as connectors are not healthy

Info code: 0x00180102

This issue can occur if none of the connectors is up/responding to the new connection.

Run a health check for the Connector Appliances on the respective resource location.

UDP/DNS request failed as connector is unreachable

Info code: 0x00180103

This issue can occur if the UDP/DNS traffic is unable to reach the connector.

Run a health check for the Connector Appliances on the respective resource location.

Failed to load the page as the NGS cookie is expired

Info code: 0x20580001

1. Restart the browser and try opening the app again.
2. If this does not resolve the issue, contact Citrix Support.

Access policy fetch failed because of a network failure

Info code: 0x20580002

1. Check the URL and the network connection.
2. Restart the browser and try opening the app again.
3. If this does not resolve the issue, contact Citrix Support.

Access policy fetch failed while parsing the JSON web token

Info code:0x20580003

1. Restart the browser and try opening the app again.
2. If this does not resolve the issue, contact Citrix Support.

Network failure to fetch access policy details

Info code:0x20580004

1. Check if the access policy is enabled.
2. Restart the browser and try opening the app again.
3. If this does not resolve the issue, contact Citrix Support.

Policy fetch failed while fetching the public certificate

Info code: 0x20580005

1. Restart the browser and try opening the app again.
2. If this does not resolve the issue, contact Citrix Support.

Policy fetch failed while validating signature of the JSON web token

Info code: 0x20580007

1. Check if the network time and user device time are in sync.
2. Restart the browser and try opening the app again.
3. If this does not resolve the issue, contact Citrix Support.

Policy fetch failed while validating the public certificate

Info code: 0x20580008

1. Restart the browser and try opening the app again.
2. If this does not resolve the issue, contact Citrix Support.

Failed to determine the store environment to form a policy URL

Info code: 0x2058000A

1. Restart the browser and try opening the app again.
2. If this does not resolve the issue, contact Citrix Support.

Failed to get a response for access policy fetch request

Info code: 0x2058000B

1. Restart the browser and try opening the app again.
2. If this does not resolve the issue, contact Citrix Support.

Access policy fetch failed due to an expired secondary DS auth token

Info code: 0x2058000C

1. Restart the browser and try opening the app again.
2. If this does not resolve the issue, contact Citrix Support.

Connector Appliance is not registered

Info code: 0x10200002

Check the Connector Appliance registration.

For details, see Register your Connector Appliance with Citrix Cloud.

Unable to connect to the Connector Appliance

Info code: 0x10200003

The Connector Appliance is unable to communicate between Citrix Cloud and resource locations.

Check the connector registration.

For details, see Register your Connector Appliance with Citrix Cloud.

Connection to Citrix Secure Private Access service failed

Info code: 0x10000301

Check the Connector Appliance network settings. For details, see Network settings for your Connector Appliance.

Proxy server is not reachable

Info code: 0x10000303, 0x10000304

Check the proxy server settings and make sure that it is reachable to Connector Appliance. For details, see Register your Connector Appliance with Citrix Cloud.

Proxy server authentication failed

Info code: 0x10000305

Check proxy server credentials and make sure that they are configured correctly in Connector Appliance. For details, see After registering your Connector Appliance.

Configured proxy servers are not reachable

Info code: 0x10000306

Check the Connector Appliance network settings, firewall settings, or proxy server settings. For details see the following topics:

- Network settings for your Connector Appliance
- Register your Connector Appliance with Citrix Cloud
- Connector Appliance communication

Received error response from backend server

Info code: 0x10000307

Check the backend web server's HTTP status code, if it is not an expected code.

Unable to send request to the target URL

Info code: 0x10000005

Check the target URL or check the Connector Appliance network settings. For details, see Network settings for your Connector Appliance.

Failed to process SSO

Info code: 0x10000107

Failure to retrieve app configuration data from Citrix Cloud.

Check the Connector Appliance network settings and make sure that the NTP server is configured and there are no time strip issues. For details, see Network settings for your Connector Appliance.

Connection to the Citrix Secure Private Access service failed

Info code: 0x10000108, 0x1000010B

Check the Connector Appliance network settings. For details, see Network settings for your Connector Appliance.

Failed to process SSO, unable to determine SSO settings

Info code: 0x1000010A

Check the SSO configuration and make sure that the server is reachable to Connector Appliance.

FormFill SSO failed, incorrect form app configuration

Info code: 0x10000101, 0x10000102, 0x10000103, 0x10000104

Check the SSO form app configuration and make sure that the user name, password, action, and login URL fields are correctly configured on the app settings.

Kerberos SSO failed

Info code: 0x10000202

Check the Kerberos SSO settings on the backend server and the domain controller. Also check the fallback NTLM authentication settings.

For Kerberos SSO settings, see Validating your Kerberos configuration.

Failed to process SSO for auth type

Info code: 0x10000203

Check the SSO settings in the Secure Private Access service and the backend server. For Secure Private Access service, see Set the preferred sign-on method.

Kerberos SSO failed but falling back to NTLM

Info code: 0x10000204

Retrieving the Kerberos ticket from the domain controller has failed. As a secondary authentication, Connector Appliance has tried the fallback NTLM authentication.

To enable successful Kerberos authentication, check the Kerberos SSO settings on the backend server and domain controller.

For details, see Validating your Kerberos configuration.

Multiple ZTNA entitled accounts configured in the Citrix Workspace™ app

Info code: 0x14000001

Configure only one ZTNA entitled account in the Citrix Workspace app.

How to collect client logs

- **Windows client:**
  a. Open the app and ensure that logging is enabled.
  b. Now connect to the Secure Private Access service and duplicate the issue you are facing.
  c. In the app, go to **Logging** and click **Collect Log Files**. This generates the log file.
  d. Save the log file on the client machine's desktop.
- **Mac client:**
  a. Open the app and go to **Logs > Verbose**.
  b. Clear the logs and proceed to reproduce the issue.
  c. Go back to **Logs > Export logs**. This creates a zip file that contains log files.

FAQs

The following sections provide more information about the frequently asked questions.

Where do I find more information about diagnostic logs?

See the topic Diagnostic logs for more information on the diagnostic logs.

How do I use the Secure Private Access troubleshooting topic to resolve a failure that I have encountered?

1. Fetch the info code for the failure that you are trying to resolve.
2. Find the info code in the Error lookup table.
3. Follow the resolution steps provided for that info code.

What is an info code? Where do I find them?

Some log events such as failures have an associated info code. Search for this info code within the Error lookup table to find the resolution steps or more information about that event.

What is a transaction ID? How do I use it?

Access failures/issues via Citrix Enterprise Browser display a Transaction ID to the end user. Admins can fetch this transaction ID from the end users and use this transaction ID to filter the exact logs that caused the issue, enabling them to identify the exact problem. Once the admins filter events with the transaction ID, only the events pertaining to the issue in hand are displayed, providing all the details to the admins on why the failure or the issue happened. Admins can then use the error code on those logs to further resolve the issues.

What are all the Secure Private Access PoP locations?

The following is the list of Secure Private Access data PoP locations.

POP NAME	ZONE	REGION
az-us-e	Azure eastus	Virginia
az-us-w	Azure westus	California
az-us-sc	Azure southcentralus	Texas
az-aus-e	Azure australiaeast	New South Wales
az-eu-n	Azure northeurope	Ireland
az-eu-w	Azure westeurope	Netherlands
az-jp-e	Azure japaneast	Tokyo, Saitama

POP NAME	ZONE	REGION
az-bz-s	Azure brazilsouth	Sao Paulo State
az-asia-se	Azure southeastasia	Singapore
az-uae-n	Azure uaenorth	Dubai
az-in-s	Azure southindia	Chennai
az-asia-hk	Azure eastasia	Hong Kong

The following is the list of Secure Private Access management PoP locations.

POP NAME	ZONE	REGION
aws-us-e-mgmt	AWS us-east-1	North Virginia
aws-in-w-mgmt	AWS ap-south-1	Mumbai
aws-eu-c-mgmt	AWS eu-central-1	Frankfurt

What do I do if I am unable to resolve my failure using the info code and the error lookup table?

Contact Citrix Support.

References

- **Add a Web app**
  - Support for Enterprise web apps
  - Configure direct access to Web apps
- **Add a SaaS app**
  - Support for Software as a Service app
  - SaaS app server-specific configuration
- **Configure client-server apps**
  - Support for client-server apps
- **Create access policies**

    - Create access policies

- **Route tables**
    - Route tables

Audit and system logs

Secure Private Access service related events are captured in **Citrix Cloud > System log**. All the events that an admin performs in the Citrix Secure Private Access™ service is sent to Citrix Cloud and captured in **System log**. The admin events can be, but not limited to, the following:

- Creating or updating an app
- Deleting an app
- Configuring or deleting an adaptive access policy
- Connector upgrade
- Creation of allowed or blocked websites

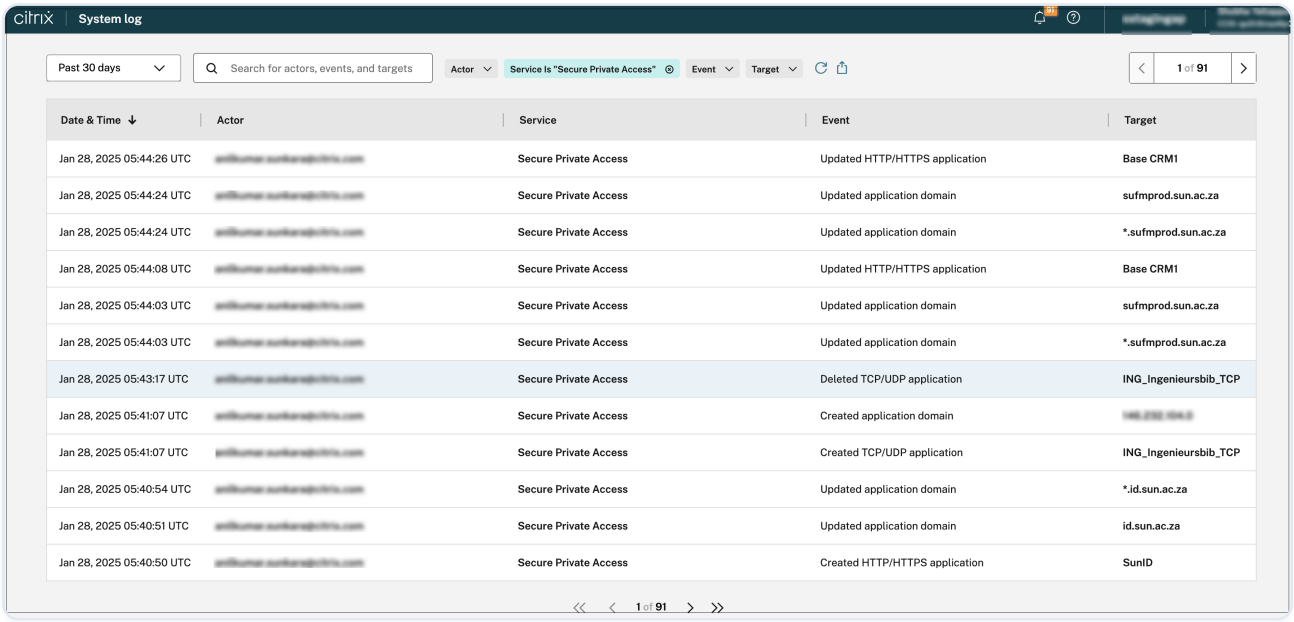
By default, **System log** displays events that occurred in the last 30 days. The most recent events are displayed first.

The logs show details about events and can be filtered by the following:

- **Date and Time:** The date and time (UTC format) when the event occurred.
- **Actor:** The user or system that triggered the event. For example, administrator, secure client, service principal.
- **Service:** The service where the event was logged. The Secure Private Access events must have **Secure Private Access** as the service.
- **Event:** A short description of the event. For example, Created SaaS application, Deleted TCP/UDP application, Updated adaptive access policy, Updated application domain.
- **Target:** The object impacted or changed as a result of the event. For example, the domain used for an application.

  The target identifier is in a human-readable format and not the actual ID.

The following figure displays the Secure Private Access events in the **System Log**.



For details such as exporting events, retrieving events for a specific time period, forwarding log events, and data retention, see System Log.

Device Posture logs and events

Administrators can monitor device compliance through the device posture dashboard. They can view all configured device posture policies that define compliance requirements for endpoints accessing organizational resources. They can also view real-time compliance status for all devices, including detailed evaluation results categorized as follows:

- **Compliant:** Devices that meet all specified security requirements and policy criteria.
- **Non-compliant:** Devices that fail to meet one or more security requirements but might still have limited access.
- **Access denied:** Devices that pose significant security risks and are blocked from accessing resources.

You can view the Device Posture logs and events in the Secure Private Access dashboard and in the Device Posture dashboard in the Identity and Access Management console.

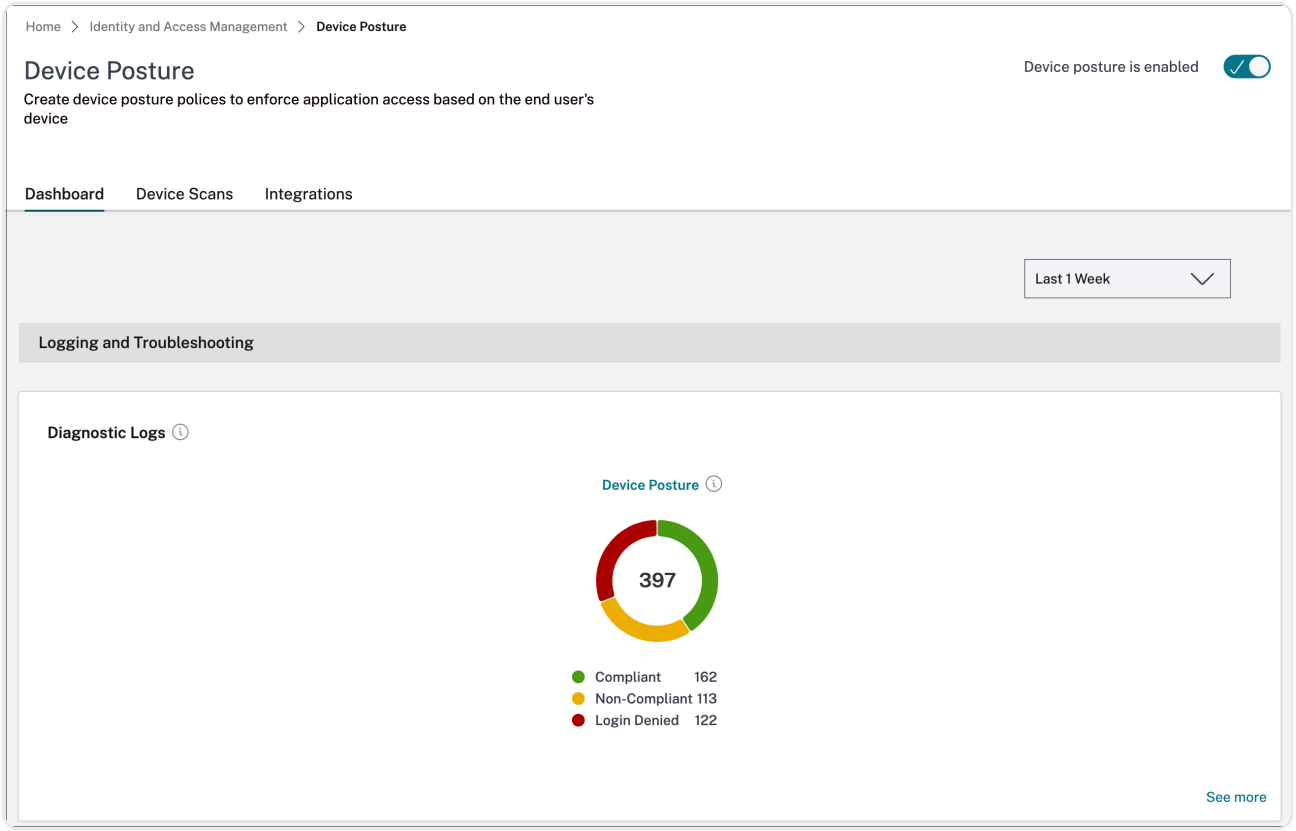
Device Posture dashboard in Identity and Access Management console

Perform the following steps to view the logs and events for the Device Posture dashboard in the Identity and Access Management console.

1. Sign into Citrix Cloud.
2. From the Citrix Cloud menu, select **Identity and Access Management**,
3. Click **Device Posture > Manage** and then click **Dashboard.**

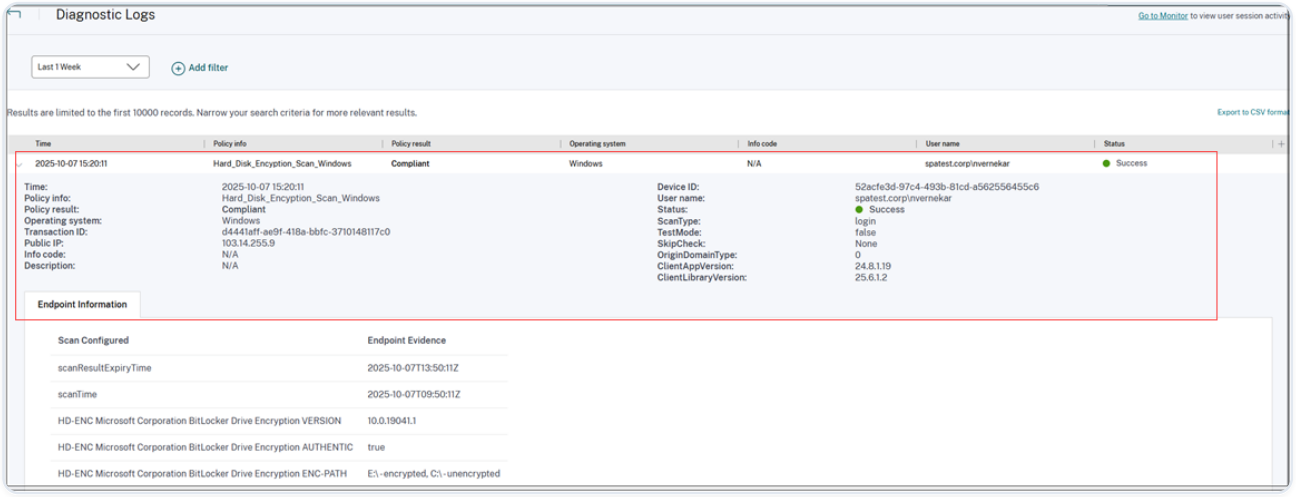
The **Logging and Troubleshooting** section displays the diagnostic logs related to the Device Posture service.

4. Click the **See more** link to view the details of the logs. You can refine your search based on the policy results (**Compliant**, **Non-Compliant**, and **Login Denied**).



You can use the **Add filter** option to refine your search based on various criteria such as policy info, policy result, operating system, transaction ID, info code, or device ID. For example, in the search field, you can click **Device-ID**, select **~ (contains some value)**, and enter 6273. All logs related to device IDs containing 6273 are displayed.

Click the expand icon next to each log entry to view comprehensive details, such as scan type, client app version, client library version, and endpoint information.



Note:

- The **ClientAppVersion** and the **ClientLibraryVersion** fields display the EPA client version and library version respectively.
- The transaction ID is also displayed to the end user whenever access is denied.
- If there's an error or a scan failure, the Device Posture service displays a transaction ID. This transaction ID is available in the Secure Private Access service dashboard. If the logs do not help resolve the issue, end users can share the transaction ID with Citrix Support to resolve the issue.

Logs location

The Windows client logs can be found at:

- %localappdata%\Citrix\EPA\dpaCitrix.txt
- %localappdata%\Citrix\EPA\epalib.txt

The macOS client logs can be found at:

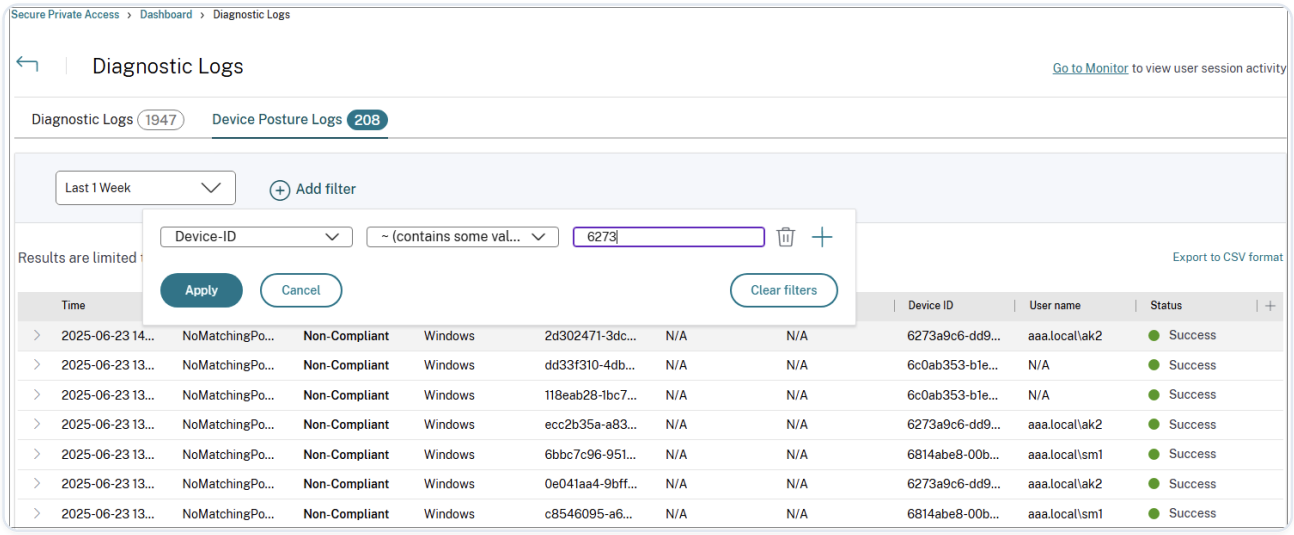
- ~/Library/Application Support/Citrix/EPAPlugin/EpaCloud.log
- ~/Library/Application Support/Citrix/EPAPlugin/epaplugin.log

Secure Private Access dashboard

Perform the following steps to view the logs and events for the Device Posture service.

1. Sign into Citrix Cloud.
2. On the Secure Private Access tile, click **Manage** and then click **Dashboard**.

   The **Logging and Troubleshooting** section displays the diagnostic logs related to the Device Posture service.
3. Click the **See more** link to view the details of the logs. You can refine your search based on the policy results (**Compliant**, **Non-Compliant**, and **Login Denied**).



Device posture error logs

The following logs related to the Device Posture service can be viewed on the Citrix Monitor and Secure Private Access dashboard. For all these logs, it's recommended that you contact Citrix Support for resolution.

- Failed to read configured policies
- Failed to evaluate endpoint scans
- Failed to process policies/expression
- Failed to save endpoint details
- Failed to process scan results from endpoints

Device posture data export

The Device Posture service events (such as device posture results and event types) can be exported to the Security Information and Event Management (SIEM) service. These events are generated when the Citrix Endpoint Analysis (EPA) client performs a posture check on a device attempting to access Citrix Virtual Apps and Desktops™ or Citrix Secure Private Access resources.

- To understand how to set up, configure, and export your Device Posture service logs to SIEM, see Security Information and Event Management (SIEM) integration.
- To know more about what events and logs you can export from the Device Posture service, see Device Posture service events.
- To understand how to diagnose and troubleshoot Device Posture service transactions, see Diagnose Device Posture service transactions.

Data exports and third-party integrations

The following sections provide more information about data exports and third-party integrations.

Security Information and Event Management integration

The integration of Secure Private Access with Security Information and Event Management (SIEM) enables administrators to export critical logs, policy outcomes, and user activity data to third-party SIEM systems using Kafka push mechanisms. This integration provides enhanced visibility, compliance tracking, and security insights for organizations using Citrix Secure Private Access services.

You can use any SIEM, such as Splunk, Google Chronicle, Microsoft Sentinel, or Elastic.

For the list of user events associated with Secure Private Access and Device Posture service in your SIEM, see the following topics:

- Secure Private Access events
- Device Posture service events

Build custom report with OData APIs

The Secure Private Access Monitor OData REST APIs enables administrators to export session data and build custom reports. This feature is useful for tracking rollouts, analyzing user activity, and gaining insights into the performance and usage of Secure Private Access services.

For information on the types of Secure Private Access data available for export, see the following topics:

- Secure Private Access sessions
- Secure Private Access applications
- Secure Private Access enumerations

Export system logs

The **Systems Log** feature in Citrix Cloud provides a timestamped record of events that occur within the Secure Private Access service. Administrators can export these logs as a CSV file for further analysis and verification. For details, see Syslog from Citrix Cloud.

Export data from Kafka

Kafka is an open-source distributed streaming platform designed for real-time data processing and analytics. Using Kafka, organizations can analyze streaming data in real-time to gain faster insights, enable proactive decision-making, and support advanced security monitoring capabilities.

You can export Secure Private Access events and Device Posture service events from Kafka to integrate with external Security Information and Event Management (SIEM) systems, analytics platforms, and custom monitoring solutions.

Secure Private Access events

The user events are received in real-time in Citrix Analytics for Security when users access applications through Citrix Secure Private Access, such as Citrix Workspace app, Citrix Secure Access clients, or Citrix Enterprise Browser.

For more information, see Secure Private Access events.

Device Posture service events

The user events are generated when the Citrix Endpoint Analysis (EPA) client performs a posture check on a device attempting to access Citrix Virtual Apps and Desktops or Citrix Secure Private Access resources.

For more information, see Device Posture service events.

Export audit and system logs

The **System log** feature in Citrix Cloud captures a complete, timestamped record of events occurring within the Secure Private Access service. These audit logs are critical for regulatory compliance, security monitoring, and troubleshooting administrative operations. Administrators can export log data as CSV files for detailed analysis, compliance verification, and seamless integration with external security monitoring systems.

The following events are captured in **System log** for the Secure Private Access service:

- Application configuration changes including creation, modification, and deletion.
- Policy updates such as access rules, security configurations, and conditional access settings.
- User and group management operations such as the addition or removal of users and groups.
- Application domains related information.
- Allowed and blocked URL lists.

Export Secure Private Access events using the SystemLog API

You can use the SystemLog API to export the Secure Private Access events. The SystemLog API allows you to retrieve events that occurred in your Citrix Cloud account for periods of time that you specify.

- For details on using the SystemLog API to export events, see Citrix Cloud - SystemLog in the Citrix Developer documentation.
- To understand the event data that **System log** captures for the Secure Private Access service, see System Log Events Reference.
- To Learn more about the Monitor service API, see About Citrix Monitor Service API.

Export sessions data using OData

The Secure Private Access Monitor OData REST APIs enables administrators to export session data and build custom reports. This feature is particularly useful for tracking rollouts, analyzing user activity, and gaining insights into the performance and usage of Secure Private Access services.

- Administrators can leverage the OData REST APIs to create custom reports that meet specific organizational needs. This flexibility allows for detailed analysis of session data, user activity, and application usage.
- The APIs enable tracking of rollouts, helping administrators monitor the adoption and effectiveness of Secure Private Access configurations and policies across the organization.
- Using OData APIs, session data can be exported for further analysis in external tools or systems.

For details about Secure Private Access Monitor OData REST APIs, see the following topics:

- Secure Private Access sessions
- Secure Private Access applications
- Secure Private Access enumerations

Role-based access control

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

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

- Full Access Administrator
- Read Only Administrator
- Full Monitor Administrator
- Helpdesk Administrator

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

> The following table provides a brief description of each role:

ROLE	DESCRIPTION
Full Access Administrator	Intended for individuals who need complete control over the configuration, management, and operation of the Secure Private Access environment. The Full Access Administrator has the following privileges.
	Access to all Secure Private Access functionalities.

ROLE	DESCRIPTION
	Permissions to create, edit, and modify apps, policies, and settings within the Secure Private Access console.
Read Only Administrator	Intended for individuals who need to monitor and analyze the Secure Private Access activities and system performance. The Read Only Administrator has the following privileges.
	Access to the Secure Private Access dashboard.
	Ability to view all Secure Private Access application configurations and settings.
	The Read Only Administrator does not have the privileges to any of the create/update/ delete functionality.
Full Monitor Administrator	Intended for users responsible for monitoring Secure Private Access activity and performance in the Monitor console. The Full Monitor Administrator has the following privileges.
	Access to all monitoring dashboards and reporting tools within Secure Private Access.
	Ability to view all Secure Private Access configurations and settings.
	The Full Monitor Administrator does not have permissions to create, edit, or modify Secure Private Access configurations, policies, or settings.
Helpdesk Administrator	Intended for Helpdesk personnel responsible for troubleshooting and triaging user access issues. The Helpdesk Administrator has the following privileges.

ROLE	DESCRIPTION
	Limited visibility into Secure Private Access configurations and settings, focusing on information relevant to troubleshooting in the Monitor console.
	Access to specific troubleshooting tools and diagnostic utilities within the Secure Private Access console.
	View the troubleshooting and the Monitor dashboard.
	The Helpdesk Administrator does not have permissions to create, edit, or modify Secure Private Access configurations or policies.

Roles and privileges

The following table summarizes the roles and privileges:

	FULL ACCESS ADMINISTRATOR	READ ONLY ADMINISTRATOR	FULL MONITOR ADMINISTRATOR	HELPDESK ADMINISTRATOR
Create/edit/ delete apps	Yes	No	No	No
Create/edit/ delete policies	Yes	No	No	No
Edit configurations/ settings	Yes	No	No	No
View configurations/ settings	Yes	Yes	Yes	Limited

	FULL ACCESS ADMINISTRATOR	READ ONLY ADMINISTRATOR	FULL MONITOR ADMINISTRATOR	HELPDESK ADMINISTRATOR
View the logging and troubleshooting widget in the Secure Private Access dashboard	Yes	Yes	Yes	Yes
Search for users	Yes	Yes	Yes	No
Retrieved configured domains	Yes	Yes	Yes	No
View the Users, Applications, Access Policies widgets in the Secure Private Access dashboard	Yes	Yes	Yes	No
View the sessions and applications in the Monitor dashboard	Yes	Yes	Yes	Limited
Access reporting tools	Yes	No	Yes	Limited

Enable role-based access to admins

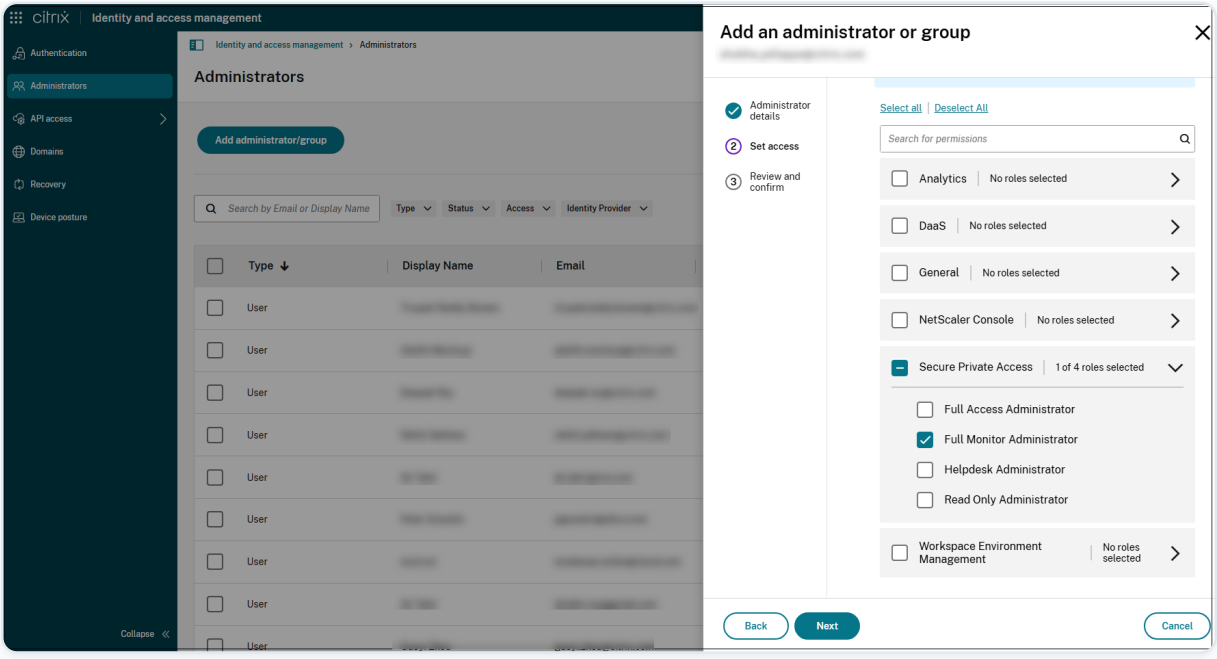
Perform the following steps to enable role-based access to admins:

1. After signing in to Citrix Cloud™, select **Identity and Access Management** from the menu.

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

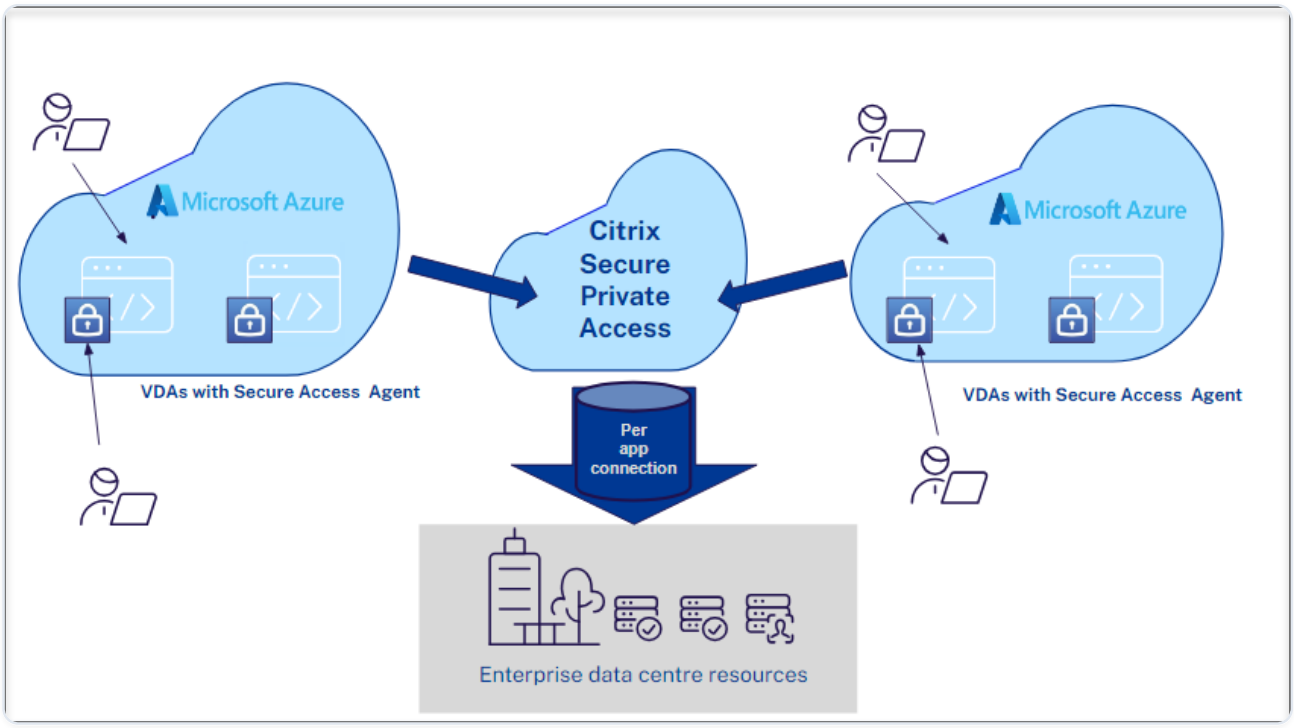
Note:

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



Support for multi-session virtual desktop infrastructure

In a multi-session virtual desktop infrastructure (VDI), multiple users share a virtual machine while maintaining individual desktop environments. Starting from the Citrix Secure Access client for Windows release 24.8.1.19, you can access your enterprise applications from multi-session VDIs for Secure Private Access deployments by ensuring that each user's session remains isolated, private, and protected.



Note:

- Multi-session VDI is supported on Windows OS starting from Windows 10 and from Windows Server 2019.
- Multi-session VDI works only on Azure based VDI.

Key features and benefits

- **Authentication:** Supports various authentication methods, including condition-based authentication.
- **Contextual access:** Allows access to authorized applications only based on Secure Private Access policies for users based on factors like location, device, and group.
- **Reduced cost:** Allows multiple users to share computer, which can help organizations save money on hardware costs. The Citrix Secure Access™ client for Windows app further enhances these cost savings by enabling users to access their virtual desktops from any device, reducing the need for dedicated workstations without depending on express routes or legacy VPN.
- **Enhanced flexibility:** Enables end users to connect from anywhere abiding to Secure Private Access policies for only allowing authorized application access.

Enable multi-session VDI

To enable multi-session VDI support in the Citrix Secure Access client for Windows app, administrators must ensure that the Citrix Secure Access client for Windows 24.8.1.19 or later is installed on the multisession OS machine.

Admin must perform the following steps to provide contextual access to users on the multi-session OS machine:

1. Open the **Registry Editor** (**regedit.exe**).
2. Navigate to **HKEY_LOCAL_MACHINE\Software\Citrix\Secure Access Client**.
3. Create `EnableMultiSessionFlow` and `EnableWFP` registries to enable the multi-session VDI. For more information, see NetScaler Gateway Windows VPN client registry keys.
4. Close the **Registry Editor**.
5. Reboot the machine to ensure the settings take effect.

For domain-joined machines where the domain controller IP address is the same as the DNS IP address, the admin must perform the following steps to enable multi-session VDI.

1. Open the **Registry Editor** (**regedit.exe**).
2. Navigate to **HKEY_LOCAL_MACHINE\Software\Citrix\Secure Access Client**.
3. Create `EnableMultiSessionFlow` and `AlwaysOnService` registries to enable the multi-session VDI. For more information, see NetScaler Gateway Windows VPN client registry keys.

4. Create a `CloudAlwaysOnUrl` registry of type **REG_SZ** and provide the connection URL.
5. Close the **Registry Editor**.
6. Reboot the machine to ensure the settings take effect.
7. On the Secure Private Access dashboard, create an application for the domain controller and cloud connector.

> **Note:**
>
> When the domain controller IP address is the same as the DNS IP address, all the calls going to the domain controller are intercepted and are dropped. To avoid domain controller packets from being dropped, it is recommended to create an application and enable access to all the users.

8. Add the domain controller IP address that matches the DNS server IP address to the application, with all TCP/UDP ports allowed.
9. Set access policies to ensure that all users can access the domain controller.
10. Add the cloud connector to the traffic routing type **External** to prevent it from being tunneled, if the host name of the cloud connector matches your suffix (for example, the host name of the cloud connector is cloudconnector.cloud.com and the suffix is *.cloud.com).

Citrix Secure Private Access for mobile devices

The Citrix Secure Private Access deployments are supported for mobile devices starting with Secure Access Client version 25.08.1 for iOS and Secure Access Client version 25.11.1 for Android. Mobile users can access corporate applications and web resources under the Secure Private Access zero-trust model, providing the same security controls, policy enforcement, and seamless experience as desktop users.

Supported versions and platforms

iOS devices:

- **CSA Client**: iOS 25.08.1 (Available on App Store)
- **iOS OS version**: Minimum iOS 16
- **Deployment models**
  - Secure Private Access for cloud deployments
  - Secure Private Access for hybrid deployments

Android devices:

- **CSA Client**: Android 25.11.1 (Available on Google Play Store)
- **Android OS version**: Minimum Android 12
- **Deployment models**
  - Secure Private Access for cloud deployments
  - Secure Private Access for hybrid deployments

Supported features

For Secure Private Access deployments, resource access is controlled through policy configuration. Administrators can define policies specifying which users or groups can access

particular applications and resources, under specific conditions and from approved devices or locations.

- Access to web, SaaS, and TCP/UDP applications according to your Secure Private Access policy conditions.
- Session security policies: Data loss prevention (DLP) controls supported by Chrome Enterprise.

For the complete list of supported features, see Citrix Secure Access client features supported in NetScaler Gateway.

Prerequisites

The Secure Private Access service must be configured and up-to-date. For details, see the following topics:

- Get started with Citrix Secure Private Access
- Secure Private Access onboarding and set up
- Apps configuration and management

Workflow for iOS and Android users with Citrix Secure Access client

The following steps summarize the Secure Private Access flow for users on iOS and Android devices with Citrix Secure Access client.

- **Citrix Secure Access client installation**: The Citrix Secure Access client must be installed on the mobile device. This can be achieved through Mobile Device Management (MDM) for corporate devices, or manually by the user downloading the application from the device's app store.
- **Access store/gateway URL**: The user then accesses the designated store or gateway URL. This URL serves as the entry point for accessing the organization's resources.
- User authentication: The user is prompted to authenticate their identity. This typically involves entering credentials such as a user name and password, or using multifactor authentication (MFA) methods.
- **Policy evaluation and access grant**:

    - Policy satisfied: If the user's authentication and device posture satisfy the defined security policies, access is granted. This allows the user to access authorized web, SaaS, and private web applications.
    - Policy failed: If the user fails to meet the policy requirements (for example, outdated operating system, unapproved device, incorrect credentials), access is either restricted or entirely denied, depending on the policy configuration.

- **Enforced session protections**: Once access is granted, data loss prevention (DLP) controls supported by Chrome Enterprise are enforced. For example:
    - Disabling incognito
    - Blocking printing
    - URL filtering
    - Blocking downloads
    - Configured (managed) bookmarks

Related topics

- Citrix Secure Private Access for cloud deployments
- Citrix Secure Private Access for hybrid deployments

Kerberos authentication using the iOS Kerberos extension

This topic outlines the end-to-end configuration required to enable Kerberos-based Single Sign-On (SSO) for internal web apps via the Citrix Secure Access for iOS app.

- iOS client configuration
- MDM server configuration
- IIS configuration
- Domain controller configuration

iOS client configuration

The following sections provide more information about iOS client configuration.

Prerequisites

Ensure that the iOS device is MDM enrolled. The iOS device must be enrolled in an MDM solution (for example, Microsoft Intune) before any SSO configuration can be applied. MDM enrollment allows the Kerberos SSO extension profile to be pushed to the device.

Validate MDM enrollment on the iOS device

1. On the iOS device, go to **Settings > General > VPN & Device Management**.

   Under Device Management, you must see your organization's MDM profile listed (for example, Microsoft Intune or your company's MDM profile name).
2. Tap the profile to confirm it is installed and the status displays **Verified** or **Installed**.
3. To confirm the Kerberos SSO extension was pushed by MDM:

   - Go to **Settings > General > VPN & Device Management**.
   - Tap the MDM profile, look for **Single Sign-On Extensions** or **Kerberos** under the profile details.
   - Alternatively, go to **Settings > General > VPN & Device Management > Single Sign-On** and verify that the Kerberos extension is listed.

   If the device is not enrolled or the profile is missing, contact your MDM administrator to enroll the device before proceeding.

MDM server configuration

> **Note:**

> The MDM SSO extension payload configuration is based on the official Apple documentation.

> - Single Sign-on device management payload settings for Apple devices
> - Kerberos Single Sign-on extension with Apple devices

> Ensure that the following fields are configured in the MDM SSO extension payload:

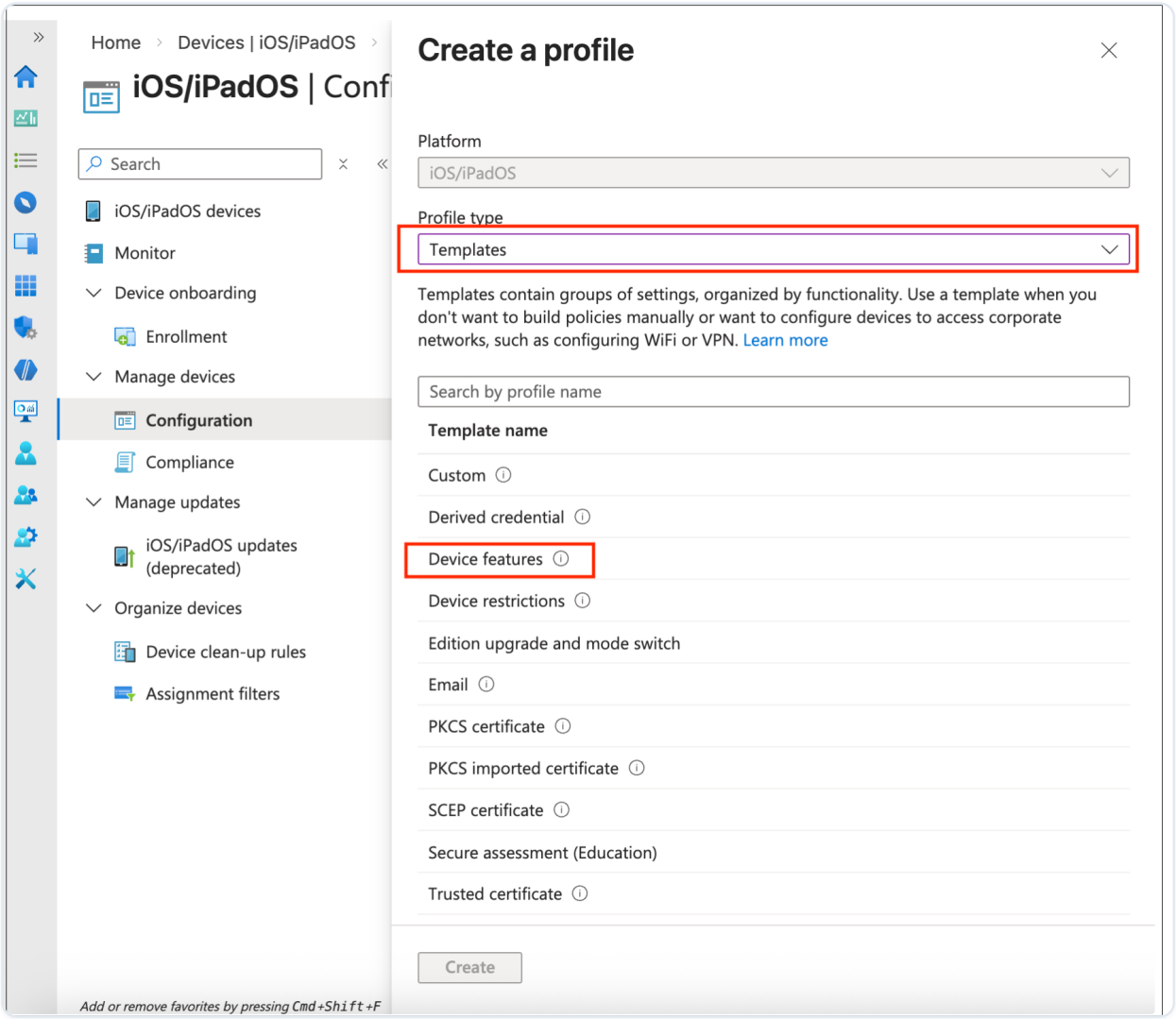
1. **Domain:** The URLs that are used for Kerberos.

2. **AppBundleIDs:** Allow list of apps that will be used. (For example, Chrome: `com.google.chrome.ios`, Citrix Secure Access: `com.citrix.securehub`)
3. **Realm:** Location of your data center.

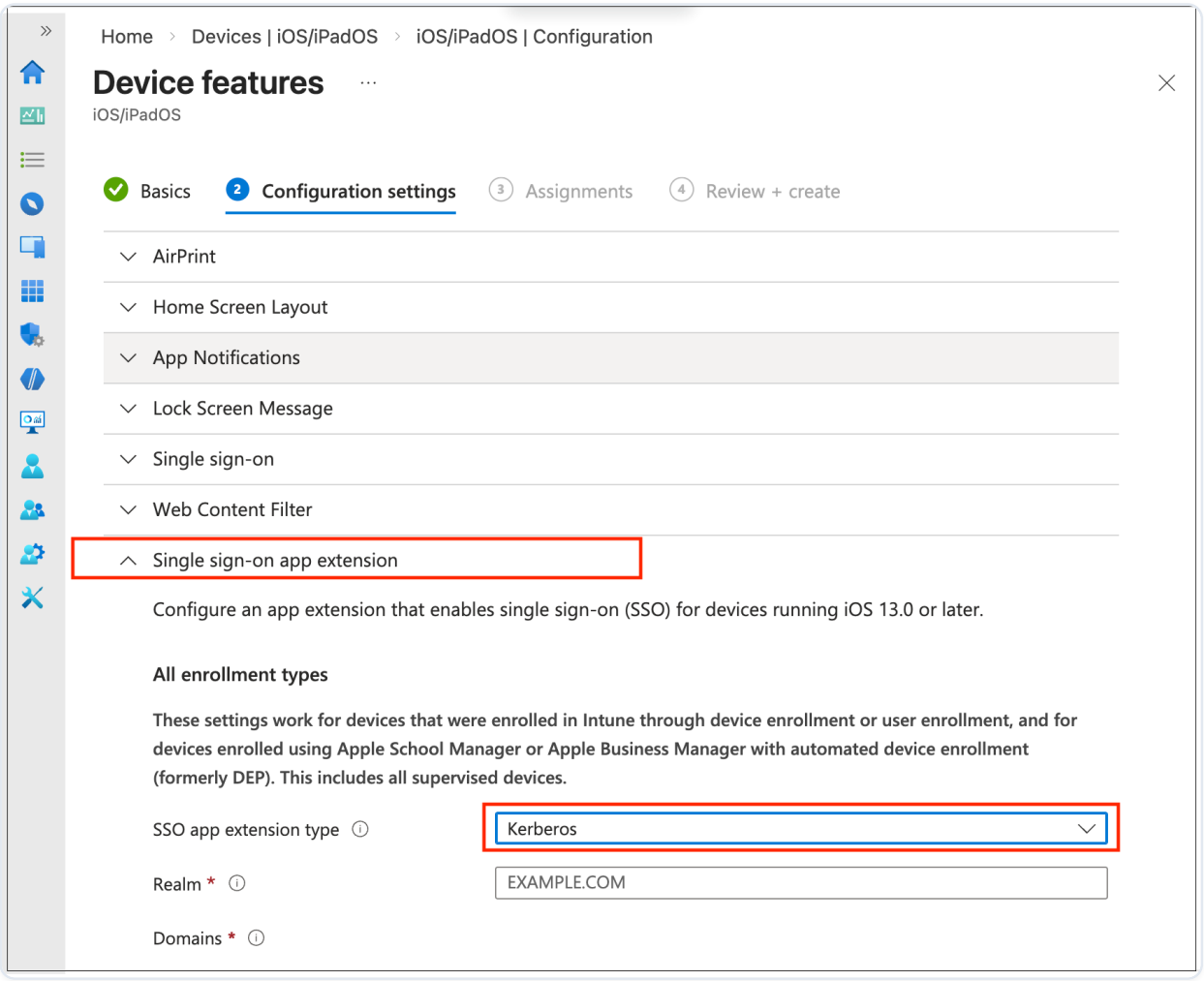
Intune policy configuration

Prerequisites: Ensure that the iOS device is enrolled into Intune.

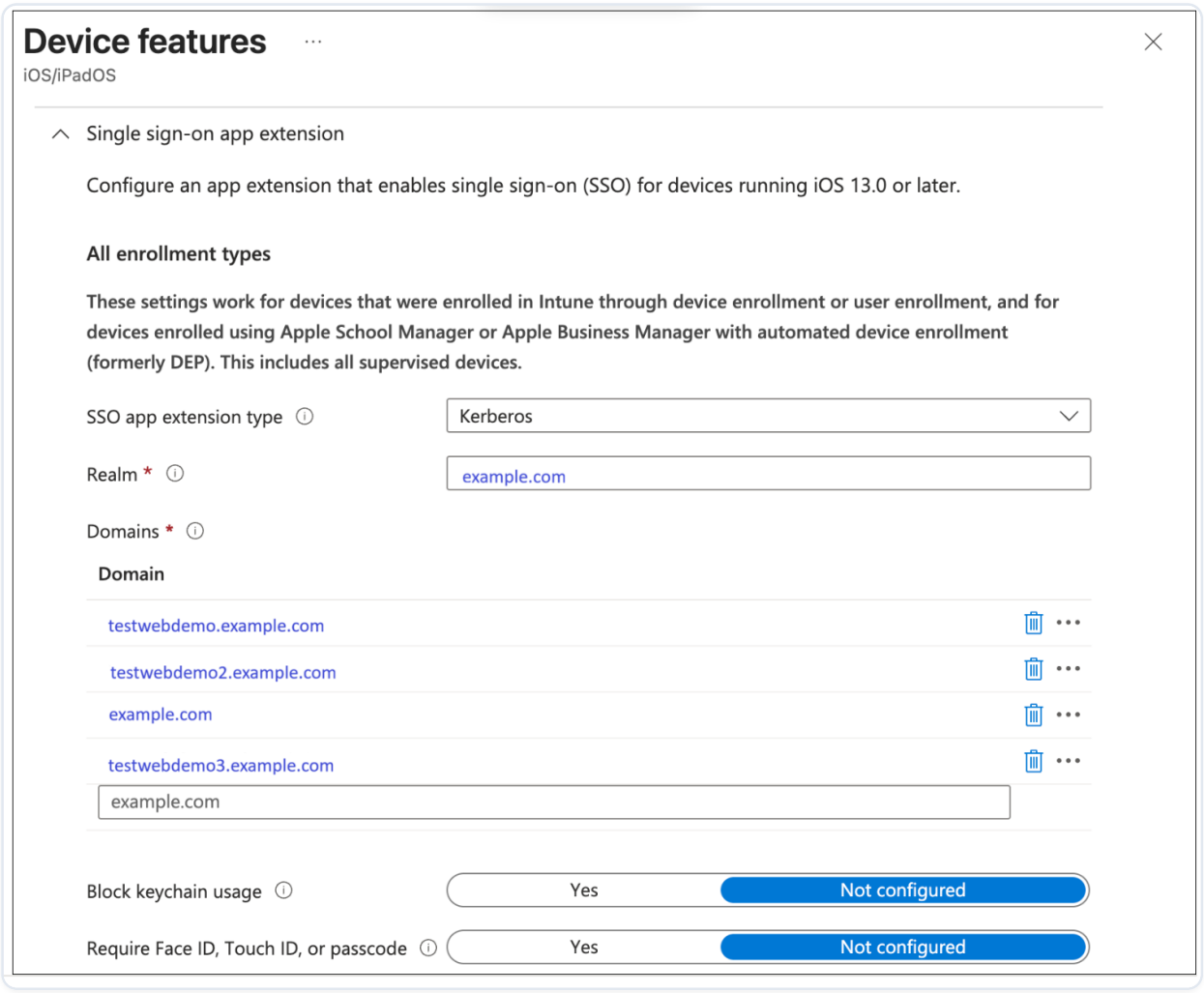
1. In the Intune Admin console, go to **Home > Devices | iOS/iPadOS → iOS/iPadOS | Configuration**.
2. Create a new policy.
3. In **Profile type** select **Templates**, and then select **Device Features**.

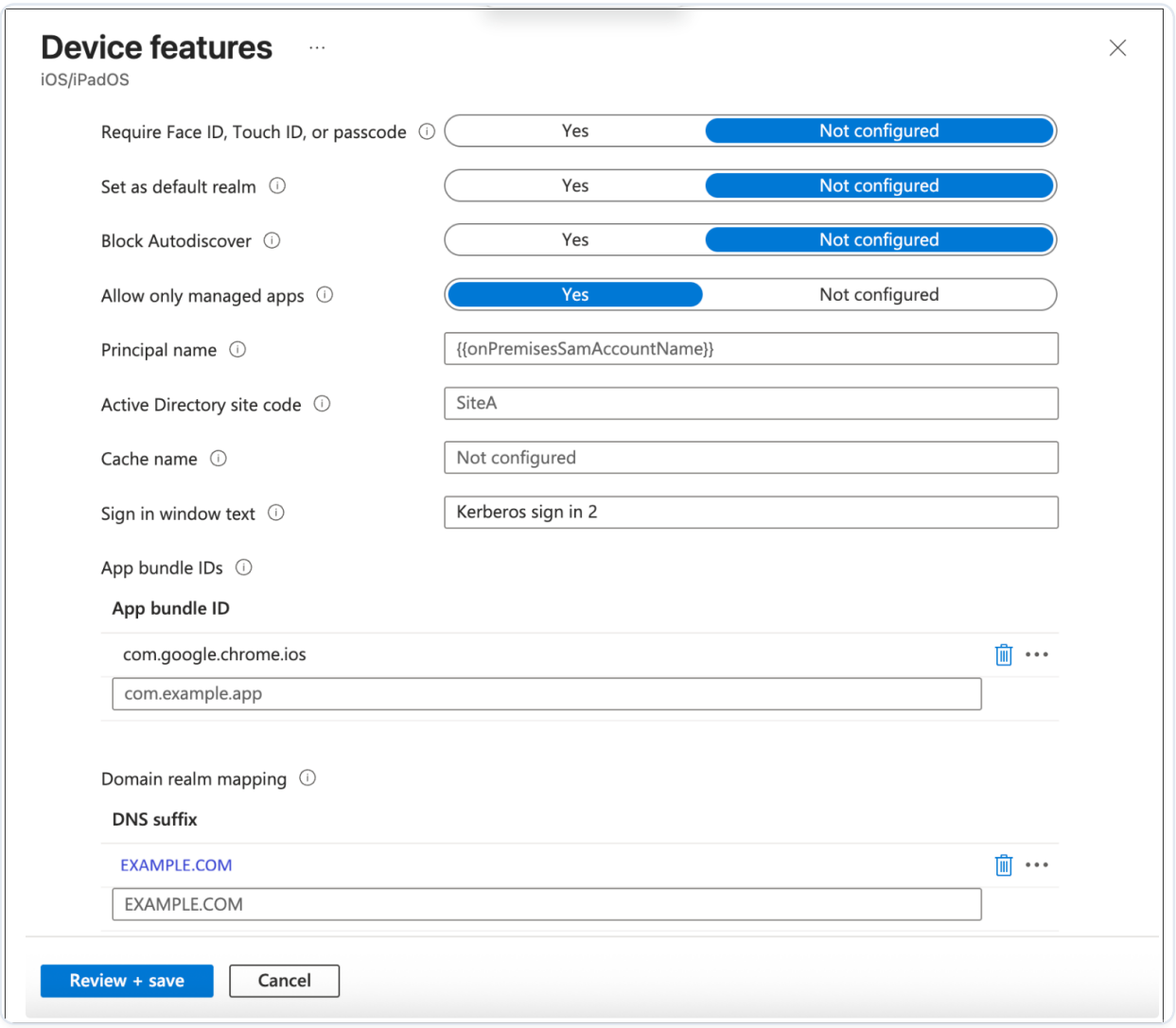


4. Press **Create**.
5. Enter a name for the policy and then proceed to **Configuration Settings**.
6. In the **Single sign-on app extension > SSO app extension type** select **Kerberos**.



7. Fill in the information according to your setup requirements.


Device features
iOS/iPadOS
Single sign-on app extension
Configure an app extension that enables single sign-on (SSO) for devices running iOS 13.0 or later.
All enrollment types
These settings work for devices that were enrolled in Intune through device enrollment or user enrollment, and for devices enrolled using Apple School Manager or Apple Business Manager with automated device enrollment (formerly DEP). This includes all supervised devices.
SSO app extension type
Kerberos
Realm *
example.com
Domains *
Domain
testwebdemo.example.com
testwebdemo2.example.com
example.com
testwebdemo3.example.com
example.com
Block keychain usage
Yes
Not configured
Require Face ID, Touch ID, or passcode
Yes
Not configured



8. Press **Review + save**.
9. Bind the policy to your device:
    - Go to **Edit Policy**, click the policy.
    - Edit **Assignments**.
    - Select your Device Group (create a Device group with your device first if not yet created).
10. Synchronize the device.

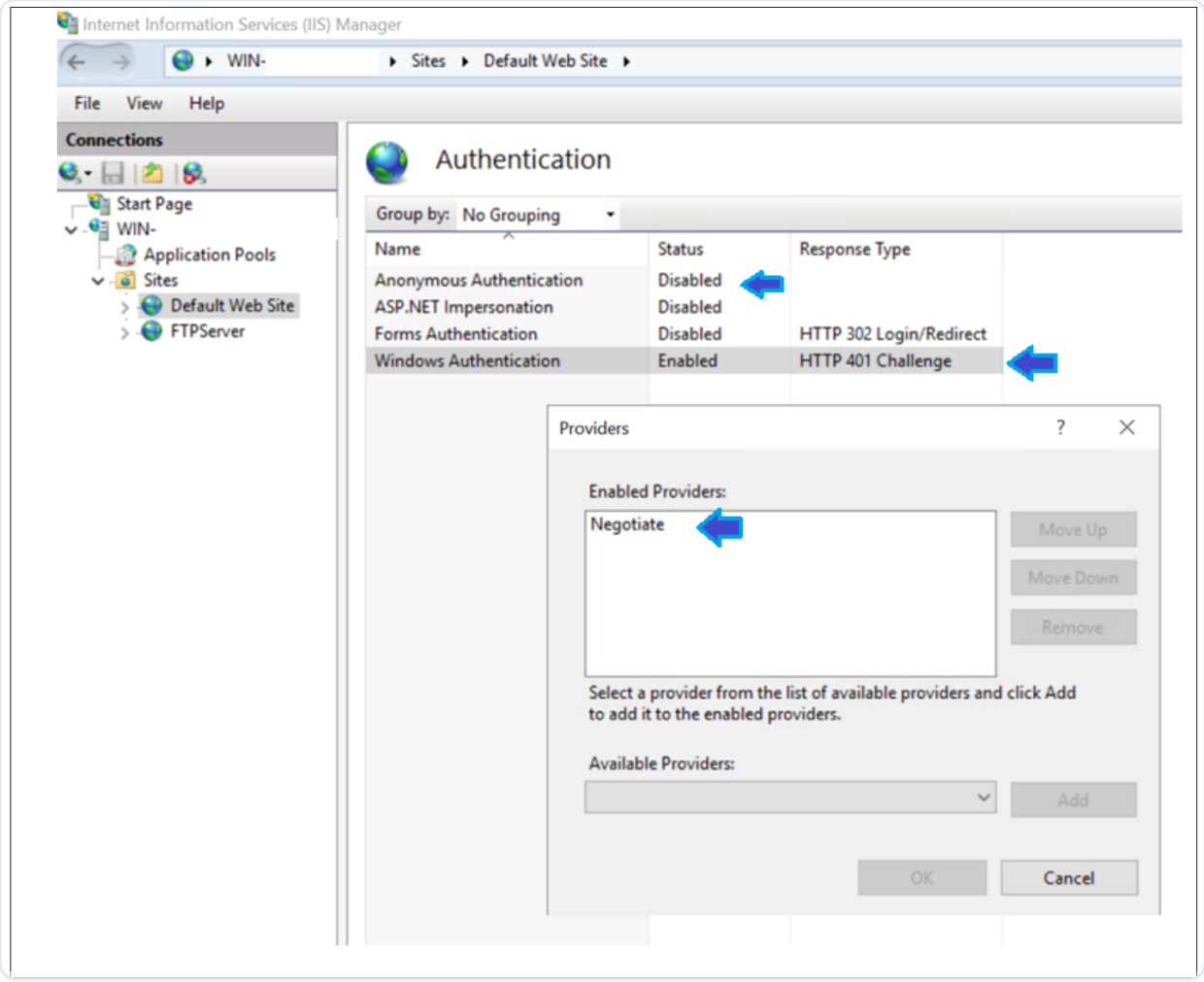
IIS configuration

On the IIS web server, enable **Windows Authentication** with the Negotiate provider and disable **Anonymous Authentication** to enforce Kerberos-based authentication.

Steps to configure IIS authentication:

1. Open IIS Manager (**inetmgr** from **Run** or **Start**).
2. In the **Connections** pane, select the site or application to configure.

3. Double-click **Authentication** in the IIS section of the Features View.
4. Disable **Anonymous Authentication**.
    - Select **Anonymous Authentication**, click **Disable** in the **Actions** pane.
5. Enable **Windows Authentication**.
    - Select **Windows Authentication**, click **Enable** in the **Actions** pane.
6. Set the Negotiate provider.
    - With **Windows Authentication** selected, click **Providers…** in the **Actions** pane.
    - Ensure **Negotiate** is listed first (above NTLM). Add it if missing.
    - Click **OK**.
7. Click **Apply** in the **Actions** pane to save the changes.
8. Optionally, run `iisreset` from an elevated command prompt to apply the configuration immediately.



Domain controller side configuration

SPN registration for short name and FQDN: Kerberos requires an exact match between the URL that the client uses and a registered SPN on the domain. A client accessing `http://testwebdemo` uses a different SPN than one accessing `http://testwebdemo.example.com`, so both must be registered.

1. Replace `<dc-hostname>` below with the host name of your Domain Controller.
2. Register both forms.
    - Short host name (used when client accesses via short name, for example `http://testwebdemo`)

      `setspn -s HTTP/testwebdemo example.com\<dc-hostname>`
    - FQDN (used when client accesses via full domain name, for example `http://testwebdemo.example.com`)

      `setspn -s HTTP/testwebdemo.example.com example.com\<dc-hostname>`
3. Verify both are registered on the correct account
    - setspn -L example.com\<dc-hostname>
4. Expected output must include both:
    - HTTP/testwebdemo
    - HTTP/testwebdemo.example.com

Feature deprecations

This article gives you advanced notice of Secure Private Access service features that are being phased out, so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when features are withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality. For details about product lifecycle support, see Product Lifecycle Support Policy.

The following table lists the Secure Private Access service features that are deprecated or planned for deprecation.

ITEM	DEPRECATION ANNOUNCED IN	DEPRECATION DATE	ALTERNATIVE
Clientless VPN access method for Web app access	January 2023	October 17, 2023	Use Citrix Enterprise Browser or Direct Access as per your use case. For more details, see About deprecation of clientless VPN access for Web app access.
Category-based web filtering	December 2022	December 31, 2022	The allow, deny, or RBI redirection functionality per website in Secure Private Access will be retained to provide selective access to non-work related websites from Citrix Enterprise Browser.
Restrict navigation security control	April 2022	15 June 2022	NA

ITEM	DEPRECATION ANNOUNCED IN	DEPRECATION DATE	ALTERNATIVE
Citrix Gateway Connector	May 2022	30 September 2022	Connector Appliance. To migrate your Gateway Connector to Connector Appliance, see Migrate Gateway Connector to Connector Appliance.

About deprecation of clientless VPN access for Web app access

- What is Clientless VPN (clientless VPN) access method?

  Citrix Secure Private Access™ uses the CVPN-based access method when an internal web app, configured without any enhanced security restrictions, is accessed via their store URL in a web browser.

  > **Note:**
  >
  > Clientless VPN access method is only used when an internal app is accessed via the store URL in a web browser. Only apps without enhanced security restrictions configured are blocked.

- Why are we deprecating this feature?

  Clientless VPN method uses client-side URL rewrites which has certain industry-wide technology limitations. In several cases, it can cause app access failures when certain links within the web apps are rewritten. This leads to a poor end-user experience. To provide the best app access experience to our customers, we are deprecating this feature and recommend moving to one of the alternatives mentioned below.

- How will it impact the end users accessing Secure Private Access configured applications?

  If any web app configured without enhanced security restrictions is accessed via the store URL from a web browser, then access to that application will be blocked. It will not impact end-user

accessing applications via Citrix Workspace app, Direct Access, Remote Browser Isolation service (RBI), or Secure Access Agent.

- What are the alternatives and what should the admins do?

  Citrix Enterprise Browser: Use the Citrix Workspace app to access these applications via the Citrix Enterprise Browser. This method provides the best end-user experience with enhanced security settings (like restricting downloads, print restrictions, watermarking, restricting clipboard access) and browser management. **Direct Access:** If you want a clientless method to access web applications, use the Direct Access method by which apps can be accessed directly from any native browser like Chrome. This method can be used for use cases where the Citrix Workspace app cannot be installed on the end device or for unmanaged devices. For more details, see Direct access to Enterprise web apps.

- Does it impact any existing applications that are accessed via Citrix Workspace app or Secure Access Agent?

  No, we are only blocking access to web applications that are accessed via a store URL opened in a web browser. This deprecation will not impact any app accessed via Citrix Workspace app or Secure Access clients that are installed on end-devices. If a web application, which is configured with enhanced security restrictions, is accessed via a web browser, then access to those applications will be blocked.

- Have more questions?

  Reach out to Citrix Support.

Data Governance

This topic provides information regarding the collection, storage, and retention of logs by the Citrix Secure Private Access service. Any capitalized terms not defined in the Definitions sections carry the meaning specified in the Citrix End User Services Agreement.

Data residency

Citrix Secure Private Access employs a multi-region architecture that ensures high availability and redundancy. For details, see Points of Presence.

- East US
- West US
- Brazil South
- Southeast Asia
- North Europe
- West Europe
- Australia East
- South India

The following are the different destinations for the service configuration and runtime logs.

- Splunk service for system monitoring and debug logs, in the US location only.
- Citrix Analytics Service for the diagnostics and user access logs, see Citrix Analytics Service Data Governance for more information.
- Citrix Application Delivery Management Service for the aggregated user access logs, see Citrix ADM Data Governance for more information.
- Citrix Cloud™ System Logs Service for admin audit logs, see the link below

For general information on Citrix Cloud Services, see Citrix Cloud Services Customer Content and Log Handling and Geographical Considerations.

Data collection

Citrix Secure Private Access enables administrators to configure and manage the service and its associated Connector Appliances through a centralized administrative interface. The service processes the following types of customer data:

- For Secure Private Access service
  - Customer private and SaaS applications
  - FQDNs and URLs for web apps or both
  - IP addresses/ranges, ports, and protocols
  - The associated resource locations
  - Single Sign-On parameters for Web and SaaS apps
- User identifiers for app entitlements
- Conditions for Adaptive Access policies
  - User identity
  - User/device geo location
  - User/device network location, through Citrix Cloud network location configuration. For details, see Optimize connectivity to stores with Direct Workload Connection.
  - Device type
- For Connector Appliance Platform, see Connector Appliance for Cloud Services related to Secure Private Access.
  - IP addresses or FQDNs
  - Users, devices, and resource location identifiers
  - Internal proxy configuration

For runtime logs collected by the service components, the key information consists of the following:

- User name
- User Object ID
- User email address
- User UPN
- User group memberships

- Client IP address and port
- Destination FQDN/address and port
- Client User-Agent
- Application name
- Application URL path
- Application access time and duration
- Request byte count
- Response byte count
- Web Filtering decision for unsanctioned applications
- HTTP transaction ID

For the comprehensive list of data sent to Citrix Analytics Service, see Citrix Analytics Service Data Governance.

Data transmission

Citrix Secure Private Access sends logs to destinations protected by transport layer security.

Data control

Citrix Secure Private Access service does not currently provide options for the customer to turn off sending logs or to prevent Customer Content from being replicated globally.

Data retention

Based on the Citrix Cloud data retention policy, the customer configuration data are purged from the service 90 days after subscription has expired.

The log destinations maintain their service-specific data retention policy.

- For details, see Data Governance for the retention policy for the Analytics logs.
- For the events stored in Citrix Application Delivery Management, see Data governance.
- The Splunk logs are archived and eventually removed after 90 days.

Data export

There are different data export options for different types of logs.

- The admin audit logs are accessible from the Citrix Cloud System Log console.
- The Secure Private Access Service diagnostics logs can be exported from the Citrix Analytics Service as a CSV file.
- The Splunk logs are not for customers to consume. These events can also be exported from Splunk as a CSV file.

Definitions

- Customer Content means any data uploaded to a customer account for storage or data in a customer environment to which Citrix is provided access to perform Services.
- Log means a record of events related to the services, including records that measure performance, stability, usage, security, and support.
- Services mean that the Citrix Cloud services outlined earlier for the purposes of Citrix Analytics.

Product certifications and compliance

Citrix Secure Private Access is a Zero Trust Network Access (ZTNA) solution that helps organizations securely connect users to applications without exposing networks directly to the internet. Secure Private Access is delivered as part of the broader Citrix Cloud and hybrid service portfolio and is governed by Citrix's cloud service compliance and audit programs.

This page summarizes the certifications and compliance attestations applicable to Secure Private Access.

Certifications and Audits

- **SOC 2® Type 2:**

  Secure Private Access is covered under Citrix's SOC 2 Type 2 audit program.

  SOC 2 Type 2 audits have evaluated the security, availability, confidentiality, processing integrity, and privacy controls applicable to Citrix Cloud services, including Secure Private Access.

- **ISO 27001 & ISO 27701:**

  Secure Private Access is included within Citrix's ISO 27001 (Information Security Management) and ISO 27701 (Privacy Information Management) certified service portfolio.

  These globally recognized certifications affirm that security and privacy management practices are formally established, documented, and continuously improved.

- **HIPAA:**

  Secure Private Access is suitable for use in environments that require HIPAA compliance when configured and contracted appropriately. Citrix's cloud compliance documentation indicates HIPAA applicability for Secure Private Access.

- **PCI DSS 4.0:**

  Secure Private Access is included within Citrix's annual PCI DSS assessments for applicable cloud services. Customers deploying Secure Private Access in PCI-scoped environments might

need to implement additional controls to meet PCI requirements. PCI DSS compliance follows a shared responsibility model between Citrix and the customer.

- **FIPS / Common Criteria:**

  Secure Private Access can be deployed as part of a FIPS-compliant solution when paired with FIPS-certified or FIPS-enabled NetScaler platforms and the FIPS-certified Citrix CryptoKit used by Citrix Workspace app.

  For Common Criteria, Secure Private Access integrates with Common Criteria (NDcPP) certified NetScaler platforms and Common Criteria certified Citrix Workspace app, enabling deployments that align with Common Criteria requirements at the solution level.

- **Australia IRAP (Information Security Registered Assessors Program):**

  Secure Private Access is included within Citrix's cloud services that undergo IRAP assessments by accredited Australian Government assessors.

  IRAP provides independent validation that Citrix Cloud services align with the Australian Government Information Security Manual (ISM) security controls.

Certificates and audit reports

Download the available certificates and audit reports through the Citrix Trust Center.

index

- Migrate Gateway Connector to Connector Appliance
- Route tables to resolve conflicts resulting from same related domains
- Single sign-on to the Citrix Secure Access™ client via Citrix Workspace app
- ADFS integration with Secure Private Access
- Citrix Secure Private Access™
- Route DNS queries to application-specific resource locations
- Configure G Suite
- Configure Jira
- Configure O365
- Configure ERP Cloud
- Configure ServiceNow
- Configure Tableau
- Configure Workday
- Configure Zoom
- Access mode-based policy enforcement
- Support for server-to-client connections - Preview

Migrate Gateway Connector to Connector Appliance

Citrix Gateway Connector™ is deprecated. Citrix recommends its customers using Citrix Gateway Connectors in their environment, to start deploying Connector Appliance for all Secure Private Access use cases that were previously supported by the Citrix Gateway Connector. This topic provides guidelines on migrating Gateway Connector to Connector Appliance.

High-level steps to migrate Gateway Connector to Connector Appliance

1. Install the Connector Appliances in addition to the Gateway Connectors in the same resource location.

2. Shut down the Gateway Connectors and test the existing Web apps for connectivity. Check if the Web app hosted on the same resource location is accessible.
3. Remove the Citrix Gateway Connector once testing is complete.

To install Connector Appliance

Use the following steps to install a Connector Appliance.

1. Sign in to Citrix Cloud.
2. From the menu in the top left of the screen, select **Resource Locations**.
3. Click the plus icon next to Connector Appliance for the resource location that you want to add a Connector Appliance.
4. Select the hypervisor and click **Download Image**.
5. Download and Install the Connector Appliance on your hypervisor.
6. Log in to the Web UI (IP address provided on the hypervisor's console) and set up a proxy if necessary.
7. Click the **Register** button and obtain the short code.
8. Paste the short code into the Citrix Cloud user interface used when downloading the Connector Appliance (step 5).

   The Connector Appliance is registered.

For detailed steps, see Connector Appliance for Cloud Services.

FAQs

- How do I download the Connector Appliance?

  Download the Connector Appliance.
- How do I install the Connector Appliance?

  Installing the Connector Appliance.
- How do I register the Connector Appliance?

  Registering the Connector Appliance.
- What are the connectivity requirements for the Connector Appliance?

  Connector Appliance Internet Connectivity Requirements.
- What are the system requirements for the Connector Appliance?

Connector Appliance System Requirements.

- How is Connector Appliance updated?

  Connector Appliance Updates

Route tables to resolve conflicts resulting from same related domains

The application domains feature of the Citrix Secure Private Access™ service enables customers to make routing decisions that allow related domains of applications to be routed externally or internally through Connector Appliances.

Consider that the customer has configured the same related domains within both a SaaS app and an internal web app. For example, if Okta is the SAML IdP for both Salesforce (SaaS app) and Jira (internal web app), then the admin might configure `*.okta.com` as a related domain in both apps' configuration. This leads to a conflict and the end user experiences inconsistent behavior. In this scenario, the admin can define rules to route these applications either externally or internally through the Connector Appliances, as per the requirement.

How the route table works

The admins can define the following route types for the apps depending on how they want to define the traffic flow.

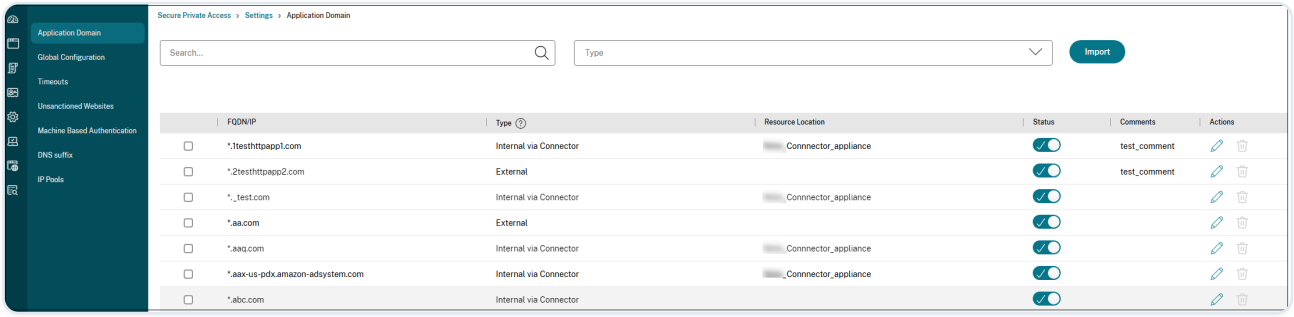
- **Internal – Bypass Proxy** - The domain traffic is routed through Citrix Cloud Connector™, bypassing the customer's web proxy configured on the Connector Appliance.
- **Internal via Connector** - The apps are external but the traffic must flow through the Connector Appliance to the outside network.
- **External** – The traffic flows directly to the internet.

> **Note:**
>
> - Route entries do not impact the security policies that are configured on the apps.
> - If admins do not intend to use an entry in the route table or if the corresponding apps are not working as intended, admins can simply disable the entry instead of deleting it.

- All Connector Appliances for a particular customer, irrespective of the app type, get the SSO settings. Previously, the SSO setting for a particular app was tied to a resource location.

Main route table

The main routing table in the Secure Private Access console (**Settings > Application Domains**) is a view-only dashboard that gives you all details about the configured domains in all the applications. This can be used to see the following information for any domain:



The main route table can be used to see the following information for any domain:

- **FQDN/IP:** FQDN or the IP address for which the type of traffic routing is desired to be configured.
- **Type**: App type. **Internal**, **Internal – Bypass Proxy**, or **External** as selected when adding the app.

  Important:

  If there are conflicts, then an alert icon is displayed for the respective row in the table. To resolve the conflict, admins must click the triangular icon and change the app type from the main table.

- **Resource location:** Resource location for routing of type **Internal**. If a resource location is not allocated, a triangular icon appears in the **Resource location** column for the respective app. When you hover on the icon, the following message is displayed.

  Missing resource location. Ensure that a resource location is associated with this FQDN.

- **Status:** The toggle switch in the **Status** column can be used to disable the route for a route entry without deleting the app. When the toggle switch is turned OFF, the route entry does not

take effect. Also, if FQDNs of exact match exist, admins can select the route to be enabled or disabled.

- **Comments:** Displays comments, if any.
- **Actions:** The edit icon is used to add a resource location or change the type of route entry. The delete icon is used to delete the route.

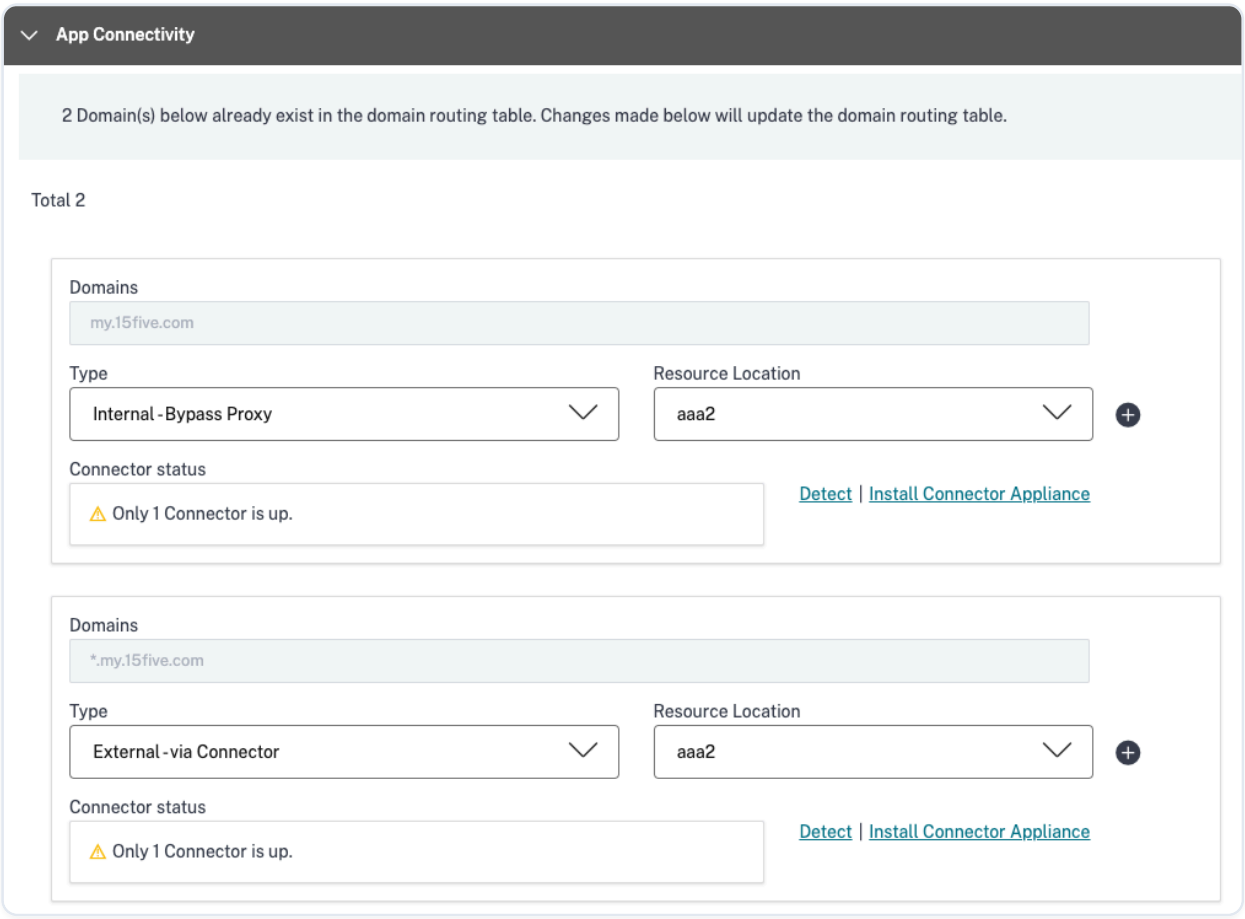
Mini route table

A mini version of the Application Domains table is available to make the routing decisions during app configuration. The mini route table available in the **App Connectivity** section in the Citrix Secure Private Access service user interface.

To add routes to the mini route table

The steps to add an app in the Citrix Secure Private Access service remain the same as described in the topics Support for software as service apps and Support for Enterprise web apps except for the following two changes:

1. Complete the following steps:
    - Choose a template.
    - Enter app details.
    - Choose enhanced security details, as applicable.
    - Select the single sign-on method, as applicable.
2. Click **App Connectivity**. - A mini version of the Application Domains table is available to make the routing decisions during app configuration.



- **Domains:** The Domains column displays one or more rows for a particular app. The first row displays the actual app URL that the admin has entered while adding the app details. The other rows are all related domains that are entered while adding the app details. If the app URL and the related domains are the same, they are displayed in one row.

One row displays the SAML assertion URL, if SAML SSO is selected.

- **Type:** Select one of the following options.
  - **Internal – Bypass Proxy** - The domain traffic is routed through Citrix Cloud™ Connector, bypassing the customer's web proxy configured on the Connector Appliance.
  - **Internal via Connector** - The apps are external but the traffic must flow through the Connector Appliance to the outside network.
  - **External** – The traffic flows directly to the internet.
- **Resource Location:** Autopopulated when you select the type Internal for an app. Change it if a different resource location is desired.
- **Connector Appliance Status:** Autopopulated, along with resource location, when you select the type Internal for an app.

Single sign-on to the Citrix Secure Access™ client via Citrix Workspace app

Citrix Secure Access client now supports single sign-on for the store URL when already logged in via Citrix Workspace app. This SSO functionality enhances the user experience by avoiding multiple authentications.

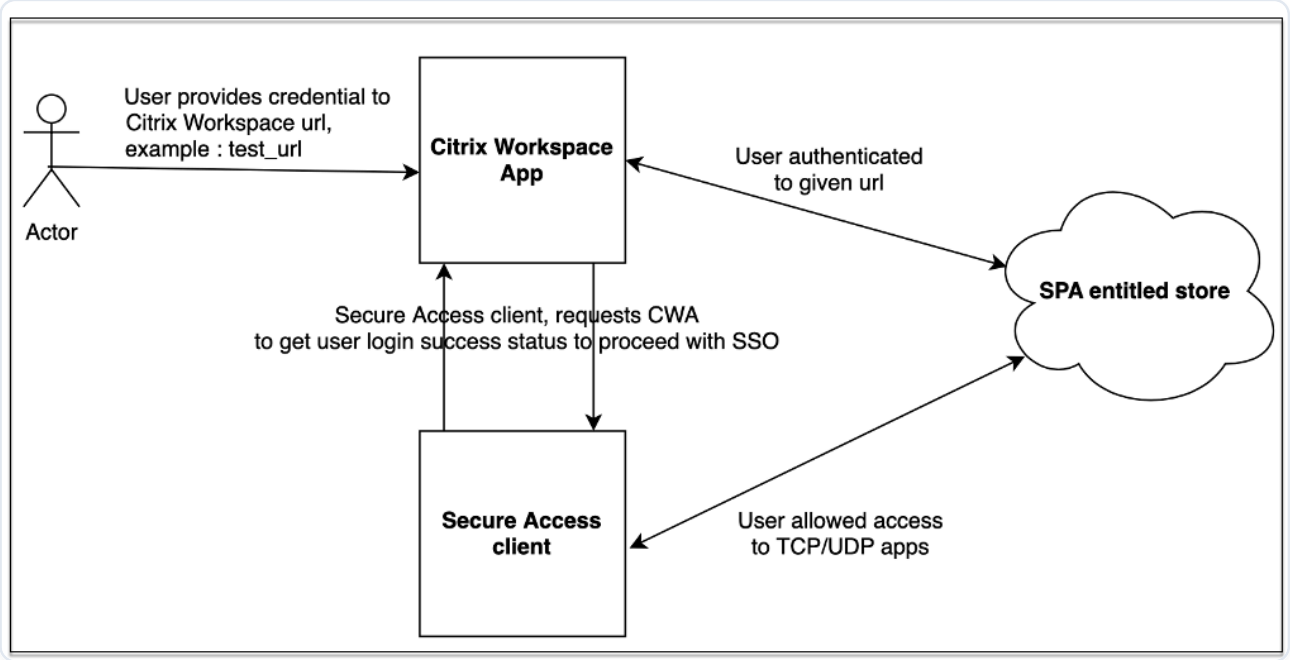
Prerequisites

- Both the Citrix Workspace app and the Secure Access client must be installed on the device.
- Users must have logged into the Citrix Workspace app first for the automatic SSO to happen in the Citrix Secure Access client.

Note:

The single sign-on feature is only supported for the primary store that is configured in Citrix Workspace app. If the user logs into any other store other than the primary store, then SSO does not happen. The user has to manually log in to the Citrix Secure Access client.

The following figure displays the SSO flow between the Citrix Workspace app and the Citrix Secure Access client.



Feature requirements for Windows

- Citrix Workspace app version - **22.10.5.14(2210.5) or above**
- Citrix Secure Access version - **22.10.1.9 or later**
- Citrix Secure Access Windows Registry - **EnableCWASSO**

The SSO feature is disabled, by default. To enable this feature, add the following registry on the end-user machine.

- Registry Name - EnableCWASSO
- Registry Path - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
- Registry Type - REG_DWORD
- Registry Value - 1

> **Important:**

> Sometimes, the end user machines might need to reboot for successfully establishing single sign-on with Citrix Workspace app.

ADFS integration with Secure Private Access

Claim rules are necessary to control the flow of claims through the claims pipeline. Claim rules can also be used to customize the claims flow during the claim rule execution process. For more information about claims, see Microsoft documentation.

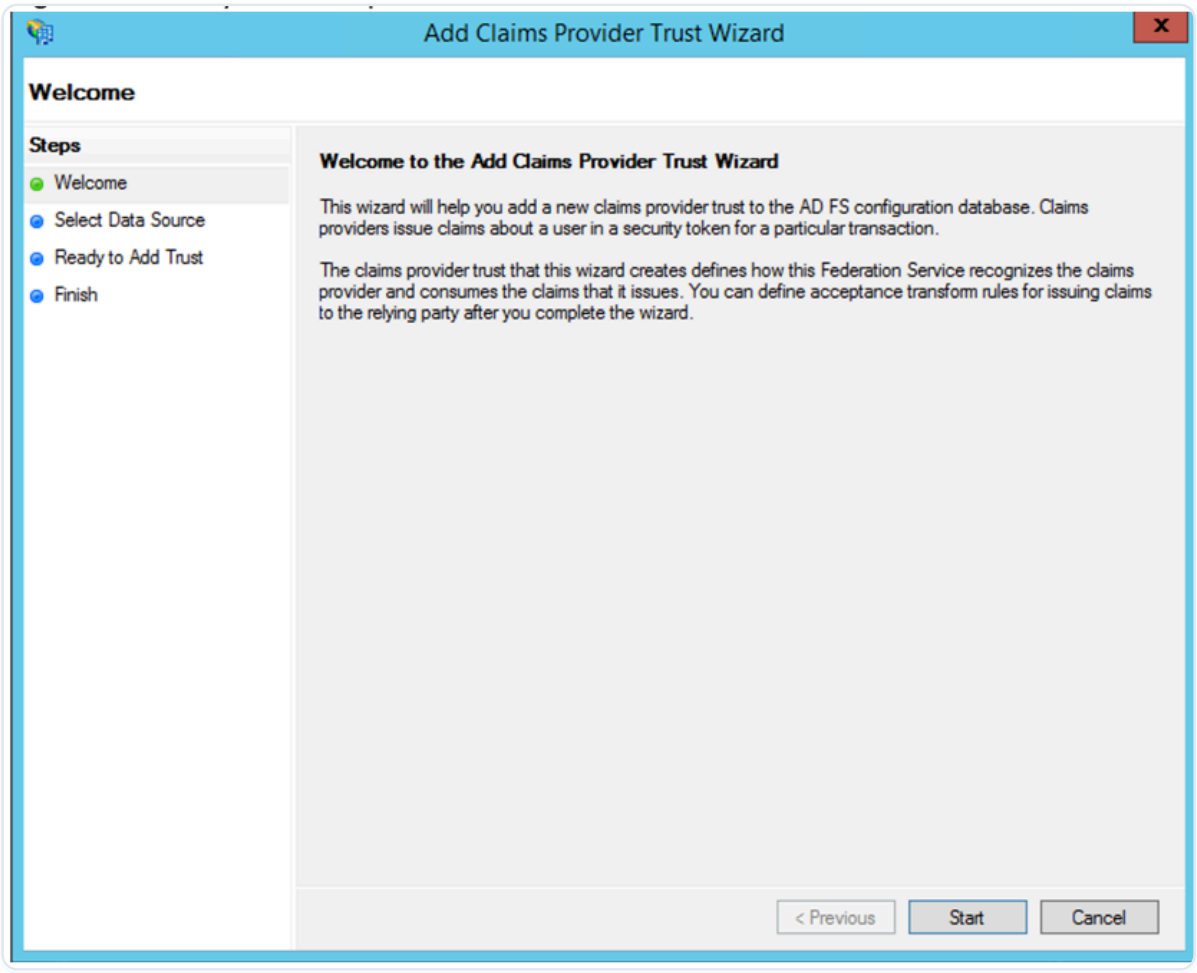
To set up ADFS to accept claims from Citrix Secure Private Access™, you must perform the following steps:

1. Add claim provider trust in ADFS.
2. Complete the app configuration on Citrix Secure Private Access.

Add claim provider trust in ADFS

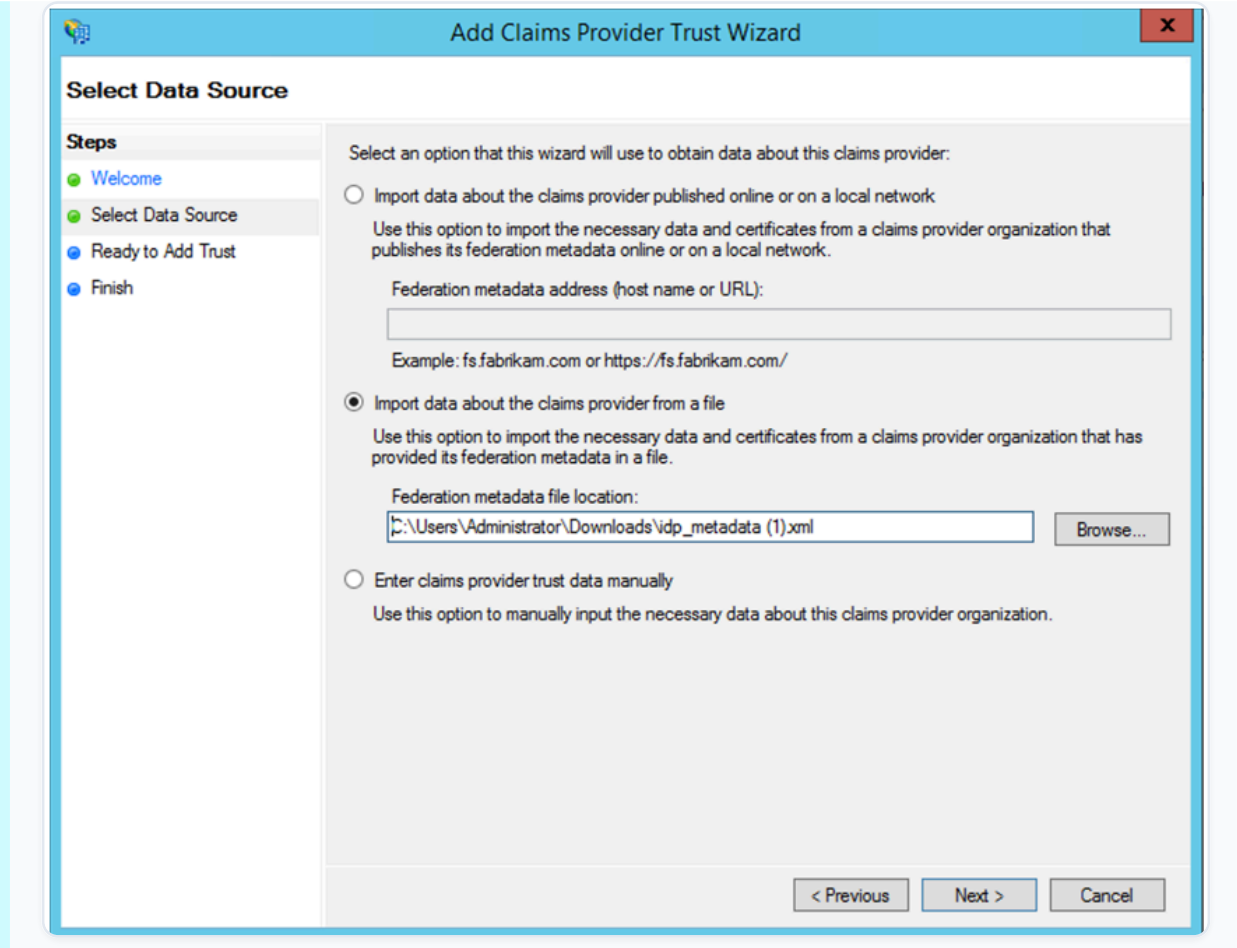
1. Open ADFS management console. Go to **ADFS > Trust relationship > Claim provider Trust**.

a. Right-click and select **Add Claim Provider Trust**.



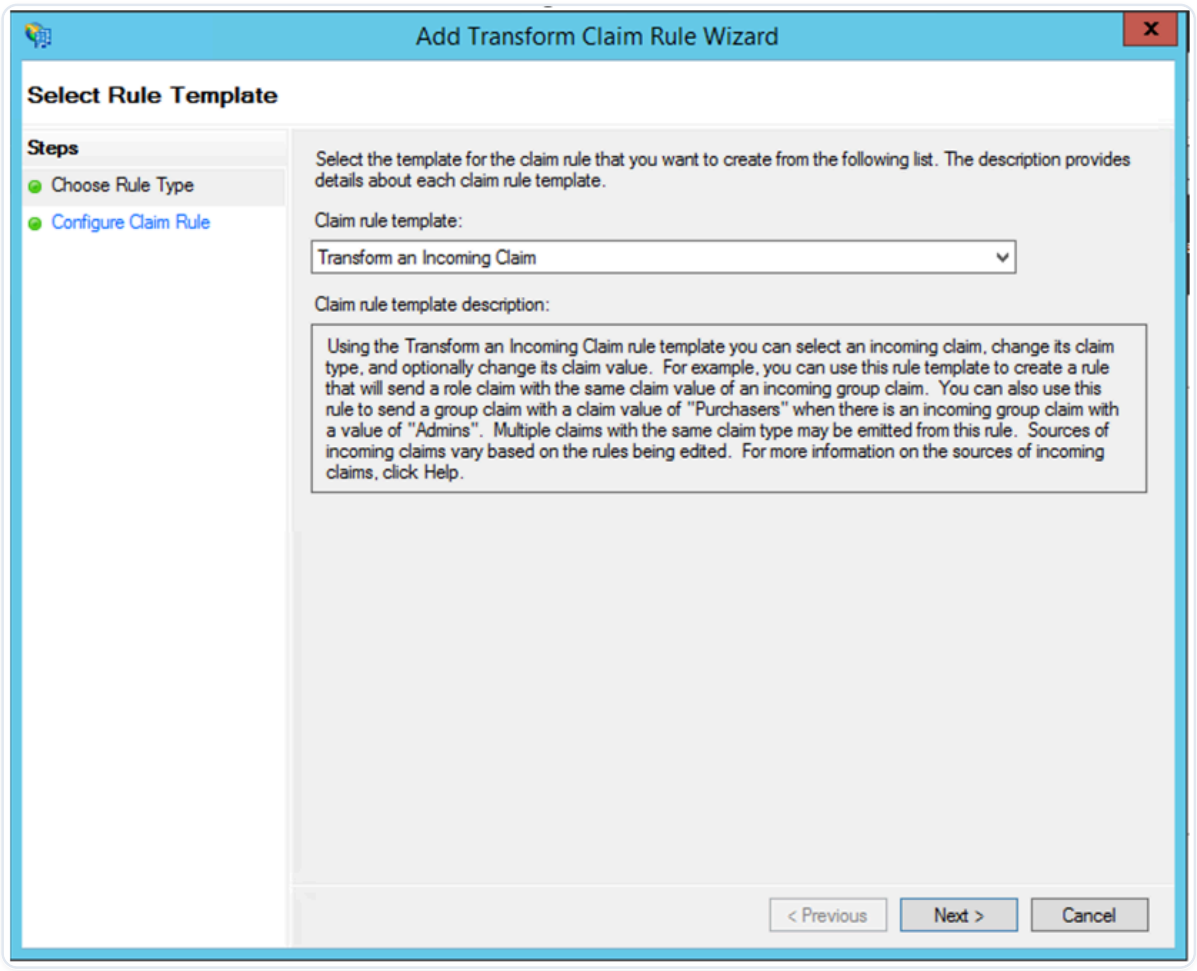
b. Add an app in Secure Private Access that is used to federate to ADFS. For details see, App configuration on Citrix Secure Private Access.

> **Note:**
>
> First add the app and from the app's SSO configuration section, you can download the SAML metadata file, and then import the metadata file into ADFS.

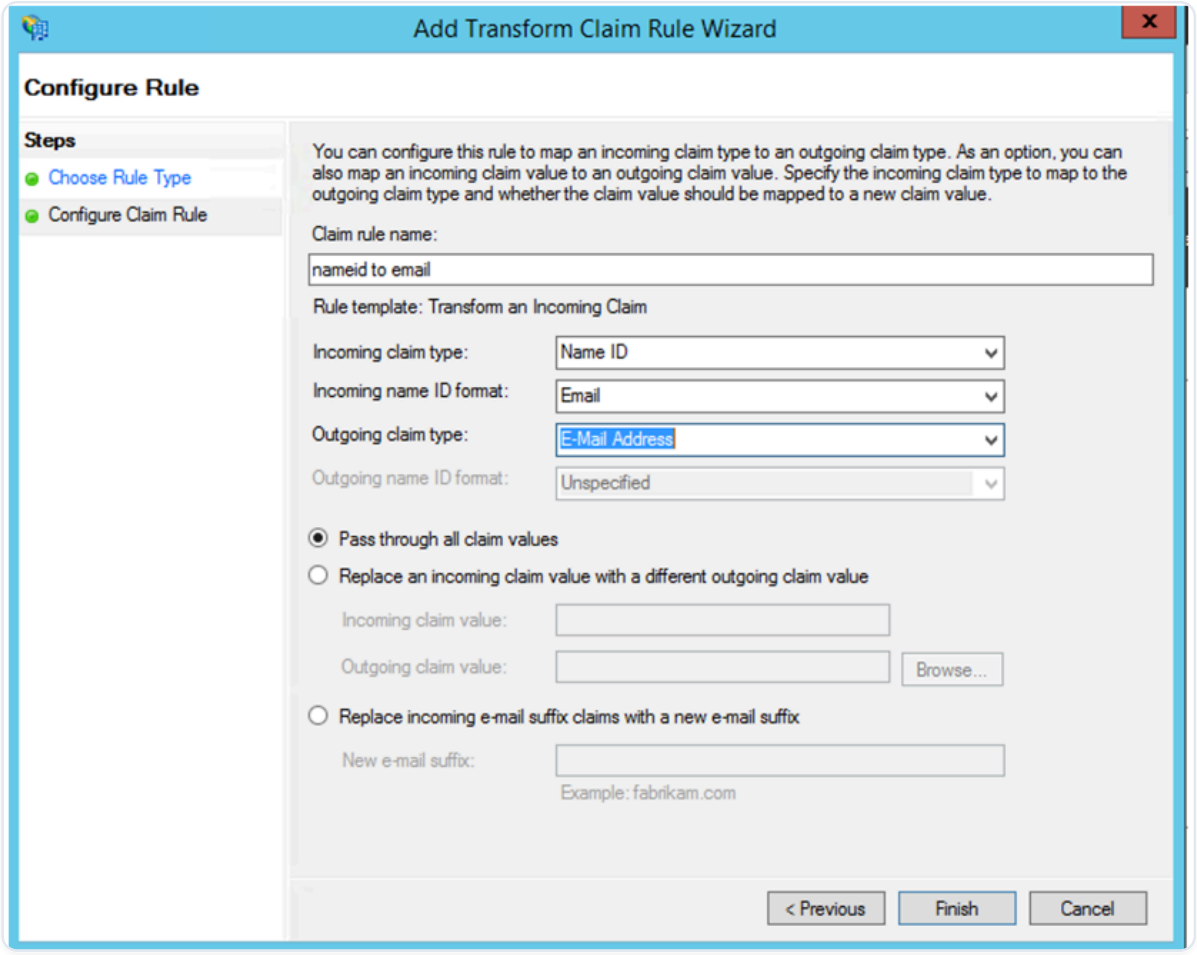


a. Complete the steps to finish adding claim provider trust. After you complete adding the claim provider trust, a window to edit the claim rule appears.

b. Add a claim rule with **Transform An Incoming Claim**.



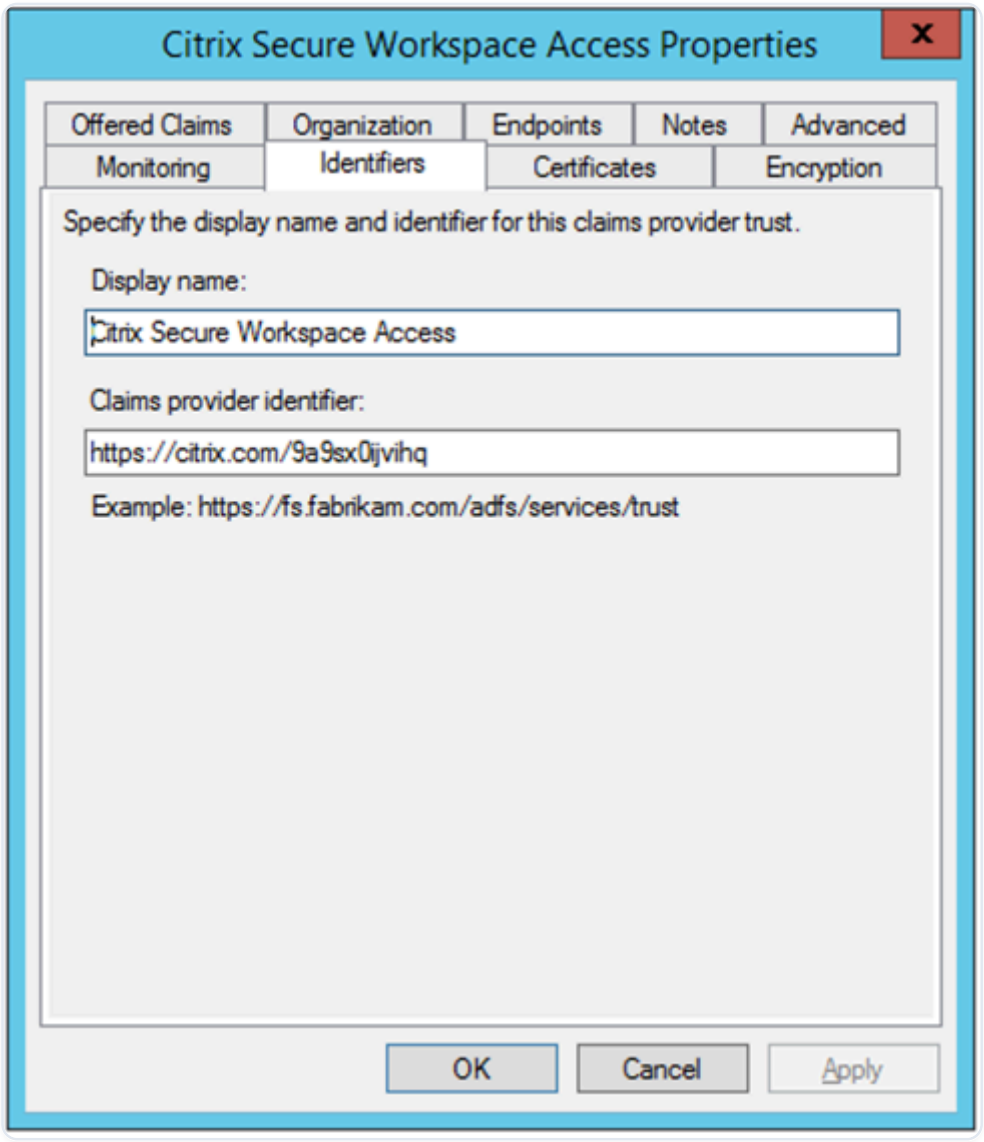
c. Complete the settings as shown in the following figure. If your ADFS accepts other claims, then use those claims and configure SSO in Secure Private Access also accordingly.



You have now configured the claim provider trust that confirms ADFS now trusts Citrix Secure Private Access for SAML.

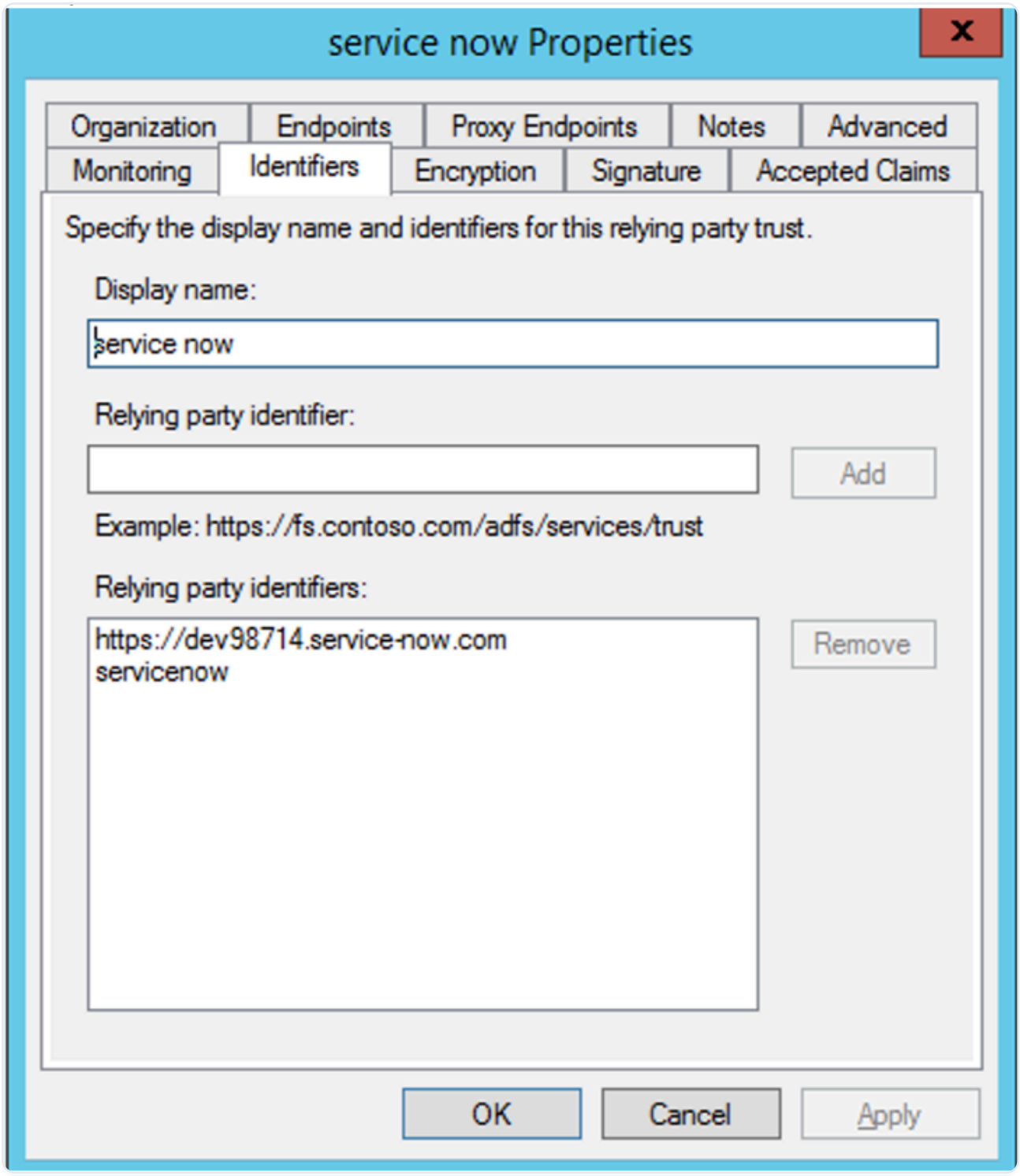
Claim Provider trust ID

Make a note of the claim provider trust id that you added. You need this ID while configuring the app in Citrix Secure Private Access.



Relaying Party Identifier

If your SaaS app is already authenticated using ADFS, then you must already have the Relaying party trust added for that app. You need this ID while configuring the app in Citrix Secure Private Access.



Enable relay state in IdP initiated flow

RelayState is a parameter of the SAML protocol that is used to identify the specific resource the users access after they are signed in and directed to the relying party's federation server. If RelayState is not enabled in ADFS, users see an error after they authenticate to the resource providers that requires it.

For ADFS 2.0, you must install update KB2681584 (Update Rollup 2) or KB2790338 (Update Rollup 3) to provide RelayState support. ADFS 3.0 has RelayState support built in. In both cases RelayState still needs to be enabled.

To enable the RelayState parameter on your ADFS servers

1. Open the file.
    - For ADFS 2.0, enter the following file in Notepad: %systemroot%\inetpub\adfs\ls\web.config
    - For ADFS 3.0, enter the following file in Notepad: %systemroot%\ADFS\Microsoft.IdentityServer.Servicehost.exe.config
2. In the microsoft.identityServer.web section, add a line for useRelyStateForIdpInitiatedSignOn as follows, and save the change: `<microsoft.identityServer.web> ... <useRelayStateForIdpInitiatedSignOn enabled="true" /> ...</microsoft.identityServer.web>`
    - For ADFS 2.0, run `IISReset` to restart IIS.
3. For both platforms, restart the Active Directory Federation Services `(adfssrv) service.` **Note:** If you have windows 2016 or Windows 10 then use the following PowerShell command to enable it. `Set-AdfsProperties -EnableRelayStateForIdpInitiatedSignOn $true`

Link to commands - `<https://docs.microsoft.com/en-us/powershell/module/adfs/set-adfsproperties?view=win10-ps>`

App configuration on Citrix Secure Private Access

You can either configure the IdP initiated flow or the SP initiated flow. The steps to configure IdP or SP initiated flow in Citrix Secure Private Access are the same except that for SP initiated flow, you must select the **Launch the app using the specified URL (SP initiated)** check box in the UI.

IdP initiated flow

1. While setting up the IdP initiated flow, configure the following.
    - **App URL** – Use the following format for the app URL. `https://<adfs fqdn>/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=<rp id>&RedirectToIdentityProvider=<idp id>`
    - **ADFS FQDN** – FQDN of your ADFS setup.
    - **RP ID** – RP ID is the ID that you can get from your relaying party trust. It is the same as the Relaying Party Identifier. If it is a URL, then URL encoding happens.

- **IDP ID** – IdP ID is the same as the claim provider trust ID. If it is a URL, then URL encoding happens.

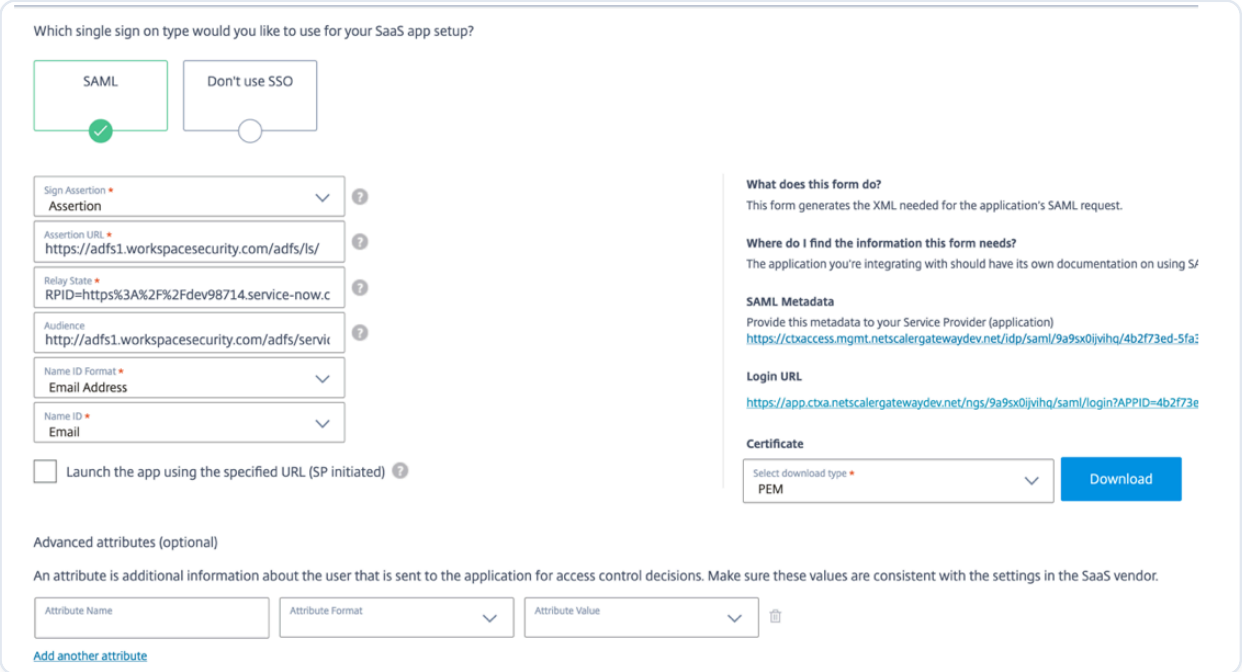
  Example: `<https://adfs1.workspacesecurity.com/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=https%3A%2F%2Fdev98714.service-now.com&RedirectToIdentityProvider=https%3A%2F%2Fcitrix.com%2F9a9sx0ijvihq>`

2. SAML SSO configuration.

   The following are the default values of the ADFS server. If any of the values are changed, get the correct values from the metadata of the ADFS server. Federation metadata of the ADFS server can be downloaded from its federation metadata endpoint, whose endpoint can be known from **ADFS > Service > Endpoints.**

   - **Assertion URL** – `https://<adfs fqdn>/adfs/ls/`
   - **Relay State** – Relay state is important for the IdP initiated flow. Follow this link to construct it properly - `https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/jj127245(v=ws.10)`

     Example: RPID=https%3A%2F%2Fdev98714.service-now.com&RelayState=https%3A%2F%2Fdev98714.service-now.com%2F
   - **Audience** – `http://<adfsfqdn>/adfs/services/trust`
   - For the other SAML SSO configuration settings, see to the following image. For more details, see Support for SaaS apps.



3. Save and subscribe the app to the user.

SP initiated flow

For SP initiated flow, configure the settings as captured in the **IDP initiated flow** section. In addition, enable the **Launch the app using the specified URL (SP initiated)** check box.

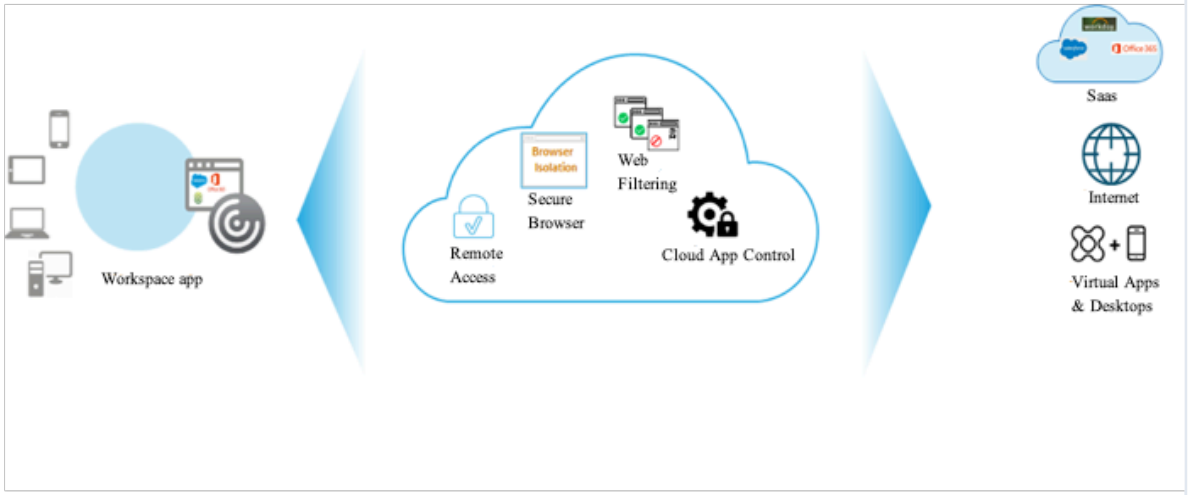
Citrix Secure Private Access™

The Citrix Secure Private Access service enables the administrators to provide a cohesive experience integrating single sign-on, remote access, and content inspection into a single solution for end-to-end access control. IT administrators can govern access to approved SaaS apps with a simplified single sign-on experience. With the Citrix Secure Private Access service, administrators can also protect the organization’s network and end user devices from malware and data leaks by filtering access to specific websites and website categories. Administrators can enforce enhanced access security policies for secure access to SaaS applications. Once authenticated, employees have access to all critical business applications from any device irrespective of whether they are in the office premises, at home, or traveling.

Administrators can monitor user activities, such as malicious, dangerous, or unknown websites visited, and the bandwidth consumed, and risky download and upload behaviors. Using the Analytics around websites and website categories accessed, administrators can take corrective action to protect the enterprise network. At the same time, the service provides end users seamless and secure access to all their hosted apps.

Administrators can also restrict actions, such as restricted printing, downloads, and clipboard access (copy-paste).

The following diagram is a visual depiction of the Secure Private Access service.



Key capabilities of Citrix Secure Private Access

Following are some of the key tasks that you can complete with the Citrix Secure Private Access service:

- **Publish SaaS apps with single sign-on access** - Once the user is authenticated to their store with a primary identity, subsequent authentication challenges to SaaS and web apps are automatically fulfilled by the single sign-on feature in the Citrix Cloud™ using SAML assertions.

By default, the SAML assertion utilizes the email address associated with the user's Active Directory account (identity provider) with the email address associated with the user's SaaS or web app account (service provider).

- **Set enhanced security policies for SaaS apps. (For example, watermark, copy-paste restriction, and prevent downloads.)** - To protect content, organizations incorporate enhanced security policies within the SaaS applications. Each policy enforces a restriction on the Citrix Enterprise Browser™ when using Workspace app for desktop or on Secure Browser when using Workspace app web or mobile.
    - Preferred browser: Disables local browser use and relies on the Citrix Enterprise Browser engine (Workspace app - desktop) or Secure Browser (Workspace app – mobile and web).
    - Restrict clipboard access: Disables cut/copy/paste operations between the app and endpoint clipboard.
    - Restrict printing: Disables ability to print from within the app browser.

    - Restrict downloads: Disables the user's ability to download from within the SaaS app.
    - Display watermark: Overlays a screen-based watermark showing the user name and IP address of the endpoint. If a user tries to print or take a screenshot, the watermark appears as displayed on the screen.

- **Provide contextual access** - Although an authorized SaaS app is considered safe, content in the SaaS app actually can be dangerous - constituting a security risk. When a user clicks a hyperlink within a SaaS app, the traffic is routed through the web filtering feature, which provides a risk assessment for the hyperlink. Based on the hyperlink's risk assessment, and the customized list of URL categories, the web filtering feature allows, denies, or redirects the hyperlink request from the user as follows:
    - Approved: The hyperlink is considered safe and the Citrix Enterprise Browser accesses within the Workspace app accesses the hyperlink.
    - Denied: The hyperlink is considered dangerous and access is denied.
    - Redirected: The hyperlink request is redirected to the Remote Browser Isolation service, where the user's internet browsing activities are isolated from the endpoint device, the corporate network, and the SaaS app.
- **Security and performance analytics** - Users invariably access SaaS apps that have enhanced security inherent in them. The Citrix Workspace app, the Secure Private Access service, and the Remote Browser Isolation service provide the Security analytics service with information about the following user and application behaviors. These analytics impact the user's overall risk score:
    - App launch time
    - App end time
    - Print action
    - Clipboard access
    - URL Access
    - Data upload
    - Data download

The web filtering feature evaluates the risk of each hyperlink selected within the SaaS application. Accessing these sites and monitoring changes in user behavior increases the user's overall risk score because it signals the endpoint device is compromised and started to infect or encrypt data or the user and device are stealing intellectual property.

Secure Private Access REST APIs

You can use the Secure Private Access REST APIs to directly configure multiple applications and policies. For details, see Citrix Secure Private Access.

Route DNS queries to application-specific resource locations

Administrators can route DNS queries for specific applications directly to their dedicated resource locations. This enables more accurate DNS resolution, intelligent traffic management, and a better user experience. Previously, all DNS queries were routed by default to the geographically nearest available DNS server, regardless of where the application is hosted. This required DNS servers across all resource locations to be synchronized, which is not always achievable.

System requirements

Citrix Secure Access client:

- macOS - V25.08.1.1 and later (Citrix Downloads), V25.08.1 and later (App Store).
- Windows - 25.7.1.11 or later.

Feature enablement

The application-specific DNS routing feature is disabled by default. To get the feature enabled for your organization, contact Citrix Support.

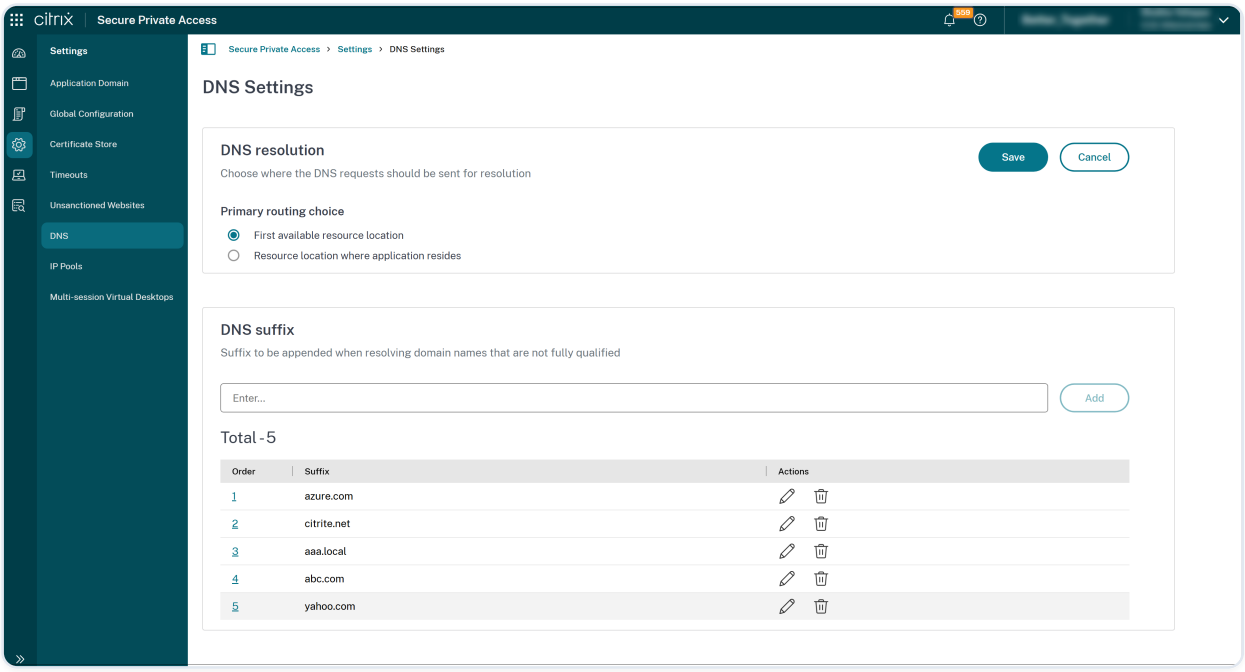
Configure routing for DNS queries

After the feature is enabled, you can route DNS queries using one of the following two options:

- **First Available resource location:** Retain the legacy behavior where all queries are routed to the geographically closest resource location. Make sure that all DNS servers in all resource locations are synchronized if you choose to use this option.
- **Resource location where application resides:** Route to the application specific resource location: you might direct DNS queries to the application's dedicated resource location based on its host name.

Perform the following steps to configure DNS routing:

1. Navigate to **Settings > DNS > DNS Resolution**.
2. Click **Add**.



3. Select one of the following options:
   - **First Available resource location**
   - **Resource location where application resides**
4. Click **Save**.

Secure Private Access supports a robust DNS routing fallback mechanism to ensure service continuity. If an application-specific resource location cannot be identified for a given DNS query, the request automatically falls back to a designated fallback route.

> **Note:**
>
> Routing for unmapped or unpublished domains can only be configured if you have set the primary routing choice as **Resource location where application resides**.

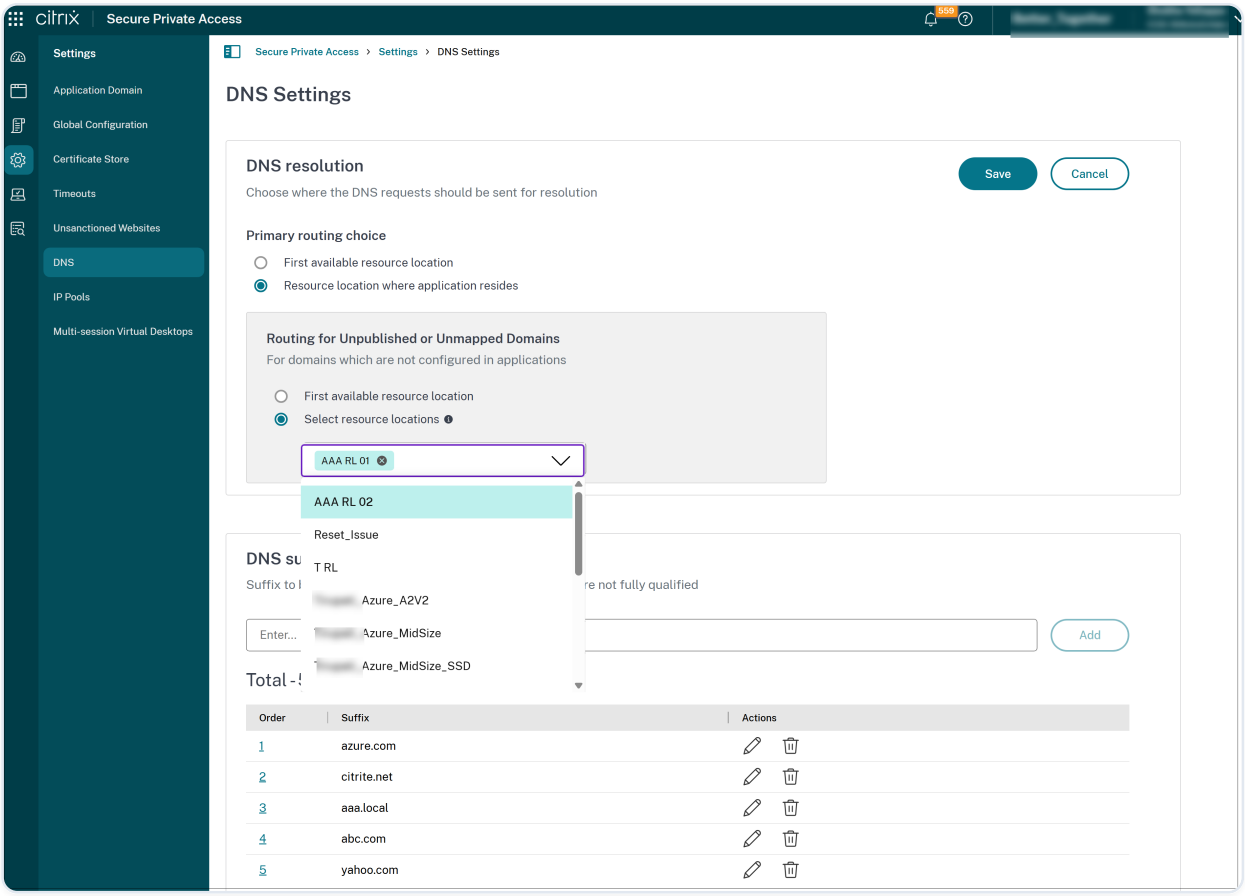
> You can configure the fallback mechanism to one of the following options:

- **First available resource location:** The nearest geographical resource location.
- **Select resource locations:** One of the locations from a list of configured resource locations defined by the administrator.

Configure fallback routing for DNS queries:

1. Navigate to **Settings > DNS > DNS Resolution**.

2. Click **Add**.



3. In **Primary routing choice**, select **Resource location where application resides**.
4. In **Routing for Unpublished or Unmapped Domains**, select one of the following options:

   - **First available resource location**
   - **Select resource locations**

   If you select the option **Select resource locations**, then select the desired resource locations from the list. You can select more than one resource locations.

5. Click **Save**.

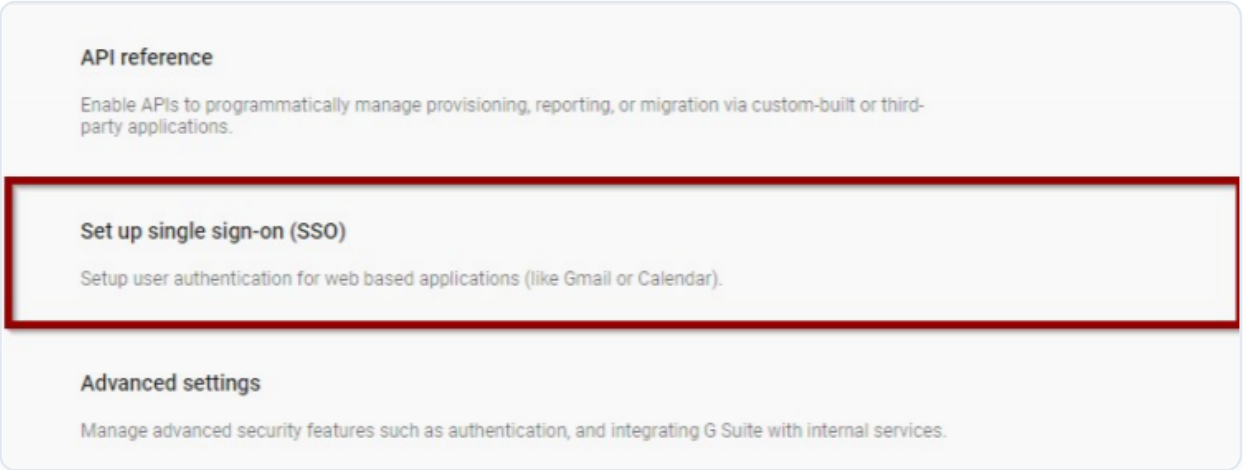
Configure G Suite

To configure G Suite for single sign-on through SAML, perform the following:

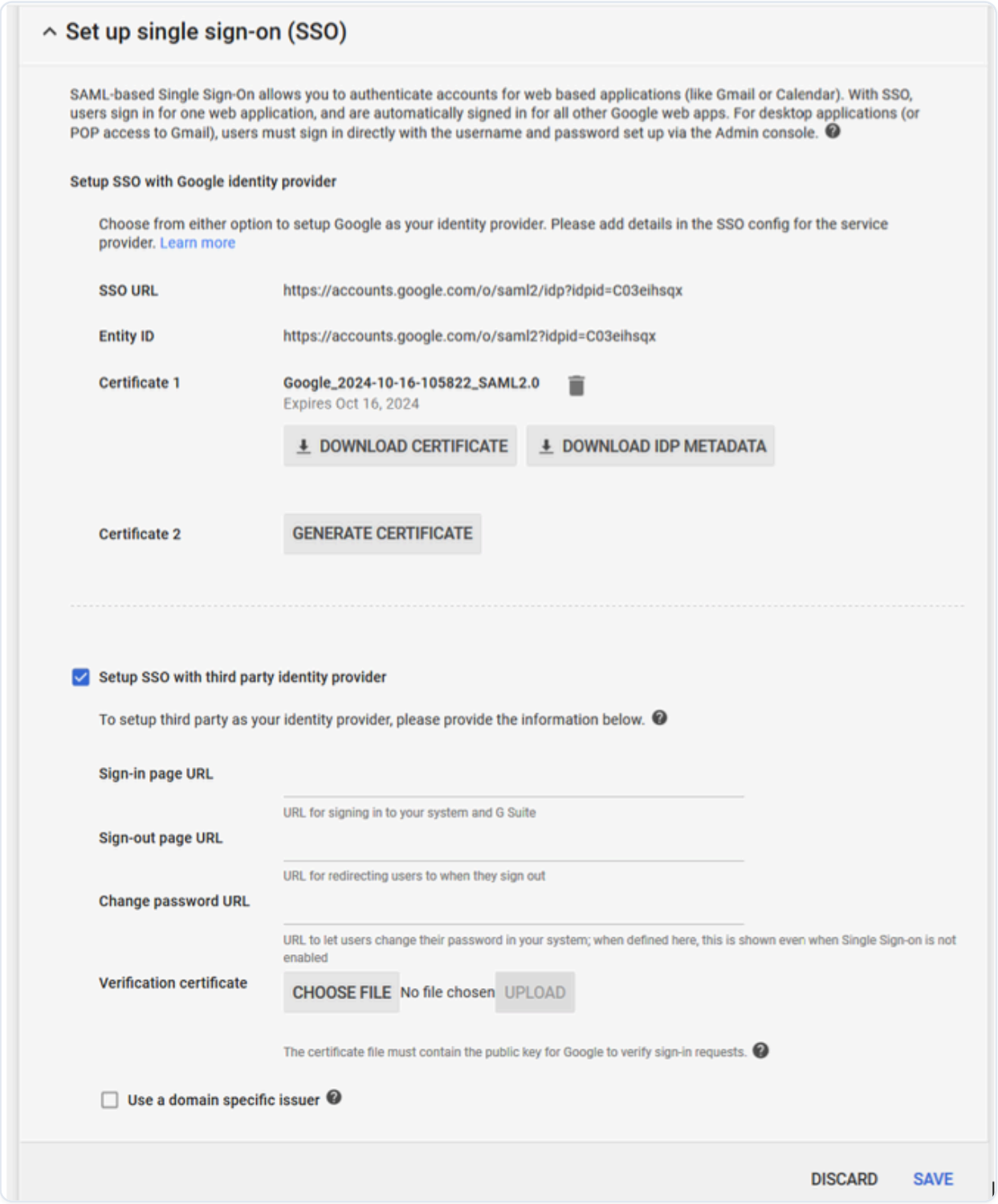
1. Log on to G Suite as an admin user.



2. Click **Security**.



3. In the **Security** page, click **Set up single sign-on (SSO)**.



4. In the **Set up single sign-on (SSO)** page, select **Setup SSO with third party identity provider** and enter the details.

   - **Sign-in page URL** - You can copy the SAML SSO login URL from the Citrix Cloud wizard (**Citrix Gateway Service > Add a Web/SaaSApp > Single sign on > Login URL**).
   - **Verification certificate** - You can download the certificate from the Citrix Cloud wizard (**Citrix Gateway Service > Add a Web/SaaS App > Single sign on > Certificate**).
   - **Use a domain specific issuer** - Select the check box.

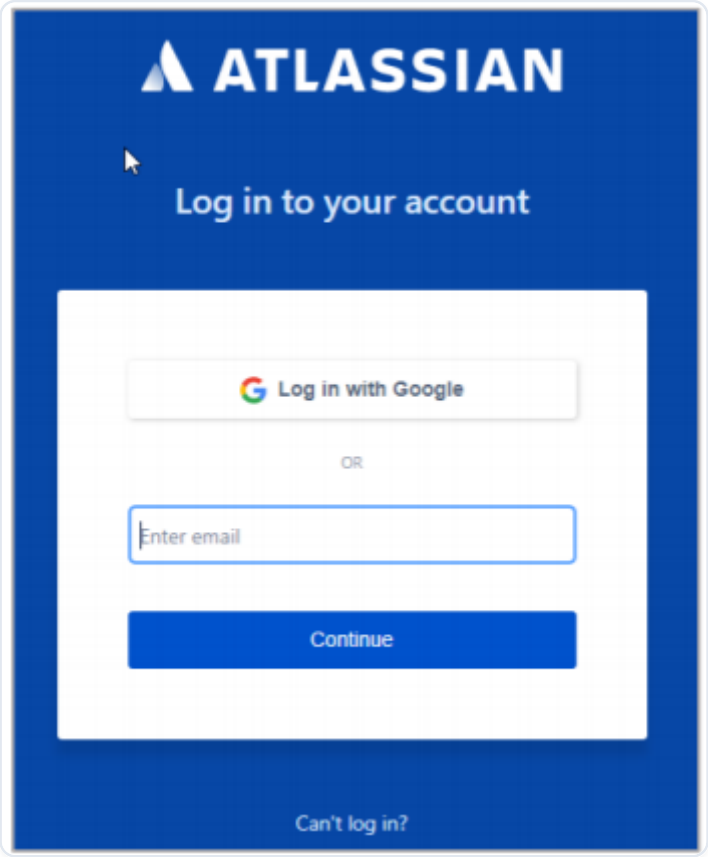
Configure Jira

The following sections provide more information about configuring Jira.

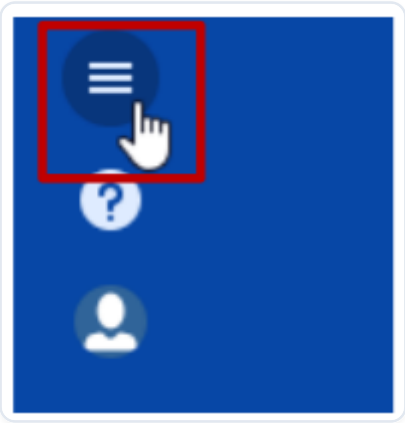
Citrix Gateway SaaS Application

Configuring Jira for SSO enables administrators to manage their users using NetScaler. Users can securely log on to Jira using their enterprise credentials. To configure Jira for SSO through SAML, perform the following:

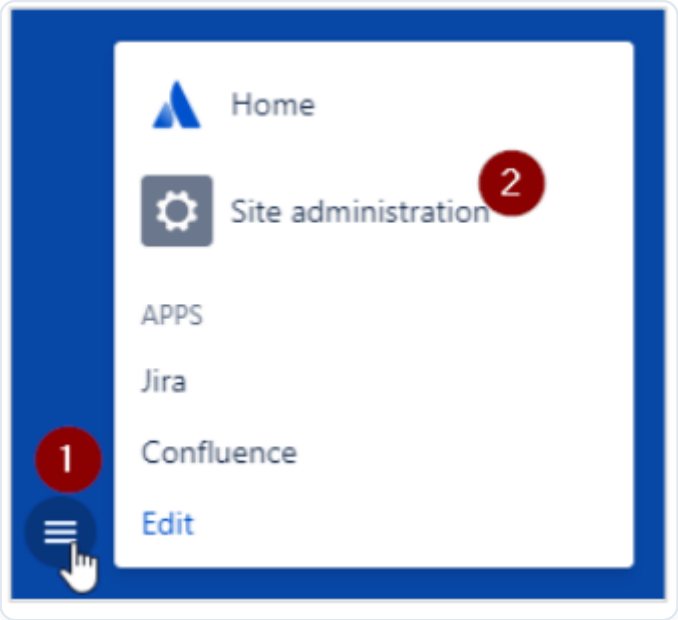
1. In a browser, type your organization's Atlassian cloud URL and press ENTER.
2. Log on to your Atlassian account.



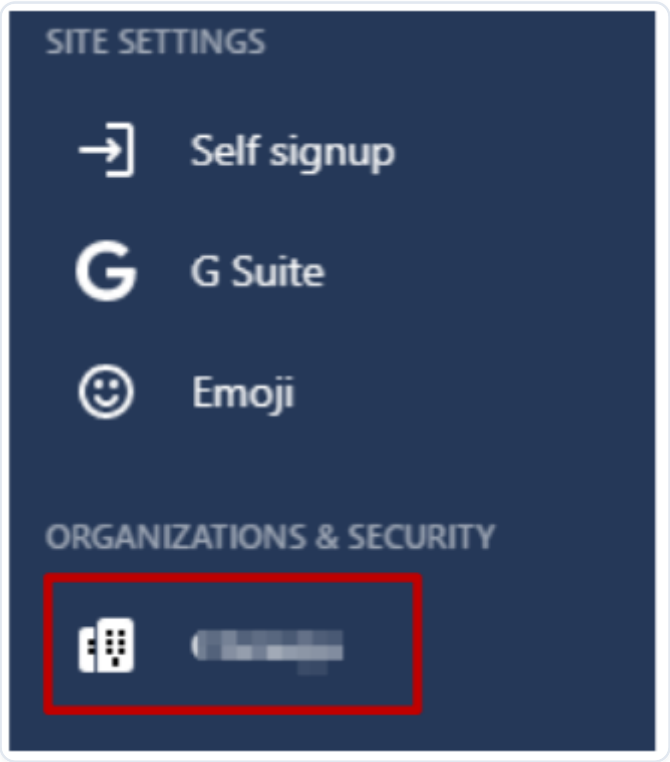
3. On the Home page, at the lower-left corner, click the ellipses icon.



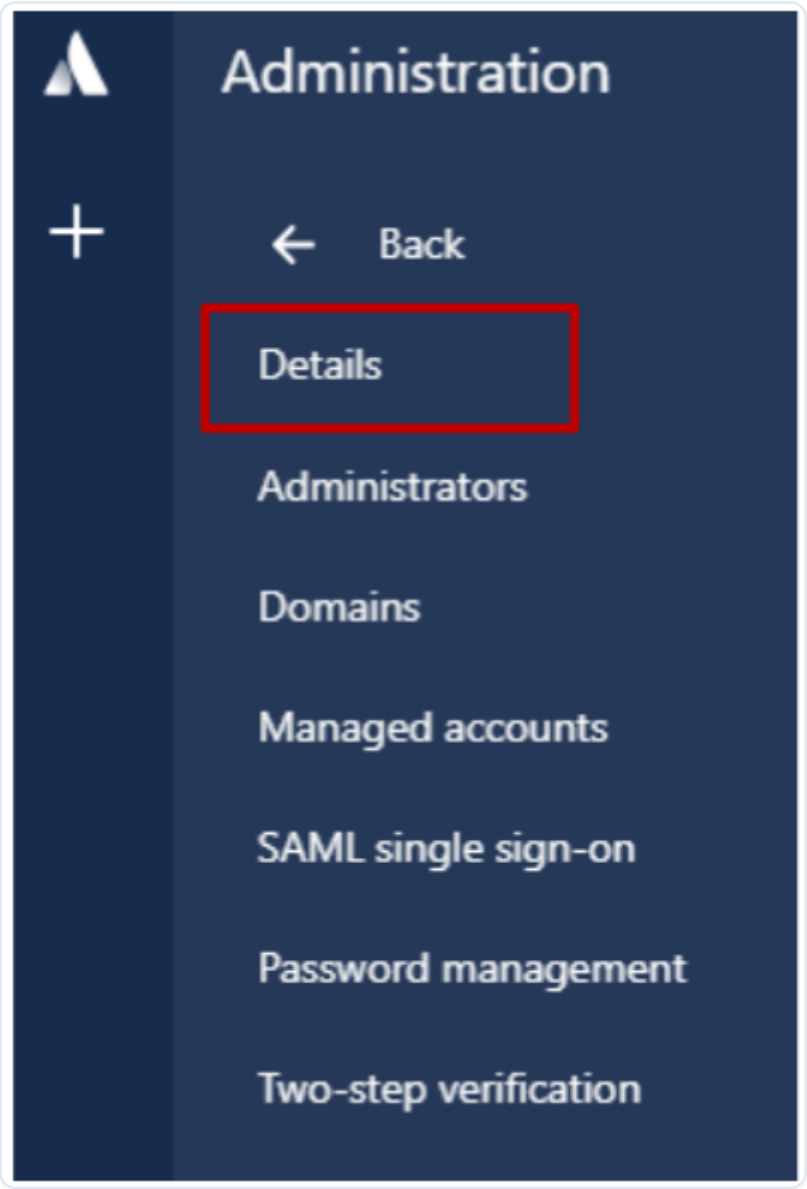
4. Click **Site administration**.



5. On the Administration page, in the ORGANIZATION & SECURITY section, click the organization name for which you want to configure SAML authentication.

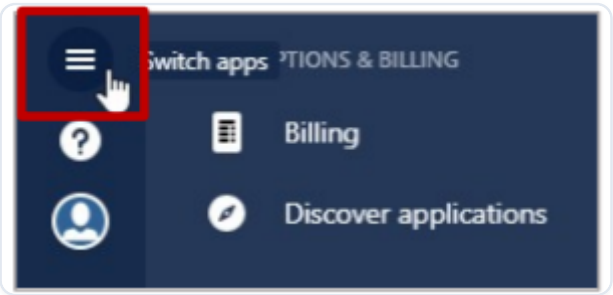


6. Click **Details** and verify the domain.

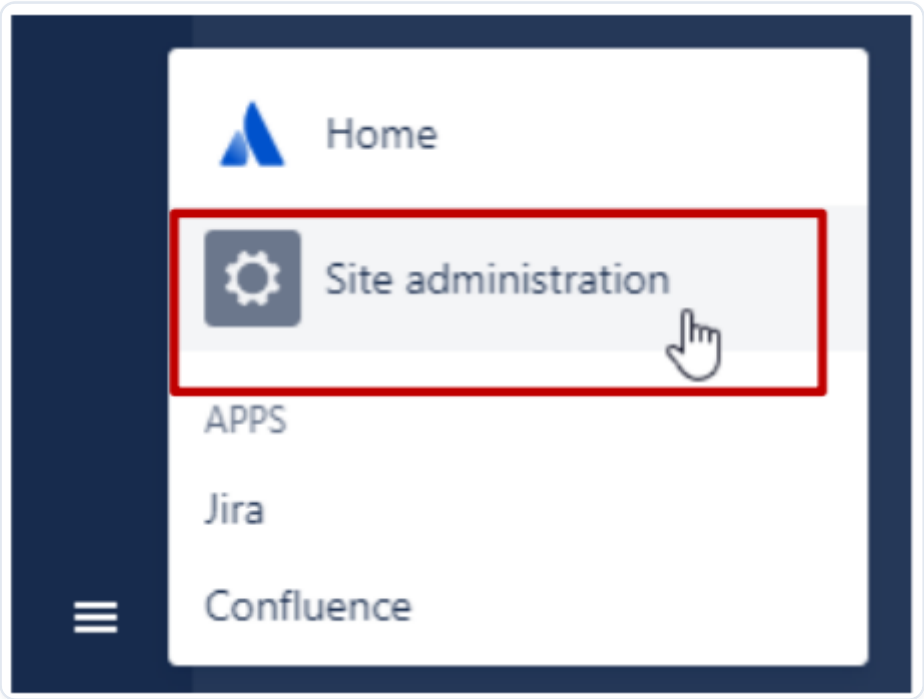


To verify the domain, perform the following:

a. Click the **Switch apps** icon in the lower-left corner.



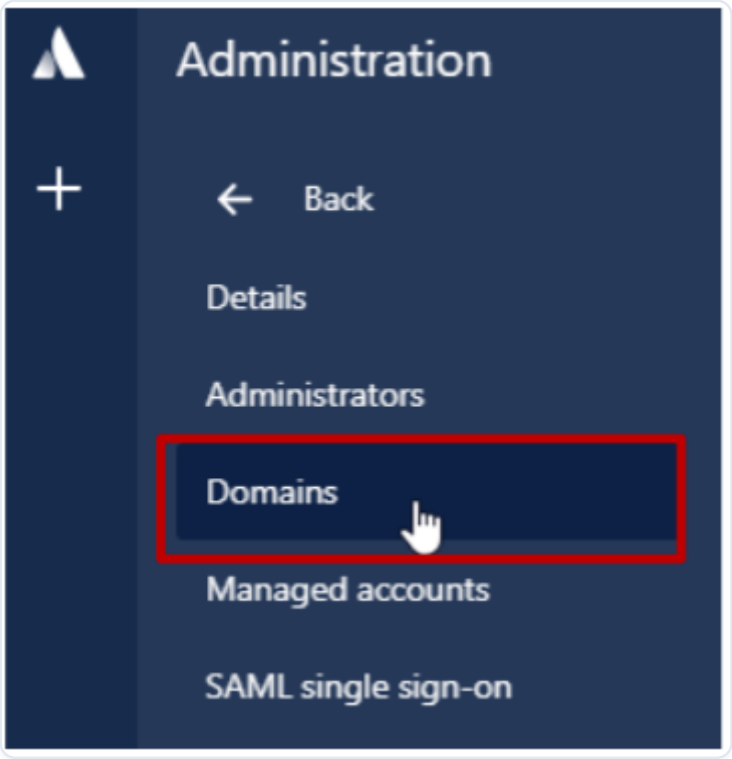
a. Click **Site administration**.



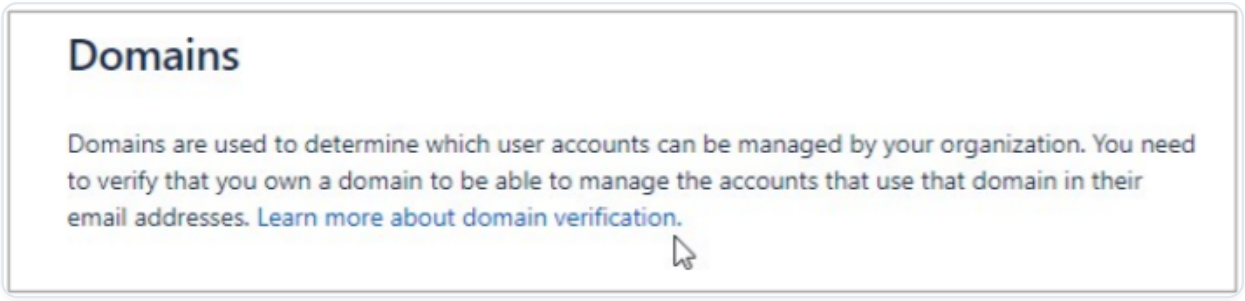
a. Click the organization name.



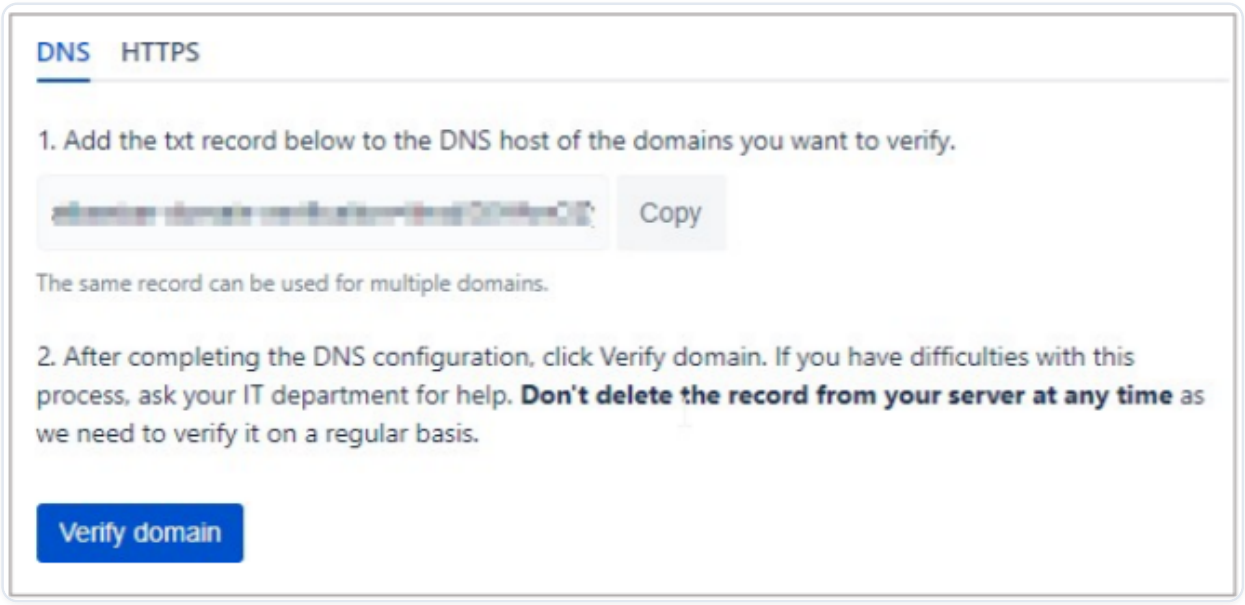
a. Click **Domains**.



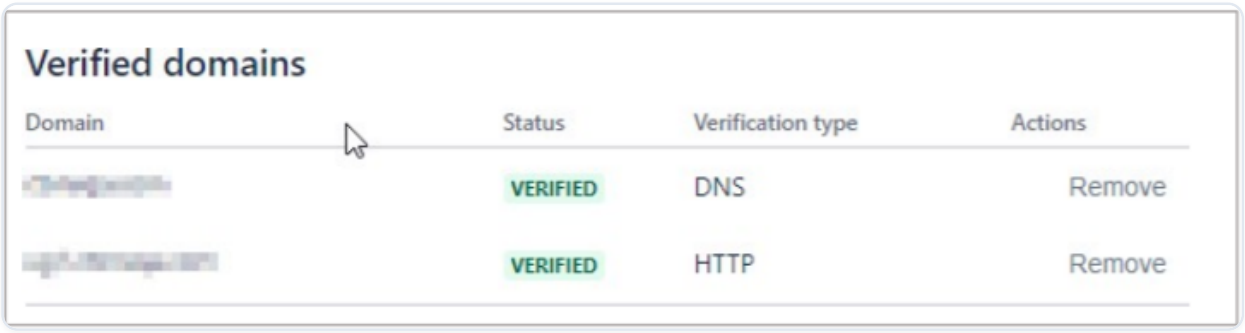
a. You can verify a domain using DNS or HTTPS. For more information about the steps to verify a domain, in the right pane under Domains section, click the Learn more about domain verification link.



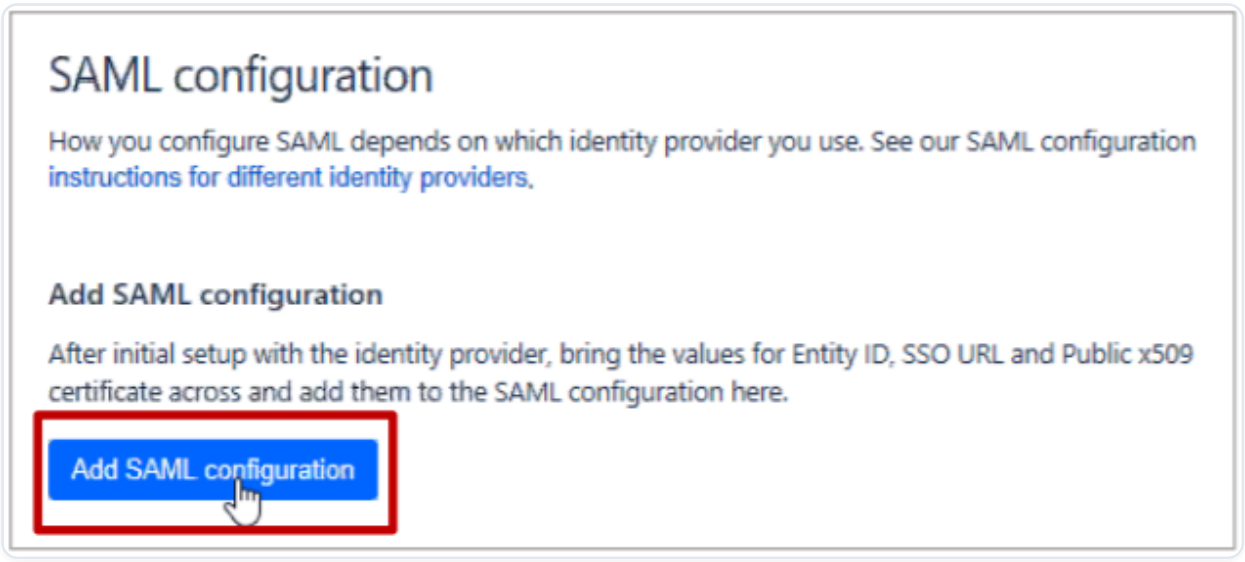
a. After completing the steps, click **Verify Domain**.



a. The Status column in the Verified Domains section displays **VERIFIED**.



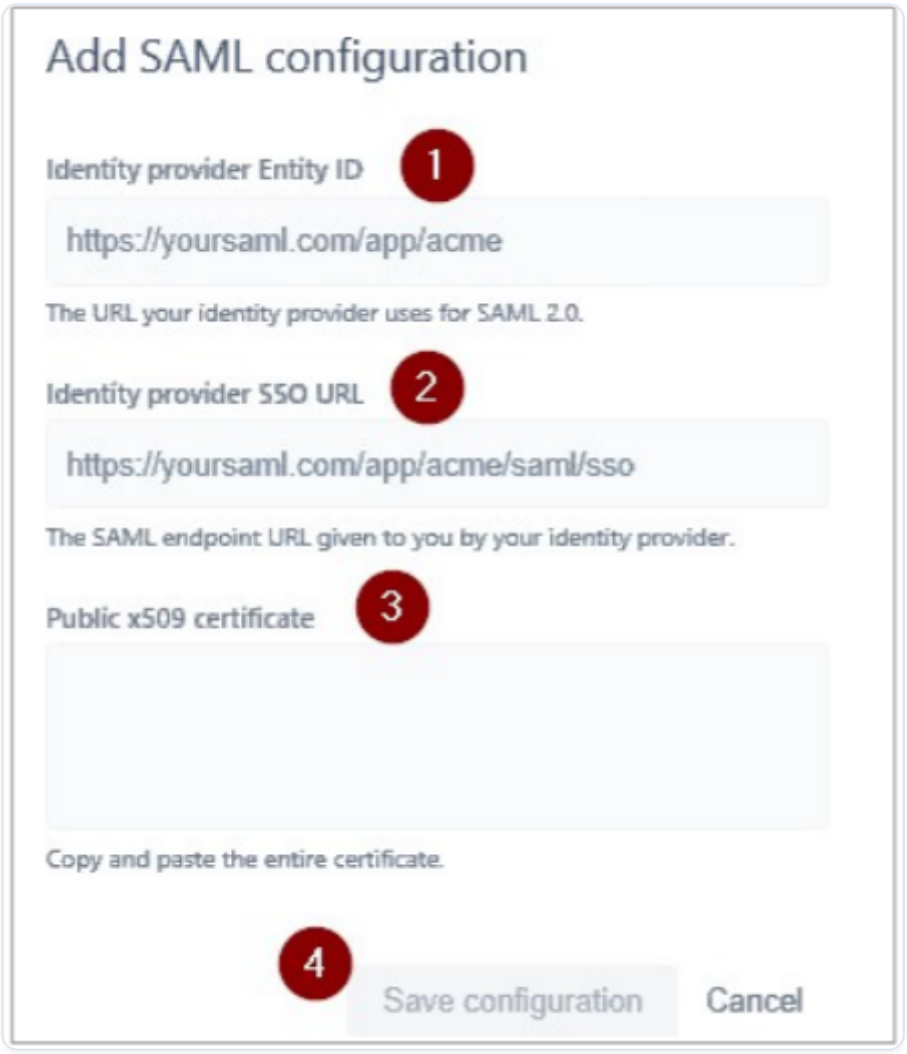
7. Click **SAML single sign-on**.
8. In the right pane, under SAML Configuration, click **Add SAML Configuration**.



9. In the **Add SAML configuration** area, specify the following information:

   - Identity Provider Entity ID - type a unique issuer ID. For example: `yourcompany_NS_Jira`
   - Identity Provider SSO URL - enter the IdP URL.

     Note: You can copy the URL from the Citrix Cloud wizard (**Citrix Gateway Service > Add a Web/SaaS App > Single sign on > Login URL**).



- Public x509 Certificate – copy and paste the SAML IdP signing certificate.

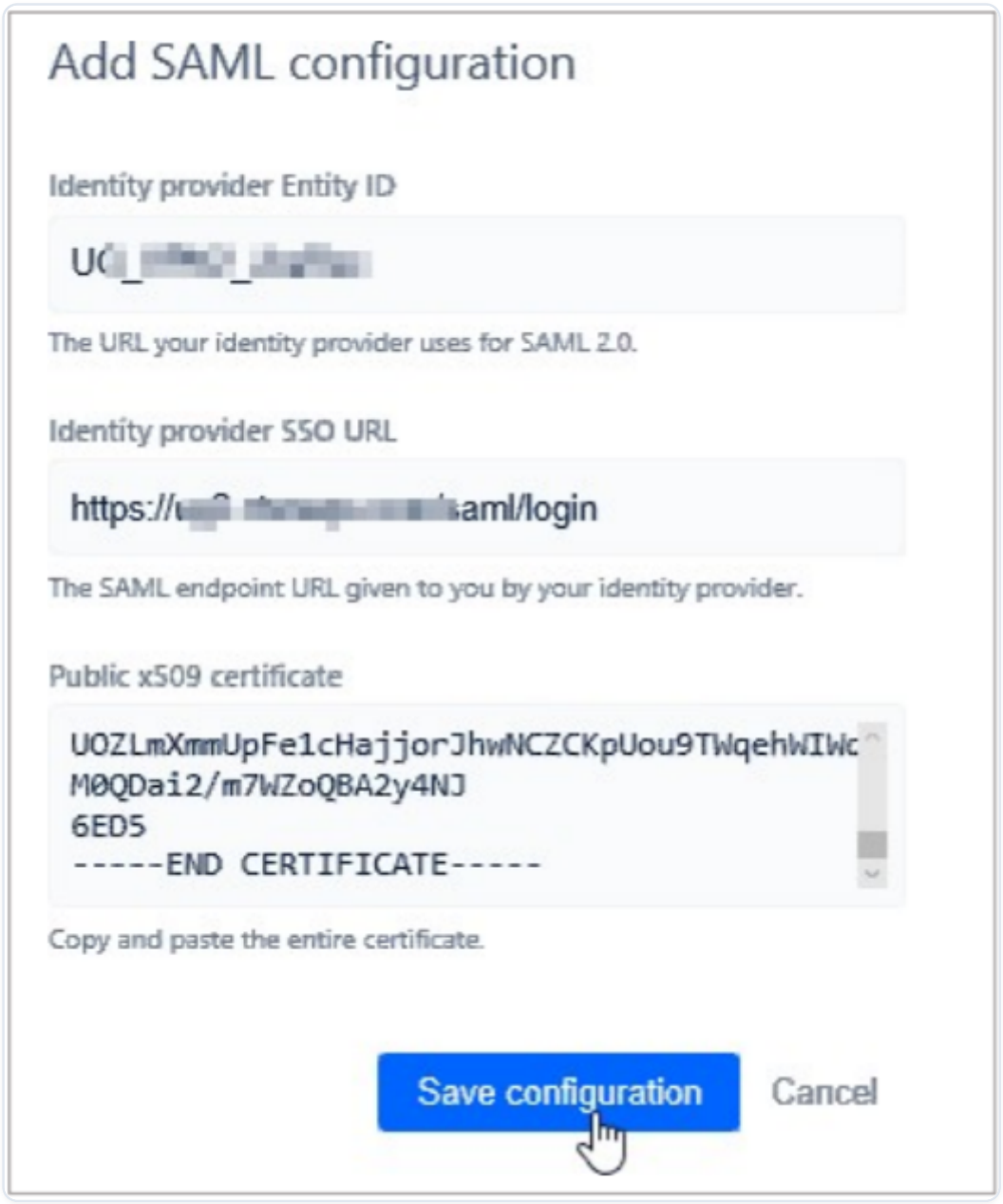
  a. Download the certificate from the Citrix Cloud wizard (**Citrix Gateway Service > Add a Web/SaaS App > Single sign on > Certificate**).



b. Copy the text between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----

c. Paste the text in a text editor and save the file in an appropriate format such as `your company name`.pem.

10. Click **Save Configuration**.



Configure O365

The following sections provide more information about configuring O365.

Prerequisites

To configure O365 apps in the Citrix Workspace app, make sure to complete the following:

- **If you have a primary domain available in Microsoft Entra ID that is not federated with other services**, you can use that domain to federate to Citrix Secure Private Access. Ensure that this domain, either the parent or the child domain of it is not already federated and the parent domain of it is not already added in the Microsoft Entra ID.

For example, if your user login using `user1@demo.citrix.com`, then demo.citrix.com is primary domain, citrix.com is parent domain, and us.demo.citrix.com is child domain.

- **If you cannot federate the primary domain**, add a new domain to Microsoft Entra ID and federate it to Citrix Secure Private Access. Create the domain and complete the verification. For details, see `<https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-custom-domain>`.

  OR

  You can add a subdomain to Microsoft Entra ID that can be leveraged to federate to Citrix Secure Private Access for SSO. For that, you must add and promote the subdomain to a root domain. For details, see `<https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/domains-verify-custom-subdomain>`.

  Note: You might need to use Microsoft Entra ID Graph Explorer instead of Microsoft Graph Explorer for the POST request to change a subdomain to a root domain.

  For details on why you need a federated domain, see How domain federation works.

- **Confirm that the new domain or the subdomain that you have added is in the "Verified" state in the Microsoft Entra ID.**
- **Set up a trust between your SAML identity provider and Microsoft Entra ID**. To set up a trust, you must have a domain that is verified in Microsoft Entra ID. When a federation is configured in Microsoft Entra ID using a domain, Microsoft Entra ID trusts the SAML provider for user authentication to Microsoft Entra ID, even if the user is from a different domain than the federated domain. In the SP initiated flow when Microsoft Entra ID must identify which IdP to use for authentication(accelerate user to federated IdP) it is identified using the `whr query param` or `domain_hint` passed to the URL `<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-authentication-for-federated-users-portal>`.

  Adding a federation for a new domain does not impact an existing federation that you have in your setup. If you have ADFS already federated to a domain, it is not impacted as you are federating on a different domain that is neither sub domain or parent domain of an already federated domain.

  SSO can have the following two flows:

  IDP initiated flow: Typically used when you want to log in to the Microsoft Entra ID portal. The Citrix Secure Private Access service posts the SAML assertion to Microsoft Entra ID. Microsoft

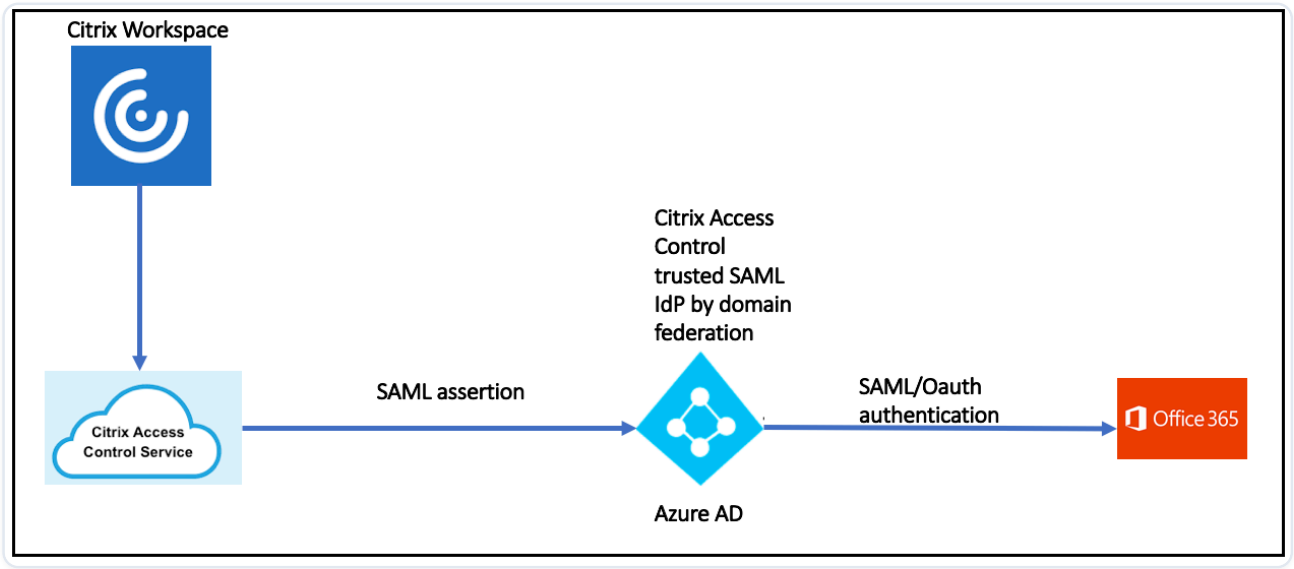
Entra ID validates it based on the federation setting that we did earlier. If the validation passes, it extracts the `nameid` attribute of SAML. The `nameid` attribute must match `immutableId` of the user which is present in the Microsoft Entra ID.

SP initiated flow: Typically used when you want to land to the app directly instead of the Microsoft Entra ID portal. In this flow, the Citrix Secure Private Access service loads the URL that is configured in the app settings. The URL goes to Microsoft Entra ID and because the URL has some indication of the federated domain, the user is redirected to the Citrix Secure Private Access service with a SAML request and a relay state. The Citrix Secure Private Access service posts the SAML assertion to Microsoft Entra ID with the same relay state that came in the request. Once SAML is validated, Microsoft Entra ID redirects a user to the context in the relay state and hence the user lands on the app directly.

- **Configure the O365 app in the Citrix Secure Private Access service**. For details see Support for Software as a Service apps.

How domain federation works

The following figure illustrates a typical flow involved after a domain federation is complete.



Consider that you want to add the Office 365 app into the Citrix Workspace and enable watermarking and restrict downloads. The typical flow is as follows:

1. You launch the Office 365 app in the Citrix Workspace.
2. The request goes to the Citrix Secure Private Access service.
3. Citrix Secure Private Access service creates the SAML assertion and forwards it to Microsoft Entra ID.

4. As the request is coming from a trusted SAML IdP, Microsoft Entra ID identifies it through the domain federation that is created and passes the SAML assertion to the Office 365 app.

   The Office 365 app is launched.

Authentication methods supported for the Office 365 app

By default, Citrix Cloud™ uses the Citrix identity provider to manage the identity information for all users in your Citrix Cloud account.

Citrix Workspace supports the following authentication methods for Office 365. Okta and Google IdP are not currently supported.

- On-premises Active Directory
- Active Directory plus Token
- Microsoft Entra ID

  Note: If Microsoft Entra ID is used to authenticate to the workspace, then you cannot federate the primary domain (user's login domain) because this creates a loop. In such cases, you must federate a new domain
- Citrix Secure Private Access
- Active Directory plus RADIUS

For more details, see Identity and access management.

Configure the O365 app in the Secure Private Access service

The following are the high-level steps to configure the O365 app in the Secure Private Access service. For more details, see Support for Software as a Service app.

1. Go to the Secure Private Access service in Citrix Cloud.
2. Search for Office 365 and choose the **Office365** template. For details on configuring an app using the template, see Support for Software as a Service apps.

   > **Note:**
   >
   > Once you select the **Office365** template, the following related domains are autopopulated in the **App Details** section.

- *.office.com
- *.office365.com
- *.sharepoint.com
- *.live.com
- *.onenote.com
- *.microsoft.com
- *.powerbi.com
- *.dynamics.com
- *.microsoftstream.com
- *.powerapps.com
- *.yammer.com
- *.windowsazure.com
- *.msauth.net
- *.msauthimages.net
- *.msocdn.com
- *.microsoftonline.com
- *.windows.net
- *.microsoftonline-p.com
- *.akamaihd.net
- *.sharepointonline.com
- *.officescriptsservice.com
- *.live.net
- *.office.net
- *.msftauth.net

3. Enable enhanced security controls, if needed.
4. Configure SSO.

   Note: The only change you must do is to make sure “Name ID” is the Active Directory GUID.
5. Ensure that advanced attributes also send `IDPEmail`.

- Attribute Name: `IDPEmail`
- Attribute Format: Unspecified
- Attribute Value: Email

6. Click SAML metadata to open in a new tab.
   - Copy “entityID”
   - Copy “Login URL”
   - Download the Certificate in CRT format

Configure domain federation from Microsoft Entra ID to Citrix Workspace

Prerequisites:

- Enable PowerShell in Microsoft Entra ID
- Install Microsoft MSOnline module

The following are the PowerShell commands to install the required modules.

```
`PS> Install-Module AzureAD -Force`


`PS> Import-Module AzureAD -Force`


`PS> Install-Module MSOnline -Force`


`PS> Import-module MSOnline -Force`
```

If the modules are already installed, then run the following command.

```
PS> connect-msolservice
```

Note: A Microsoft cloud account is required to connect to `msolservice`. For example, `admin.user@onmicrosoft.com`.

Steps to configure domain federation from Microsoft Entra ID to Citrix Workspace

1. **Run the following commands in the PowerShell to configure the federation:**

   - `PS> $dom = "ad-domain.com"`

   Note: ad-domain.com is the new domain added to Microsoft Entra ID

   - `PS> $IssuerUri = "https://citrix.com/[customerID]"`

   Note: The customerID can be found from the following locations:

   - **Citrix Cloud > Identity and Access Management > API Access**
   - **Citrix Cloud > Citrix Secure Private Access.** the customer ID can be found in the app configuration details (**Single sign > SAML Metadata file > entityID**).
   - `PS> $fedBrandName = “CitrixWorkspace”`
   - `PS> $logoffuri = "https://app.netscalergateway.net/cgi/logout"`
   - `PS> $uri = "https://app.netscalergateway.net/ngs/[customerID]/saml/login?APPID=[AppID]”`

   Note: $uri can be copied from **Citrix Secure Private Access Service > Add a Web/SaaSApp > Single sign on > Login URL** or from **SAML Metadata > Location.**

   - `PS> $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2(“<location of certificate downloaded from Citrix Secure Private Access service/filename.crt>”)`

     For example: `PS> $cert = New-Object System.Security.Cryptography.X509Certificates.X509Certificate2("c:\cert\saml_idp.crt")`

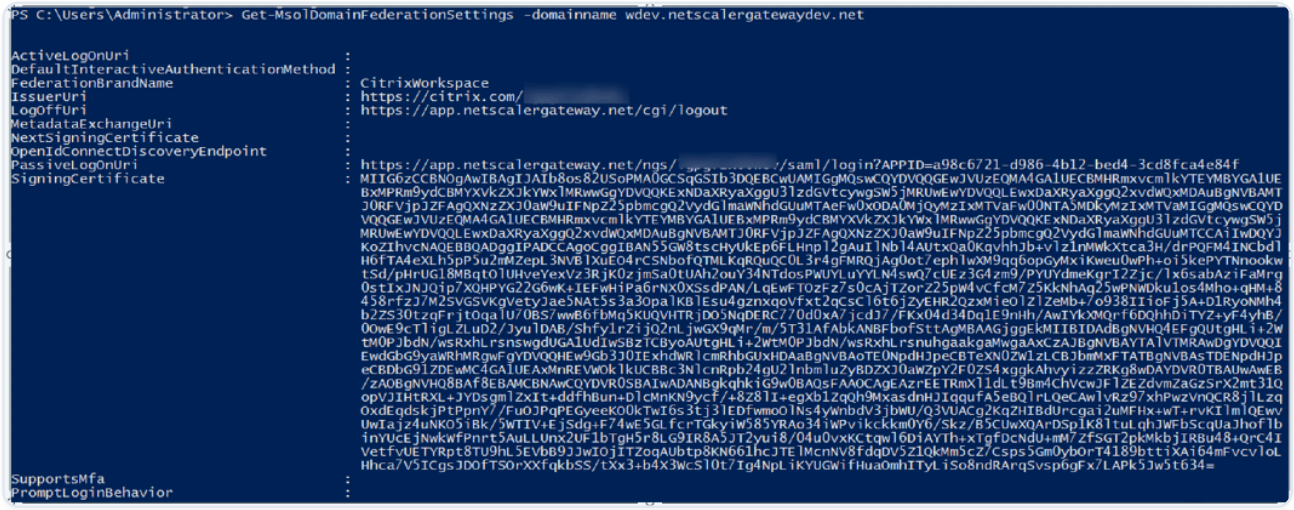
   `PS> $certData = [system.convert]::tobase64string($cert.rawdata)`

2. **Run the PS string to complete the Federation to Citrix Secure Private Access:**

   `PS> Set-MsolDomainAuthentication -DomainName $dom –federationBrandName $fedBrandName -Authentication Federated -PassiveLogOnUri $uri -LogOffUri $logoffuri -SigningCertificate $certData -IssuerUri $IssuerUri -PreferredAuthenticationProtocol SAMLP`

3. **Verify domain federation settings by running the following command:**

```
Get-MsolDomainFederationSettings -DomainName <domain name>
```



Automated domain federation from Microsoft Entra ID to Citrix Workspace

In the manual domain federation from Microsoft Entra ID to Citrix Workspace, users have to switch between cloud portal and PowerShell to copy data and run the scripts. For example;

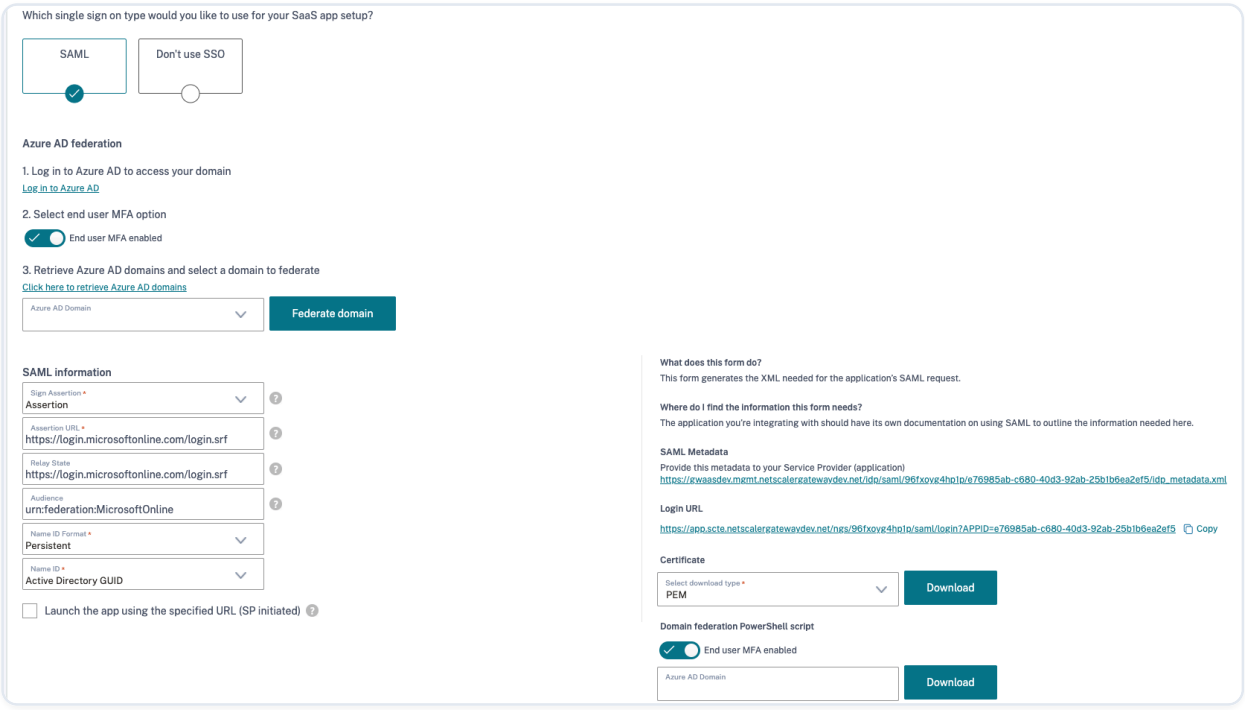
- Copy data, such as customer ID and app ID from the cloud portal.
- Download the certificate from the cloud portal.
- Run the PowerShell scripts.

This manual copy-paste action might introduce errors because of which the federation might not be successful.

The steps to federate a domain are now integrated within the Citrix Secure Private service user interface making the federation process automated. The PowerShell scripts are run in the back end when users click the appropriate links in the interface. Users do not have to switch between cloud portal and PowerShell.

Steps to federate a domain automatically

1. Configure the O365 app. For details, see Configure the O365 app in the Secure Private Access service.
2. In Single sign on, select **SAML**.



3. Log on to Microsoft Entra ID using your credentials. When you click **Log in to Entra ID**, you are directed to the Microsoft Entra ID logon portal for authentication.
    - OAuth protocol is used for authentication. After the authentication is successful, you must provide consent for federating the domain.
    - **Select end user MFA option** is enabled, by default.
4. Click **Click here to retrieve Entra ID Domains** to view the list of all domains.
5. Select the domain that you want to federate and click **Federate domain**.

> **Note:**
>
> - When you click **Federate domain**, the PowerShell scripts are run in the back end and the domain is federated.
> - You can also download the PowerShell scripts, if necessary, from the interface. In **Domain federation PowerShell script**, click **Download**.

Suppress multifactor authentication (MFA)

An option is added to the advanced attributes of O365 apps that suppresses MFA when the user has already entered the MFA during user authentication to Citrix Workspace.

- **Attribute Name:** "`http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod`",
- **Attribute Value:** "`http://schemas.microsoft.com/claims/multipleauthn`"

For the Microsoft Entra ID to accept this claim, federate using the following PowerShell command:

```
Set-MsolDomainAuthentication -DomainName $dom –federationBrandName $fedBrandName
-Authentication Federated -PassiveLogOnUri $uri -LogOffUri $logoffuri
-SigningCertificate $certData -IssuerUri $IssuerUri
-PreferredAuthenticationProtocol SAMLP -SupportsMfa $true
```

> **Note:**
>
> IdP initiated flow does not honor relay state. Use SP initiated flow to land on the app directly.

Configuring individual Office suite applications in Citrix Workspace

Perform the following to configure individual office suite applications:

1. Complete the domain federation as detailed in previous sections.
2. Choose the O365 template.
3. Change the name of the app to, for example, MS Word.
4. Change the app URL to accordingly.

Word: `https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2Fwww.office.com%2Flaunch%2FWord%3domain>`

Powerpoint: `<https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2Fwww.office.com%2Flaunch%2Fpowerpdomain>`

Excel: `https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2Fwww.office.com%2Flaunch%2FExcel%domain>`

CRM/Dynamics Online: `https://<tenant>.crm.dynamics.com/?whr=<federated domain>`

OneDrive for Business: `https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2F<tenant>-my.sharepoint.com%2F&whr=<federated domain>`

Outlook Calendar: `https://outlook.office.com/owa/?realm=<federated domain>&path=/calendar/view/Month`

Outlook Web Access to Exchange Online: `https://outlook.com/owa/<federated domain>`

SharePoint Online: `https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1%2E6206%2E0&wreply=https%3A%2F%2F<tenant>.sharepoint.com%2F&whr=<domain>`

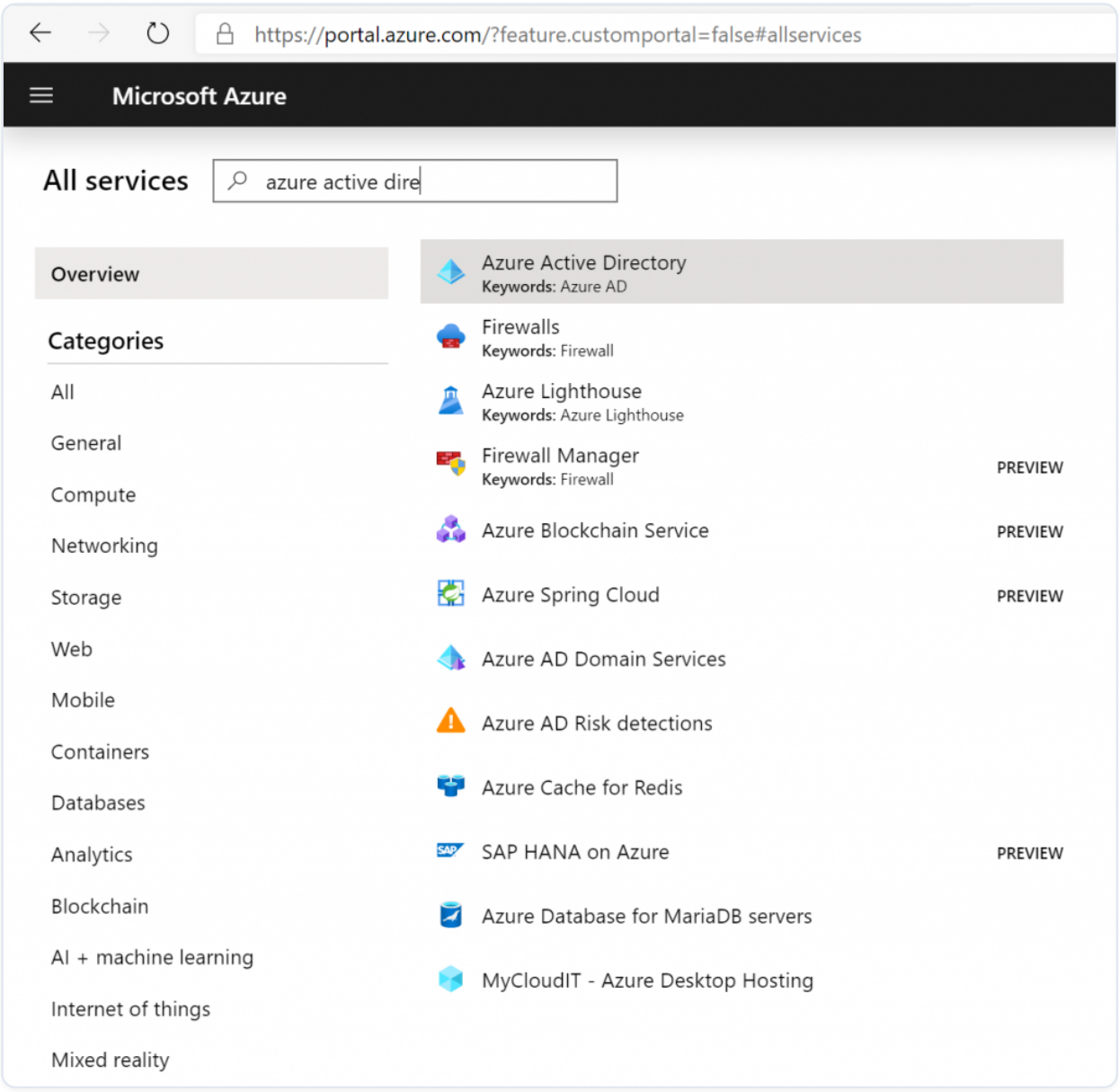
Teams: `https://login.microsoftonline.com/common/oauth2/authorize?client_id=cc15fd57-2c6c-4117-a88c-83b1d56b4bbe&response_mode=form_post&response_type=code+id_token&scope=openid+profile&domain>`

Third party apps integrated into Microsoft Entra ID

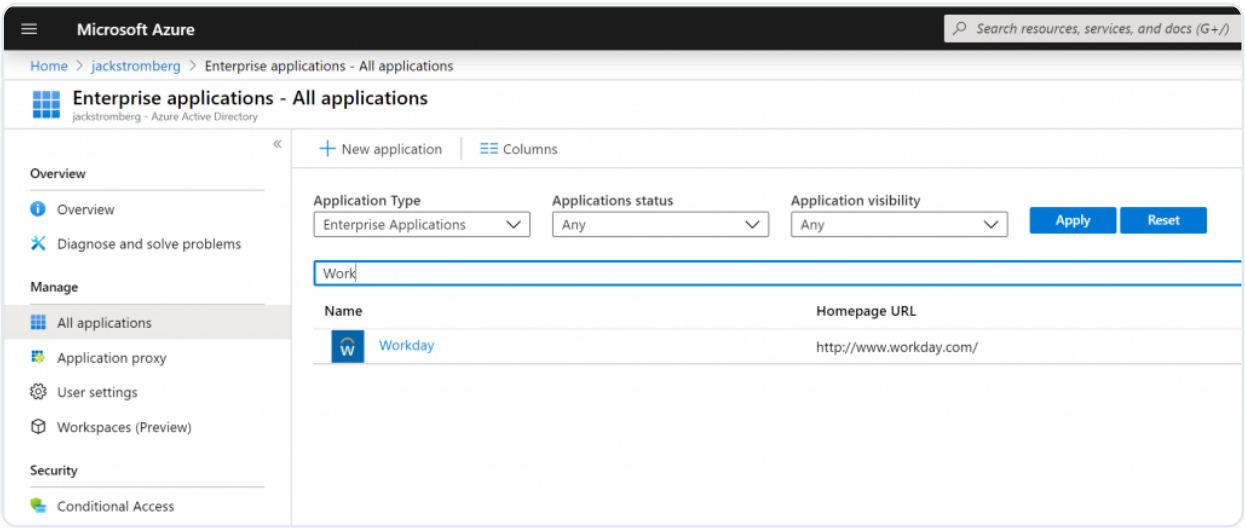
If you have integrated third party applications like Box, Salesforce, ServiceNow, Workday, you can obtain the Smart Links for these apps from the Microsoft Entra ID.

Perform the following steps.

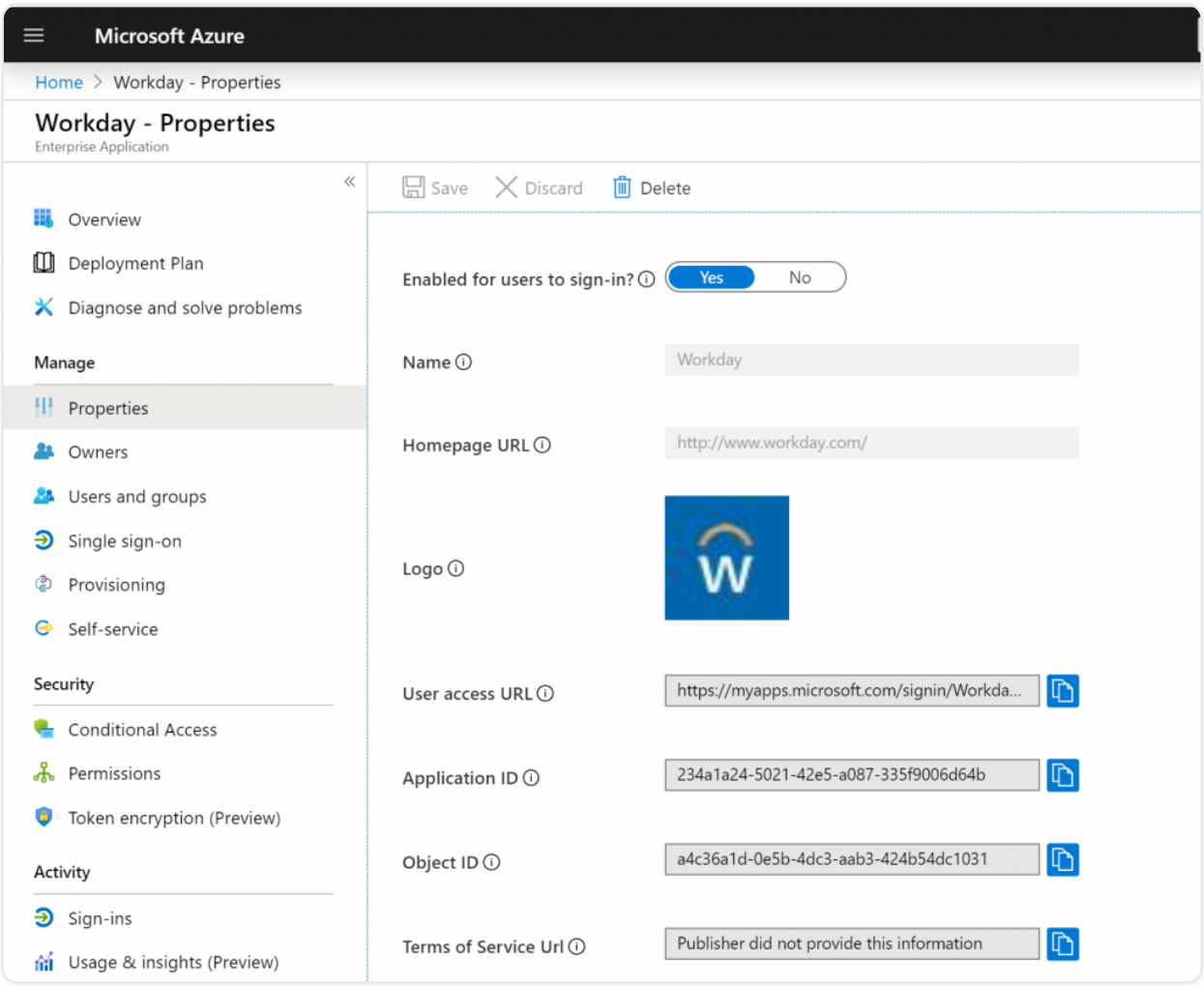
1. Log in to your Microsoft Entra ID Portal `<https://portal.azure.com>`.
2. Select **All Services > Azure Active Directory**, and select your directory.



3. Select **Enterprise Applications** and then choose the application you want to generate a Smart Link to.



4. Select **Properties** and copy the User access URL.



5. After you append `whr` to the URL, the `whr` parameters appear as shown in the example URL.

   Example URL: `https://myapps.microsoft.com/signin/Workday/12345678912345678912345678896d64b&whr=ctxnsqa.net`

   Note: Append `whr` to the URL so that Microsoft Entra ID knows which IdP to use to authenticate a user based on federation setting and auto redirect to that IdP.

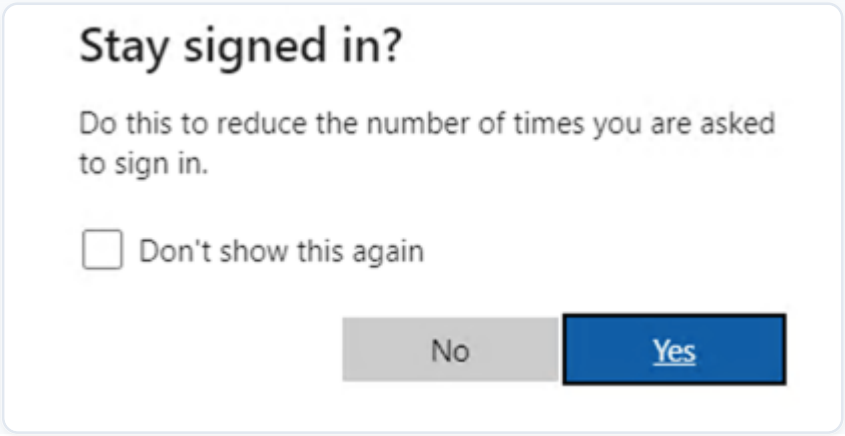
6. Set enhanced security controls.
7. Configure SSO.

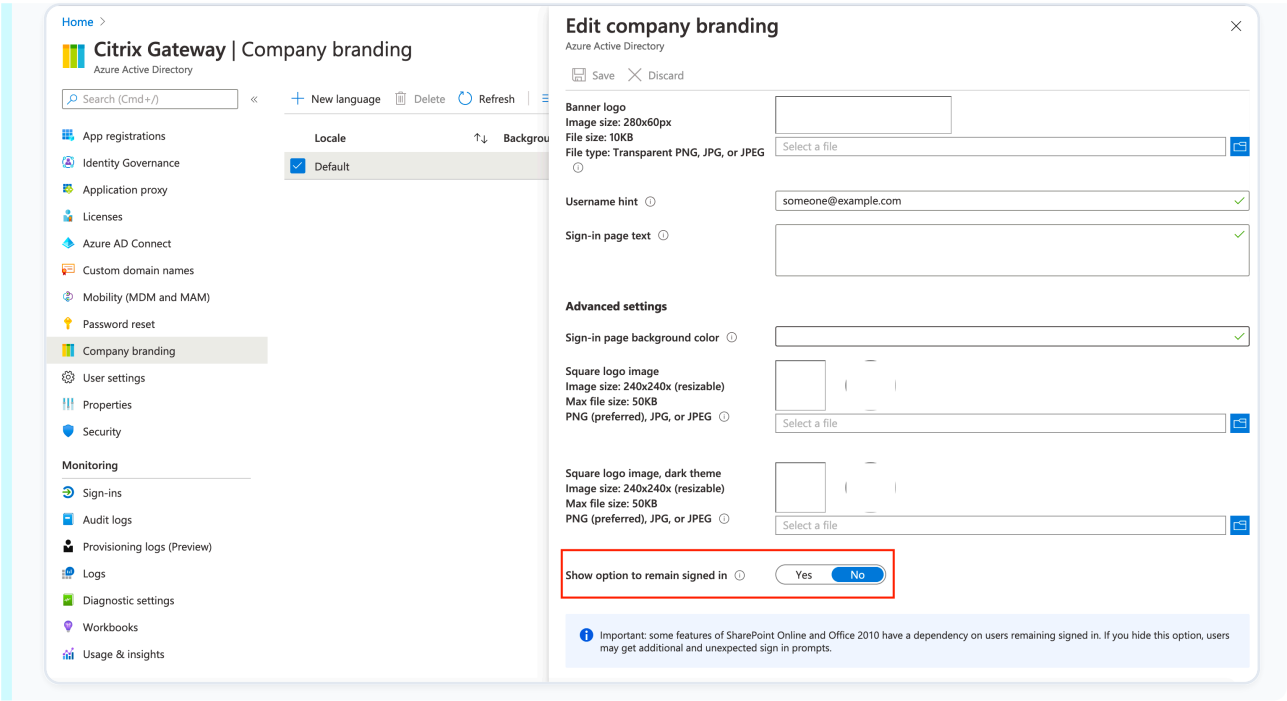
   - Name ID = AD GUID
   - Enable SP-initiated checkbox
   - Assertion URL = Login URL

     When you perform an IdP initiated flow, users are redirected to the Microsoft Entra ID portal page. If you want to land directly on the app page, then SP initiated flow is needed as it sends the correct relay state in the SAML assertion.

Note:

- When federation of the primary domain is enabled, all Microsoft Entra ID users are redirected to Citrix Workspace when authenticating to any Office 365 applications. This might cause an outage/incident for customers if done without understanding the impact.
- If users log on to Citrix Workspace using Microsoft Entra ID, then the primary domain of the users that is used to log in must not be federated to the Citrix Gateway service. This results in a loop. In such cases, use another domain different from the domains of users login to Microsoft Entra ID to federate to the Citrix Secure Private Access service.
- If the primary domain is federated to the Citrix Secure Private Access service, then all user logins on that domain in Microsoft Entra ID are redirected to the Citrix Secure Private Access service. For POC, if needed, you can federate a test domain before federating the primary domain.
- If Microsoft Entra ID has the location policy turned on, users must be from the list of allowed IP addresses of a corporate network only. In such cases, you can publish the O365 app as a Web app and route its traffic via the Connector Appliance.
- When logging on to the Microsoft Entra ID, if you want to avoid the **Stay signed in?** prompt, you can change this setting by using the Microsoft Entra ID. Note the important message that appears when you change the setting and revert if necessary.





Reference Links

Azure PowerShell Module Reference

Deploy Office 365 Directory Synchronization in Microsoft Azure

Configure ERP Cloud

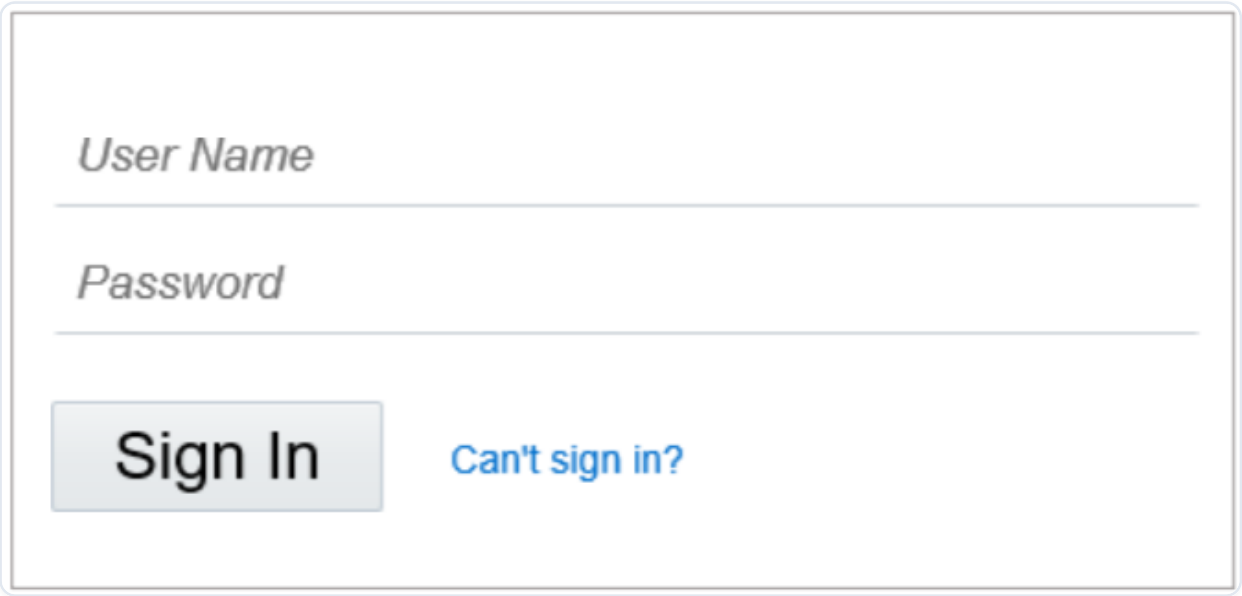
The following sections provide more information about configuring ERP Cloud.

Citrix Gateway SaaS Application

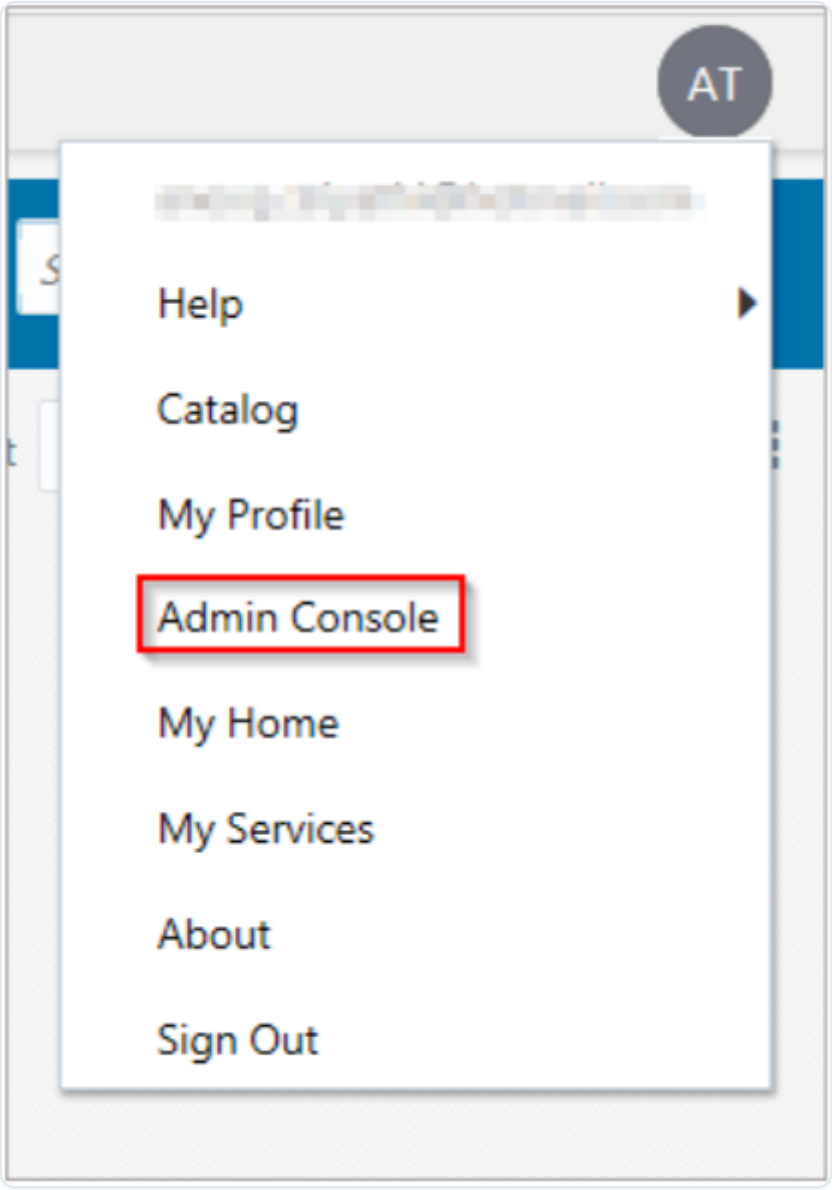
Users can securely log on to ERP Cloud using their enterprise credentials.

To configure ERP Cloud for SSO through SAML, perform the following:

1. In a browser, type: `https://<organizationid>.identity.oraclecloud.com/ui/v1/adminconsole/?root=security&security=external-idp` and press Enter.
2. Log on to your ERP Cloud account.

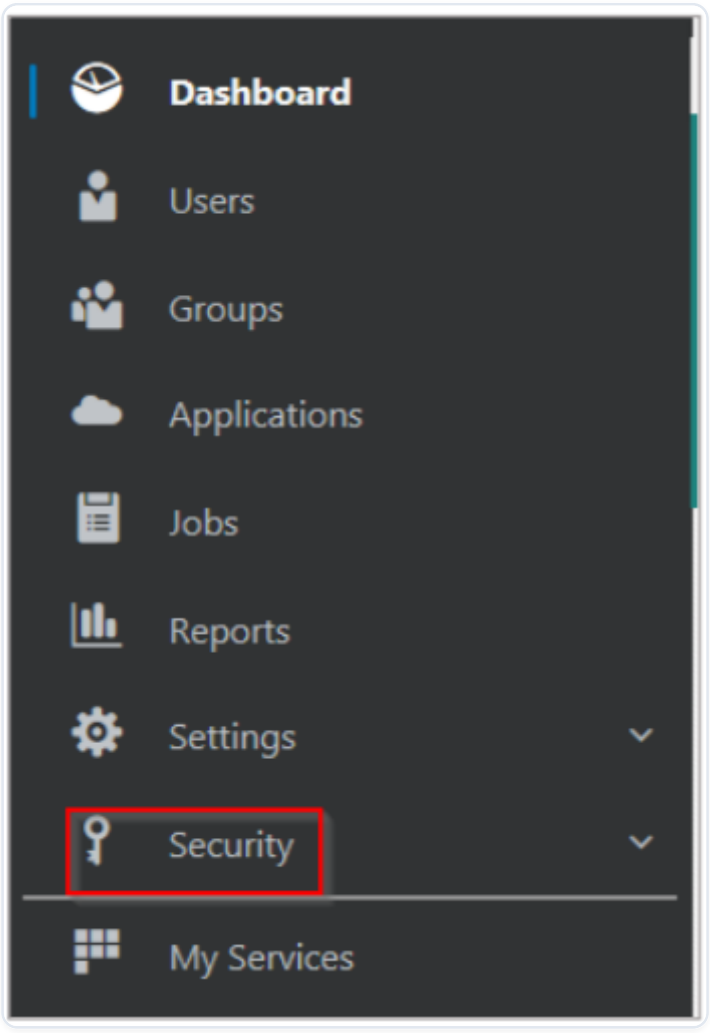


3. On the home page, in the upper right corner, click your profile initials and click Admin Console.

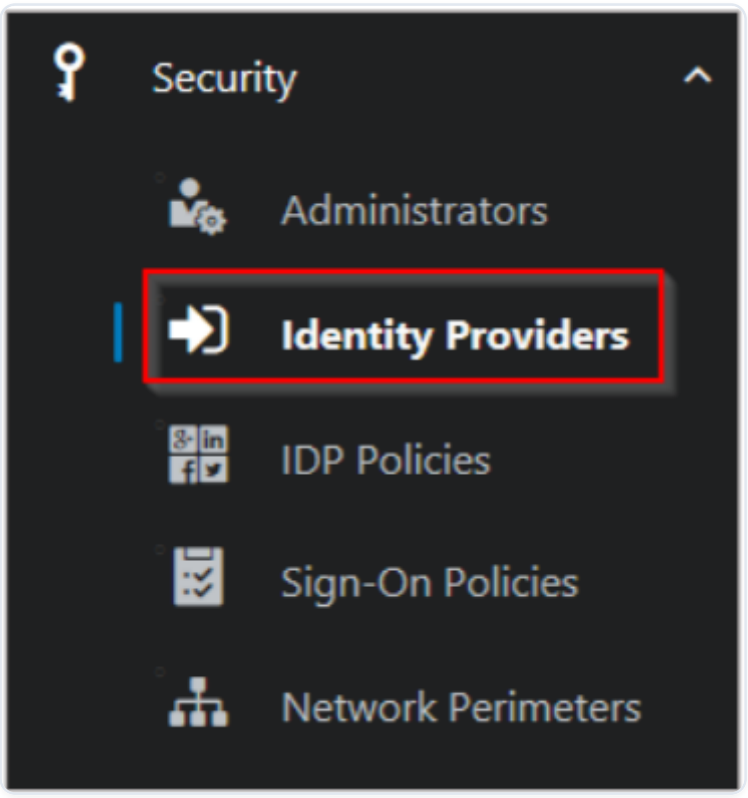


4. In the upper left corner, click the ellipses.

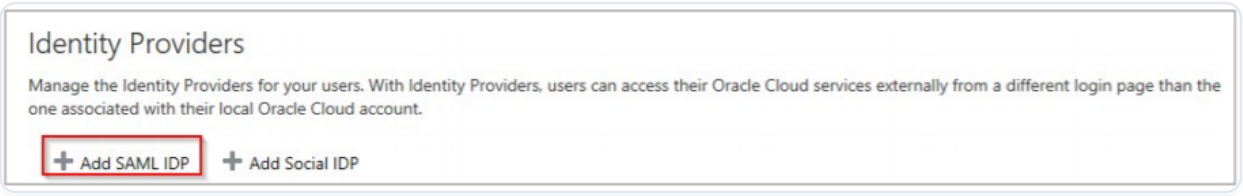
5. Click Security.



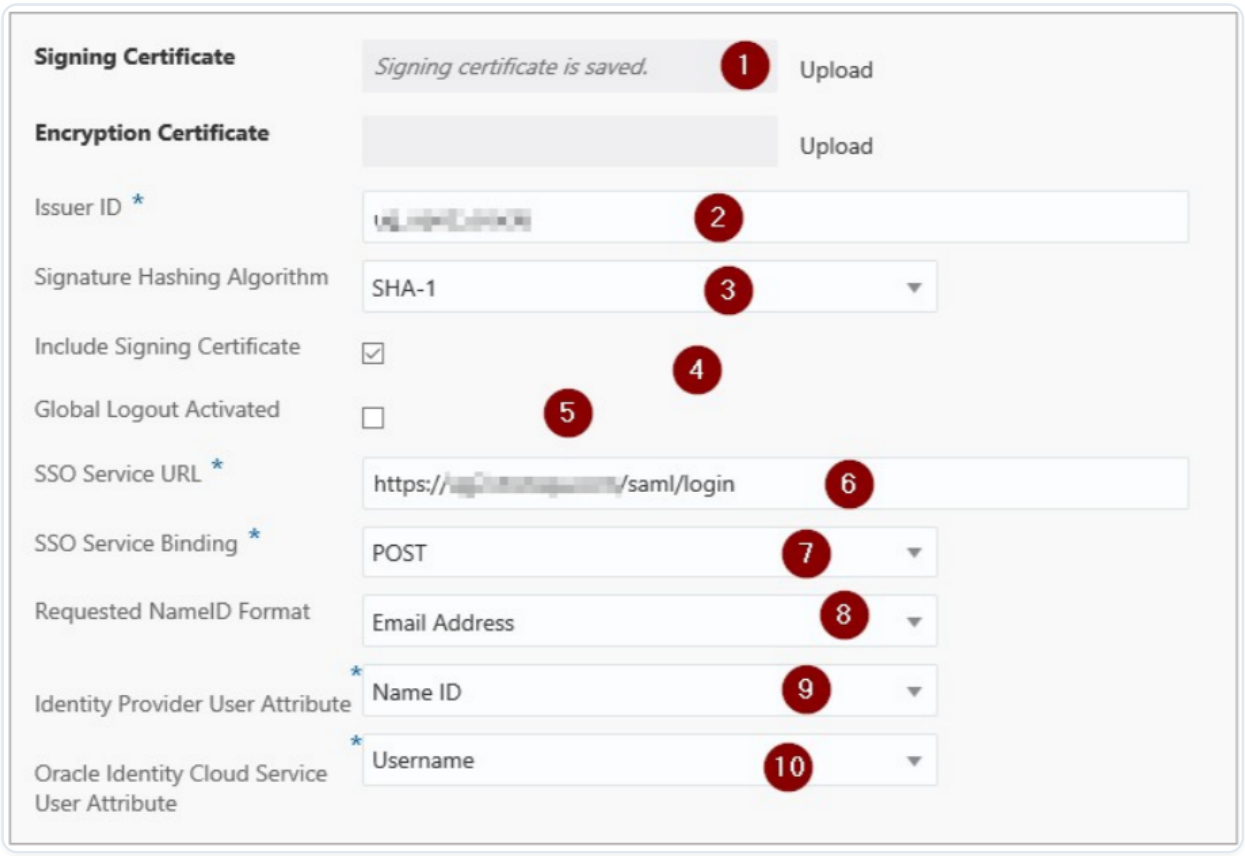
6. Click Identity Providers.



7. On the Identity Providers page, click Add SAML IdP.



8. On the Identity Providers page, specify the following information:



a. Signing Certificate– paste the PEM certificate.

To obtain your IdP certificate, perform the following:

- Remotely access your NetScaler® instance using PuTTY.
- Navigate to /nsconfig/ssl folder (using shell command `cd` /nsconfig/ssl) and press Enter.
- Type cat `<certificate-name>` and press Enter.
- Copy the text from -----BEGIN CERTIFICATE----- to -----ENDCERTIFICATE-----
- Paste the text in a text editor and save the file in an appropriate format such as `your organization name`.pem



b. Issuer ID – type a unique name.

c. Signature Hashing Algorithm – select hashing algorithm used to sign SAML messages.

d. Include Signing Certificate - select the check box if you want to include signing certificate to verify the signature of the messages for the IdP.

e. Global Logout Activated - select the check box if you want to activate SAML global logouts.

f. SSO Service URL – enter the IdP URL followed by /saml/ login. For example: `https://<netscalerinstance>.com/saml/ login`

g. SSO Service Binding– click the appropriate option to send an authentication request.

h. Requested NameID Format – click the appropriate format for mapping the user's attribute value in IdP to the corresponding attribute in Oracle Identity CloudService.

i. Identity Provider User Attribute – click the appropriate attribute value received from IdP to uniquely identify the user.

j. Oracle Identity Cloud Service User Attribute– click the appropriate attribute that you use to map the attribute received from IdP.

9. Click Save Changes.

Configure ServiceNow

Users can securely log on to ServiceNow using their enterprise credentials.

To configure ServiceNow for SSO through SAML, perform the following:

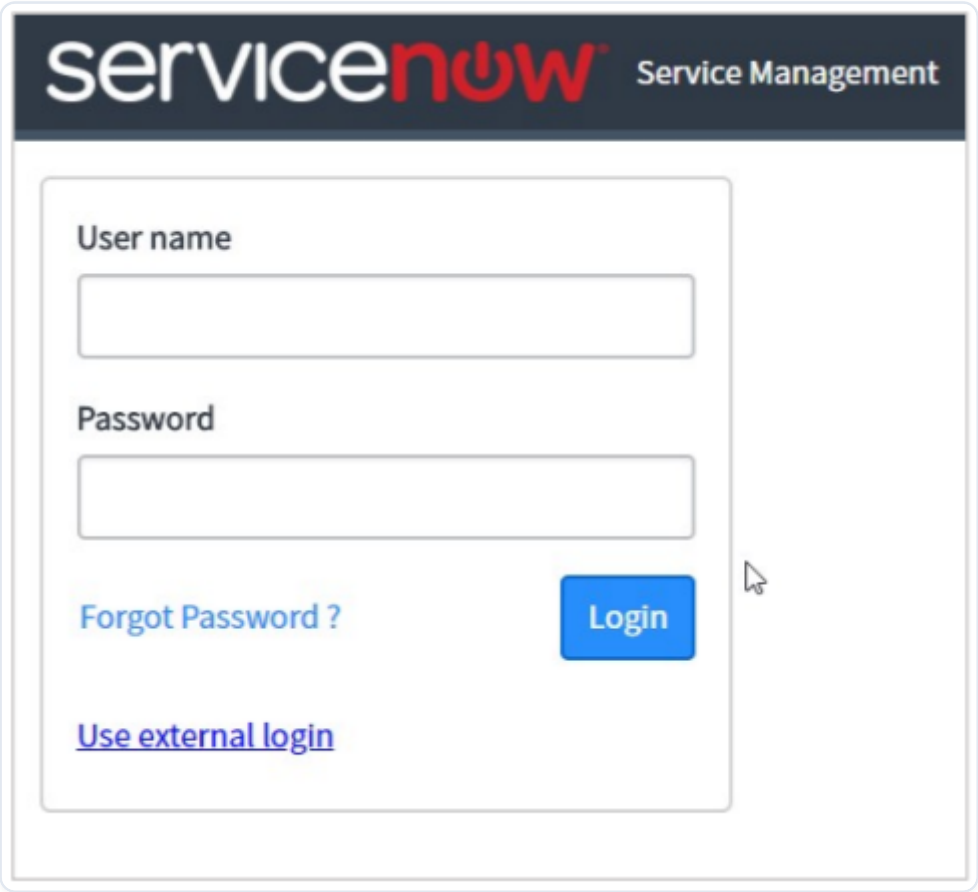
1. In a browser, type `https://<your-organization>.service-now.com/` and press **Enter**.

   For example, if the URL you use to access ServiceNow is `https://myserver.servicenow.com`, then you must replace `<your-organization>` with `myserver`.

   NOTE:

   - Ensure that the following details are provided in the Citrix Gateway service user interface when adding the ServiceNow app.
     - Assertion URL: `https://<your-organizaton>.service-now.com/navpage.do`
     - Relay State: `https://<your-organizaton>.service-now.com/`
     - Audience: `https://<your-organizaton>.service-now.com/`
     - Name ID Format: Select "Email Address"
     - Name ID: Select "User Principal Name (UPN)"
   - The Name ID format and Name ID attributes depend on the method of authentication chosen for ServiceNow.

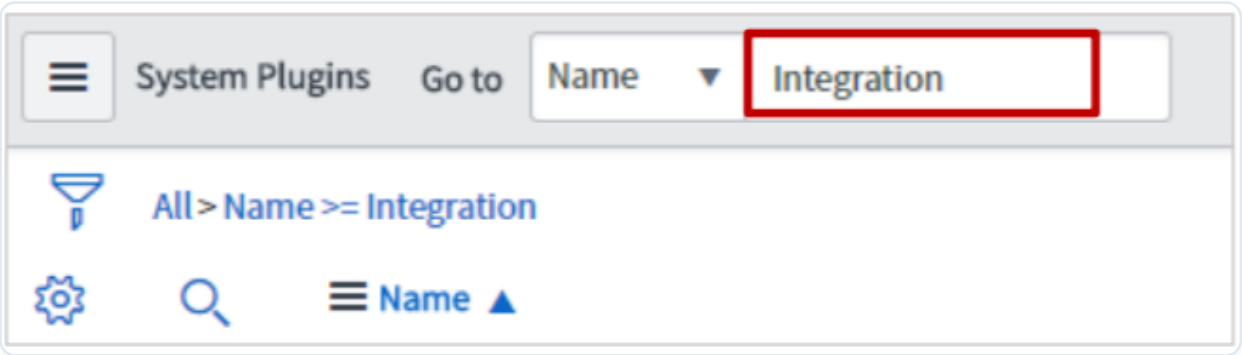
2. Log on to your ServiceNow account as an administrator.



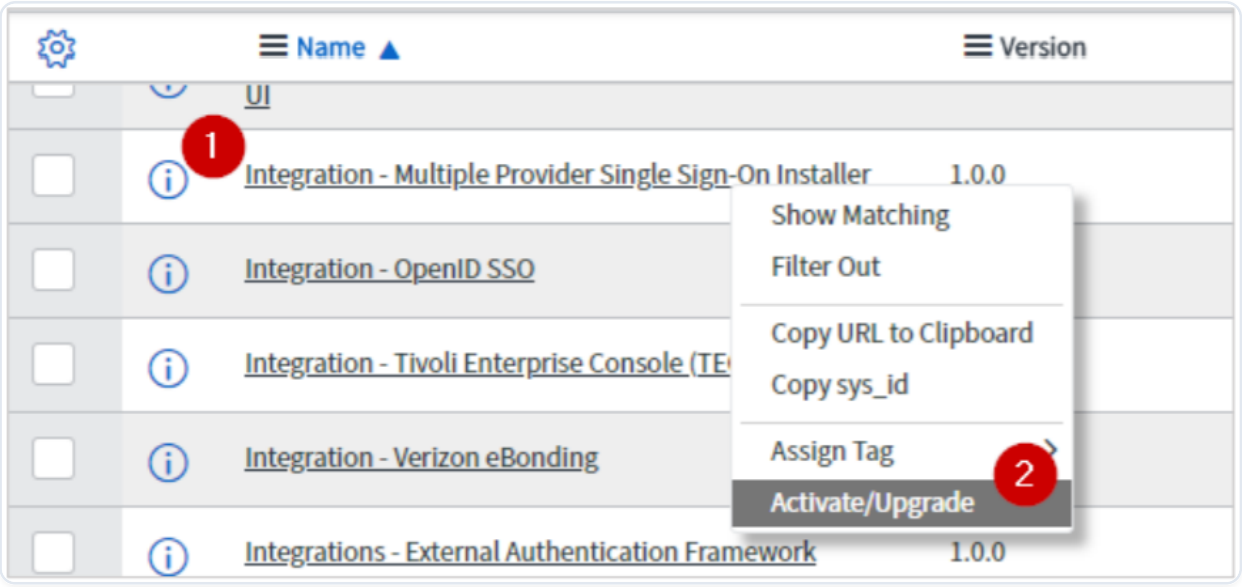
3. In the upper-left corner, using the Filter Navigator, search for plug-ins, and click **Plugins** in the search results.



4. In the right pane, in **System Plugins** section, search for integration.



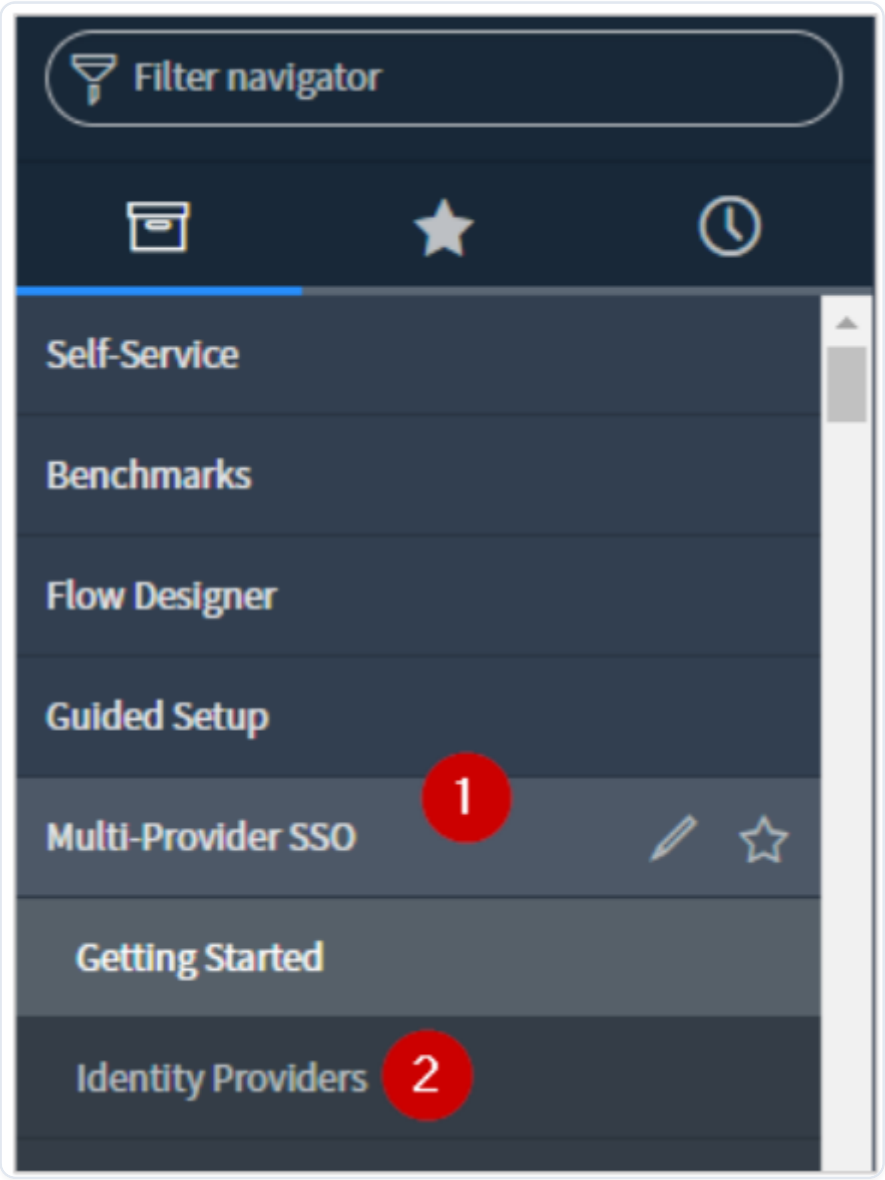
5. In the search results, right-click **Integration - Multiple Provider Single Sign-OnInstaller** and click **Activate/Upgrade**.



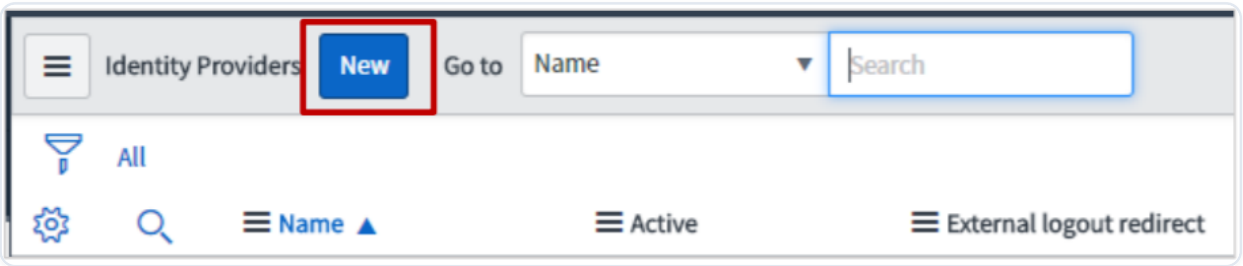
6. Click **Activate**.

   A progress bar indicates the completion of the activation process.

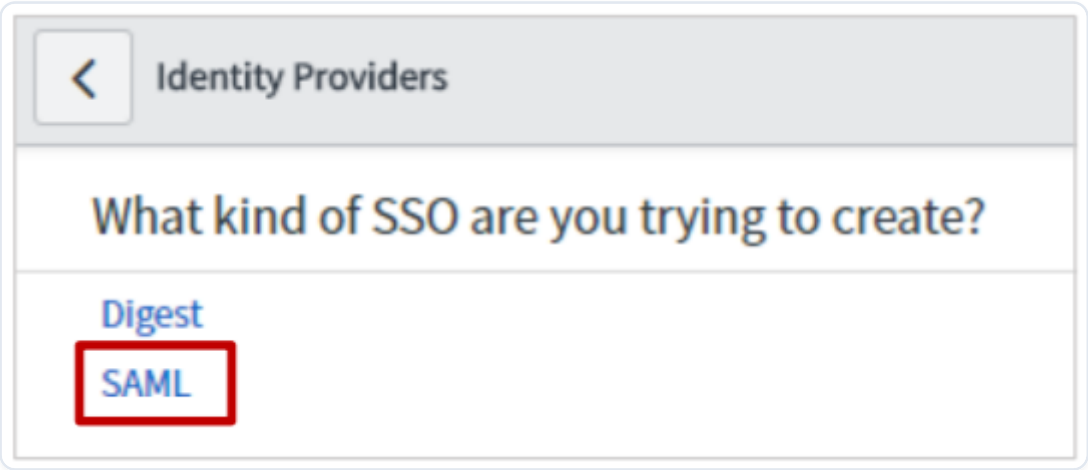
7. In the left pane, scroll down to the Multi-Provider SSO section and click **Multi-ProviderSSO > Identity Providers**.



8. In the right pane, click **New**.



9. Click **SAML**.

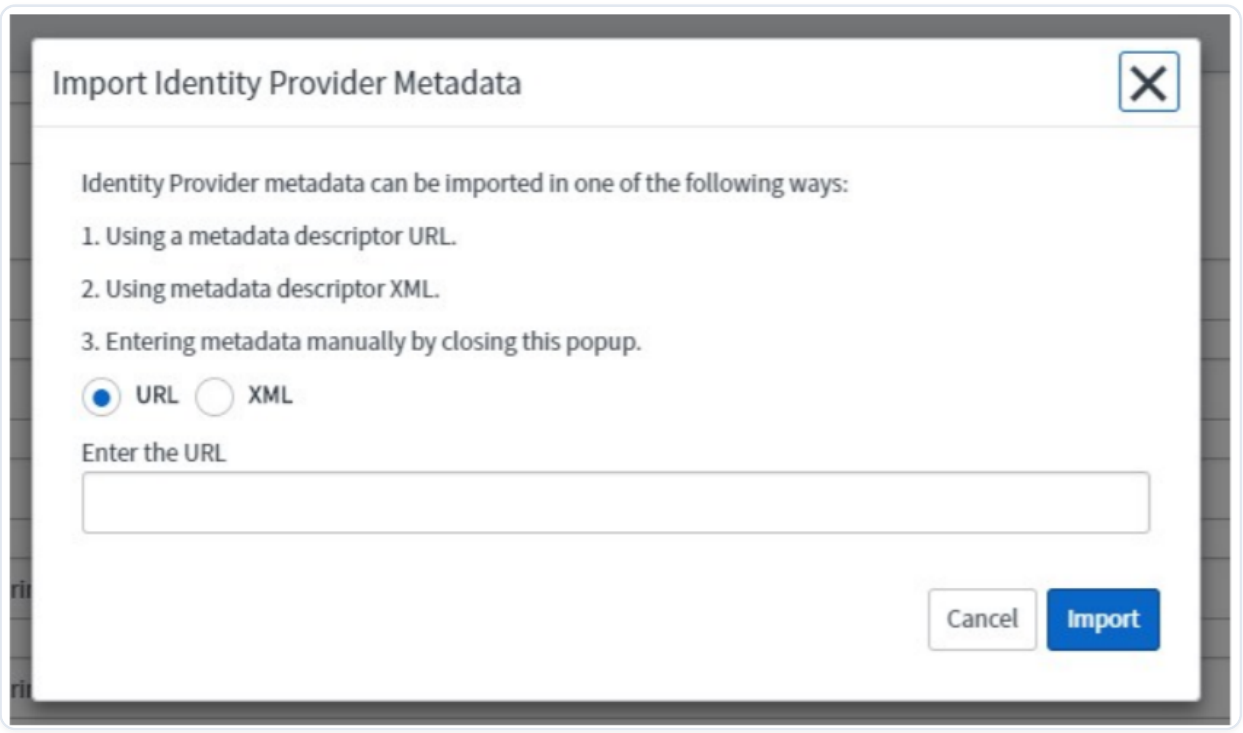


10. If you have the metadata URL, in the **Identity Provider New Record** section, in the **Import Identity Provider Metadata** pop-up window, click **URL** and enter the metadata URL and click **Import**.

    The values for the Identity Provider record fields are automatically populated.

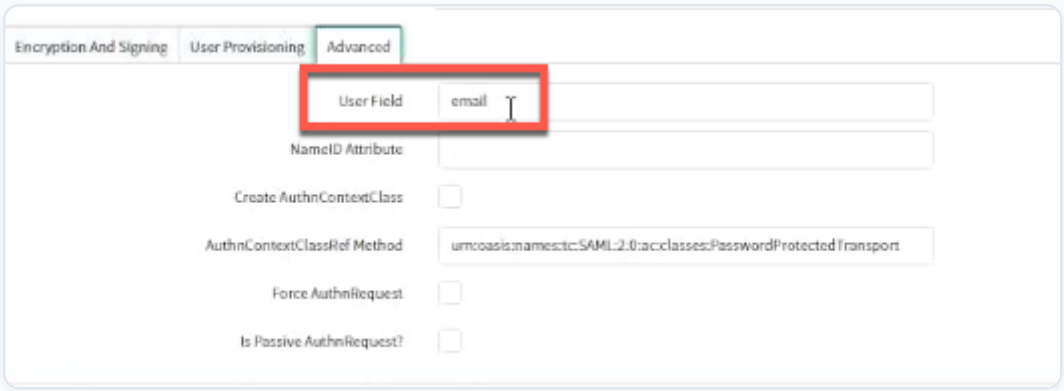
    If you have the metadata XML file, click the XML. Copy the Identity Provider Metadata XML data and paste in the box. Click **Import.**

    The values for the Identity Provider record fields are automatically populated. You can update the values if necessary.

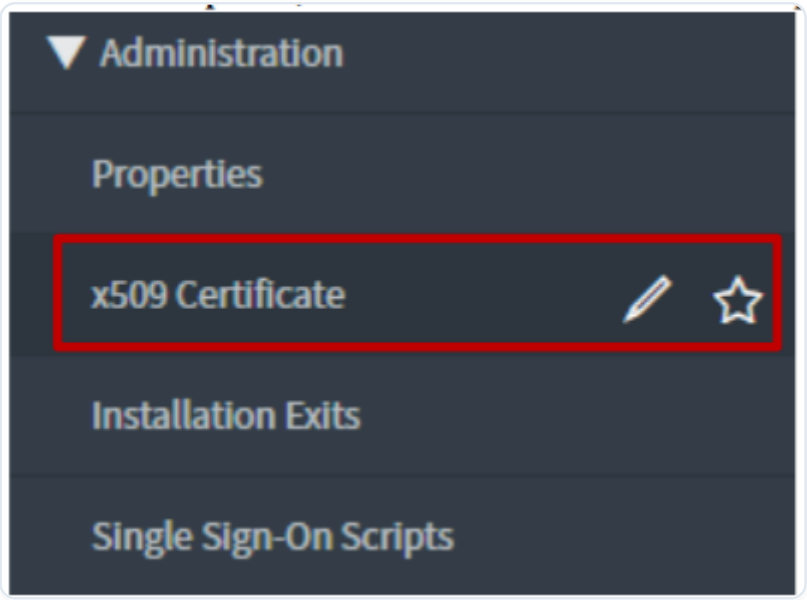


> **Important:**

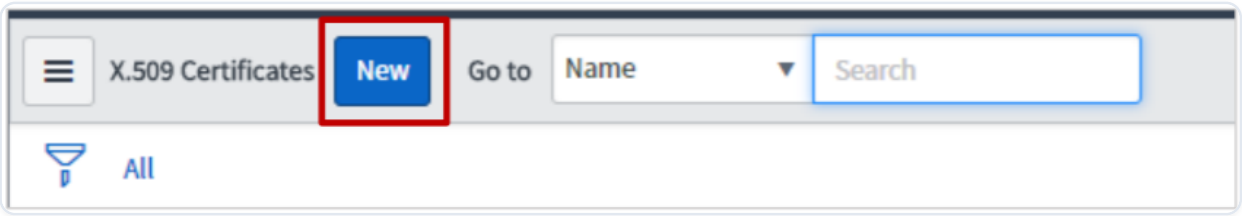
- Citrix recommends that you import the metadata XML file instead of configuring it manually. You can import the metadata XML file from the Citrix Cloud wizard (**Citrix Gateway Service > Add a Web/SaaS App > Single sign on > SAML Metadata**).
- While configuring the parameters in the **Advanced** tab, ensure that the **User Field** value matches with the value that is configured for the **Name ID** field in the Citrix Gateway service user interface.



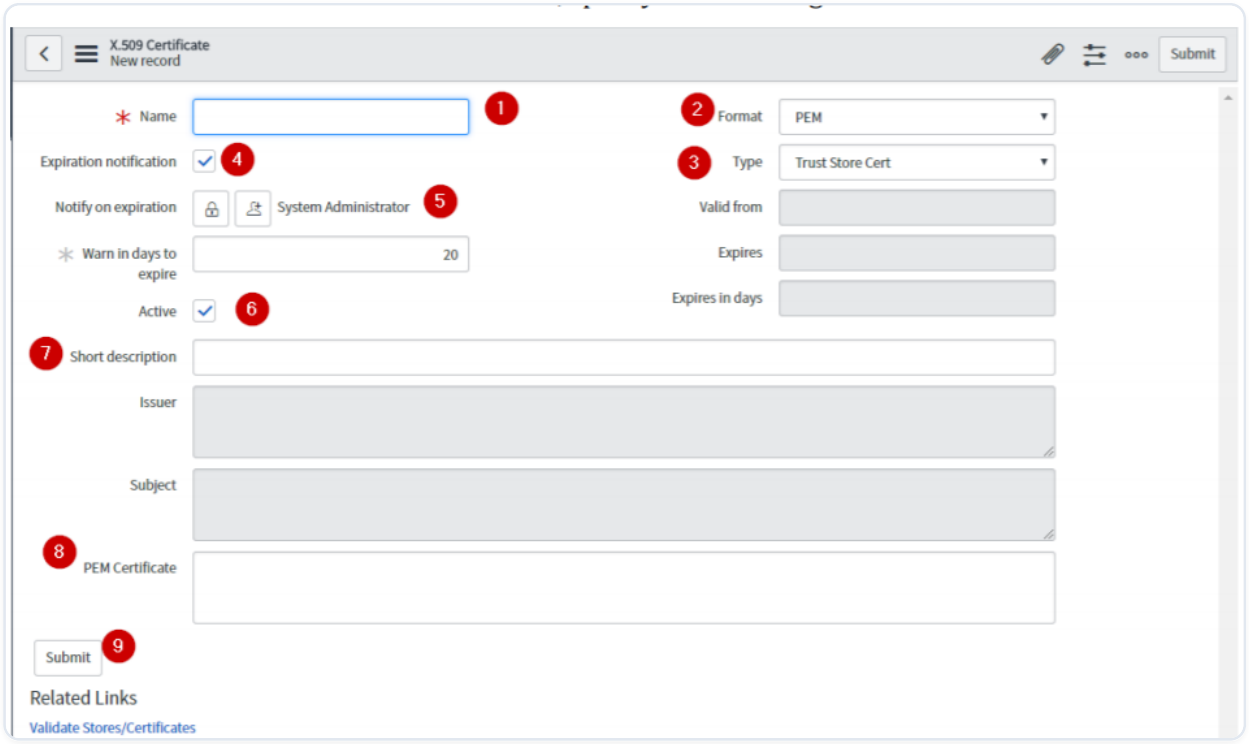
11. Click **Submit**.
12. In the left pane, click x509 Certificate to upload x509 certificate.



13. In the right pane, click **New**.



14. In the X.509 Certificate New record section, specify the following information:



Name – type a certificate name.

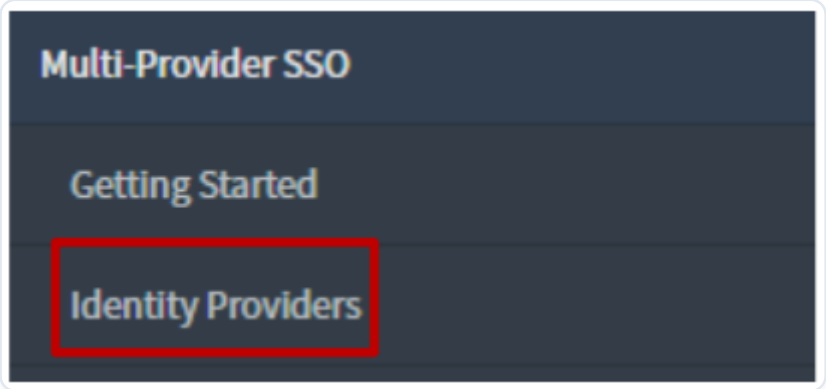
- Format – click the appropriate format: for example PEM.
- Expiration notification – select the check box.
- Type – click the appropriate type.
- Notify on expiration – click the Add me icon to get notified. Click the Unlock Notify on expiration to add more users.
- Active – select the check box.
- Short Description – type description for the certificate.
- PEM Certificate – paste the PEM certificate.
    - Download the certificate from the **Citrix Cloud wizard (Citrix Gateway Service > Add a Web/SaaS App > Single sign on > Certificate)**.
    - Copy the text from ——BEGIN CERTIFICATE—— to ——ENDCERTIFICATE——
    - Paste the text in a text editor and save the file in an appropriate format such as `<your organization name>.`

Note: If you have used an XML file to configure the IdP, you do not have to configure the certificate.

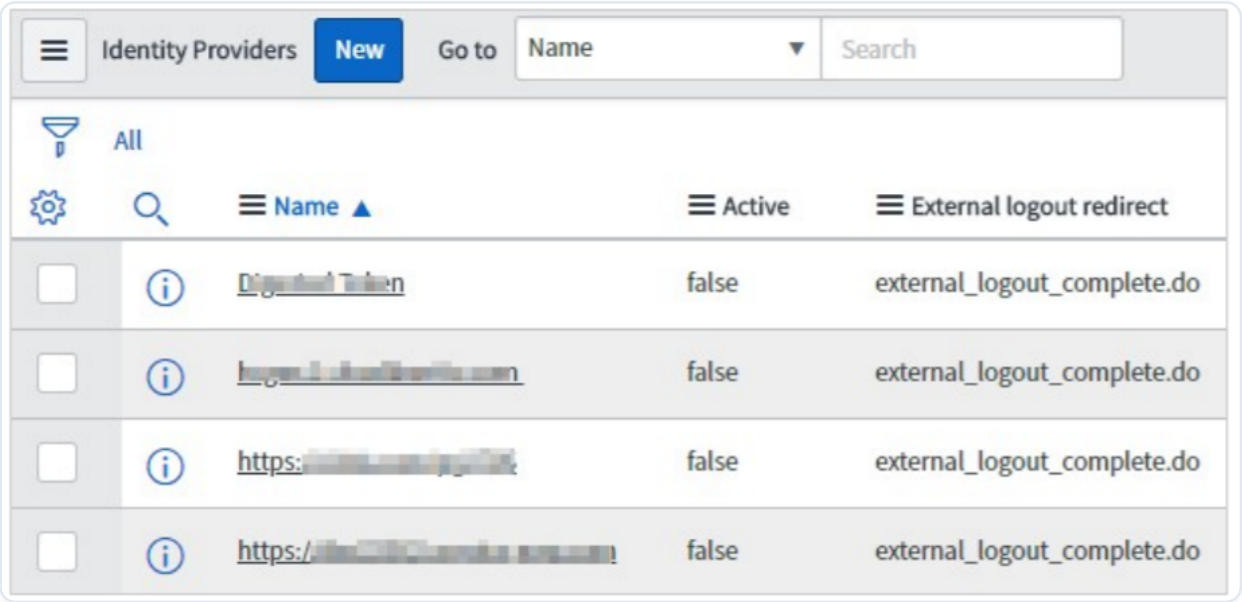


Click **Submit**.

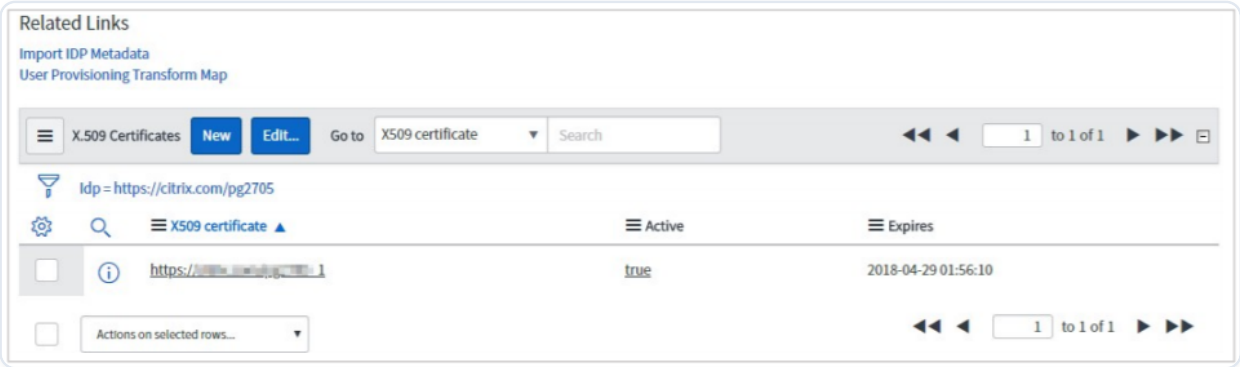
15. In the left pane, click **Identify Providers**.



16. Click the Identity Provider that you have added.

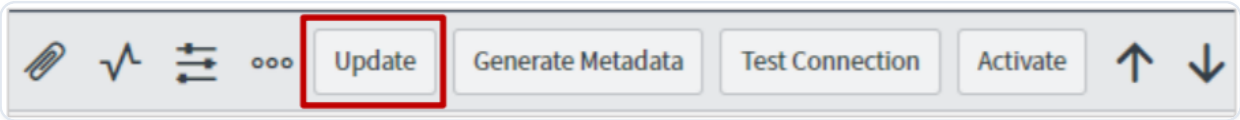


17. On the identity Provider details page, scroll down to the Related Links section. In the X.509 Certificate row, search for the X.509 certificate, and add the appropriate certificate for the identity provider by clicking **Edit.**



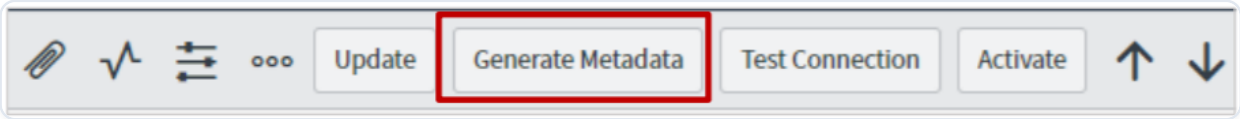
To add a new x.509 certificate, click **New** and to add or remove the certificates, click **Edit.**

18. Click **Update** on the identity provider details page to save the changes.

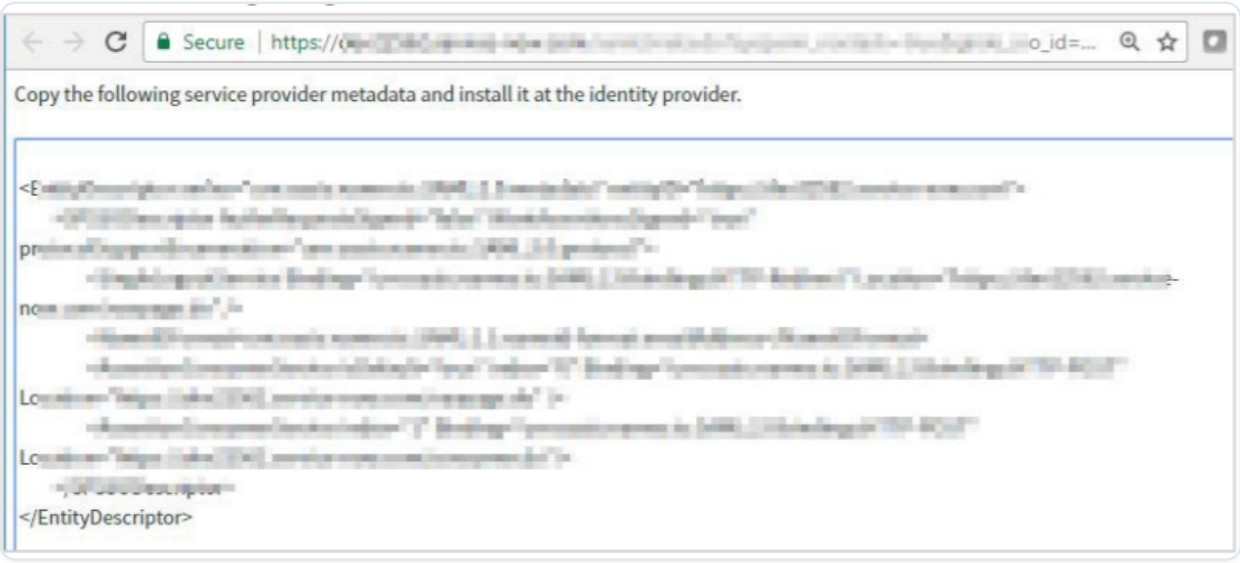


19. To obtain metadata to be used for IdP configuration, click **Generate Metadata**.

Note: You must click **Generate Metadata** to complete the updates.



The service provider metadata appears in a new window. You can use the metadata to validate the entities across both, SP and IdP.

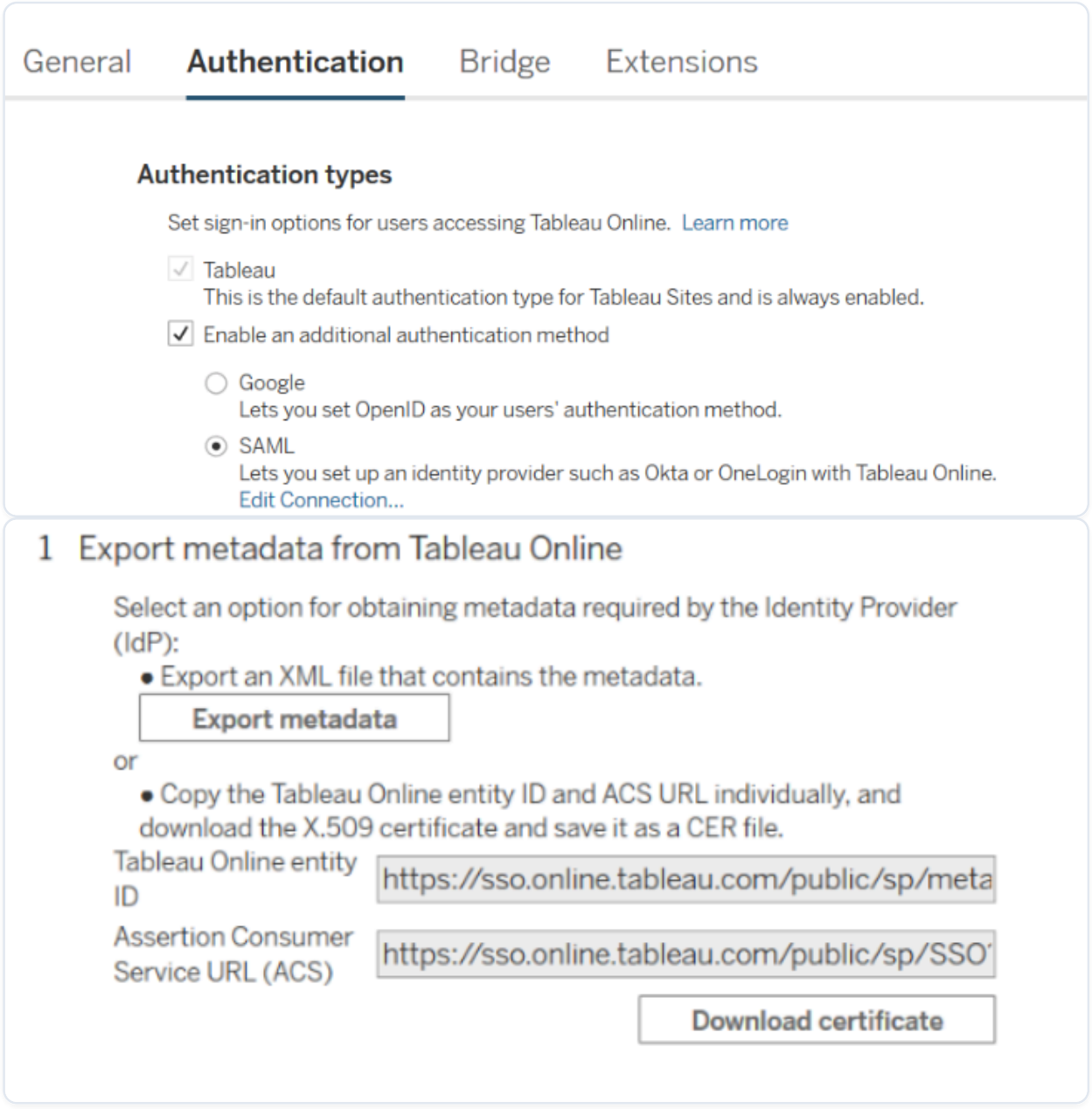


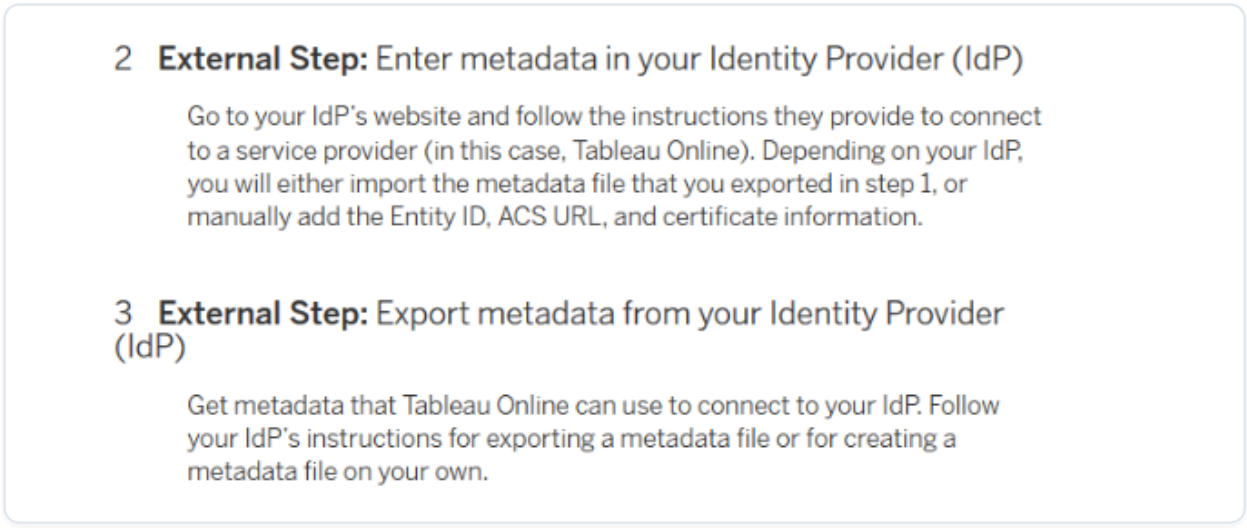
Configure Tableau

Users can securely log on to Tableau using their enterprise credentials.

To configure Tableau for SSO through SAML, perform the following:

1. Log on to Tableau as an admin.
2. Click **Settings** in the menu bar.
3. Click **Authentication**.
4. In Authentication types, select **SAML** and click **Edit Connection**.

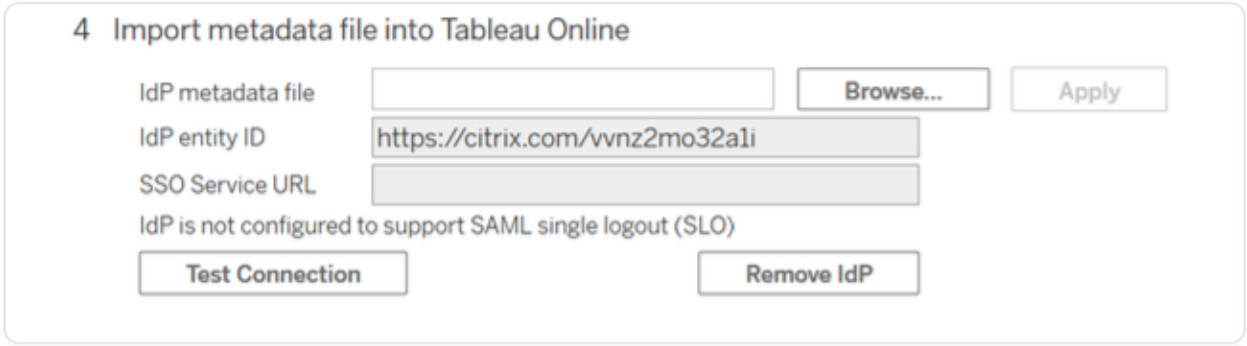




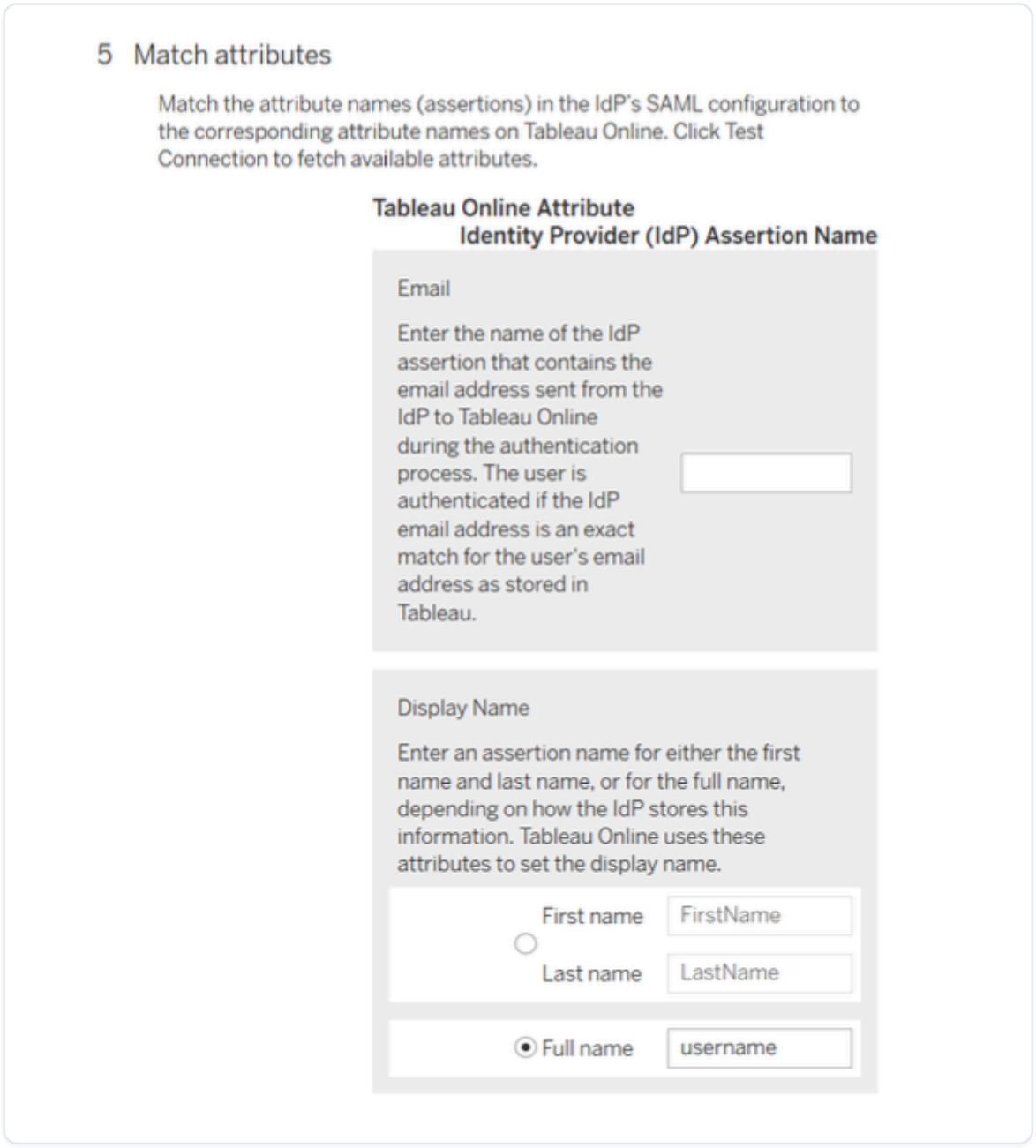
5. Download the metadata file from the Citrix Cloud wizard (**Citrix Gateway Service > Add a Web/SaaS App > Single sign on > SAML Metadata**).

> **Note:**
>
> - Citrix® recommends that you import the metadata XML file instead of configuring it manually.
> - You can download the certificate from the Citrix Cloud wizard (**Citrix Gateway Service > Add a Web/SaaS App > Single sign on > Certificate**).

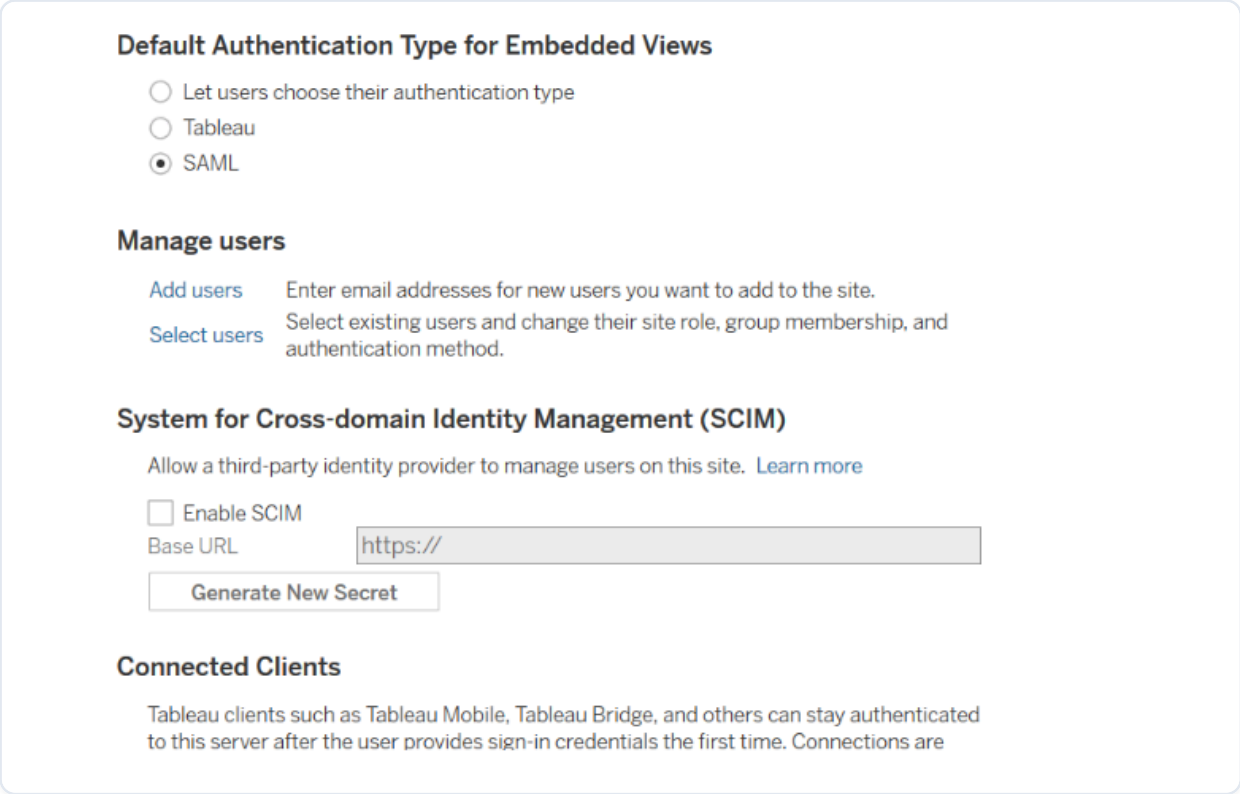
6. Import the IdP metadata file into **Tableau Online**.



7. Enter the IdP entity ID in the format `https://citrix.com/<customerID>`.
8. Click **Test Connection**.
9. Match your IdP Attributes with Tableau Attributes then click **Apply**.



10. Scroll down and select **SAML** as the default authentication type for an embedded view.



11. Add or select users for SSO, as required.

    - To add new users, click **Add users** and enter the email address.
    - For existing users, click **Select users** and make changes as required.

Configure Workday

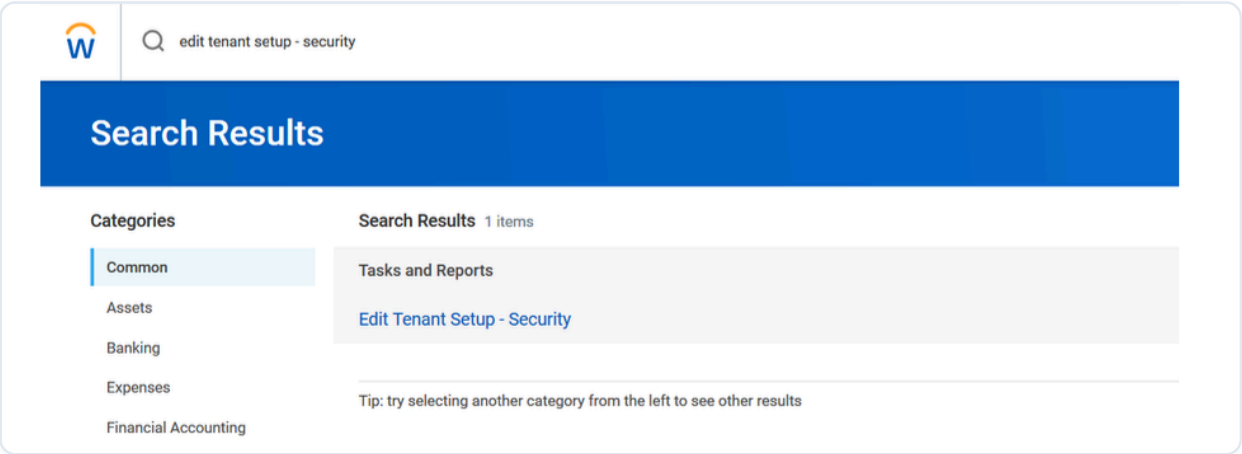
The following sections provide more information about configuring Workday.

Citrix Gateway SaaS Application

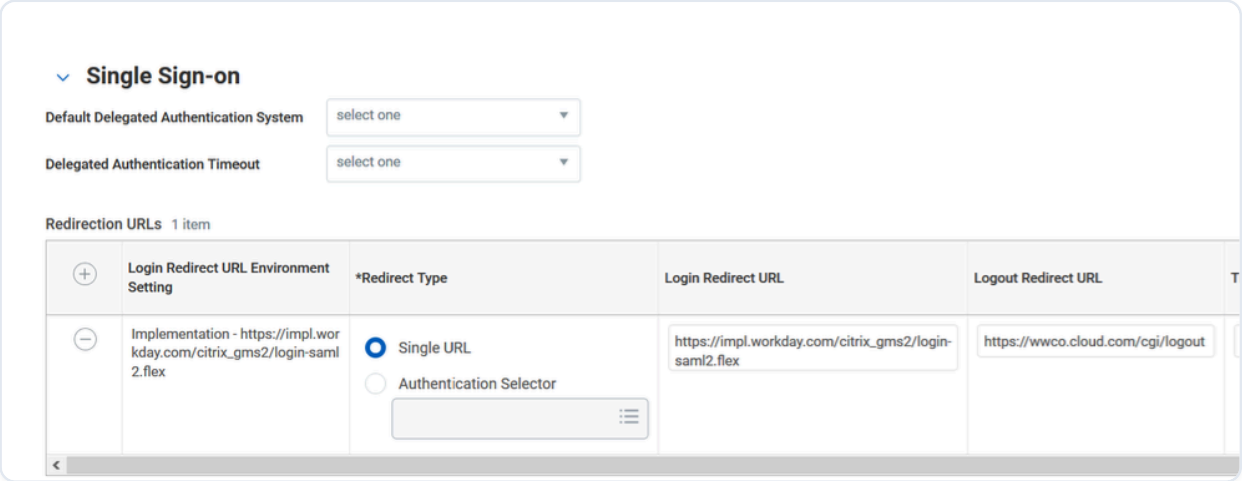
Users can securely log on to Workday using their enterprise credentials.

To configure Workday for SSO through SAML, perform the following:

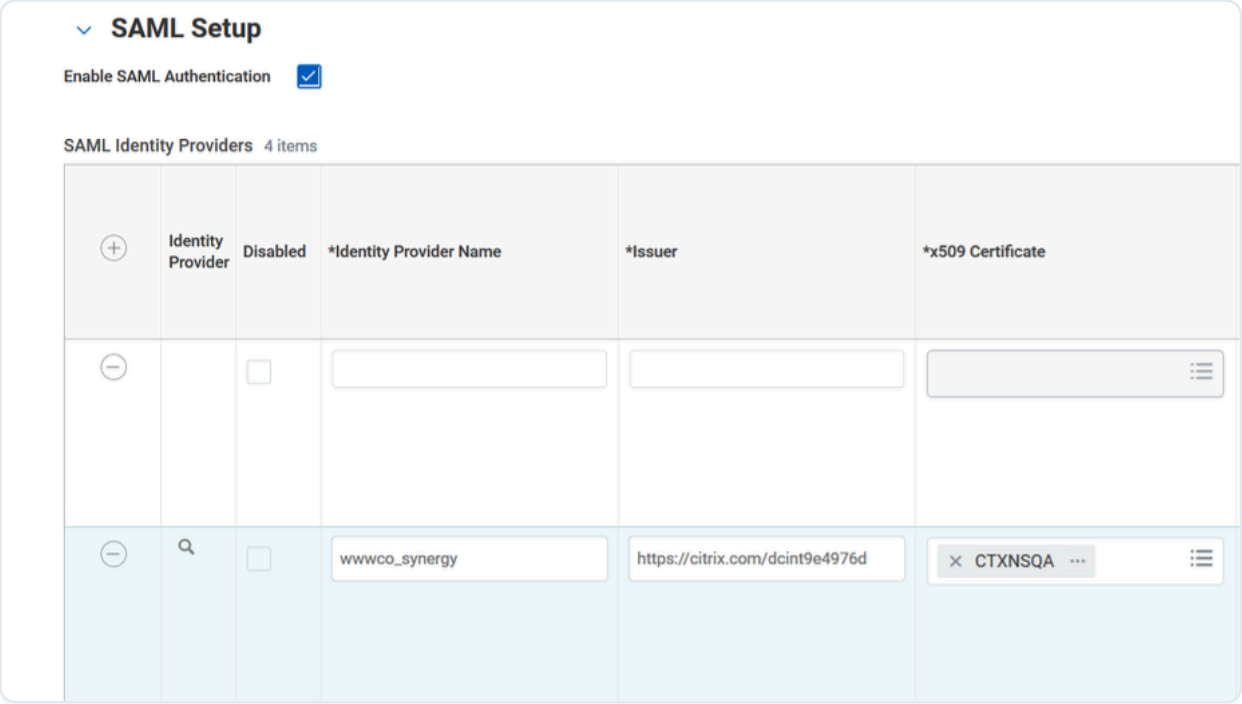
1. Log on to Workday as an administrator.
2. Navigate to **Edit Tenant Setup - Security** and then click **Edit Tenant Setup**.



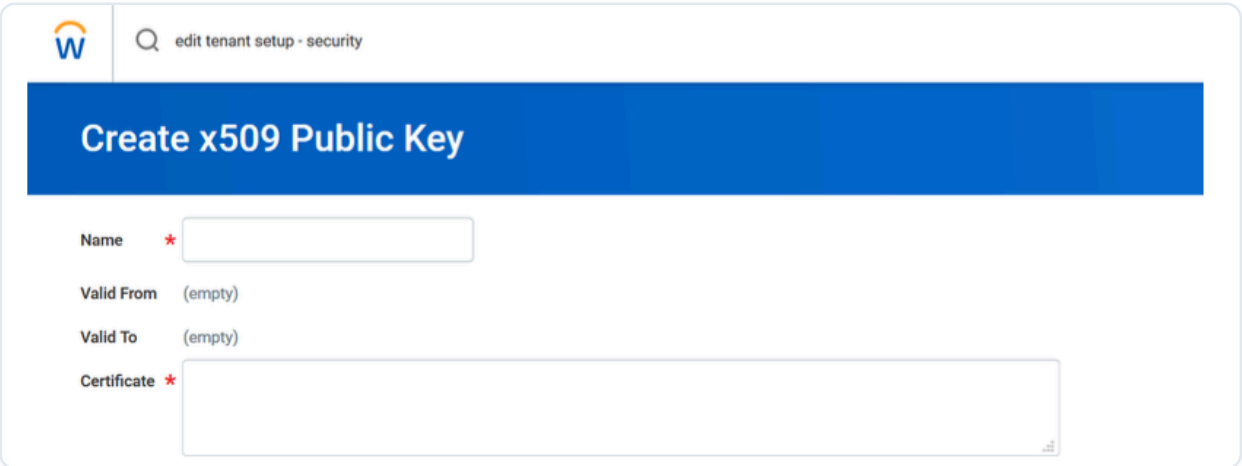
3. Click **Single Sign-on**.



4. Click the plus icon in the Redirection URLs table.
5. In **Login Redirect URL**, enter the URL in the format `https://impl.workday.com/<customer>/login-saml2.flex`.
6. Click **Enable SAML Authentication**.



7. Click the plus (+) icon under SAML Identity Providers to add a row, and specify the following information:
   a. **Identity Provider Name** - type Citrix Gateway.
   b. **Issuer** - type a unique issuer name.
8. In **x509 Certificate**, click the X509 Certificate icon and then click **Create x509 Public Key**.
9. Download the certificate from the Citrix Cloud wizard (**Citrix Gateway Service > Add a Web/SaaS App > Single sign on > Certificate**).



10. Copy the text in the certificate from —–BEGIN CERTIFICATE—– to —–ENDCERTIFICATE and paste the certificate in the Certificate field.
11. Click **OK**.

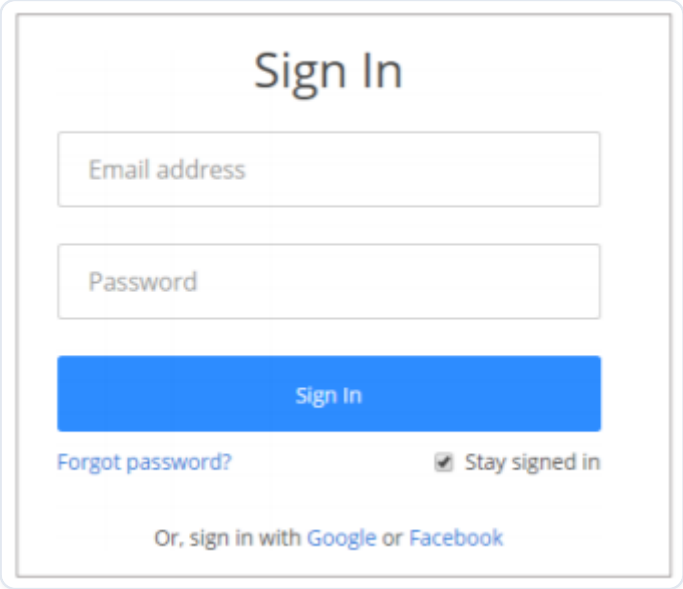
Configure Zoom

The following sections provide more information about configuring Zoom.

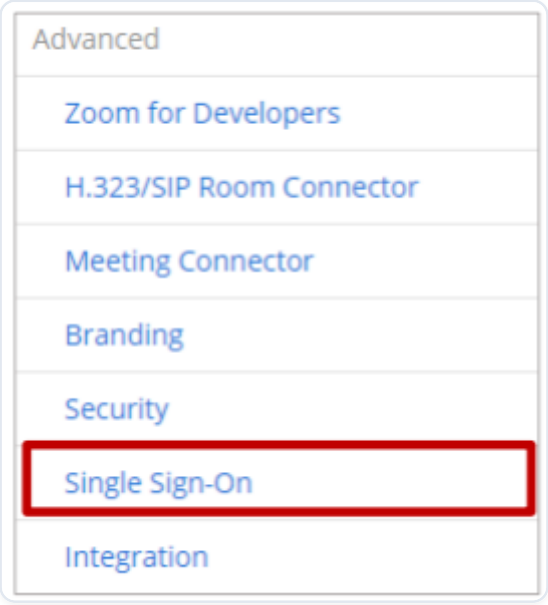
Citrix Gateway SaaS Application

Configuring Zoom for SSO enables administrators to manage their users using NetScaler. Users can securely log on to Zoom using their enterprise credentials.

1. In a browser, type `https://zoom.us/signin` and press enter.
2. Log on to your Zoom account



3. On the **My Profile** page, in the left pane, under **Advanced** section, click **Single Sign-On**.



4. In the SAML tab, copy the URL that the Vanity URL box displays. This URL is required for NetScaler configurations.

5. In the Sign-in Page URL box, enter the IdP URL of your NetScaler app: `https://<NetscalerGateway FQDN>/saml/login`
6. In the Sign-out Page URL box, enter https:< NetScaler Gateway FQDN >.com/cgi/tmlogout.
7. In the Identity provider certificate box, you must paste the Identity provider certificate.
8. To upload your IdP certificate, perform the following:
   - Remotely access your NetScaler instance using PuTTY.
   - Navigate to the /nsconfig/ssl folder (cd/nsconfig/ssl) and press Enter.
   - Type cat certifcate-name.pem and press Enter.

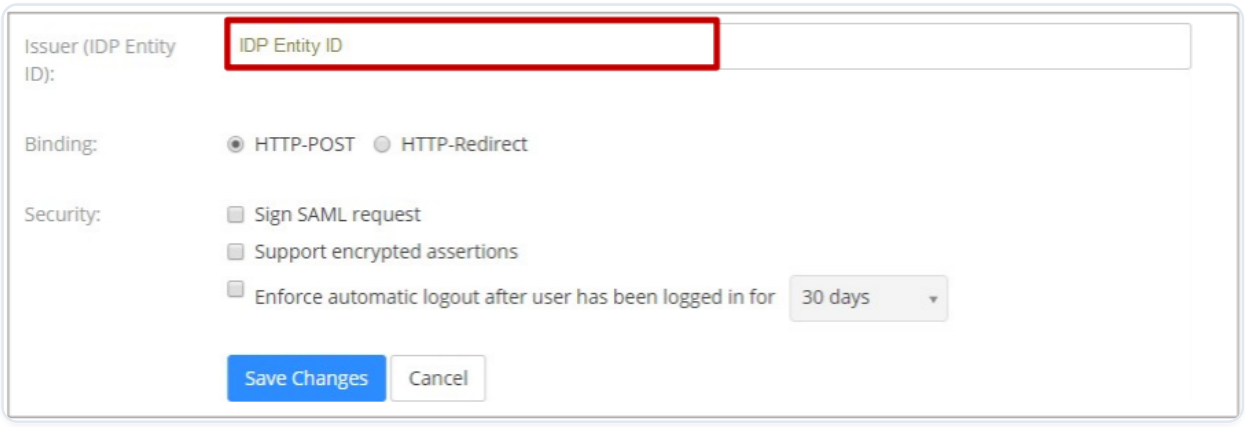
     Note: This is your SAML IdP signing certificate.
   - Copy the text between -----BEGIN CERTIFICATE----- and -----ENDCERTIFICATE-----



9. Copy the URL displayed by the Service Provider (SP) Entity ID box.



10. In the Issuer (IdP Entity ID) box, type a unique issuer ID and click SaveChanges.



Access mode-based policy enforcement

Access mode-based policy enforcement lets administrators restrict how a user connects to an application. The connection can be through a browser-based client or the Citrix Secure Access client. Previously, Secure Private Access had no way to restrict access based on which a client initiates the session. Access mode adds that capability.

For example, administrators can configure that SSH and RDP applications are only reachable through a browser, such as Chrome Enterprise Premium, and not tunneled through the Citrix Secure Access client. This ensures that browser-based security controls always apply.

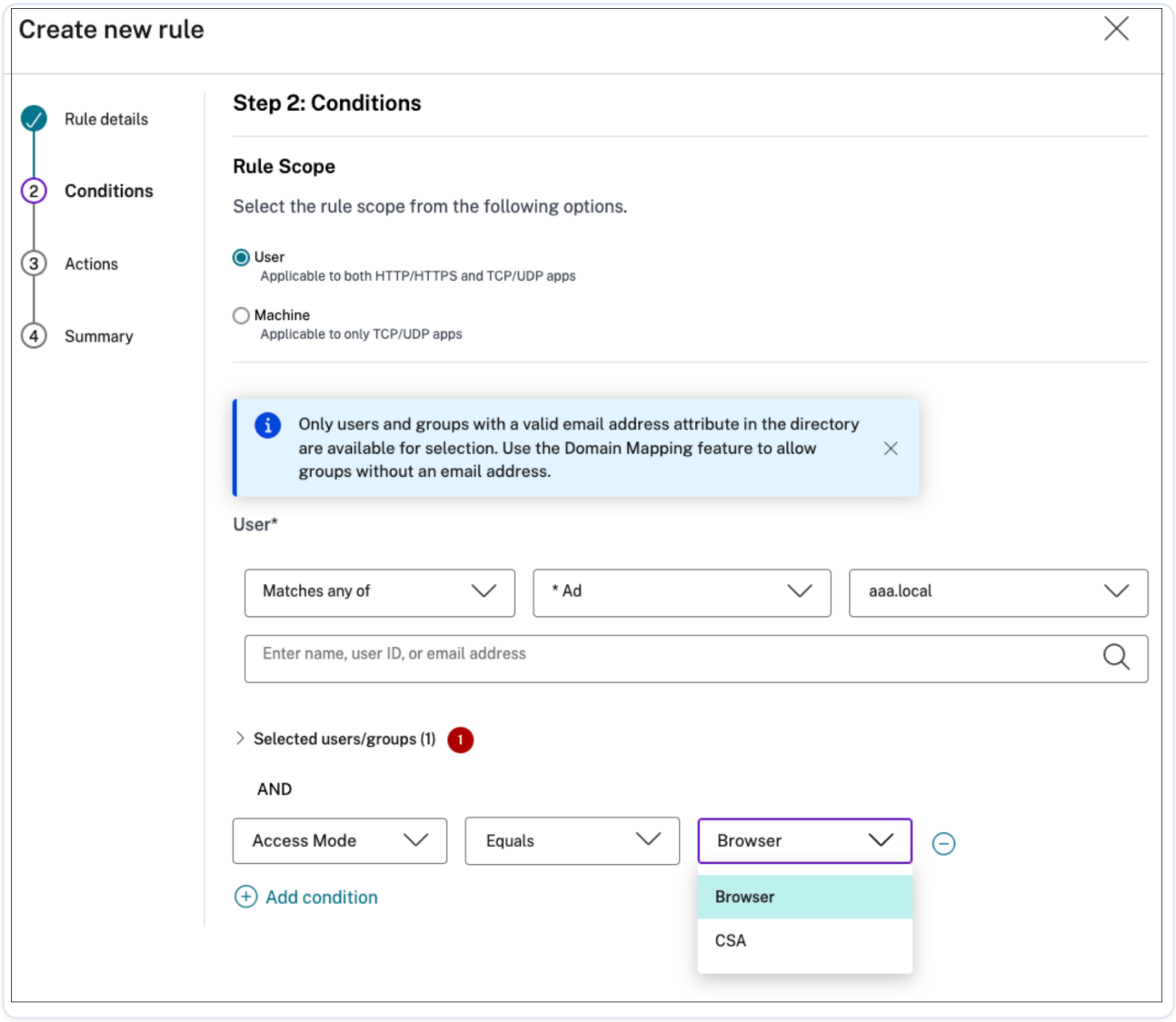
> **Note:**
>
> Access mode is a restricting condition only. It can narrow down the access but cannot grant access on its own. All other conditions in the policy are still evaluated.

How it works

Access mode is configured in the Secure Private Access admin console and can be added to a rule in any of the three policy types.

- Adaptive access policy
- Session policy
- Browser policy

The following figure displays a sample acess policy rule condition.



End-user experience

Based on the access mode, application enumeration and launch are either allowed or restricted.

- **Matching client** — The application is enumerated and launches normally.
- **Non-matching client** — The application is not shown in the app list during enumeration, and a launch attempt is blocked. The user is sent to the standard access-denied page. No new denial message is introduced.
- **Undeterminable session** — When the access mode cannot be determined (for example, some mobile Secure Access sessions), the access mode condition is skipped and the session is unaffected. All other conditions still apply.

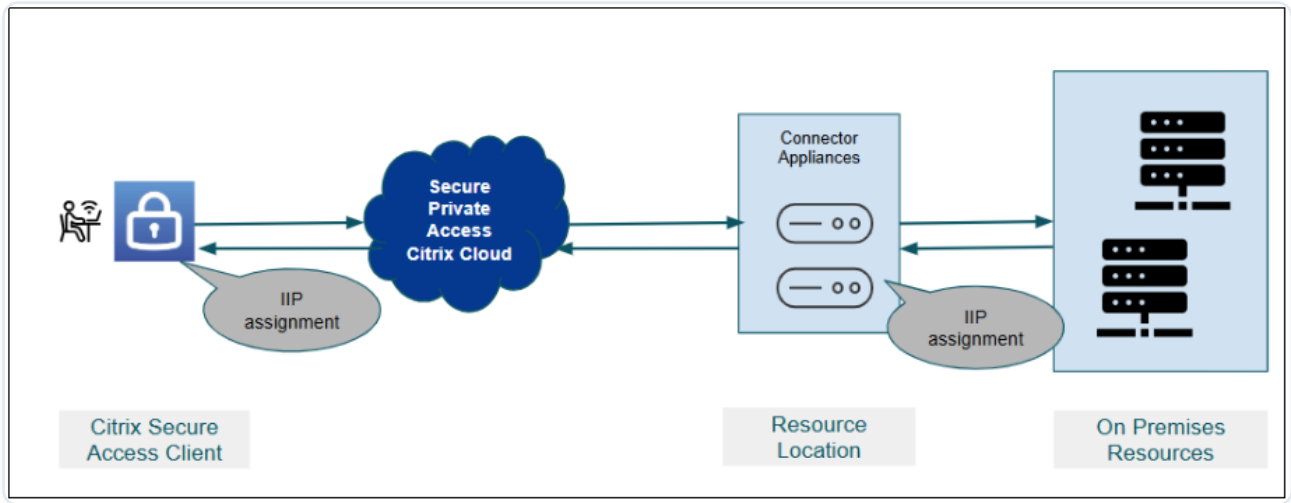
Support for server-to-client connections - Preview

In a traditional client-server setup, the remote users can access resources in customer resource locations using the HTTP, TCP, and UDP connections. However, there are scenarios where the server or the back-end system needs to initiate a connection with the remote client devices (example laptops, smart phone, tablet) for tasks such as push configurations, remote assistance, application access, or app installation while safeguarding user privacy and security. Secure Private Access supports server-to-client connections wherein the servers in the customer's resource location can establish a TCP/UDP connection with the remote client.

- To enable server-to-client connection, Secure Private Access introduces the server-to-client app. This app can be configured with the client details (port, protocol) and the back-end server's IP CIDR range.
- After the server-to-client app type is created, then appropriate access policies must be configured for these applications to enable server-to-client connections.

How server-to-client connection works

The following diagram displays a sample server-to-client connection architecture.



The following steps illustrate the server-to-client connection workflow:

1. When a user logs in to the Citrix Secure Access™ client, the user is assigned an Internal IP address from the designated client internal IP address pool. This assignment is based on the configured resource location, IP CIDR, and user context in the IP address pool configuration.
2. This assigned IP address is then associated with a specific Connector Appliance within the configured resource location and IP pool. This Connector Appliance owns and manages connections related to this IP address for back-end customer resource location.

3. The back-end server initiates a TCP/UDP connection to the remote client using the assigned client internal IP address using the port of the client application specified in the server-to-client application configuration.
4. The connector communicates with Secure Private Access to establish a connection with the client.
5. The Secure Private Access verifies if the back-end server is configured in the server-to-client application, then evaluates the relevant access policy to determine whether to allow or block access to the client machine.
6. If the policy allows access, then Secure Private Access connects with the remote client machine. If the client machine is domain-joined, then the FQDN of that machine is registered with the IIP address. The machine can be accessed either by FQDN or the internal IP address.
7. When a user logs out, the assigned internal IP address is released both from the Connector Appliance and the active session. If the same user logs in again within 15 days, the user gets the same IP address, else it is released for other user's usage.

Create a server-to-client app

The following sections provide details about creating a server-to-client app.

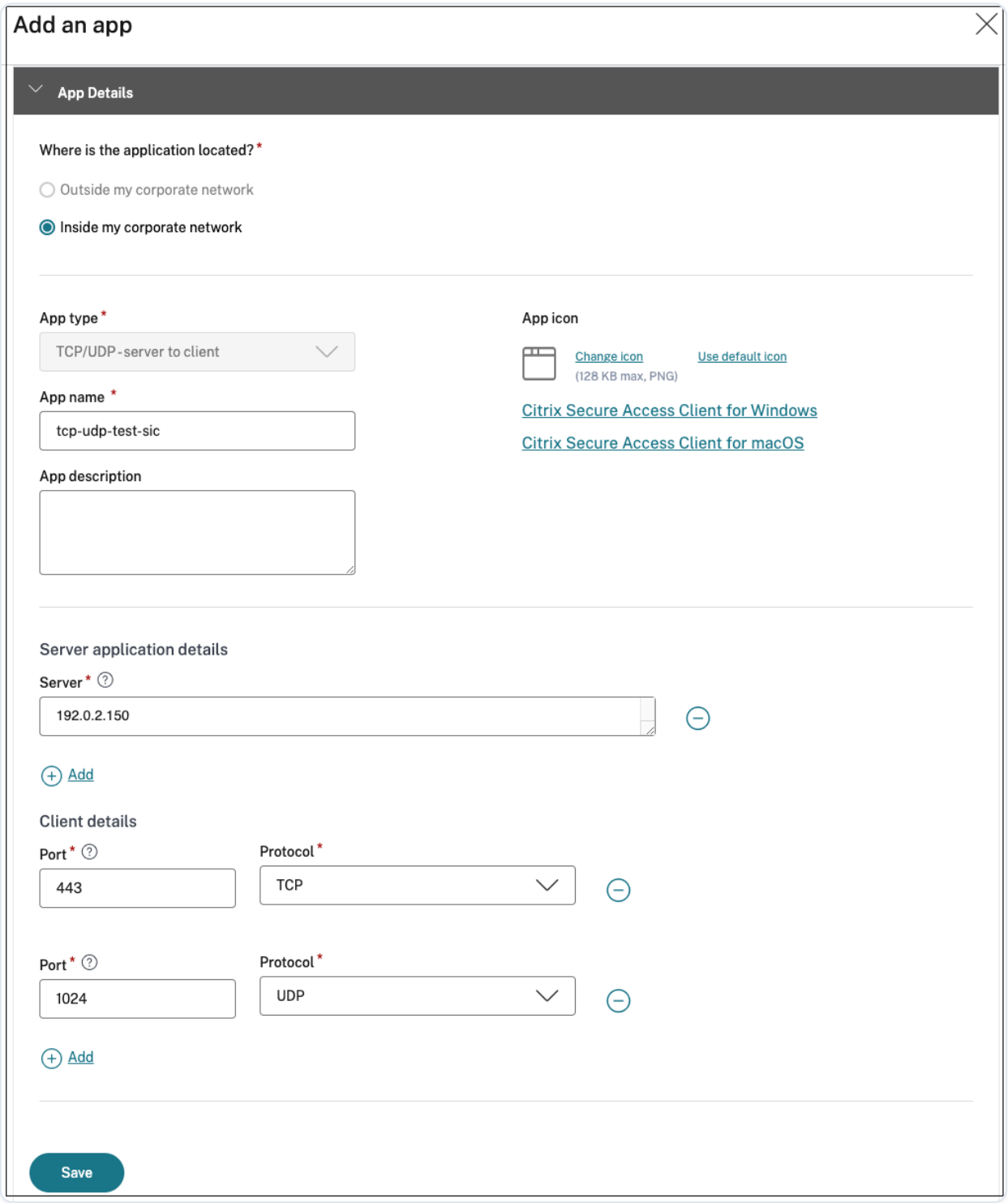
Prerequisites

- The client internal IP address pool is created. The IP address pool is essential for assigning a unique IP address to a user and the associated device. For details, see Client internal IP address pools.
- The customer's admin must allocate a free Intranet IP CIDR subnet for the resource location network. This IP CIDR must not conflict with other resource IP addresses.
- The customer's admin must determine which group/context users are allocated the Intranet IP address from which resource location. It is recommended to maintain a user-to-IP address ratio of 1:3. That is if the number of users logging in is 1000, it is recommended to allocate 3000 IP addresses in the Client IP Pool.
- The free IIP subnet and the connector's primary IP address must belong to the same network and subnet.
- Interconnections must be maintained between resource locations to allow servers in other locations (not configured in the IP pool) to connect to the client.
- Ensure that you use the Citrix Secure Access clients versions that support server-to-client apps.

- Windows 24.11.1.17 and later
- macOS 25.01.1 and later
- Linux 25.2.2 and later

Perform the following steps to configure server to client TCP/UDP apps

1. Log in to Citrix Cloud and select **Secure Private Access**.
2. Click **Applications > App Configuration** and then click **Add an app**.
3. In the **Choose a template** section, click **Skip**. Templates are available only for SaaS apps.



4. Select the location **Inside my corporate network**.
5. 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** - IP address range of the back-end server that can establish a connection with the client machine. This ensures that only the servers with IP addresses within this range can access the client's ports.
- **Port** – The client machine's port number to which the back-end server can initiate a connection.
- **Protocol** – TCP or UDP.

6. Click **Add** to add more servers and ports.
7. 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.

After you create the server-to-client app, create access policies as per the requirement.

> **Note:**
>
> All the existing access policies are supported for server-to-client applications. The server-to-client access is allowed to users whose context is evaluated to "Allow" for the configured access policy.

Citrix Secure Private Access Document History

The following table describes important changes to the Citrix Secure Private Access service documentation. To receive notifications about these updates, subscribe to the RSS feed.

DATE	CHANGE	TOPIC
30 Sep 2026	Added/updated topics for new features/enhancements	What's new
03 Sep 2026	Added/updated topics for new features/enhancements	What's new
05 Aug 2026	New routing method to access SaaS applications	What's new
31 Jul 2026	Added topics for Citrix Secure Access controls for Chrome Enterprise	What's new
24 Jun 2026	Added/updated topics for new features/enhancements	What's new
09 Jun 2026	Update on Edge configuration	Citrix Secure Private Access Edge configuration update
20 May 2026	Data regionalization support	Data regionalization
29 Apr 2026	Added/updated topics for new features/enhancements	What's new
28 Apr 2026	Added topic for troubleshooting CEP integration issues	Troubleshoot CEP integration

DATE	CHANGE	TOPIC
07 Apr 2026	Context-based app routing support for hybrid deployments	Context-based application routing
07 Apr 2026	Updated the changes in the Choose a template section of the app configuration page	Configure a SaaS app
12 Feb 2026	Added a topic for port-based application routing	Port-based routing using Routing Exceptions
05 Feb 2026	Updated the topic on Citrix Enterprise Browser (CEB) to Citrix Enterprise Premium (CEP)	Citrix Enterprise Browser to Chrome Enterprise Premium migration
05 Feb 2026	Added a topic for domain mapping	Domain mapping for user groups without email addresses
16 Jan 2026	Added a topic for local LAN access support	Seamless access to local LAN resources
18 Dec 2025	Secure access to SSH and RDP apps within the browser	Secure access to SSH apps within the browser and Secure access to RDP apps within the browser
16 Dec 2025	Support for routing DNS queries to the application specific resource locations	Route DNS queries to application-specific resource locations
12 Dec 2025	Added a topic for Google Cloud Directory Sync (GCDS)	Google Cloud Directory Sync (GCDS)
11 Dec 2025	Support for Citrix Enterprise Browser to Chrome Enterprise Premium migration	Citrix Enterprise Browser to Chrome Enterprise Premium migration

DATE	CHANGE	TOPIC
25 Nov 2025	Secure Private Access for hybrid deployments release 2511 released	What's new in this release
30 Oct 2025	Enhancements to the Chrome Enterprise Premium integration	Integration with Google Chrome Enterprise Premium
17 Sep 2025	Citrix Secure Private Access support for mobile devices	Citrix Secure Private Access for mobile devices
13 Aug 2025	Support for adding custom store URLs	Custom store URLs for accessing apps via Citrix Enterprise Browser
13 Aug 2025	Enhancements to the policy modeling tool	Policy modeling tool
11 Aug 2025	Added error codes 6003 and 6007	Citrix Secure Access client failed to do SSO
14 Jul 2025	Secure Private Access release 2508.1 and 2505.5	What’s new
06 Jun 2025	New administrator roles	Role-based access control
03 Jun 2025	Certificates management	Manage certificates in the Secure Private Access console
15 May 2025	Citrix Secure Private Access with Google Chrome Enterprise Premium	Integration of Citrix Secure Private Access with Google Chrome Enterprise Premium
09 May 2025	Multi-doman support for on-premises deployments	Multi-domain environments
29 Apr 2025	Secure Private Access on-premises 2503 released	What’s new

DATE	CHANGE	TOPIC
28 Apr 2025	Secure Private Access for hybrid deployments release 2502 released.	Citrix Secure Private Access hybrid deployment
24 Apr 2025	Hybrid data path support	Hybrid data path for Secure Private Access service
24 Apr 2025	Display of contextual routing insights in Monitor	Contextual routing insights in Monitor
24 Apr 2025	Delete IP address pools immediately or over time	Delete an IP address pool
24 Apr 2025	Configure secondary resource locations	Configure a SaaS app
22 Apr 2025	Import applications using the nsconfig file	Applications import tool
10 Apr 2025	Added topic for Connector Appliance scale and size considerations	Scale and size considerations
03 Apr 2025	Added resolution steps to the Secure Private Access error codes in Monitor	Secure Private Access sessions codes in DaaS Monitor
20 Feb 2025	Enhancements to the admin audit logging feature	Audit logs
20 Feb 2025	Search and add users based on UPN and email address	Configure an access policy
08 Jan 2025	Dynamically route entire sessions using session policies	Route internal corporate users directly to back-end applications
07 Jan 2025	Added information about connector stickiness	Connector stickiness

DATE	CHANGE	TOPIC
07 Jan 2025	Added information about client IP address stickiness	Client IP address stickiness
07 Jan 2025	Support for creating internal IP address pools	Client internal IP address pools
07 Jan 2025	Support for server-to-client connections	Support for server-to-client connections
02 Jan 2025	Support to import VPN applications to ZTNA	CSV-based applications import tool