



# Citrix Secure Private Access™

## Contents

<b>What's new</b>	<b>3</b>
<b>Secure Private Access service solution overview</b>	<b>24</b>
<b>Integration of Citrix Secure Private Access with Google Chrome Enterprise Premium</b>	<b>36</b>
<b>Get started with Citrix Secure Private Access</b>	<b>46</b>
<b>Secure Private Access service deployment models</b>	<b>49</b>
<b>Points of Presence (PoPs) locations for Citrix Secure Private Access™ service</b>	<b>50</b>
<b>Secure Private Access onboarding and set up</b>	<b>51</b>
<b>Apps configuration and management</b>	<b>61</b>
<b>Support for Enterprise web apps</b>	<b>61</b>
<b>Support for SaaS apps</b>	<b>73</b>
<b>Support for TCP/UDP apps</b>	<b>101</b>
<b>Always On before Windows Logon</b>	<b>113</b>
<b>Reserved CIDR addresses for the TCP and UDP servers</b>	<b>129</b>
<b>DNS suffixes to resolve FQDNs to IP addresses</b>	<b>130</b>
<b>Support for server-to-client connections - Preview</b>	<b>135</b>
<b>Agentless access to Enterprise web apps</b>	<b>139</b>
<b>Manage certificates in the Secure Private Access console</b>	<b>150</b>
<b>Citrix Secure Access™ client</b>	<b>155</b>
<b>Best practices for Web and SaaS application configurations</b>	<b>156</b>
<b>App access end-user experience explained</b>	<b>162</b>
<b>Adaptive access policy configuration and management</b>	<b>165</b>
<b>Access restriction options</b>	<b>177</b>
<b>Connector Appliance for Secure Private Access</b>	<b>195</b>

<b>Scale and size considerations</b>	<b>206</b>
<b>Advanced Secure Private Access features</b>	<b>207</b>
<b>Custom workspace domains for accessing apps via Citrix Enterprise Browser™</b>	<b>208</b>
<b>Hybrid data path for Secure Private Access service</b>	<b>211</b>
<b>Discover applications, domains, or IP addresses within your network</b>	<b>220</b>
<b>Context-based app routing and resource locations selection</b>	<b>226</b>
<b>Policy modeling tool</b>	<b>235</b>
<b>Applications import tool - Preview</b>	<b>240</b>
<b>Client internal IP address pools - Preview</b>	<b>251</b>
<b>Maintain consistent connections</b>	<b>255</b>
<b>Terminate active sessions and add users/machines to the block list</b>	<b>259</b>
<b>Timeouts for user sessions</b>	<b>262</b>
<b>Configuration reports</b>	<b>264</b>
<b>ADFS integration with Secure Private Access</b>	<b>266</b>
<b>Secure Private Access dashboard</b>	<b>275</b>
<b>Logging and troubleshooting</b>	<b>284</b>
<b>Integration with DaaS Monitor</b>	<b>325</b>
<b>Secure Private Access sessions codes in DaaS Monitor</b>	<b>327</b>
<b>Audit logs</b>	<b>340</b>
<b>Citrix Enterprise Browser</b>	<b>342</b>
<b>Unsanctioned websites</b>	<b>342</b>
<b>Role-based access control</b>	<b>345</b>
<b>Support for multi-session virtual desktop infrastructure</b>	<b>350</b>
<b>Feature deprecations</b>	<b>353</b>

## What's new

September 6, 2025

### 13 August 2025

- **Custom workspace domains for accessing apps via Citrix Enterprise Browser™**

The custom workspace domain 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. For details, see [Custom workspace domains for accessing apps via Citrix Enterprise Browser](#).

- **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:

1. The routing of UDP DNS queries to the application-specific resource location is disabled by default. To enable this functionality, contact Citrix Support.
2. 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.
3. 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](#).

1 Client internal IP address pools feature is under preview.

- **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](#).

[CSAClients-10642]

## 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

For details, see [Access restriction options](#).

- **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. For details, see [Unsanctioned websites](#).

## 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

For details, see [Access restriction options](#).

- **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](#).

[SPA-746]

## 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](#).

[ACS-2325]

## 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](#).

[SPAOP-1]

## 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](#).

[ACS-2490]

## 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](#).

[AAUTH-90]

- **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](#).

[ACS-1399]

## 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](#).

[ACS-1888]

- **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](#).

[ACS-3018]

## 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](#).

[ACS-3018]

- **Support for UDP apps**

The Secure Private Access service now supports access to UDP apps. For details, see [Preview features](#).

[ACS-1430]

## 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](#).

[ACS-877]

- **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](#).

[ACS-99]

- **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](#).

[ACS-1850]

- **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](#).

[ACS-655]

- **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](#).

[ACS-2480]

- **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.

[ACS-1546]

- **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](#).

[ACS-876]

- **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](#).

[ACS-805]

- **Troubleshooting Guide**

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

[ACS-2719]

## 15 July 2022

- **Enable access to an application only if an access policy is configured**

Access to the apps is now enabled only after the admin adds an access policy in addition to the app subscription. App subscription alone does not enable access to the applications. With this change, admins can enforce adaptive security based on context like users, location, device, risk. Admins must migrate the existing app security controls and access policies to the new access policy framework. For details, see [Migration of app security controls and access policies](#).

[ACS-1850]

## 01 June 2022

- **Adaptive Authentication service**

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

[CGS-6510]

## 04 April 2022

- **Rebranding changes**

Citrix Secure Workspace Access service is now rebranded to Citrix Secure Private Access service.  
[ACS-2322]

- **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).

[ACS-1102]

- **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).

[ACS-1169]

- **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).

[ACS-970]

- **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).

[ACS-878, ACS-879, ACS-882]

- **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).

[ACS-876]

- **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).

[ACS-805]

- **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.

[CGS-6510]

## 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](#)

[ACS-870]

## 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 **Workspace configuration > Access > External Connectivity**. For details, see [External connectivity](#). There is no change in the functionality, otherwise.

[NGSWS-16761]

## 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.

[ACS-833]

- **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.

[ACS-944]



## 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.

[ACS-243]

## 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.

[ACS-222]

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

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

[NGSWS-17100]

## 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.

[ACS-388]

- **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.

[ACS-351]

- **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.

[NGSWS-17212]

## 15 March 2021

- **Platform enhancements**

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

[ACS-85]

- **Improved web apps performance**

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

[NGSWS-16469]

- **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.

[NGSWS-16068]

## 11 November 2020

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

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

[NGSWS-14934]

## 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.

[ACS-123]

## 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.

[NGSWS-13754]

- **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.

[NGSWS-14427]

## 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.

[ACS-286]

## 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.

[NGSWS-8581]

## 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.

[ACS-205]

## 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.

[NGSWS-10799]

- **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.

[NGSWS-8580]

## V2019.04.02

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

[NGSWS-6410]

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.

[NGSWS-6445]

- **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.

[NGSWS-6532]

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

[NGSWS-6926]

## 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.

[CGOP-6358]

- **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.

[CGOP-6205]

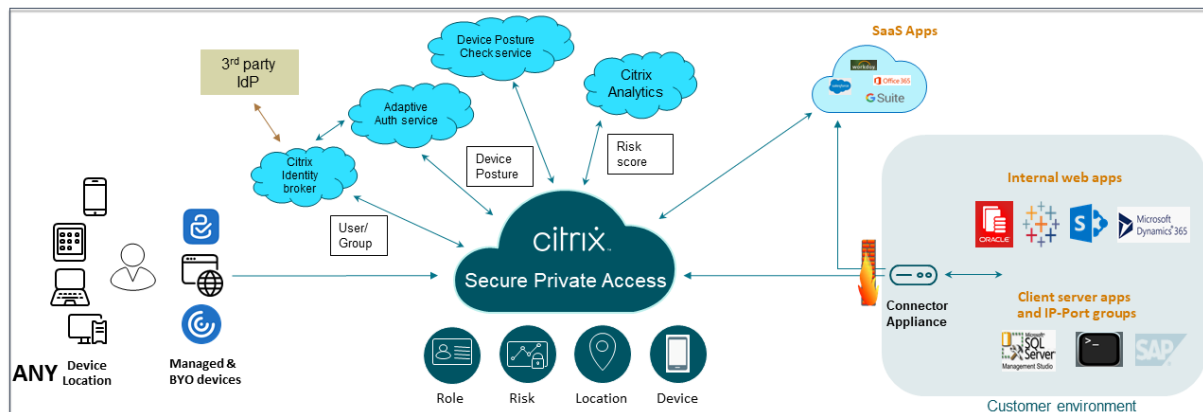
## Secure Private Access service solution overview

September 6, 2025

### 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 enables end users to safely browse the internet with a centrally managed and secured enterprise browser. When an end user launches a SaaS or private web app, several decisions are dynamically made to decide how best to serve this application. For details, see [Browser Security](#).

## 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 with Citrix Workspace™, 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 a native 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 <https://www.citrix.com/downloads/citrix-secure-access/>.
- For macOS, the client version (22.02.3 and later) can be downloaded from the App Store.

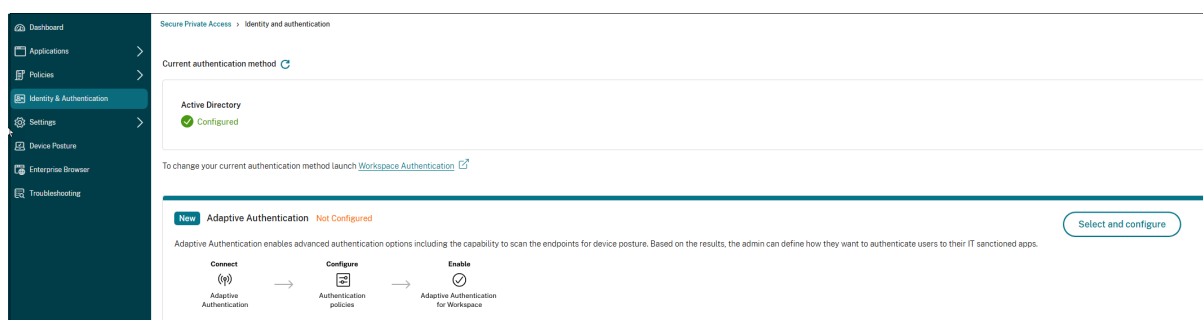
For details, see [Support for client-server apps](#).

## Set up Citrix Secure Private Access

Enable zero trust network access to SaaS apps, internal web apps, TCP, and UDP apps using the Secure Private Access admin console. This console includes configuration of Adaptive Authentication, applications including user subscription and adaptive access policies.

### Set up identity and authentication

Select the authentication method for the subscribers to log in to Citrix Workspace. Adaptive Authentication is a Citrix Cloud™ service that enables advanced authentication for customers and users logging in to Citrix Workspace.



For details, see [Set up identity and authentication](#).

### Enumerate and publish apps

After you have selected the authentication method, configure the Web, SaaS, or the TCP and UDP apps using the admin console. For details, see [Add and manage apps](#).

### Enable enhanced security controls

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.

- **Restrict clipboard access:** Disables cut/copy/paste operations between the app and the system clipboard.
- **Restrict printing:** Disables the ability to print from within the Citrix Enterprise Browser.
- **Restrict downloads:** Disables the user's ability to download from within the app.
- **Restrict uploads:** Disables the user's ability to upload within the app.
- **Display watermark:** Displays a watermark on the user's screen displaying the user name and IP address of the user's machine.



- **Restrict key logging:** Protects against key loggers. When a user tries to log on to the app using the user name and password, all the keys are encrypted on the key loggers. Also, all activities that the user performs on the app are protected against key logging. For example, if app protection policies are enabled for Office 365 and the user edit an Office 365 word document, all key strokes are encrypted on key loggers.
- **Restrict screen capture:** Disables the ability to capture the screens using any of the screen capture programs or apps. If a user tries to capture the screen, a blank screen is captured.

✓ Rule details

✓ Conditions

3 Actions

4 Summary

Step 3: Action

Action for HTTP/HTTPS apps \*

Allow access

Allow access with restrictions

Deny access

0 selected

View selected only

Search

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

Action for TCP/UDP apps \*

Allow access

Deny access

Cancel

Back

Next

For details, see [Configure an access policy](#).

**Enable Citrix Enterprise Browser for application launches**

Secure Private Access enables end users to launch their apps using the Citrix Enterprise Browser (CEB). CEB is a chromium-based browser integrated with the Citrix Workspace app that enables a seamless

© 1997–2025 Citrix Systems, Inc. All rights reserved.

29

and secure access experience to access web and SaaS apps within Citrix Enterprise Browser.

CEB can be configured as preferred browser or as your work browser for all the internally hosted web apps or SaaS apps with security policies. CEB allows users to open all configured SaaS/web app domains inside a secure and controlled environment.

**Enable Citrix Enterprise Browser** Administrators can use Global App Configuration service (GACS) to configure Citrix Enterprise Browser as the default browser to launch web and SaaS apps from the Citrix Workspace app.

#### Configuration through API:

To configure, here is an example JSON file to enable Citrix Enterprise Browser for all apps, by default:

```
1  "settings": [  
2      {  
3          "name": "open all apps in ceb",  
4          "value": "true"  
5      }  
6  ]  
7  
8
```

The default value is true.

#### Configuration through GUI:

Select the devices for which CEB must be made the default browser for the app launches.

**Open All SaaS Apps Through Citrix Enterprise Browser**  
This feature makes the Citrix Enterprise Browser the default browser to open SaaS apps without enhanced security controls from the Citrix Workspace app. If disabled, unprotected SaaS apps open through the native browser on the device.

<input type="checkbox"/> Android	This setting is not applicable.
<input type="checkbox"/> iOS	This setting is not applicable.
<input type="checkbox"/> Mac	<input type="checkbox"/>
<input checked="" type="checkbox"/> Windows	<input checked="" type="checkbox"/>
<input type="checkbox"/> HTML5	This setting is not applicable.
<input type="checkbox"/> Linux	This setting is not applicable.
<input type="checkbox"/> ChromeOS	This setting is not applicable.

For details, see [Manage Citrix Enterprise Browser through GACS](#).

### Configure tags for contextual access using Device Posture

After the device posture verification, the device is allowed to log in and the device is classified as compliant or non-compliant. This classification is made available as tags to the Secure Private Access service and are used to provide contextual access based on device posture.

1. Sign into Citrix Cloud.
2. On the Secure Private Access tile, click **Manage**.
3. Click **Access Policies** on the left navigation and then click **Create policy**.
4. Enter the policy name and description of the policy.
5. In **Applications**, select the app or set of apps on which this policy must be enforced.
6. Click **Create Rule** to create rules for the policy.
7. Enter the rule name and a brief description of the rule, and then click **Next**.
8. Select the users' conditions. The Users condition is a mandatory condition to be met to grant access to the applications for the users.
9. Click **+** to add device posture condition.
10. Select **Device posture check** and the logical expression from the drop-down menu.
11. Enter one of the following values in custom tags:

The screenshot shows the 'Step 2: Conditions' configuration page. On the left, a sidebar lists 'Rule details', 'Conditions', 'Actions', and 'Summary'. The 'Conditions' section is highlighted. The main area shows a 'User\*' condition with 'Matches any of' and 'Select a domain' dropdowns, and a 'Device posture check' condition with 'Matches any of' and 'Compliant, Non-Compliant' dropdowns. There are 'Cancel', 'Back', and 'Next' buttons at the bottom.

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

12. Click **Next**.
13. Select the actions that must be applied based on the condition evaluation, and then click **Next**.

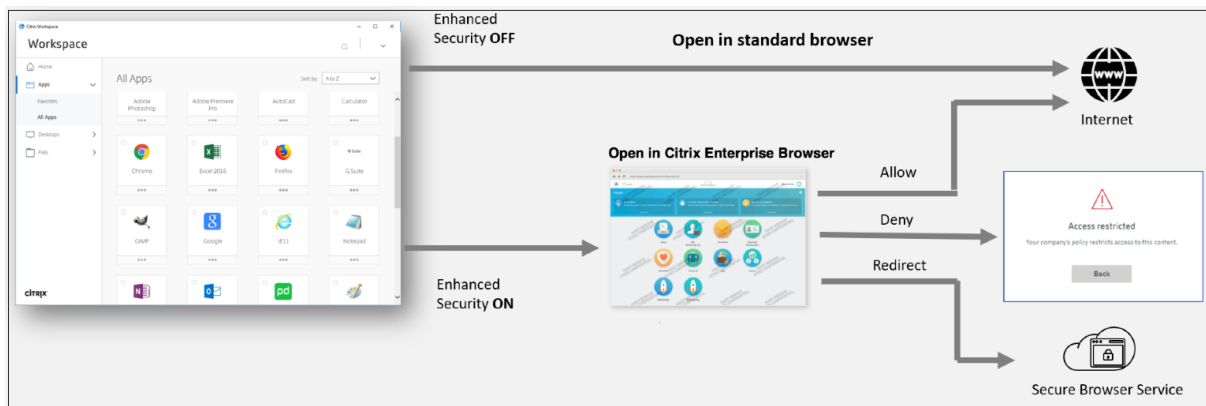
The Summary page displays the policy details.

14. Verify the details and click **Finish**.**Note:**

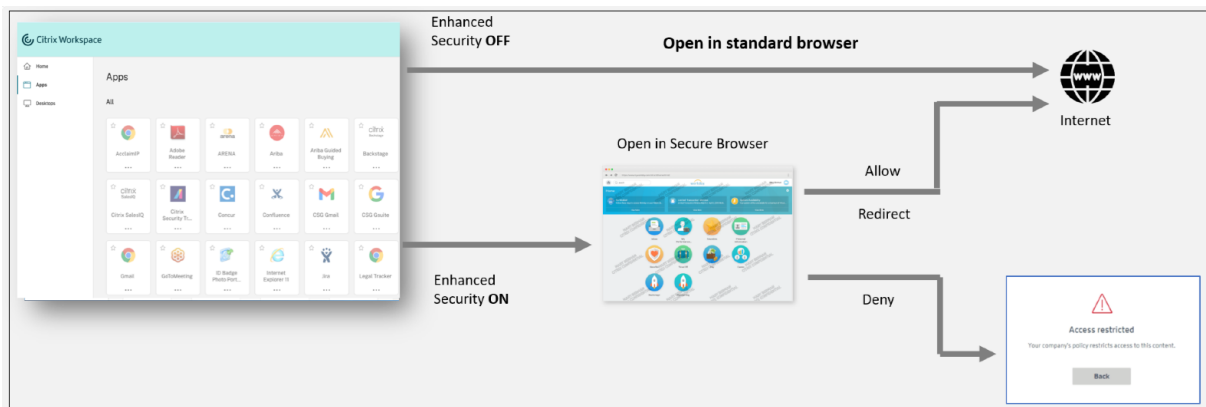
Any Secure Private Access application which is not tagged as compliant or non-compliant in the access policy is treated as the default application and is accessible on all the endpoints regardless of device posture.

**End-user experience**

The Citrix administrator has the power to extend security control with the help of Citrix Secure Private Access. Citrix Workspace app is an entry point to access all resources securely. End users can access virtual apps, desktops, SaaS apps, and files through Citrix Workspace app. With Citrix Secure Private Access, administrators can control how a SaaS Application is accessed by the end user via Citrix Workspace Experience web UI or native Citrix Workspace app client.



When the user launches the Workspace app on the endpoint, they see their applications, desktops, files, and SaaS apps. If a user clicks the SaaS application when enhanced security is disabled, the application opens in a standard browser which is locally installed. If the administrator has enabled enhanced security, then the SaaS apps open on the CEB within the Workspace app. Accessibility to hyperlinks within SaaS apps and web apps is controlled based on the unsanctioned websites policies. For details on Unsanctioned websites, see [Unsanctioned websites](#).



Similarly, with the Workspace Web portal, when enhanced security is disabled, SaaS applications are opened in a standard browser which is natively installed. When enhanced security is enabled, SaaS apps are opened in the secure Remote Browser. Users can access the websites within SaaS apps based on the unsanctioned websites policies. For details on Unsanctioned websites, see [Unsanctioned web-sites](#).

## Analytics 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 metrics are broadly classified into the following categories.

- Logging and troubleshooting
- Users
- Applications
- Access policies

For details, see [Dashboard](#).



Troubleshoot app issues

The Diagnostics Logs chart in the Secure Private Access dashboard provides visibility into the logs related to authentication, application launch, app enumeration, and device posture logs.

- **Info code:** Some log events such as failures have an associated info code. Clicking the info code redirects the users to the resolution steps or more information about that event.
- **Transaction ID:** The diagnostic logs also display a transaction ID that correlates all Secure Private Access logs for an access request. One app access request can have multiple logs generated, starting from authentication, then app enumeration within the workspace app, and then app access itself. All these events generate their own logs. Transaction ID is used to correlate all of these logs. You can filter the diagnostic logs using the transaction ID to find all logs related to a particular app access request.

For details, see [Troubleshoot Secure Private Access issues](#).

The table displays the following data for the last week:

Time	Category	App name	App type	App FQDN	Transaction ID	Mode of access	Info code	User name	Status
2024-10-31 20:16:28	N/A	N/A	SaaS	N/A	21196A21-F44B-46D8-A8CB-A8B...	N/A	N/A	aaa.local\ak2	Success
2024-10-31 20:16:28	N/A	N/A	SaaS	N/A	21196A21-F44B-46D8-A8CB-A8B...	N/A	N/A	aaa.local\ak2	Success
2024-10-31 20:15:31	App Access	N/A	UDP	173.16.255.1	38775602-C378-4197-B6FF-FB8...	N/A	0x10000409	aaa.local\ak2	Failure
2024-10-31 20:15:28	Login/Logoff	N/A	SaaS	N/A	A2968309-2E22-419C-A44F-82...	N/A	N/A	aaa.local\ak2	Success
2024-10-31 20:14:29	Login/Logoff	N/A	N/A	N/A	a956311d-0efb-4509-b6ed-40bb...	N/A	N/A	aaa.local\ak2	Success
2024-10-30 09:37:25	Login/Logoff	N/A	SaaS	N/A	15c5b70e-b0f2-1721-9678-0022...	N/A	0x1800d3	adsg8a4thridnb/565...	Failure
2024-10-30 09:37:13	Login/Logoff	N/A	N/A	N/A	72171b1-d9f2-4b77-9887-6a38a...	N/A	N/A	N/A	Success
2024-10-30 07:18:19	Login/Logoff	N/A	SaaS	N/A	01606a6d-905d-1721-9678-000d...	N/A	0x1800d3	adsg8a4thridnb/565...	Failure
2024-10-30 07:18:11	Login/Logoff	N/A	N/A	N/A	a8fb92ae-54b8-4521-a7bd-93fa...	N/A	N/A	N/A	Success
2024-10-29 13:32:38	Login/Logoff	N/A	SaaS	N/A	2d8a1285-9689-1720-9678-000d...	N/A	0x1800d3	adsg8a4thridnb/565...	Failure
2024-10-29 13:31:44	Login/Logoff	N/A	N/A	N/A	d199cf38-adff-4b11-a827-d4224...	N/A	N/A	N/A	Success

## 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 Citrix Enterprise Browser](#)
- [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](#)
- [Citrix Enterprise Browser](#)
- [Manage Citrix Enterprise Browser through GACS](#)
- [Admin-guided workflow for easy 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 Enterprise Browser: [About this release](#)
- Citrix Workspace: [What's new](#)
- Citrix DaaS: [What's new](#)
- Citrix Secure Access client [NetScaler Gateway Clients](#)



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

September 6, 2025

### Solution overview

This integrated solution from Citrix enables customers to use Google Chrome Enterprise Premium as the enterprise browser solution for secure access to private web apps and SaaS applications along with secure connectivity provided by Citrix Secure Private Access.

The integrated solution is comprised of the following components:

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

### Chrome Enterprise Premium advanced security features

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

- **Data loss prevention (DLP):** Implement granular controls and policies to prevent sensitive data from being leaked or accidentally shared.

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

For more information, see [Chrome Enterprise Premium overview](#).

## Prerequisites for the integrated solution

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

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

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

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

- Windows - 25.4.1.9 and later
- macOS - 25.03.1 and later
- **Create or recreate policies and security controls:** Policies and security controls configured in the Secure Private Access console only apply to Citrix Enterprise Browser. When Google Chrome is set as the enterprise browser, security controls must be configured as policies and rules in the Google Admin console.
  - Policies are configured in the **Google Admin console > Devices > Chrome > Settings**. These settings allow you to manage browser settings, such as block javascript and allow list of printers.
  - Rules are configured in **Google Admin console > Rules**. These rules are advanced settings related to DLP, such as adding a watermark, blocking the download of files with social security numbers, and URL filtering.

#### Notes:

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

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

- [Set Chrome Enterprise connector policies for Chrome Enterprise](#)
- [Data protection rules](#)

## ICA® Proxy settings in a SPA hybrid deployment

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

### Enable ICA Proxy for Workspace for Web:

#### Using the NetScaler GUI:

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

#### Note:

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

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

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

← Create NetScaler Gateway Session Profile

Name\*

Web\_Browser\_Profile ⓘ

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration	Client Experience	Security	<b>Published Applications</b>	Remote Desktop	PCoIP
-----------------------	-------------------	----------	-------------------------------	----------------	-------

Override Global

ICA Proxy\*

ON ▾ ☒ Override Global ⓘ

Web Interface Address

https://storefront.com ☒ Override Global ⓘ

Web Interface Address Type\*

IPv4 ▾

Web Interface Portal Mode

☐ Override Global

Single Sign-on Domain

MyDomain ☒ Override Global ⓘ

Citrix Receiver Home Page

☐ Override Global

Account Services Address

☐ Override Global

Create Close

For details, see [Create a session policy for web browser-based access](#).

### Using the CLI:

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

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

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

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

## Using the GUI:

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

For details, see [Configuring Authorization Policies](#).

The screenshot shows the 'Configure Authorization Policy' interface in the NetScaler ADC VPX (Freemium) GUI. The 'Name' field is set to 'ALLOW\_STOREFRONT'. The 'Action' dropdown is set to 'ALLOW'. The 'Expression' field is populated with the following text: `(HTTP.REQ.HOSTNAME.SET_TEXT_MODE(IGNORECASE).STARTSWITH("storefront.mydomain.com")) || CLIENT.SSLVPN.MODE.EQ("ICAPROXY") && HTTP.REQ.URL.SET_TEXT_MODE(IGNORECASE).STARTSWITH("/Citrix")`. The 'Advanced Policy' radio button is selected. At the bottom, there are 'OK' and 'Close' buttons.

## Using the CLI:

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

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

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

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

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

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

For more information, see [Google Directory sync](#).

## Set Google Chrome as your enterprise browser

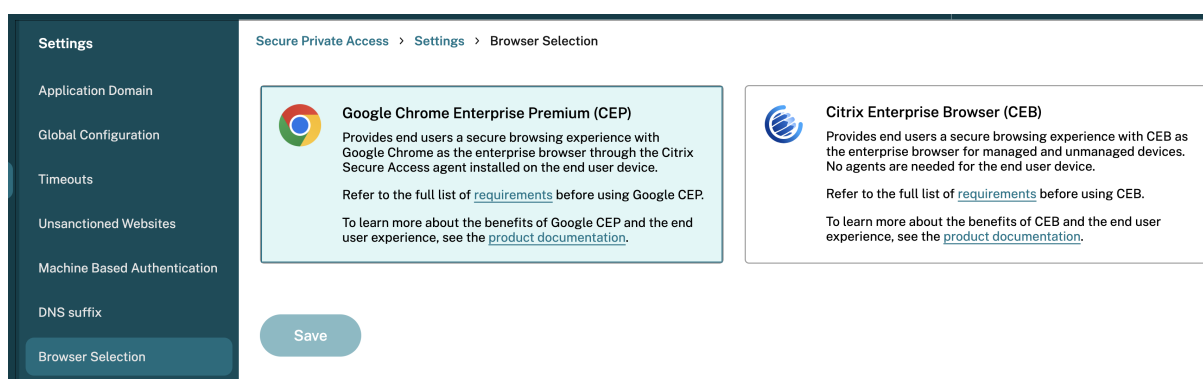
You can set Google Chrome as your default enterprise browser from the Secure Private Access admin console.

### Note:

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

Perform the following steps:

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



### Note:

- You can switch between Citrix Enterprise Browser and Google Chrome at any time.
- Global application configuration service (GACS): (Not applicable for hybrid deployments)  
When using Citrix Workspace with GACS, the **App Configuration > Citrix Enterprise Browser** setting in Workspace Configuration determines whether the target URL opens

in Citrix Enterprise Browser or Google Chrome. Ensure that the **Open All SaaS Apps Through Citrix Enterprise Browser** setting is disabled. For details on disabling this setting, see [Manage Citrix Enterprise Browser through Global App Configuration service](#). Also, Google Chrome must still be set as the default system browser as per the guidelines in [Prerequisites for the integrated solution](#).

- Disabling the enterprise browser setting in Workspace Configuration prevents the enforcement of security controls, causing all applications to launch in the device's native browser. Hence, Google Chrome must be set as the default system browser as per the guidelines in [Prerequisites for the integrated solution](#).

## Considerations prior to switching browser

Note the following prior to switching browsers:

- When you switch between Google Chrome and Citrix Enterprise Browser, you must log out of the Citrix Secure Access client and login again because switching between browsers does not terminate the Citrix Secure Access session. As a result, app launches might not work as intended.
- Chrome cannot enforce access to SaaS apps, because these apps are not tunneled through Citrix Secure Private access. To enable SaaS app access enforcement with Chrome and prevent the use of other browsers, route these apps through the Citrix Secure Private Access tunnel by changing the app routing type to **Internal**. For details, see [Steps to change the routing type or resource location](#).
- When Google Chrome is used as the enterprise browser, DLP policies and security controls configured in Citrix Secure Private Access are not enforced. Therefore, all necessary security policies must be recreated in the Google Admin console to maintain consistent data protection. For details, see [Prerequisites for the integrated solution](#).
- The URL filtering (Unsanctioned websites) feature is not supported when using Chrome as the enterprise browser. Any URL filtering policies must be recreated within the Google Admin console.

## Citrix Secure Private Access - Supported deployment modes

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

- **Citrix Secure Private Access service:** This deployment mode utilizes the fully cloud-managed Citrix Secure Private Access service. All components, including the control plane and gateway infrastructure, are hosted and managed by Citrix. For more information, see [Citrix Secure Private Access](#).



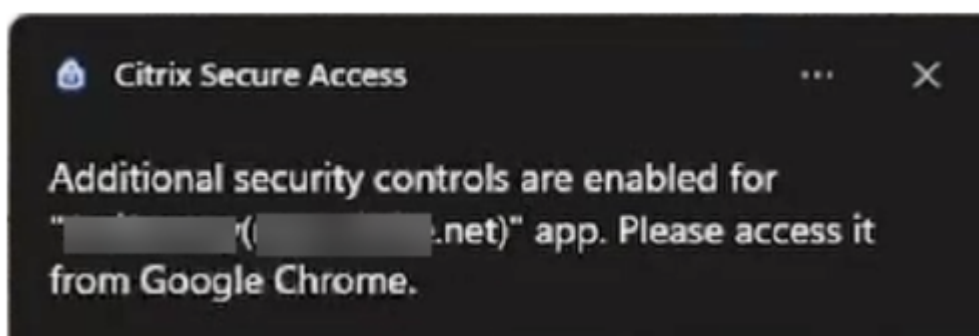
- **Citrix Secure Private Access hybrid deployment:** This deployment allows customers to implement a Zero Trust Network Access (ZTNA) solution using on-premises StoreFront and NetScaler Gateway components and use the Citrix Cloud for managing the configuration, administration, and monitoring functions.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

## End user experience

### Google Chrome as your enterprise browser

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

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



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

### Citrix Enterprise Browser as your enterprise browser

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

- **Launch apps from Citrix Workspace app:**

- The application is launched using the Citrix Enterprise Browser.
- Any security controls that have been enabled for the application are enforced accordingly.

- **Launch apps from Citrix Secure Access:**

- After the connection is established, open Chrome and launch the same app.
- Any security controls that have been enabled for the app are enforced accordingly.

**Note:**

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

## End-user application access methods

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

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

**Legal**

Chrome Enterprise Premium is provided by Google LLC and your use is subject to [Google’s Acceptable Use Policy](#) and [Service Specific Terms](#).

**Get started with Citrix Secure Private Access**

September 6, 2025

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 Mac 10.11 and above.

**Browser support:** Access workspaces using the latest versions of Edge, Chrome, Firefox, or Safari.

**Citrix Workspace™ support:** Access workspaces using Citrix Workspace for any of the desktop platforms (Windows, Mac).

**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	Workspace Experience/Workspace App
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

---

Functionality	Service/Component providing the functionality
Secure browsing	Remote Browser Isolation service
Visibility into website access and risky behavior	Citrix Analytics

---

## Get started with Citrix Secure Private Access service

1. Sign up for Citrix Cloud.
2. Request for the Secure Private Access service entitlement.
3. Post entitlement, Secure Private Access service is provisioned under **My Services**.
4. Access the Secure Private Access service UI.

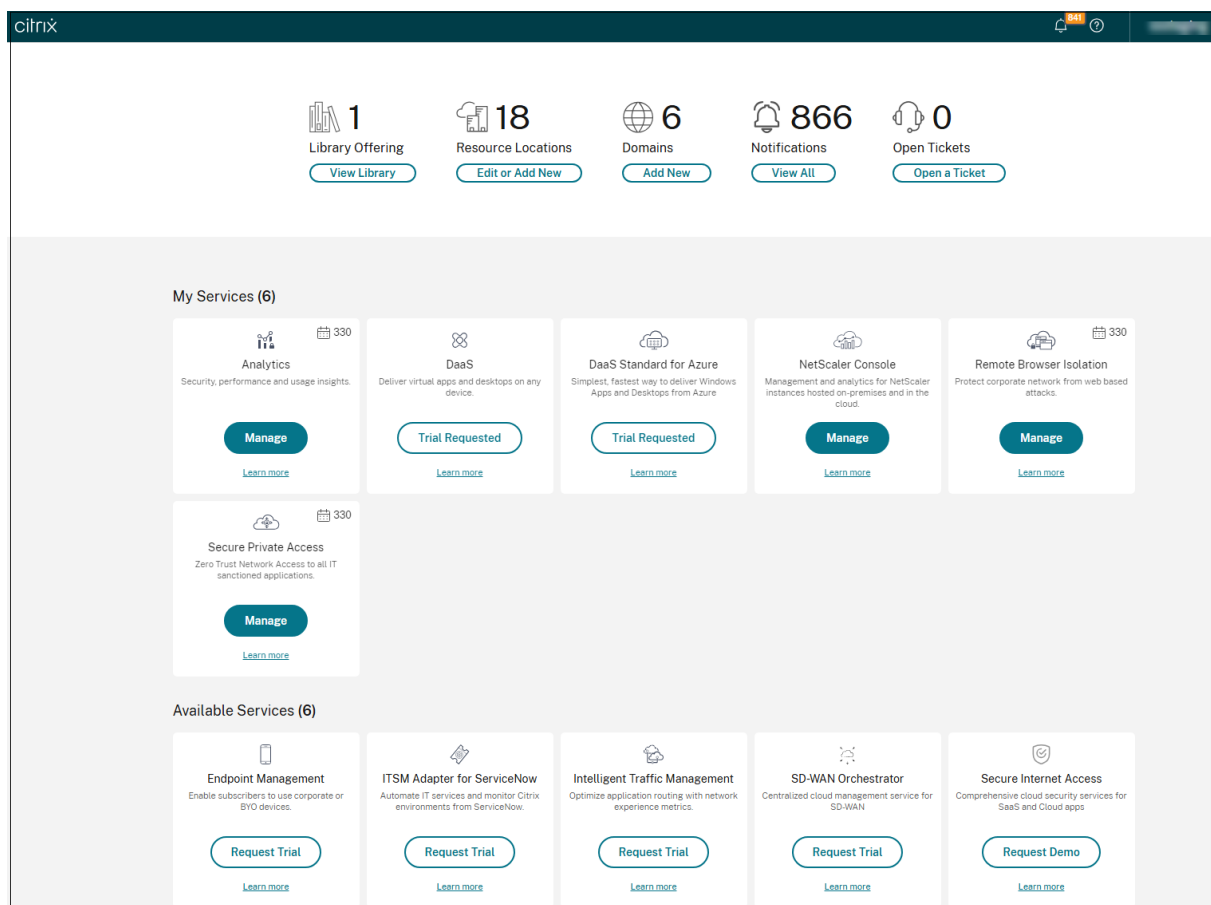
### Step 1: Sign Up for Citrix Cloud

To start using the Secure Private Access service, you must first create a Citrix Cloud account or join an existing one that is created by someone else in your company. For detailed processes and instructions on how to proceed, see [Signing Up for Citrix Cloud](#).

### Step 2: Request for the Secure Private Access service entitlement

To request for the Secure Private Access service entitlement, on the **Citrix Cloud** screen, under the **Available Services** section, click the **Request Trial** tab present in the Secure Private Access service tile.

For license details, see <https://www.citrix.com/buy/licensing/product.html>.



### Step 3: **Post entitlement, Secure Private Access service is provisioned under My Services**

After you receive the Secure Private Access service entitlement, the Secure Private Access service tile moves to **My Services** section.

### Step 4: **Access the Secure Private Access service UI**

Click the **Manage** tab on the tile to access the Secure Private Access service UI.

### Step 5: **Select the deployment type**

Select **Cloud-Native Service Architecture**

#### **Note:**

- For your end users to use the workspace and access the apps, they must download and use the Citrix Workspace app or use the workspace URL. You must have a few SaaS apps published to your workspace to test the Citrix Secure Private Access solution. The Workspace app can be downloaded from <https://www.citrix.com/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](#).

- You can add only one Workspace account.

## Secure Private Access service deployment models

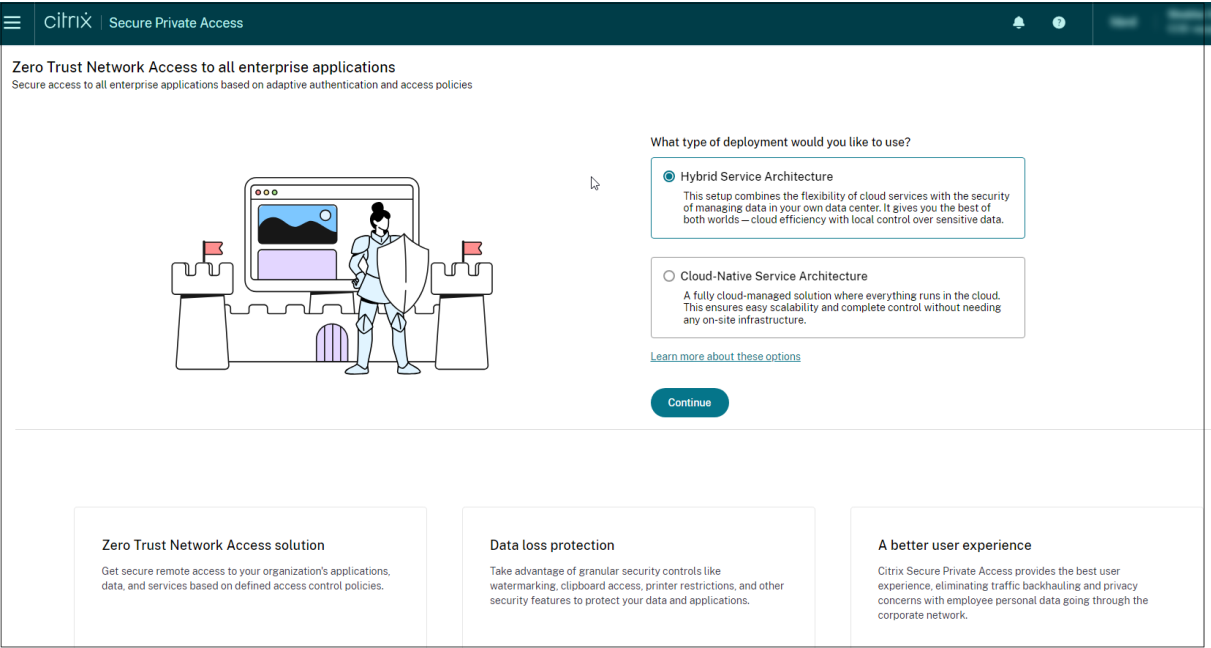
September 6, 2025

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.
2. Click **Manage** in the **Secure Private Access** service tile.
3. Choose **Hybrid Service Architecture** or **Cloud Native Service Architecture** as per your requirement.



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

September 6, 2025

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
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

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

## Secure Private Access onboarding and set up

September 6, 2025

The Secure Private Access service offers a streamlined admin experience that simplifies the process of configuring Zero Trust Network Access. This enhanced feature provides a step-by-step guide to set up access for a range of apps, including SaaS apps, internal web apps, and TCP apps. The admin console allows administrators to configure device posture scans, create apps, and access policies all within a single, unified interface.

The high-level steps to onboard and setup Secure Private Access include the following:

1. [Create Device Posture scans.](#)
2. [Add apps for your users.](#)
3. [Assigns permissions for app access by creating the required access policies.](#)
4. [Review the app configuration.](#)

### Access the Secure Private Access admin-guided workflow wizard

Perform the following steps to access the wizard.



1. Log in to Citrix Cloud™ and then click **Secure Private Access**.
2. Select **Fully Cloud-delivered Service architecture** and then click **Continue**.

**Zero Trust Network Access to all enterprise applications**  
Secure access to all enterprise applications based on adaptive authentication and access policies

What type of deployment would you like to use?

☐ Hybrid Service architecture  
This deployment mode combines the flexibility of cloud services for management and monitoring with the security of routing data traffic through your own premises. It gives you the best of both worlds – simplicity of the cloud coupled with control over traversal of application data traffic.

☒ Fully Cloud-delivered Service architecture  
A fully cloud-managed solution where everything including management, monitoring, control plane and data traffic runs in the cloud. This ensures you can fully leverage the scalability and efficiency of the cloud for your ZTNA solution without needing any on-site infrastructure.

[Learn more about these options](#)

**Continue**

**Zero Trust Network Access solution**  
Get secure remote access to your organization's applications, data, and services based on defined access control policies.

**Data loss protection**  
Take advantage of granular security controls like watermarking, clipboard access, printer restrictions, and other security features to protect your data and applications.

**A better user experience**  
Citrix Secure Private Access provides the best user experience, eliminating traffic backhauling and privacy concerns with employee personal data going through the corporate network.

## Create device posture scans

### Note:

Configuring device posture is optional for onboarding and can be completed later, during the post-deployment phase.

The device posture scans ensure that only compliant subscriber devices can access your Workspace services. The Device Posture checks determine if devices are compliant or non-compliant and then use this information to provide adaptive access to all types of apps and desktops.

1. In the **Device Posture** page, click **Next**.
2. (Optional) Connect to any third-party solutions integrated with the Device Posture service. For details, see [Third-party integration with device posture](#).
3. Click **Next** and then click **Create device policy**. For details, see [Configure Device Posture policies](#).
4. After creating the device posture policy, click **Next** in the **Step 1: Device Posture** page.

**Zero Trust Network Access to all enterprise applications**  
Secure access to all enterprise applications based on adaptive authentication and access policies

1

Device Posture

2

Applications

3

Access Policies

4

Review

**Step 1: Device Posture**  
Create device posture scans and enable optional integrations to enforce application access control policies.

**About Device Posture**  
Use Device Posture to only allow trustworthy subscriber devices that comply with your established Device Posture policies to access your Workspace services.

The Device Posture feature ensures that Citrix DaaS and Secure Private Access subscriber devices accessing corporate resources through Workspace can be trusted and are secure. Device Posture tries to accomplish zero trust by checking subscriber devices for multiple conditions (OS and browser version, disk encryption, antivirus status, etc) to determine if the devices are Compliant or Non-Compliant. DaaS and Secure Private Access administrators can then use this information to provide adaptive access to all types of apps and desktops, as well as contextual access/SmartAccess services.

When enabled Device Posture will install an app on subscriber devices to begin scanning subscriber devices to determine security risk.

[Learn more about Device Posture](#)

**How Device Posture works**

The device posture policy is a combination of rules that a device must meet to gain access to the resources. A set of rules make up a policy and a set of policies make up the entire device posture.

Policies are evaluated in priority order until a policy is applied to the device. If no policies apply, the device is denied access or classified as non-compliant. You can specify access to non-compliant devices in DaaS or SPA.

Device postures are defined independently for each platform

Integrate with third party services.

Microsoft

CROWDSTRIKE

If all of the following conditions are met...

AND

AND

Then this policy can be used to classify the device as...

☒ Compliant

☐ Non-compliant

☐ Deny access

1

2

3

4

OR

OR

OR

Deny access or default configured behavior

Enable Device Posture once all policies are defined and ready to be checked by devices.

Device Posture is enabled ☒

Next Cancel

**Note:**

The authentication mechanism for Secure Private Access is inherited from the identity provider that is connected in the **Workspace configuration > Authentication** tab.

**Add and manage apps**

For the first-time users, the **Applications** landing page does not display any apps. Add an app by clicking **Add an app**. You can add SaaS apps, Web apps, and TCP/UDP apps from this page. To add an app, click **Add an app**.



For details on adding apps, see the following topics.

- **Add an Enterprise 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](#)
- **Launch an app**
  - [Launch a configured app - end user workflow](#)
- **Role-based access to admins**
  - [Role-based access control in Secure Private Access](#)

## Configure access policies

### Note:

Setting up access policies is not necessary to complete the onboarding process and can be defined later.

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

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.

In addition, you can enable restricted access to the apps by enabling security restrictions. For details, see [Available access restrictions](#).

For more information on these restrictions, see [Available access restrictions](#).

1. On the navigation pane, click **Access Policies** and then click **Create policy**.

For the first-time users, the **Access Policies** landing page does not display any policies. Once you create a policy, you can see it listed here.

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.

**Step 3: Access Policies**  
Create policies to enforce application access rules based on user context.

**Create policy**  
Create a policy to enforce application access rules based on application context.

Policy name \*

policy-test

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

10000ft Demo Test

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
----------------	-----------	------------	-----------	-------------	--------	--------

Showing 1-0 of 0 items Page 1 of 0 10 rows

☐ Enable policy on save

Save Cancel

5. Enter the rule name and a brief description of the rule, and then click **Next**.

**Step 1: Rule details**

Selected applications for this rule

DNS Suffix Testing BitBucket

Rule name \*

Allow with restrictions

Rule description

Enable access with restrictions

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

**Create new rule**

Step 2: Conditions

**Rule Scope**

Select the rule scope from the following options.

☒ **User**  
Applicable to both HTTP/HTTPS and TCP/UDP apps

☐ **Machine**  
Applicable to only TCP/UDP apps

User\*

Matches any of ▼ \* Ad ▼ aaa.local ▼

ak1-ak1@gmail.com 🔍

+ Add condition

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

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

- **Desktop or Mobile device** –Select the device for which you want to enable access to the apps.
- **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.
- **User risk score** –Select the risk score categories based on which the users are provided access to the apps.
- **Workspace URL** - Admins can specify filters based on the fully qualified domain name corresponding to the Workspace.

- **Matches any of** - Allow access only when the incoming user connection meets any of the configured Workspace URLs.
- **Matches all of** - Allows access only when the incoming user connection meets all of the configured Workspace URLs.

8. Click **Next**.

9. Select the actions that must be applied based on the condition evaluation.

- For HTTP/HTTPS apps, select the following:

- **Allow access**
- **Allow access with restrictions**
- **Deny access**

**Note:**

If you select **Allow access with restrictions**, then you must select the restrictions that you want to enforce on the apps. For details on the restrictions, see [Available access restrictions](#). You can also specify if you want the app to open in a remote browser or in Citrix Secure Browser.

- For TCP/UDP access, select the following:

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

**Step 3: Action**

**Action for HTTP/HTTPS apps \***

☒ Allow access

☐ Allow access with restrictions

☐ Deny access

**Action for TCP/UDP apps \***

☒ Allow access

☐ Deny access

**Routing exceptions**

Changing the routing type or resource location for these domains will create a routing exception. Routing exceptions will to all users in this access policy only. [Learn more](#)

Search for a domain

FQDN/IP	Routing Type	Resource Location	Actions
ak1.mgmt.netScalerGatewaydev...	Internal	AAA-ConnApp	
pki-goog.l.google.com	Internal	AAA-ConnApp	
*.ak1.mgmt.netScalerGatewa...	Internal	AAA-ConnApp	
ven01955.service-now.com	External		
*.service-now.com	External		

**Change routing details**

Changing the routing type or resource location for this domain will create a routing exception. This routing exception will apply to all users in the access policy.

URL \*  
ak1.mgmt.netScalerGatewaydev.net

Routing type \*  
Internal

Resource location \*  
AAA-ConnApp

10. (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.

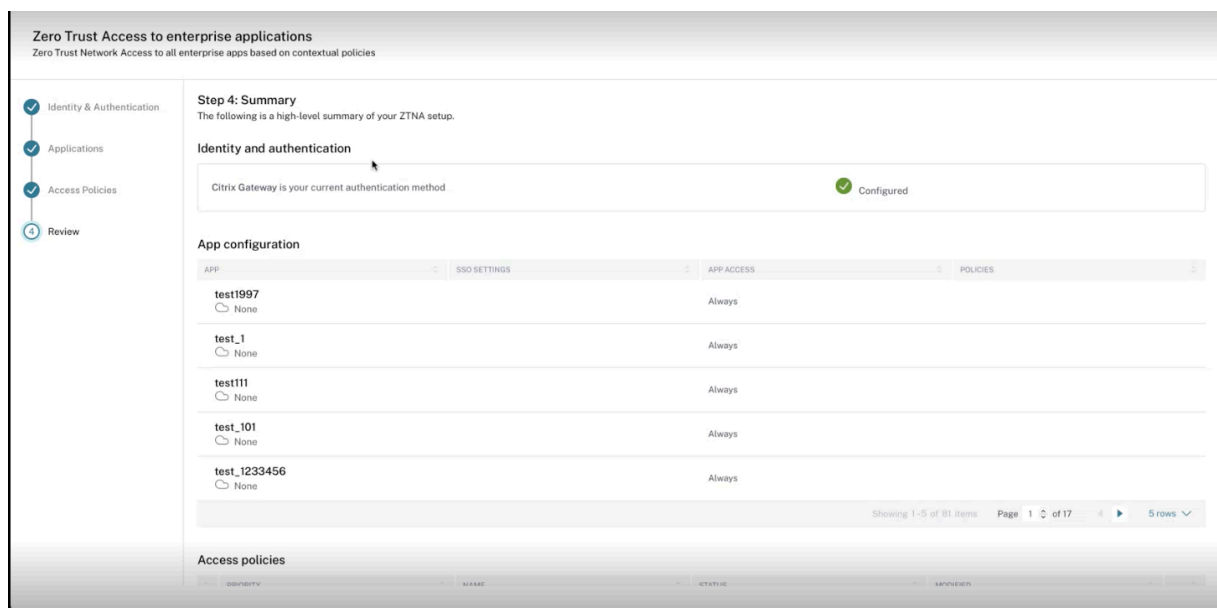
For more information about contextual routing, see [Context-based app routing and resource locations selection](#).

11. Click **Next**. The **Summary** page displays the policy details.
12. You can verify the details and click **Finish**.

## Review the configuration

The **Review** page provides a comprehensive overview of the end user's configuration, including the authentication mechanism used for their access. This authentication mechanism is not configured independently for the Secure Private Access service. It is inherited from the identity provider that is connected in the **Workspace configuration > Authentication** tab. You can click the **Identity and Access Management > Authentication** link to view the list of identity providers available for a user.



**Important:**

- After you have completed the configuration using the wizard, you can modify the configuration of a section by directly going to that section. You do not have to follow the sequence.
- If you delete all the configured apps or the policies, you must add them again.

**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.

**Note:**

If none of the rules are evaluated, then the app is not enumerated to the users.

## Available access restrictions options

When you select the action **Allow access with restrictions**, you must select at least one of the security restrictions. These security restrictions are predefined in the system. Admins cannot modify or add other combinations. The following security restrictions can be enabled for the app. For details, see [Available access restrictions options](#).

## Apps configuration and management

September 6, 2025

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](#)

## Support for Enterprise web apps

September 6, 2025

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.

Web apps can be accessed using Citrix Workspace™ using the Secure Private Access service. The Secure Private Access service coupled with Citrix Workspace provides a unified user experience for the configured Web apps, SaaS apps, configured virtual apps, or any other workspace resources.

## System requirements

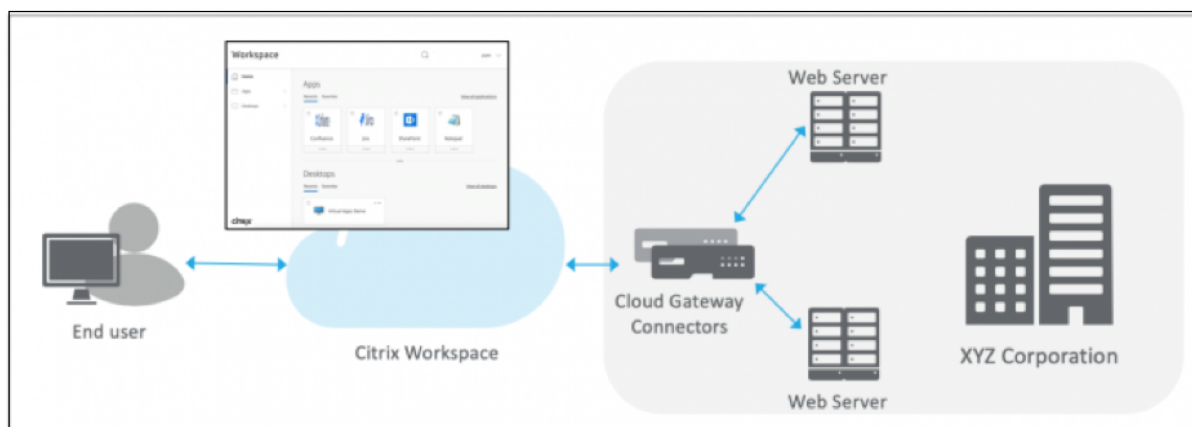
**Connector Appliance** - Use the Connector Appliance with the Citrix Secure Private Access service to support VPN-less access to the Enterprise Web apps in the customers' data center. For details, see [Connector Appliance for Secure Private Access](#).

## 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 Workspace using a VPN-less connection.

The following figure illustrates accessing web applications using Citrix Workspace.



## Configure a Web app

Configuring a Web app involves the following high-level steps.

1. [Configure the application and define application routing details](#)
2. [Set the preferred sign-on method](#)

## Configure application details

1. On the **Secure Private Access** tile, click **Manage**.
2. On the Secure Private Access landing page, click **Continue** and then click **Add an app**.

### Note:

The **Continue** button appears only for the first time when you use the wizard. Subsequently, you can directly navigate to the **Applications** page and then click **Add an app**.

3. Select the app that you want to add or click **Skip**.
4. In **Where is the application location?**, select the location.
5. Enter the following details in the **App Details** section and click **Next**.

**Add an app**

To add an app, complete the steps below.

Choose a template

**App Details**

Where is the application located? \*

☐ Outside my corporate network

☒ Inside my corporate network

App type \*

HTTP/HTTPS

App name \*

docs-portal

App description

App icon

[Change icon](#) (128 KB max, PNG) [Use default icon](#)

☐ Do not display application icon in Workspace app

☐ Add application to favorites in Workspace app

☐ Allow user to remove from favorites

☐ Do not allow user to remove from favorites

App category ?

Ex.: Category\SubCategory\SubCategory

☐ Agentless Access

Enable direct browser-based access to internal web applications.

- **App type** –Select the app type. You can select from **HTTP/ HTTPS** or **UDP/TCP** apps.
- **App name** –Name of the application.

- **App description** - A brief description of the app. This description is displayed to your users in the workspace.
- **App category** - Add the category and the subcategory name (if applicable) under which the app that you're publishing must appear in the Citrix Workspace UI. You can add a new category for each app or use existing categories from the Citrix Workspace UI. Once you specify a category for a web or a SaaS app, the app shows up in the Workspace UI under the specific category.
  - The category/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 Citrix Workspace UI and the category name entered in the **App category** field, the category gets listed as a new category.

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

- **App icon** –Click **Change icon** to change the app icon. The icon file size must be 128x128 pixels. 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](#).

- **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 these apps must be removed manually from the favorites list in Citrix Workspace. The apps aren’t auto deleted from the Workspace app 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.

**App Connectivity**

URL \*

Routing Type \*

Primary Resource Location \* ⓘ

Secondary Resource Location (optional) ⓘ

2 connectors are available [Refresh](#)  
 1 connector is available [Refresh](#)  
 ⚠ Add another for high availability [Add](#)

Related Domains

Related Domains	Routing Type	Primary Resource Location	Available Connectors	Actions
*.docs.citrix.com ⚠	Internal via Connector	AAA RL 01	2	<a href="#">Edit</a> <a href="#">Delete</a>

Showing 1-1 of 1 items Page 1 of 1 5 rows ▾

☐ Maintain consistent connection ⓘ  
 Use the same connector appliance for the entire length of the session while accessing the application.

^ Single Sign On

- **Routing Type** - Select one of the following:
  - **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 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.



## Edit related domain

Domain

\*.wikipedia.org


Routing Type \*

Internal via Connector

Primary Resource Location \* ?

aaa.local RL2


1 connector is available [Refresh](#)

 Add another for high availability [Add](#)

Secondary Resource Location (optional) ?

aaa.local

1 connector is available [Refresh](#)

 Add another for high availability [Add](#)

**Note:**

Setting the backup resource location and using the **First Available** option feature is currently in Preview.

- **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.

## Set the preferred sign-on method

1. 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.

Single Sign On

Your Workspace authentication is currently set to use

Which single sign on type would you like to use for your Web app setup? [Help me choose](#)

Kerberos

Basic SSO

Kerberos

Form-Based

SAML

Don't use SSO

NEXT

Connects on my Gateway Connectors (?)

- **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**.

Which single sign on type would you like to use for your Web app setup? ?

Form-Based ✓

Action URL \* ?

/default.aspx?ReturnURL=/\_layouts/Authentication/

Logon URL \* ?

/\_forms/default.aspx

Username Format \* ?

User Name ✓

Username Form Field \* ?

ct100\$PlaceholderMain\$SignInControl\$UserName


Password Form Field \* ?


ct100\$PlaceholderMain\$SignInControl\$Password

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.**


Which single sign on type would you like to use for your Web app setup? 


SAML 

**SAML information**


This form generates the XML needed for the application's SAML request.

**Sign Assertion** \* 


Assertion 


**Assertion URL** \* 


`https://sharepoint.onelogin/saml_assertion`


**Relay State** 


`&RelayState = /apex/SSO_Redirect?param1=value1`


**Audience** 

**Name ID Format** \* 

Email Address 

**Name ID** \* 

User Name 

☒ Launch the app using the specified URL (SP initiated) 

- **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.
2. In **Advanced attributes (optional)** add additional information about the user that is sent to the application for access control decisions.
  3. Download the metadata file by clicking the link under **SAML Metadata**. Use the downloaded metadata file to configure SSO on the SaaS apps server.

**Note:**

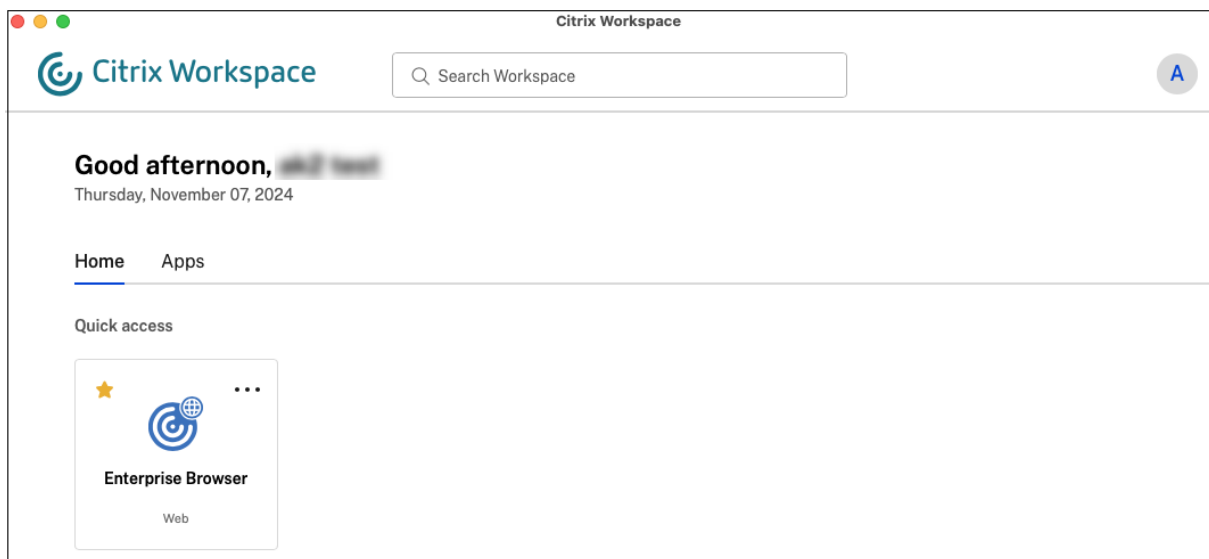
- You can copy the SSO login URL under **Login URL** and use this URL when configuring SSO on the SaaS apps server.
- You can also download the certificate from the **Certificate** list and use the certificate when configuring SSO on the SaaS apps server.

4. 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**

When you publish a Web or a SaaS app from the Secure Private Access service and if that app isn't hidden, the Citrix Enterprise Browser™ app shows up automatically in the Citrix Workspace UI. In addition, the Citrix Enterprise Browser is also added as a favorite app, by default. End users can launch the workspace browser without a URL and access internal websites using the workspace browsers.

**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](#).
- For the list of available access restrictions, see [Access restriction options](#).

## Support for SaaS apps

September 6, 2025

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.

SaaS apps can be accessed using Citrix Workspace™ using the Secure Private Access service. The Secure Private Access service coupled with Citrix Workspace provides a unified user experience for the configured SaaS apps, configured virtual apps, or any other workspace resources.

SaaS app delivery using the Secure Private Access service provides you an easy, secure, robust, and scalable solution to manage the apps. SaaS apps delivered on the cloud have the following benefits:

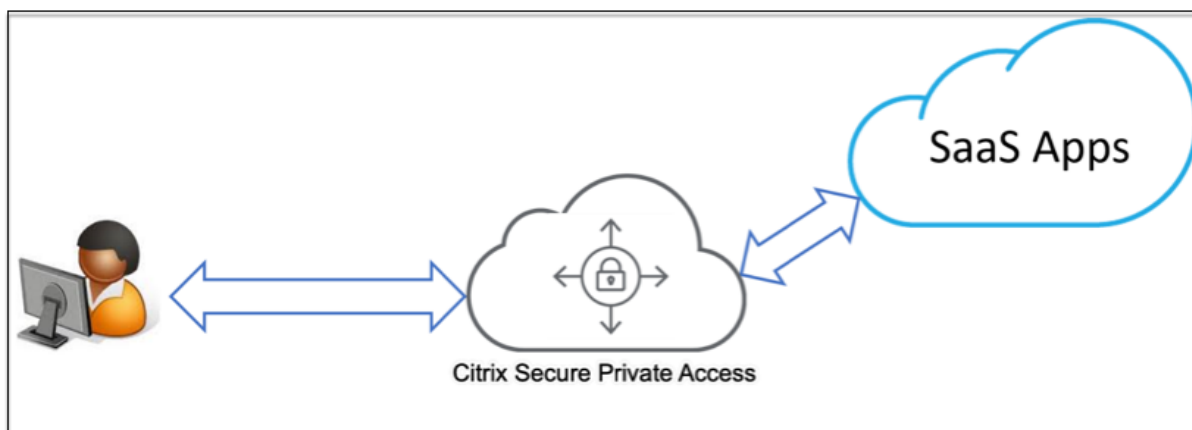
- **Simple configuration** – Easy to operate, update, and consume.
- **Single sign-on** – Hassle free logon with Single sign-on.
- **Standard template for different apps** – Template based configuration of popular apps.

## 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 service URL to the users to access Citrix Workspace.
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 Citrix Workspace for a unified user experience.



## Configure a SaaS app

Configuring a SaaS app involves the following high-level steps.

1. [Configure the application and define application routing details](#)
2. [Set the preferred sign-on method](#)

### Note:

- SaaS apps configuration on the Secure Private Access service is simplified by provisioning a template list for popular SaaS apps. The SaaS app to be configured can be selected from the list. The template pre-fills much of the information required for configuring applications. However, the information specific to the customer must still be provided. For details, see [SaaS apps configuration using a template](#).

- For the list of supported SaaS apps and guidance on app server specific configuration, see [SaaS app server specific configuration](#).

## Configure application details

1. On the **Secure Private Access** tile, click **Manage**.
2. Click **Continue** and then click **Add an app**.

### Note:

- The **Continue** button appears only for the first time when you use the wizard. Subsequently, you can directly navigate to the **Applications** page and then click **Add an app**.
- You can add a SaaS app manually by entering the app details or select an app template that is available for a list of popular SaaS apps. The template pre-fills much of the information required for configuring applications. However, the information specific to the customer must still be provided. For SaaS app configuration template details, see [SaaS app server specific configuration](#).

3. Configure the app.

- To enter the app details manually, click **Skip**.
- To configure the app using a template, click **Next**.

The **Outside my corporate network** is enabled by default for a SaaS app.

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

App Details

Where is the application located? \*

☒ Outside my corporate network

☐ Inside my corporate network

---

App name \*

Aha

App description

Product roadmap and marketing planning tool to build products and launch campaigns.

App category ⓘ

Ex.: Category\SubCategory\SubCategory

App icon

[Change icon](#) [Use default icon](#)  
(128 KB max, PNG)

☐ Do not display application icon in Workspace app

☐ Add application to favorites in Workspace app

☐ Allow user to remove from favorites

☐ Do not allow user to remove from favorites



- **App name** –Name of the application.
- **App description** - A brief description of the app. This description is displayed to your users in the workspace.
- **App category** - Add the category and the subcategory name (if applicable) under which the app that you're publishing must appear in the Citrix Workspace UI. You can add a new category for each app or use existing categories from the Citrix Workspace UI. Once you specify a category for a web or a SaaS app, the app shows up in the Workspace UI under the specific category.
  - The category/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 Citrix Workspace UI and the category name entered in the **App category** field, the category gets listed as a new category.

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

- **App icon** –Click **Change icon** to change the app icon. The icon file size must be 128x128 pixels. 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](https://salesforceformyorg.salesforce.com/?so=123754) 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](#).

- **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 these apps must be removed manually from the favorites list in Citrix Workspace. The apps aren't auto deleted from the Workspace app 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](#).

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.

**App Connectivity**

URL \*

Routing Type \*

Primary Resource Location \* ⓘ

Secondary Resource Location (optional) ⓘ

2 connectors are available [Refresh](#)

1 connector is available [Refresh](#)

⚠ Add another for high availability [Add](#)

Related Domains

Related Domains	Routing Type	Primary Resource Location	Available Connectors	Actions
*.aha.io	External			<a href="#">Edit</a> <a href="#">Delete</a>

Showing 1-1 of 1 items Page 1 of 1 5 rows

☐ Maintain consistent connection ⓘ  
Use the same connector appliance for the entire length of the session while accessing the application.

- **Routing Type** - Select one of the following:
  - **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 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.

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

## Edit related domain

Domain

\*.wikipedia.org


Routing Type \*

Internal via Connector

Primary Resource Location \* ?

aaa.local RL2


1 connector is available [Refresh](#)

 Add another for high availability [Add](#)

Secondary Resource Location (optional) ?

aaa.local

1 connector is available [Refresh](#)

 Add another for high availability [Add](#)

**Note:**

Setting the backup resource location and using the **First Available** option feature is

currently in Preview.

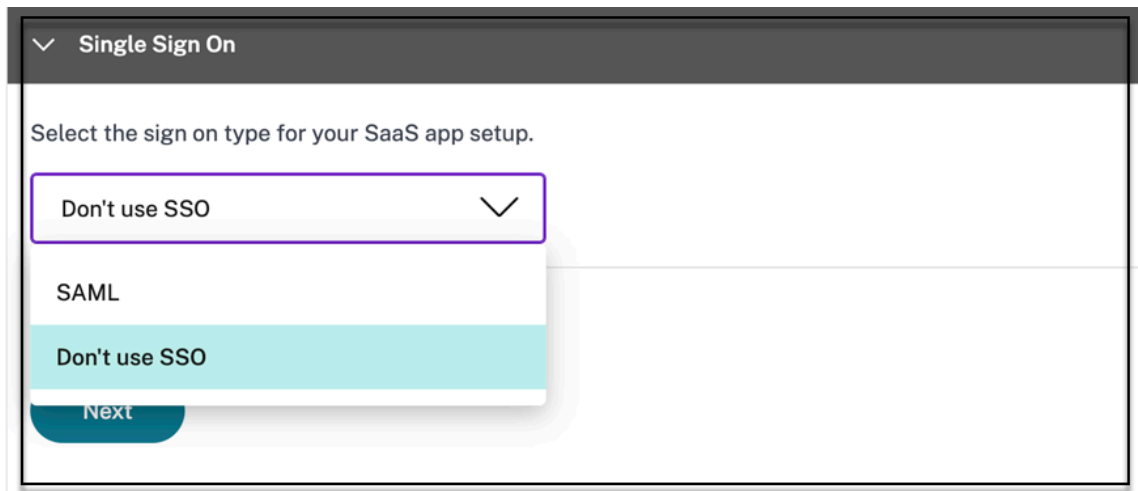
- **Maintain consistent connection** - Select this checkbox to enable consistent connection to the same Connector Appliance. For details about consistent connections, see [Maintain consistent connections](#).

**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.

### Set a preferred sign-on method

1. 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.
2. In **Advanced attributes (optional)**, add additional information about the user that is sent to the application for access control decisions.

Single Sign On

Select the sign on type for your SaaS app setup.

SAML

SAML

Don't use SSO

This form generates the XML needed for the application's SAML request.

Sign Assertion \*

Assertion

Assertion URL \*

https://login.microsoftonline.com/login.srf

Relay State

https://login.microsoftonline.com/login.srf?wa=wsignin1%2E0&rver=6%2E1

Audience

urn:federation:MicrosoftOnline

Name ID Format \*

Persistent

Name ID \*

Active Directory GUID

Advanced attributes (optional)

An attribute is additional information about the user that is sent to the application for access control decisions. Make sure these values are consistent with the settings in the SaaS vendor.

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

**Note:**

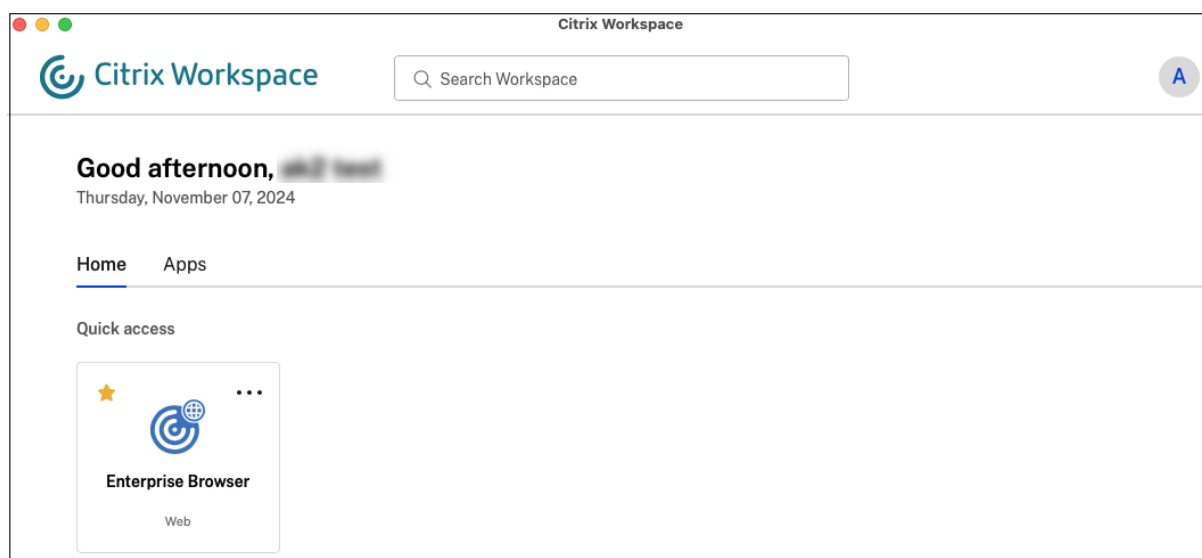
- You can copy the SSO login URL under **Login URL** and use this URL when configuring SSO on the SaaS apps server.
- You can also download the certificate from the **Certificate** list and use the certificate when configuring SSO on the SaaS apps server.

**4. 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**

When you publish a Web or a SaaS app from the Secure Private Access service and if that app isn't hidden, the Citrix Enterprise Browser™ app shows up automatically in the Citrix Workspace UI. In addition, the Citrix Enterprise Browser is also added as a favorite app, by default. End users can launch the workspace browser without a URL and access internal websites using the workspace browsers.



## # SaaS apps configuration using a template

SaaS apps configuration with single sign-on on the Secure Private Access service is simplified by provisioning a template list for popular SaaS apps. The SaaS app to be configured can be selected from the list.

The template pre-fills much of the information required for configuring applications. However, the information specific to the customer must still be provided.

**Note:**

The following section has the steps to be performed on the Secure Private Access service for configuring and publishing an app using a template. The configuration steps to be performed on the app server is presented in the subsequent section.

## Configure and publish apps using a template

On the **Secure Private Access** tile, click **Manage**.

1. Click **Continue** and then click **Add an app**.

**Note:**

The **Continue** button appears only for the first time that you use the wizard. In the subsequent usages, you can directly navigate to the **Applications** page and then click **Add an app**.

2. Select the app that you want to configure in the **Choose a Template** list and click **Next**.
3. Enter the following details in the **App Details** section and click **Save**.

**App name** –Name of the application.

**App description** - A brief description of the app. This description that you enter here is displayed to your users in the workspace.

**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 user is redirected to this URL if;

- SSO fails or

- **Don't use SSO** option is selected.

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

For example, if you are 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 have 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.



**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.

App details

Where is the application?

☒ Outside my corporate network

☐ Inside my corporate network

Tell us a little more about this application.

Name •  
Aha

Customer domain name  
Enter domain name to be used in URL

URL •  
https://<your-organization>.aha.io

Related Domains •  
\*.aha.io

[Add another related domain](#)

**Aha!** [Change icon](#) (128 kb max, PNG)

Description  
Product roadmap and marketing planning tool to build products and launch campaigns.

Next

4. Enter the following SAML configuration details in the **Single Sign On** section and click **Save**.

**Assertion URL** –SaaS app SAML assertion URL 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 are 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** –Service provider for whom the assertion is intended.

**Name ID Format** –Supported format type of user.

**Name ID** –Name of the format type of user.

Single sign on

Which single sign on type would you like to use for your SaaS app setup?

**SAML** ☒ **Don't use SSO** ☐

Sign Assertion \* **Assertion**

Assertion URL \* **https://mycompanysalesforce.com/login/callb**

Relay State **https://mycompanysalesforce.com**

Audience **https://mycompanysalesforce.com/saml/<youi**

Name ID Format \* **Email Address**

Name ID \* **Email**

☐ Launch the app using the specified URL (SP initiated)

What does this form do?  
This form generates the XML needed for the application's SAML request.

Where do I find the information this form needs?  
The application you're integrating with should have its own documentation on using SAML to outline the information needed here.

**SAML Metadata**  
Provide this metadata to your Service Provider (application)  
[https://gwaasdev.mgmt.netScalerGatewaydev.net/idp/saml/11p6adi99yg/1574e9c5-cc3e-4564-8d4c-a956c712fb88/idp\\_metadata.xml](https://gwaasdev.mgmt.netScalerGatewaydev.net/idp/saml/11p6adi99yg/1574e9c5-cc3e-4564-8d4c-a956c712fb88/idp_metadata.xml)

**Login URL**  
<https://app.scte.netScalerGatewaydev.net/ngs/11p6adi99yg/saml/login?APPID=1574e9c5-cc3e-4564-8d4c-a956c712fb88> [Copy](#)

**Certificate**  
Select download type \* **PEM** **Download**

**Advanced attributes (optional)**  
An attribute is additional information about the user that is sent to the application for access control decisions. Make sure these values are consistent with the settings in the SaaS vendor.

Attribute Name	Attribute Format	Attribute Value

[Add another attribute](#)

**Save**

**Note:**

When the **Don't use SSO** option is selected, the user is redirected to the URL configured under the **App Details** section.

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

**Note:**

- 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.

- Click **Next**.

- In the **App Connectivity** section, define routing for the related domains of applications, if the domains must be routed externally or internally through a Citrix Connector Appliance. For details, see [Route tables to resolve conflicts if the related domains in both SaaS and web apps are the same](#).

App Connectivity

2 Domain(s) below already exist in the domain routing table. Changes made below will update the domain routing table.

Total 2

Domains

my.15five.com

Type: Internal

Resource Location: aaa2

Connector status: Only 1 Connector is up. [Detect](#) | [Install Gateway Connector](#) | [Install Connector Appliance](#)

Domains

\*.my.15five.com

Type: External

Next

8. 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 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](#).

## 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.
- [Bugsnap](#) - 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.
- [Flutter 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](#) - An 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.
- [Shufflr](#) - 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](#).
- [Access restriction options](#)

## Support for TCP/UDP apps

September 6, 2025

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

#### Important:

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

1. On the Citrix Secure Private Access™ tile, click **Manage**.
2. Click **Continue** and then click **Add an app**.

#### Note:

The **Continue** button appears only for the first time when you use the wizard. Subsequently, you can directly navigate to the **Applications** page and then click **Add an app**.

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.

3. In the **Choose a template** section, click **Skip** to configure the TCP/UDP app manually.
4. In the **App Details** section, select **Inside my corporate network**, enter the following details, and click **Next**.

Add an app

To add an app, complete the steps below.

Choose a template

App Details

Where is the application located? \*

Outside my corporate network

Inside my corporate network

App type \*

TCP/UDP

App icon

[Change icon](#)  
(128 KB max, PNG)

[Use default icon](#)

[Citrix Secure Access Client for Windows](#)

[Citrix Secure Access Client for macOS](#)

App name \*

Application Name

App description

Destinations and connectivity

Destination \* ⓘ

Port \* ⓘ

Protocol \*

10.2.2.2

443

TCP

Routing Type \*

Primary Resource Location \* ⓘ

Secondary Resource Location (optional) ⓘ

Internal via Connector

aaa.local

None

1 connector is available [Refresh](#)

Add another for high availability [Add](#)

Destination \* ⓘ

Port \* ⓘ

Protocol \*

10.3.3.3

443

UDP

Routing Type \*

Primary Resource Location \* ⓘ

Secondary Resource Location (optional) ⓘ

Internal via Connector

aaa.local RL2

None

1 connector is available [Refresh](#)

Add another for high availability [Add](#)

[+ Add another destination](#)

Maintain consistent connection ⓘ

Use the same connector appliance (Connector ID) or end user device IP (Client IP) for the entire length of the session while accessing the application.

Connector ID

Save

- **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 <b>Note:</b> The wildcard must always be the starting character of the domain and only one *. is allowed.

Destination input	How to access the app
info.citrix.com	End user is expected to access <a href="https://info.citrix.com">info.citrix.com</a> only and no subdomains. For example, <a href="https://sub1.info.citrix.com">sub1.info.citrix.com</a> 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.

**Destinations and connectivity**

Destination \* ⓘ  Port \* ⓘ  Protocol \*  ⓘ

Routing Type \*  ⓘ Primary Resource Location \* ⓘ  ⓘ Secondary Resource Location (optional) ⓘ  ⓘ

● 2 connectors are available [Refresh](#) ● 1 connector is available [Refresh](#)  
 ⚠ Add another for high availability [Add](#)

[+ Add another destination](#)

---

**Maintain consistent connection** ⓘ  
 Use the same connector appliance (Connector ID) or end user device IP (Client IP) for the entire length of the session while accessing the application.

ⓘ

[Save](#)

- **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 appli-

cation 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.

## Edit related domain

Domain

\*.wikipedia.org

Routing Type \*

Internal via Connector

Primary Resource Location \* ⓘ

aaa.local RL2

1 connector is available [Refresh](#)  
⚠ Add another for high availability [Add](#)

Secondary Resource Location (optional) ⓘ

aaa.local

1 connector is available [Refresh](#)  
⚠ Add another for high availability [Add](#)

**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 Workspace URL to be shared with the users, from the Citrix Cloud™ menu, click **Workspace Configuration**, and select the **Access** tab.

## Workspace Configuration ?

**Access** Authentication Customize Service Integrations Sites

### Workspace URL

This is the URL your subscriber will use to access their Workspace from their browser. Customize the URL by editing it

[https://\[redacted\].cloud.com](https://[redacted].cloud.com)

## 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 in-

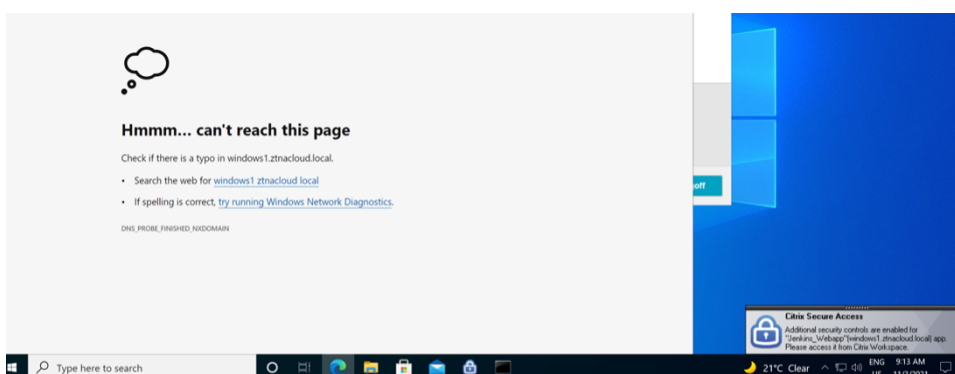
stall at least one (recommended two for high-availability) Connector Appliance in your resource location. The connector appliance can be installed on-premises, in the data center hypervisor, or in the public cloud. For details of Connector Appliance and its installation, see [Connector Appliance for 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.
- 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 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

Conflict Scenarios	Existing application domain entry	New entry from app addition	Behavior
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. 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

September 6, 2025

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.

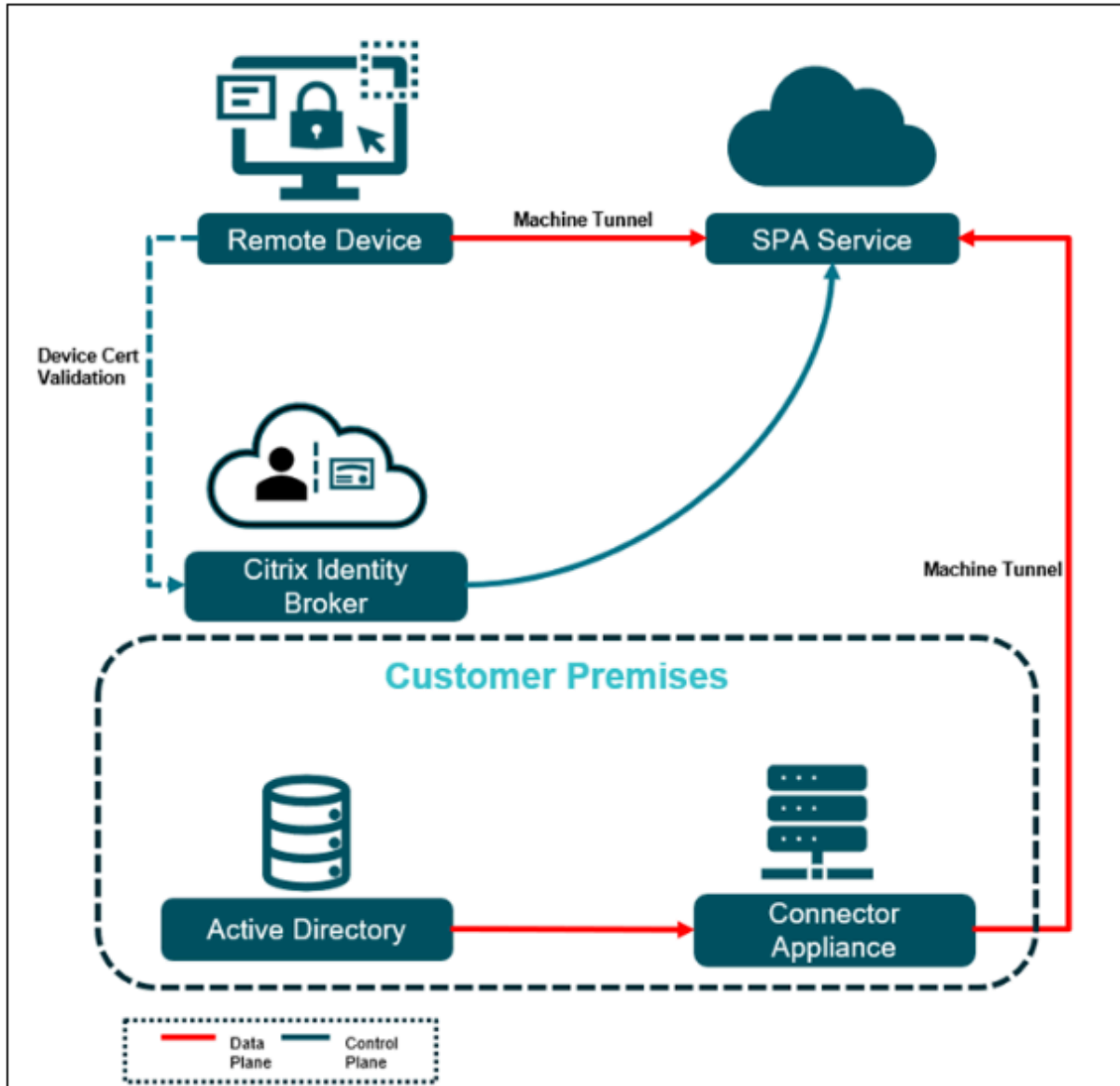
### **Note:**

- 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 / Adaptive Authentication configuration. For details, see [Connect an on-premises Citrix Gateway as an identity provider to Citrix Cloud and Provision Adaptive Authentication](#) and [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 ADFS by navigating to Workspace Configuration\Customize\Preferences-Federated Identity Provider Sessions and disable the toggle.

## 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.



The screenshot shows the 'Certificate Enrollment Agents' dialog box with the 'Extensions' tab selected. The 'Select extension:' dropdown is set to 'CRL Distribution Point (CDP)'. Below it, the text reads: 'Specify locations from which users can obtain a certificate revocation list (CRL)'. A text box contains the following text: 'C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><Idap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortName>http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><Deltafile:///<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaC'. Below the text box are 'Add...' and 'Remove' buttons. There are six checkboxes, all of which are checked: 'Publish CRLs to this location', 'Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.', 'Include in CRLs. Clients use this to find Delta CRL locations.', 'Include in the CDP extension of issued certificates', 'Publish Delta CRLs to this location', and 'Include in the IDP extension of issued CRLs'. At the bottom are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

Enrollment Agents	Auditing	Recovery Agents	Security
General	Policy Module	Exit Module	
Extensions	Storage	Certificate Managers	

Select extension:  
CRL Distribution Point (CDP)

Specify locations from which users can obtain a certificate revocation list (CRL).

C:\Windows\system32\CertSrv\CertEnroll\<CaName><CRLNameSuffix><Idap:///CN=<CATruncatedName><CRLNameSuffix>,CN=<ServerShortName>http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><Deltafile:///<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaC

< Add... Remove

☒ Publish CRLs to this location

☒ Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.

☒ Include in CRLs. Clients use this to find Delta CRL locations.

☒ Include in the CDP extension of issued certificates

☒ Publish Delta CRLs to this location

☐ Include in the IDP extension of issued CRLs

OK Cancel Apply Help

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.

The screenshot shows the 'ncstesting-alwayson-trial-SAN Properties' dialog box with the 'Subject Name' tab selected. The 'Subject name format' is set to 'Common name'. The 'Include this information in alternate subject name' section has 'User principal name (UPN)' checked. The 'Cancel' button is highlighted with a blue border.

**ncstesting-alwayson-trial-SAN Properties**

Superseded Templates Extensions Security Server

General Compatibility Request Handling Cryptography Key Attestation

**Subject Name** Issuance Requirements

☐ Supply in the request

☐ Use subject information from existing certificates for autoenrollment renewal requests (\*)

☒ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

Common name

☐ Include e-mail name in subject name

Include this information in alternate subject name:

☐ E-mail name

☐ DNS name

☒ User principal name (UPN)

☐ Service principal name (SPN)

\* Control is disabled due to [compatibility settings](#).

OK Cancel Apply Help

- 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**.

GeneralCompatibilityRequest HandlingCryptographyKey Attestation

Subject NameIssuance Requirements

Superseded TemplatesExtensionsSecurityServer

Group or user names:

Authenticated Users

Anmol Garg (anmolg@spaztnablr.net)

Domain Admins (SPAZTNABLR\Domain Admins)

Domain Computers (SPAZTNABLR\Domain Computers)

Enterprise Admins (SPAZTNABLR\Enterprise Admins)

Add...Remove

Permissions for Authenticated Users

	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Write	<input type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

Advanced

OK

Cancel

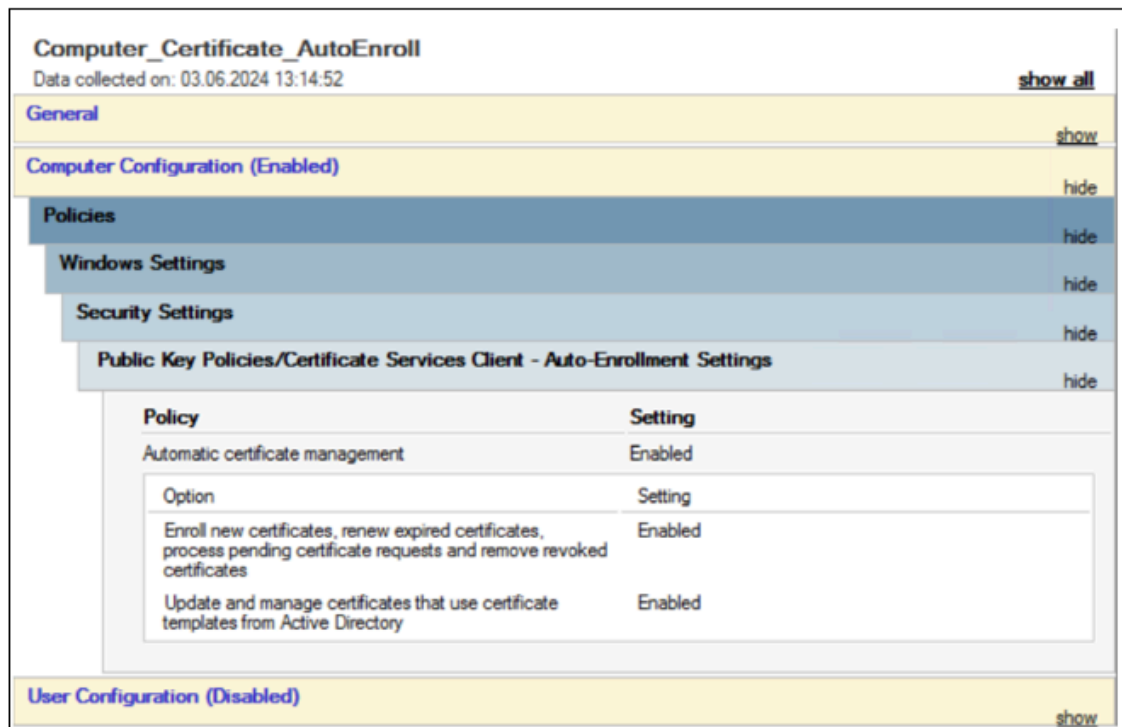
Apply

Help

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

### 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](#).

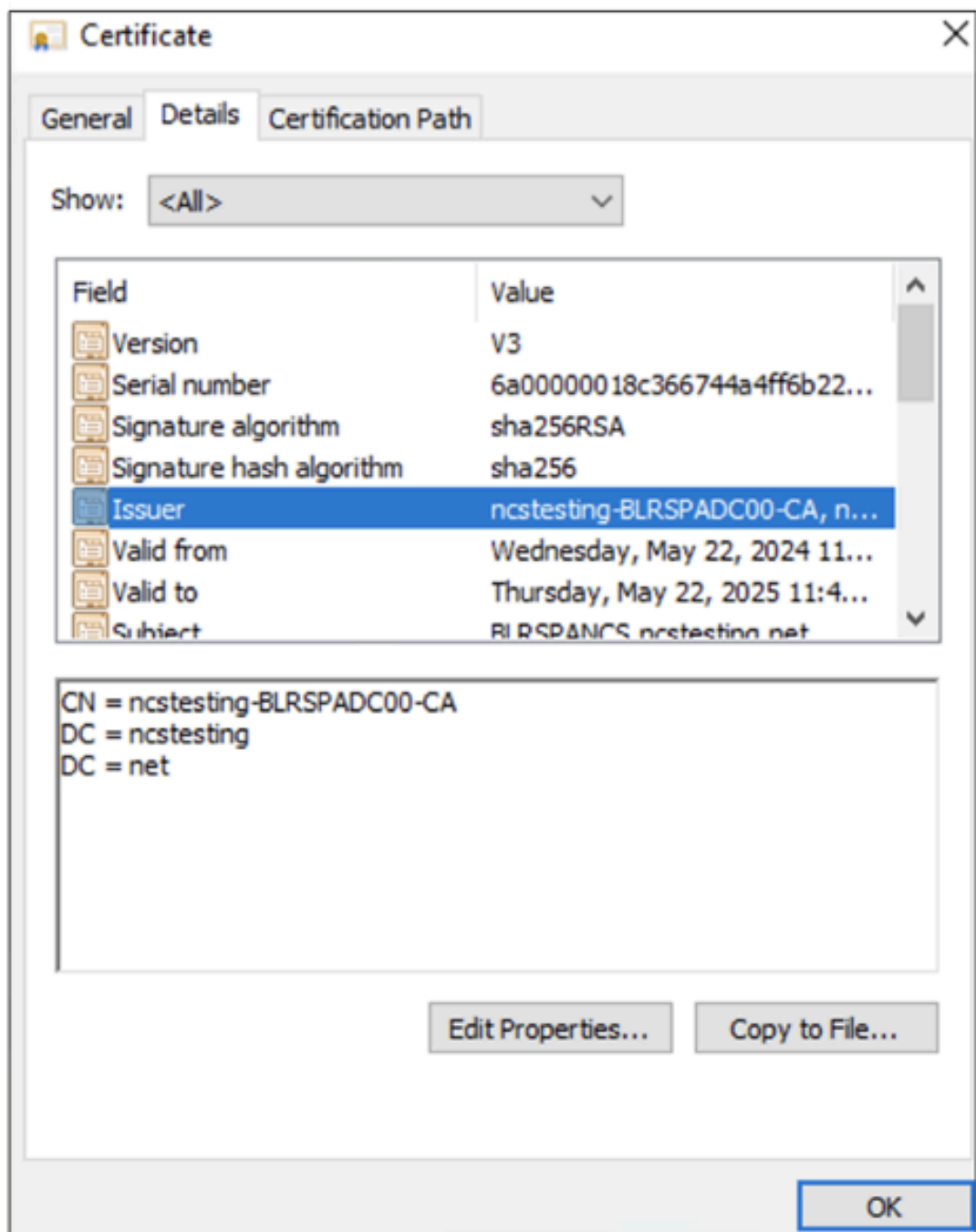
The policy is listed on the Access Policies page. A priority order is assigned to the policy, by default. The priority with a lower value has the highest preference. The policy with the lowest priority number is evaluated first. If the policy does not match the conditions defined, the next policy is 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.

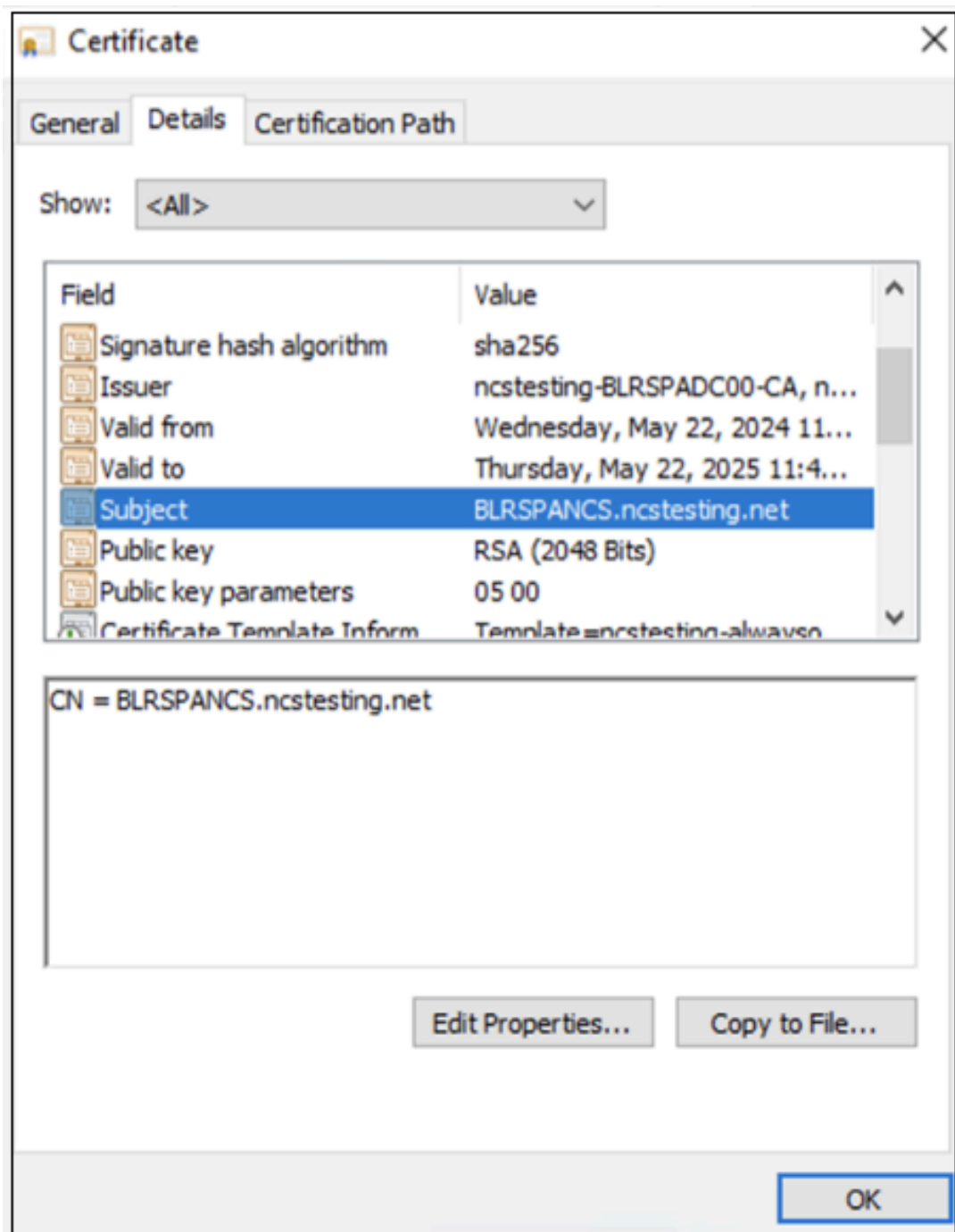
## **Client configuration**

- 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.

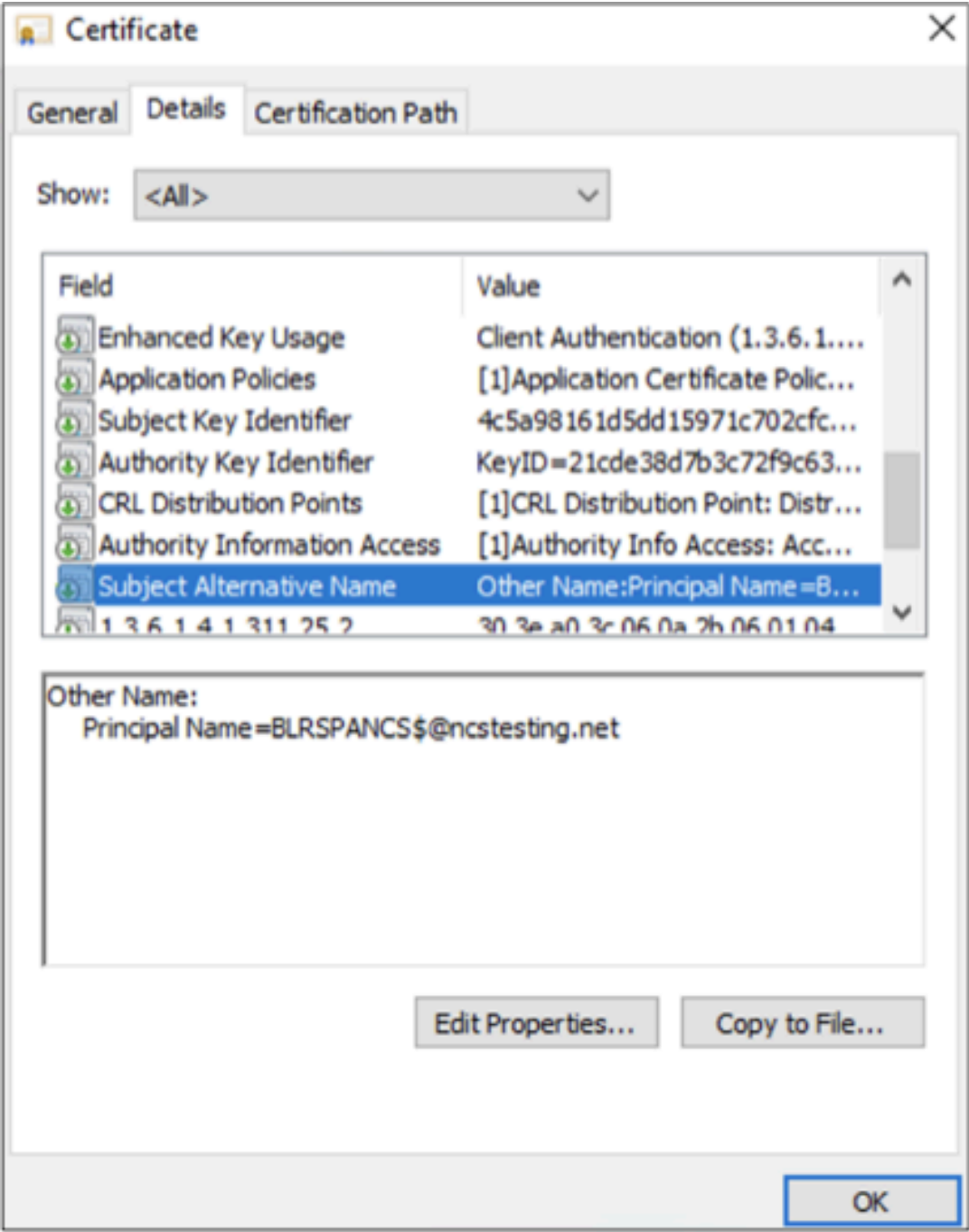


- Subject must contain the common name of the computer.

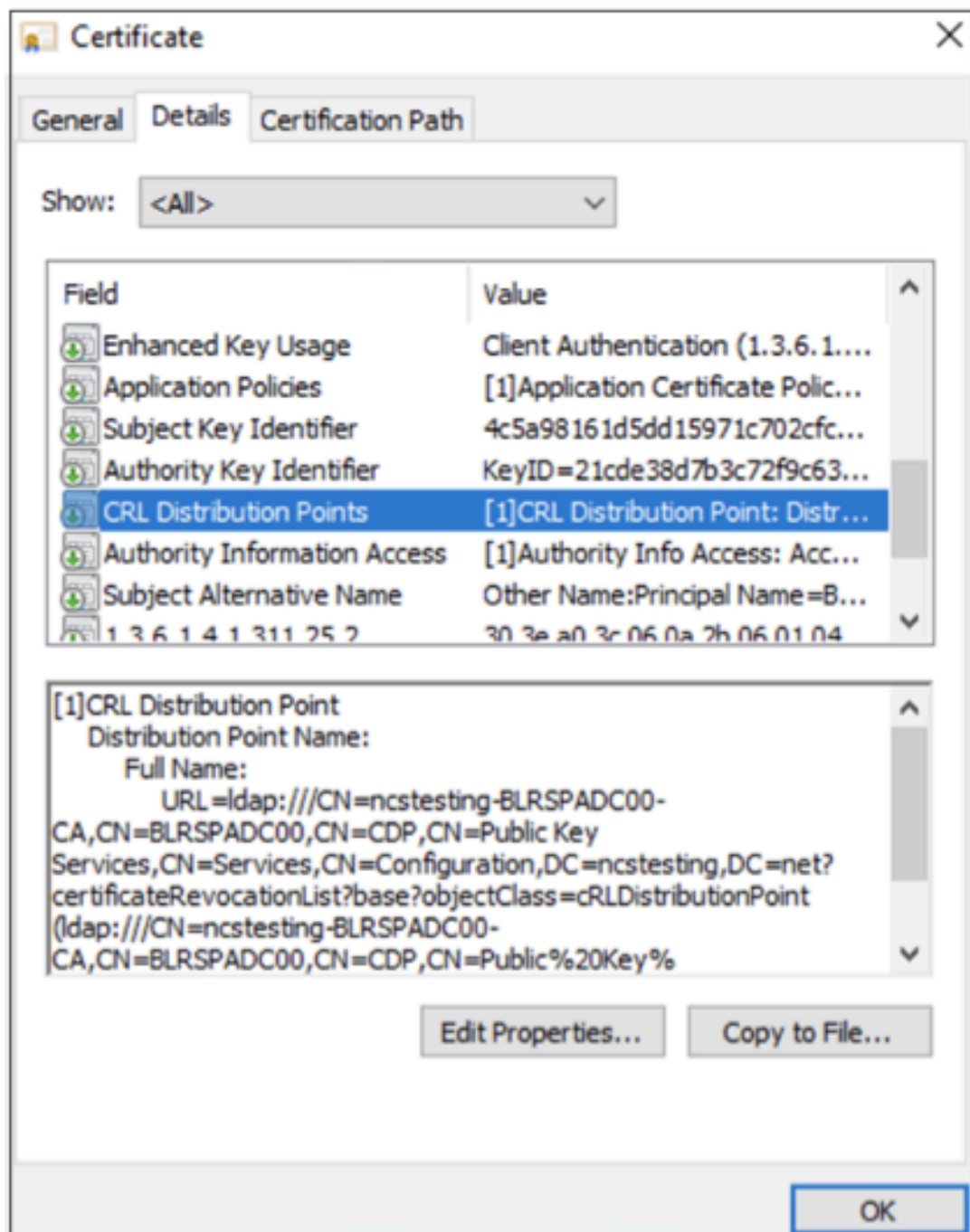




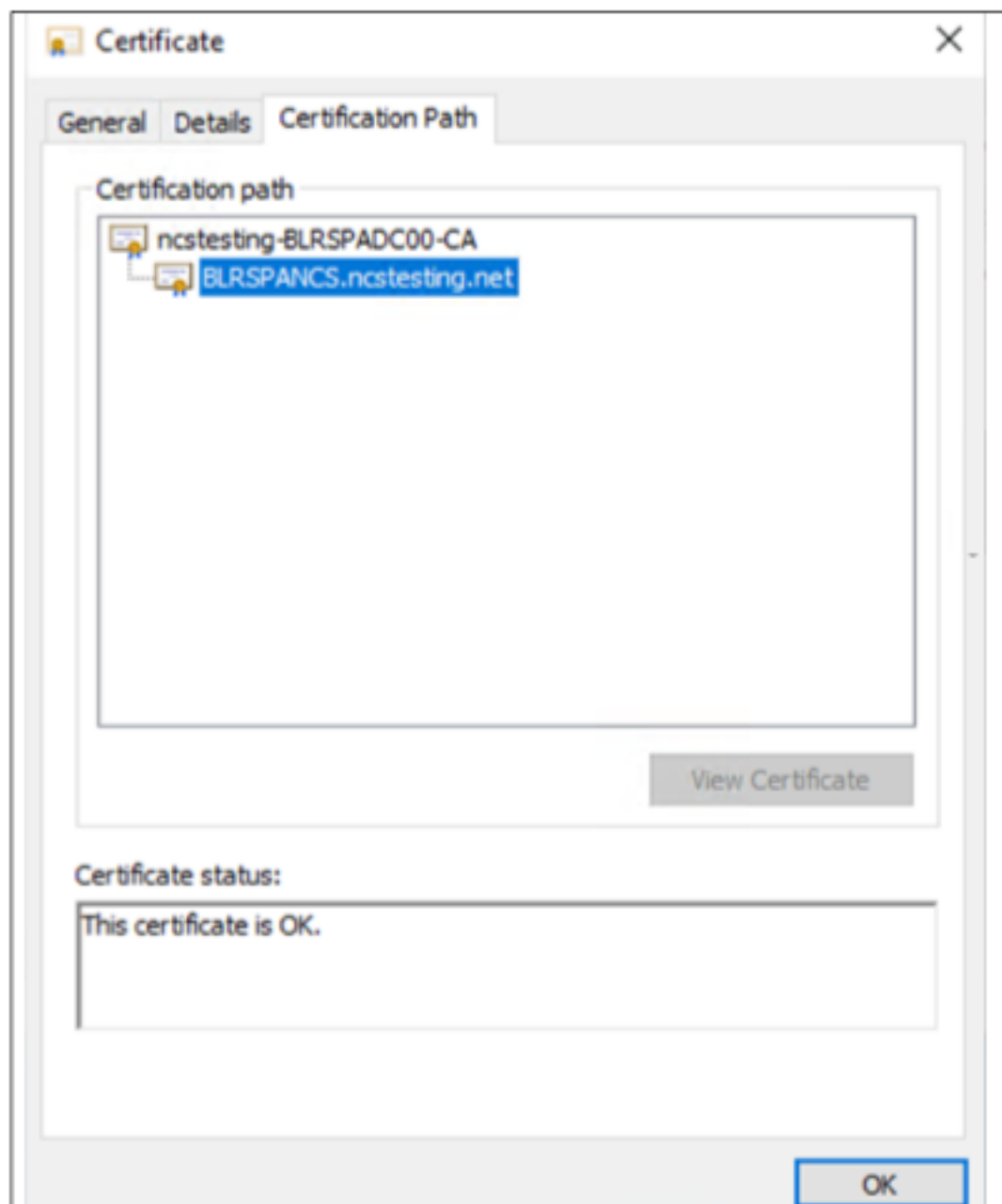
- Subject Alternate Name (SAN) must contain the UPN of the computer.



- 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 Workspace 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 Workspace authentication configuration.

- Workspace authentication with Active Directory (with no second factor) - AD credential SSO
- Workspace authentication with Citrix Gateway/Adaptive Auth configured with Kerberos SSO
- Workspace authentication with Azure Active Directory (SSO with Primary Refresh Token (PRT) of Microsoft Entra ID authentication).

#### **Note:**

Disable ADFS by navigating to Workspace Configuration\Customize\Preferences-Federated Identity Provider Sessions and disable the toggle.

### **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

September 6, 2025

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

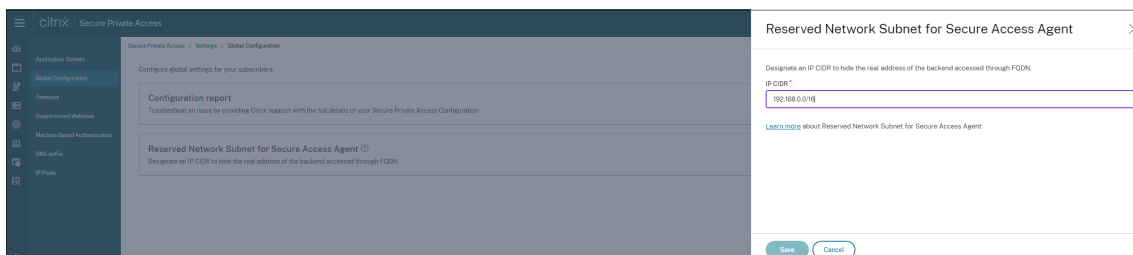
### Note:

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

September 6, 2025

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.

Order	Suffix	Actions
1	google.com	
2	test.com	

## 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.	<p>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.</p> <p><b>Note:</b> End user can access the Workday app with 192.0.2.1 or workday.citrix.net or “workday”.</p> <p>Without DNS Suffix configuration, access through “workday” and “workday.citrix.net” are denied.</p>
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.	<p>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.</p>

	DNS suffix and app configuration	End-user experience
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.	<p><b>Note:</b> End user can access the Workday app with workday.citrix.net or “workday.”</p> <p>Access to 192.0.2.1 is denied as there is no app configured with this IP address.</p> <p>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.</p> <p><b>Note:</b> End user can access Workday with workday.citrix.net or “workday”.</p> <p>Access to 192.0.2.1 is denied as there is no app configured with this IP address.</p>

	DNS suffix and app configuration	End-user experience
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, 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.	When user1 tries to connect to “workday”, “citrix.net” is suffixed to Workday (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.

## Support for server-to-client connections - Preview

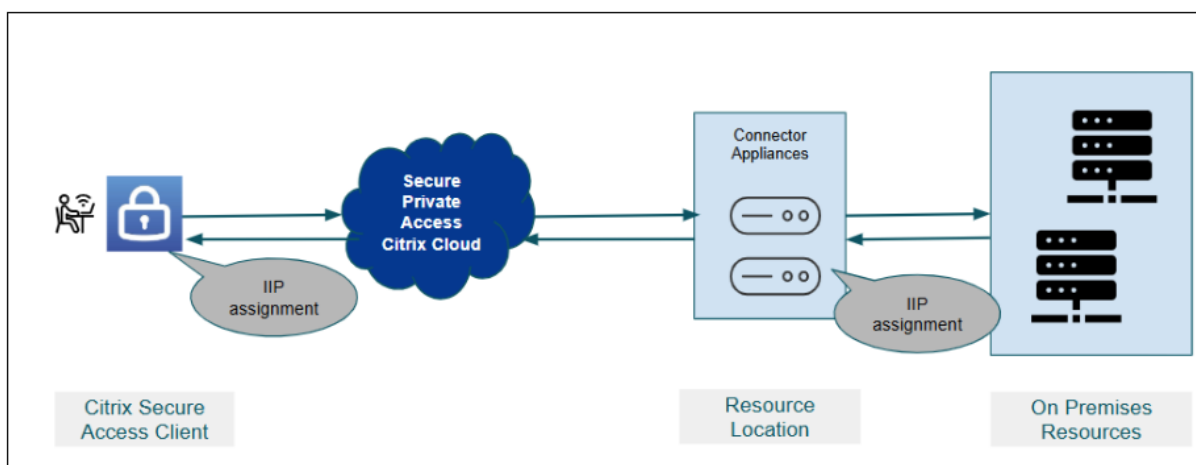
September 6, 2025

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

### 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 from the admin console**

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

Add an app


App Details

Where is the application located? \*

☐ Outside my corporate network  
☒ Inside my corporate network

---

App type \*  
TCP/UDP - server to client

App icon  

[Change icon](#)  
(128 KB max, PNG)  
[Use default icon](#)  
[Citrix Secure Access Client for Windows](#)  
[Citrix Secure Access Client for macOS](#)

App name \*  
tcp-udp-test-sic

App description

---

Server application details

Server \* ?  
192.0.2.150

+ Add

Client details

Port \* ?  
443

Protocol \*  
TCP

+ Add

Port \* ?  
1024

Protocol \*  
UDP

+ Add

Save

1. Select the location **Inside my corporate network**.
2. 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.
3. Click **Add** to add more servers and ports.
  4. Click **Save**. The app is added to the **App Configuration** page.

You can edit or delete an app from the Applications page after you have configured the application. To do so, click the ellipsis button 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.

## Agentless access to Enterprise web apps

September 6, 2025

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 Citrix Workspace experience. 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.

### Procedure to configure agentless access to Enterprise web apps:

#### Important:

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

1. On the Secure Private Access home page, click **Continue**.

#### Note:

The **Continue** button appears only for the first time when you use the wizard. Subsequently you can directly navigate to the **Applications** page and, then click **Add an app**.

2. Set up identity and authentication. For details, see [Admin-guided workflow for easy onboarding and set up](#).
3. Proceed to add an app. For details, see [Add and manage applications](#).
4. Select the app that you want to add and click **Skip**.
5. In **Where is the application location?**, select the location.
6. Enter the following details in the **App Details** section and click **Next**.

App type \*

HTTP/HTTPS

App name \*


docs-portal2

App description

App category ?

Ex.: Category\SubCategory\SubCategory

App icon

 [Change icon](#) [Use default icon](#)  
(128 KB max, PNG)

☐ Do not display application icon in Workspace app

☐ Add application to favorites in Workspace app

- ☐ Allow user to remove from favorites
- ☐ Do not allow user to remove from favorites

☒ Agentless Access

Enable direct browser-based access to internal web applications.

URL \*

https://www.citrix-docs2.com

SSL certificate \* ?

pasdev.pem

[+ Add new SSL certificate ?](#)

Related Domains \* ?

\*.citrix-docs2.com

[+ Add another related domain](#)


SSL certificate ?

DA-.pem

[+ Add new SSL certificate ?](#)

CName (Canonical name) record ?

directaccess.netscalergateway.net

 Copy

☐ Maintain consistent connection ?

Use the same connector appliance for the entire length of the session while accessing the application.

- **App type** –Select the app type (HTTP or HTTPS).
- **App name** –Name of the application.
- **App description** - A brief description of the app. This description is displayed to your users in the workspace.
- **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**.

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

- **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. Self-signed certificates aren't 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](#).

- **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.
8. 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.

**App Connectivity**

URL \*  SSL certificate ②  [Add new SSL certificate](#) ③

Routing Type \*  Primary Resource Location \* ①  Secondary Resource Location (optional) ①

● 2 connectors are available [Refresh](#) ● 1 connector is available [Refresh](#)  
 ⚠ Add another for high availability [Add](#)

Related Domains  [Add](#)

Related Domains	Routing Type	Primary Resource Location	Available Connectors	Actions
*.docs.citrix.com ⚠	Internal via Connector	AAA RL 01	2	<a href="#">Edit</a> <a href="#">Delete</a>

Showing 1-1 of 1 items Page 1 of 1 5 rows ▾

CName (Canonical name) record ③  [Copy](#)

☒ Maintain consistent connection ②  
 Use the same connector appliance for the entire length of the session while accessing the application.

- **Routing Type** - Select one of the following:
  - **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 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.

### Edit related domain

Domain

\*.wikipedia.org

Routing Type \*

Internal via Connector

Primary Resource Location \* ?

aaa.local RL2

1 connector is available [Refresh](#)

⚠ Add another for high availability [Add](#)

Secondary Resource Location (optional) ?

aaa.local

1 connector is available [Refresh](#)

⚠ Add another for high availability [Add](#)

**Note:**

Setting the backup resource location and using the **First Available** option feature is in Preview.

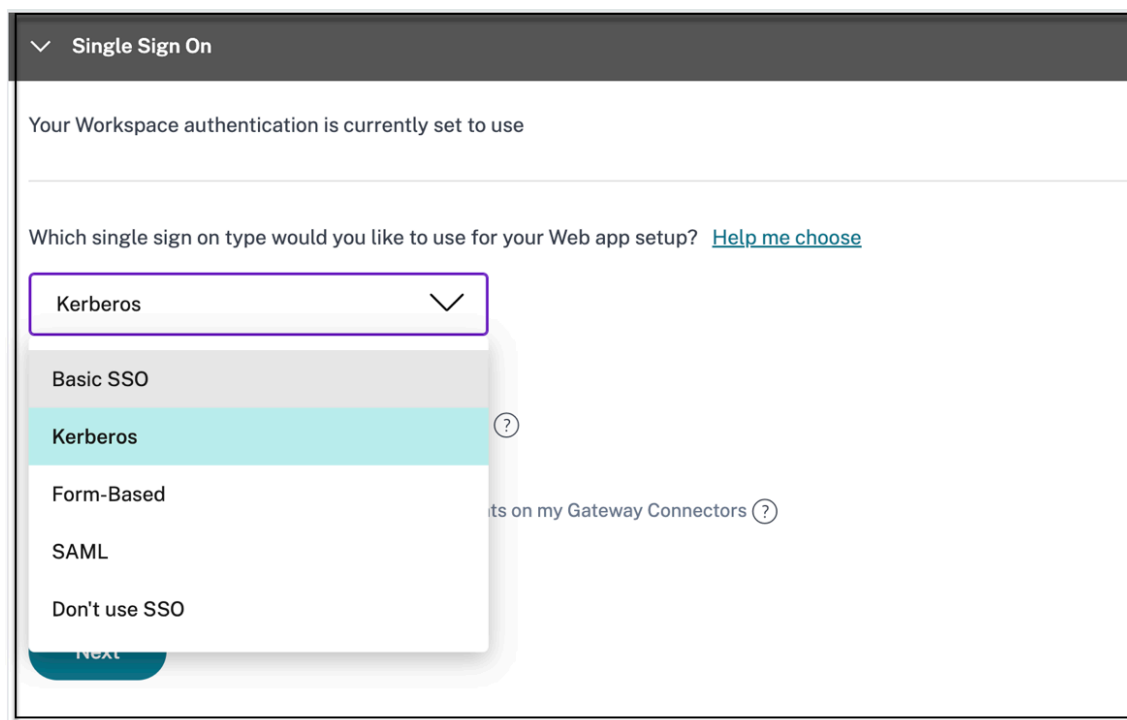
- **Maintain consistent connection** - Select this checkbox to enable consistent connection

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.

9. Click **Next**.
10. In the **Single sign on** section, select your preferred single sign-on type to be used for your application and click **Next**.



Single Sign On

Your Workspace authentication is currently set to use

Which single sign on type would you like to use for your Web app setup? [Help me choose](#)

Kerberos

Basic SSO

Kerberos

Form-Based

SAML

Don't use SSO

Next

11. In the **App Connectivity** section, you can either select an existing resource location or create one and deploy a new Connector Appliance. To choose an existing resource location, click one of the resource locations from the list of resource locations, for example My Resource Location, and click **Next**. For details, see [Route tables to resolve conflicts if the related domains in both SaaS and web apps are the same](#).

App Connectivity

2 Domain(s) below already exist in the domain routing table. Changes made below will update the domain routing table.

Total 2

Domains

my.15five.com

Type

Internal - Bypass Proxy

Resource Location

aaa2

Connector status

Only 1 Connector is up.

[Detect](#) | [Install Connector Appliance](#)

Domains

\*.my.15five.com

Type

External - via Connector

Resource Location

aaa2

Connector status

Only 1 Connector is up.

[Detect](#) | [Install Connector Appliance](#)

- 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](#).
- For the list of available access restrictions, see [Access restriction options](#).

## 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](#).

**Create device policy**

With device posture, you can define a set of conditions that control which devices have access to various services and data sources.

**Platform**  
Select the operating system for this device posture scan. ⓘ

Windows

**Policy rules**  
Select a condition and apply access rules for your services and data. ⓘ

Device Certificate

Issued by AAACA14.pem ×

+ Import Issuer Certificate

+ Add another rule

**Policy result**  
If policy conditions and rules are met, the device scan will classify the user device as one of the following: ⓘ

☒ **Compliant**  
The device will be considered compliant and full access will be granted.

☐ **Non-compliant**  
The device will be considered "non-compliant" and restricted access will be granted.

☐ **Denied access**  
The device will be denied access to all resources.

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](#).



### Add an app

**App type \***

HTTP/HTTPS

**App name \***


translator

**App description**

**App category ?**

Ex.: Category\SubCategory\SubCategory

**App icon**

 [Change icon](#)  
(128 KB max, PNG) [Use default icon](#)

☐ Do not display application icon in Workspace app

☐ Add application to favorites in Workspace app

☐ Allow user to remove from favorites

☐ Do not allow user to remove from favorites

☒ **Direct Access**

Enable direct browser-based access to internal web applications.

**URL \***

https://www.translator.com

**SSL certificate \* ?**

AAACA14.pem

[+ Add new SSL certificate ?](#)

- 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](#).

**Create new rule**

Step 2: Conditions

**Rule Scope**

Select the rule scope from the following options.

☒ User  
Applicable to both HTTP/HTTPS and TCP/UDP apps

☐ Machine  
Applicable to only TCP/UDP apps

User\*

Matches any of

AND

+ Add condition

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 Citrix Workspace.

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 Citrix Workspace or from the browser using the app URL.

- **Non-compliant device:**
  - The app is not enumerated in Citrix Workspace.
  - The user cannot launch the app from the browser using the app URL.
  - An access blocked page is displayed to the user.

## Manage certificates in the Secure Private Access console

September 6, 2025

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

### 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.

Secure Private Access > Settings > Certificate Store

Certificates

Server Machine Authentication

The first root CA certificate in the table is selected by default for machine based authentication. You can change the priority as per your requirement.

☒ Enforce machine level tunnel before users log on  
(Support only for Microsoft Windows)

Add certificate

	Priority Order	Common Name	Validity	Issuer	Status	
⬆	1	DC = net, DC = spaztnablir, CN = spaztnablir-BLRSPA...	May 28 05:48:53 2024 GMT to May 28 05:...	CN=spaztnablir-BLRSPADC03-CA, DC=spaztnablir, D...	<input checked="" type="checkbox"/>	🗑
⬆	2	DC = net, DC = ebricks-inc, CN = ebricks-inc-CERT1...	Jul 14 15:20:04 2021 GMT to Jul 14 15:30:03...	CN=ebricks-inc-CERT166-CA-1, DC=ebricks-inc, DC...	<input checked="" type="checkbox"/>	🗑
⬆	3	CN=aaa-rootca,DC=aaa,DC=local	Jul 20 02:33:19 2017 UTC to Jul 20 02:43:19...	CN=aaa-rootca, DC=aaa, DC=local	<input checked="" type="checkbox"/>	🗑

Showing 1-3 of 3 items Page 1 of 1 10 rows

### 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

#### 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**.

Secure Private Access > Settings > Certificate Store

Certificates

Server

Machine Authentication

These certificates are used for SPA application access.

Search by name or subject

Status Filter

Add certificate

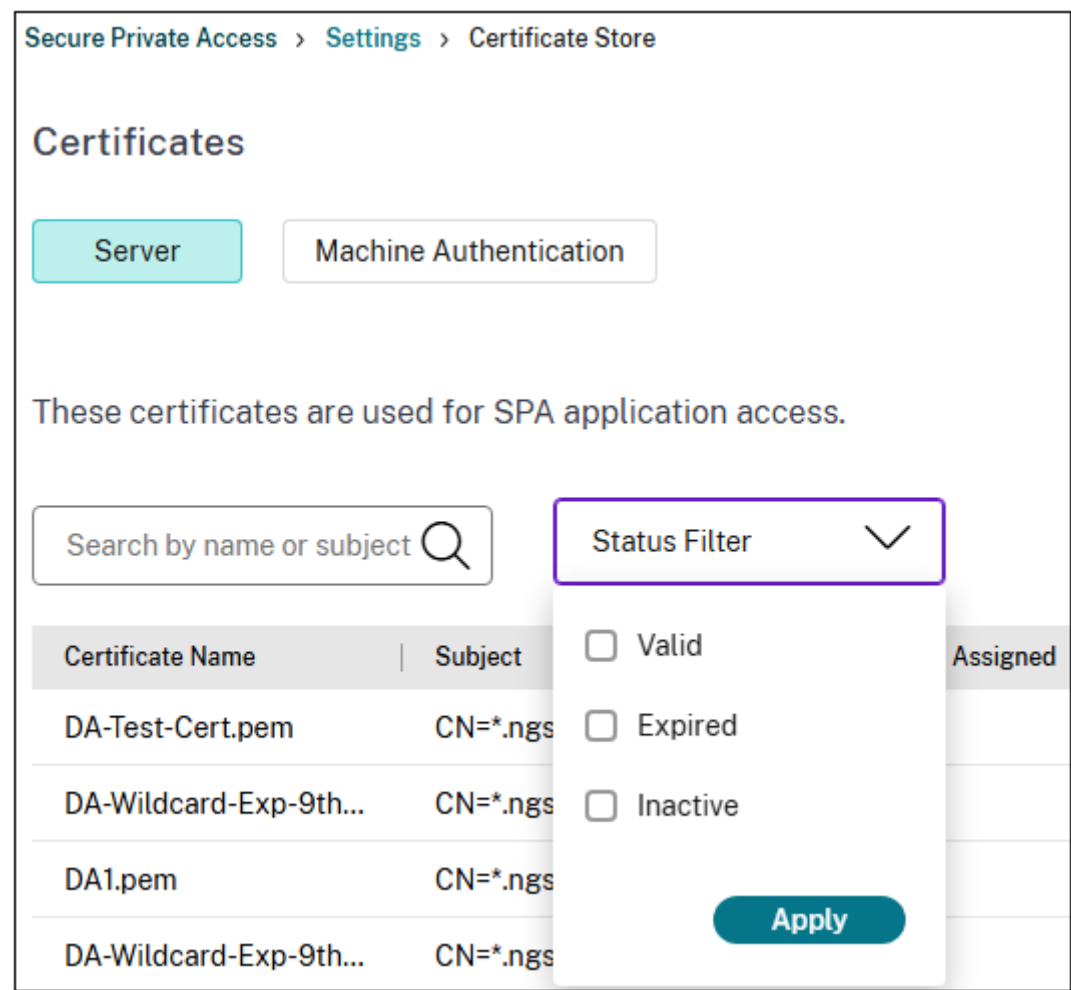
Certificate Name	Subject	Applications Assigned	Valid From	Valid Until	Days To Expire	Status	Actions
DA-Test-Cert.pem	CN=*.ngsautomation...	1	January 9, 2025	April 9, 2025	0	Expired	
DA-Wildcard-Exp-9th...	CN=*.ngsautomation...	0	January 9, 2025	April 9, 2025	0	Expired	
DA1.pem	CN=*.ngsautomation...	1	January 9, 2025	April 9, 2025	0	Expired	
DA-Wildcard-Exp-9th...	CN=*.ngsautomation...	0	January 9, 2025	April 9, 2025	0	Expired	
AAACA14.pem	CN=aaa-rootca, DC=a...	0	July 20, 2017	July 20, 2037	4442	Valid	
CMS-DA.pem	CN=*.ngsautomation...	1	January 9, 2025	April 9, 2025	0	Expired	
New-DA.pem	CN=*.ngsautomation...	0	January 9, 2025	April 9, 2025	0	Expired	
Test-DA.pem	CN=*.ngsautomation...	0	January 9, 2025	April 9, 2025	0	Expired	
CRoot.pem	CN=spaztnablr-BLRS...	0	May 28, 2024	May 28, 2029	1468	Valid	
AAACA14.pem	CN=aaa-rootca, DC=a...	0	July 20, 2017	July 20, 2037	4442	Valid	

Showing 1-10 of 10 itemsPage 1 of 120 rows

- 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

September 6, 2025

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/iOS](#).

### 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

September 6, 2025

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 [Access policies](#).

- **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. For details, see [Configure rules for unsanctioned websites](#).

## 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	<code>https://app.intranet.local</code>	<code>*.cdn.com</code>
Wiki	<code>https://wiki.intranet.local</code>	<code>*.intranet.local</code>

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

### 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 on workspace. For information, see [Configure application details](#).

App Details

Where is the application located? \*

☒ Outside my corporate network

☐ Inside my corporate network

App type \*

HTTP/HTTPS

App name \*

Web App/Cloud App


App description

Collaboration incidents response tool to manage IT incidents in real

App category ⓘ

Ex.: Category\SubCategory\SubCategory

App icon

 [Change icon](#) [Use default icon](#)

(128 KB max, PNG)

☐ Do not display application icon in Workspace app

☐ Add application to favorites in Workspace app

- ☐ Allow user to remove from favorites
- ☐ Do not allow user to remove from favorites

**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	<a href="https://code.example.net">https://code.example.net</a>	example.okta.com
App2	<a href="https://info.example.net">https://info.example.net</a>	example.okta.com

Policy name	Priority	User and associated apps
Deny App1 to HR	High	User group <a href="#">HR</a> for <a href="#">App1</a>
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:

1. Remove example.okta.com as a related domain from all apps.
2. Create a new app just for Okta (with the application URL of <https://example.okta.com> and a related domain of \*.okta.com).
3. Hide this app from workspace.
4. 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 Workspace.
- If the app must not appear in Workspace, then while publishing the app, select the **Do not display application icon to users** option to hide it from Workspace.

**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](https://example.okta.com/deep-link-app-1).

In this case, separately create an IdP app with URL <https://example.okta.com> and then related domain as [\\*.example.okta.com](https://example.okta.com).

## App access end-user experience explained

September 6, 2025

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.
- **Through Citrix Enterprise Browser™:** End users can access their enterprise web apps directly through Citrix Enterprise Browser which is integrated into the Workspace environment.

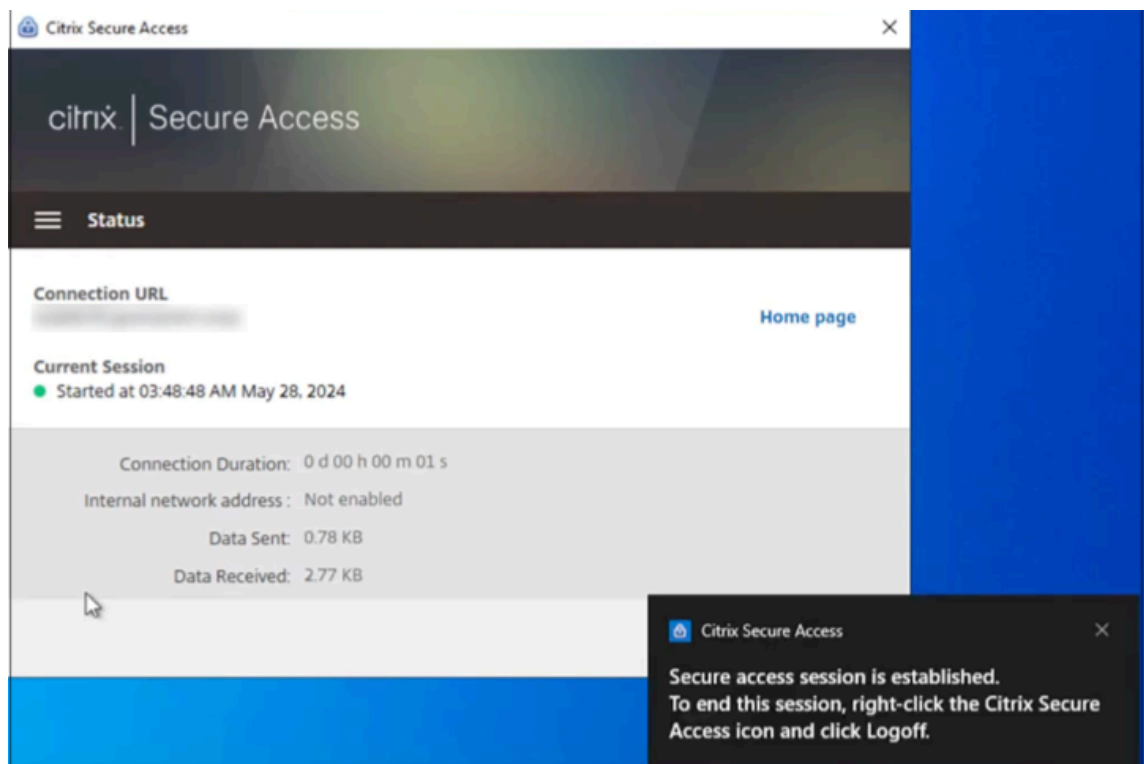
### Access a Web app through the Citrix Secure Access client

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.

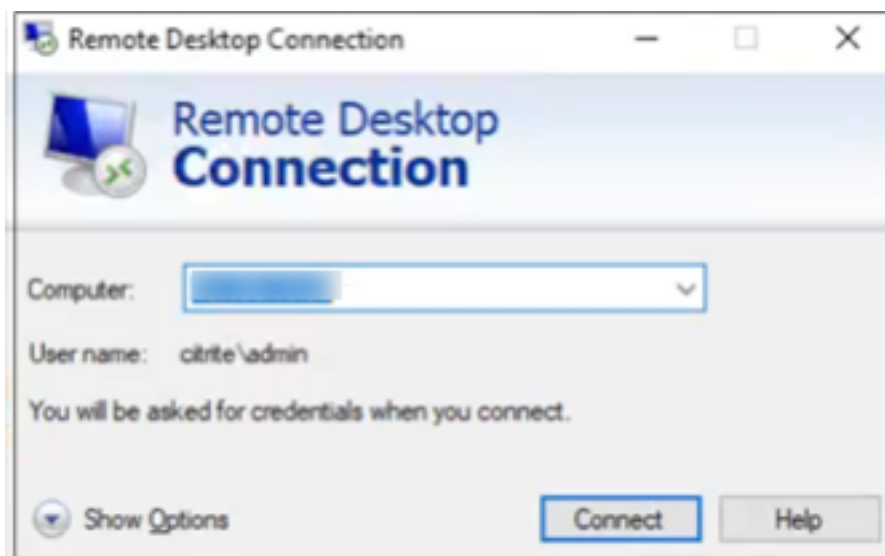
### Access a TCP/UDP app through the Citrix Secure Access client

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](#).

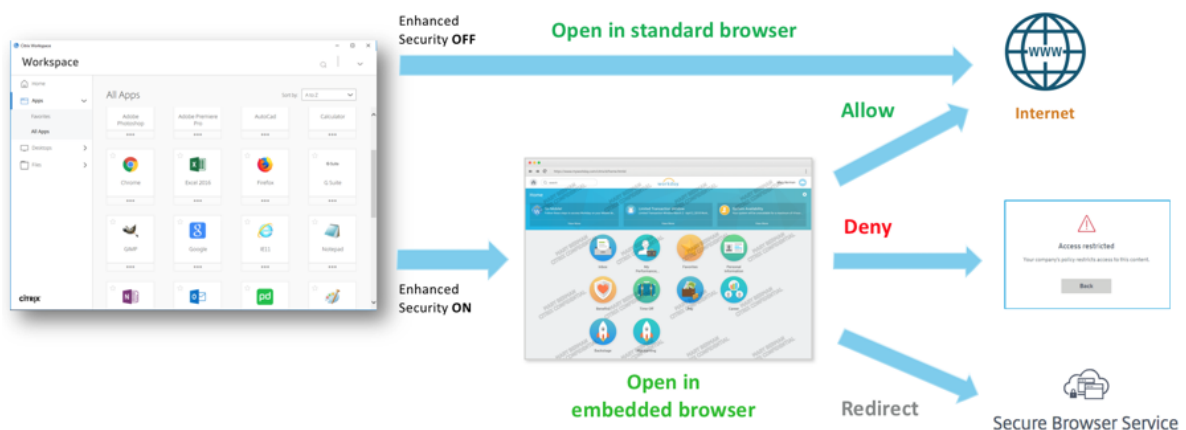
### Access an app through Citrix Enterprise Browser

1. Download the Citrix Workspace app from <https://www.citrix.com/downloads>. In the **Find Downloads** list, select **Citrix Workspace app**.
2. Log on and search for your SaaS apps. Click the app to launch it.

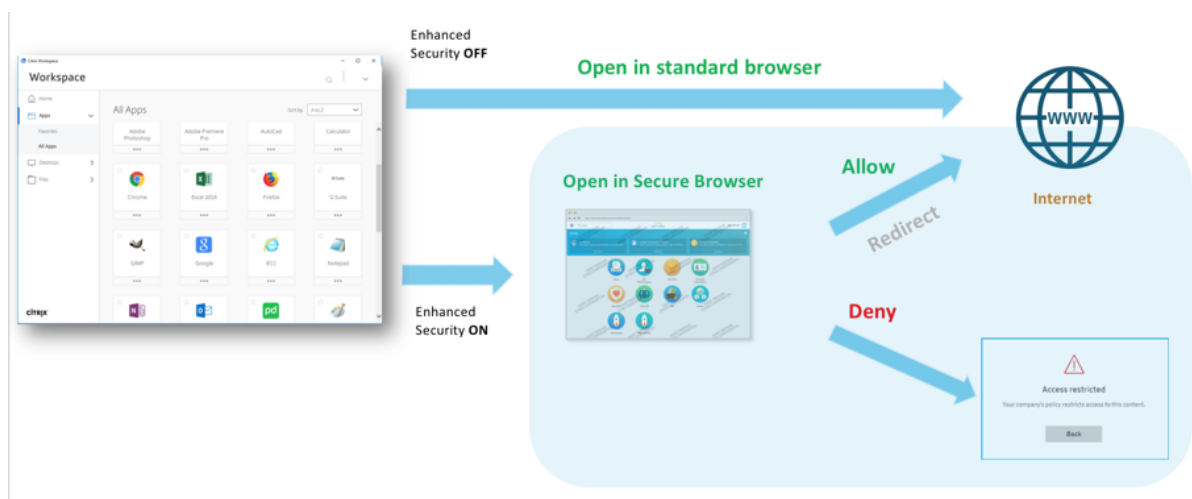
You can now use the SaaS app from within the Citrix Workspace™ app.

Depending on the admin configured settings, your SaaS apps open by using the browser engine within the Workspace app or you are redirected to a secure browser.

The following diagram shows the high-level flow for the Citrix Workspace app.



The following diagram shows the high-level flow for the Citrix Workspace web portal.



For more information about Citrix Enterprise Browser, see [Citrix Enterprise Browser](#).

## Adaptive access policy configuration and management

September 6, 2025

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)
- Risk (user risk score)

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, the location (country or network location) from where the user is accessing the application, and the user risk score.

The adaptive access policies take precedence over the application-specific security policies that are configured while adding the SaaS or a Web app in the Secure Private Access service. The per-app level security controls are overwritten by the adaptive access policies.

### The adaptive access policies are evaluated in three scenarios:

- During a Web, TCP, or a SaaS 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 workspace.
- 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.
- When the app is opened in a Citrix Enterprise Browser™ or a Remote Browser Isolation service –The Citrix Enterprise Browser enforces some security controls. These controls are enforced by the client. When the Citrix Enterprise Browser is launched, the server evaluates the adaptive policies for the user and returns those policies to the client. The client then enforces the policies locally in the Citrix Enterprise Browser.

## Create an adaptive access policy with multiple rules

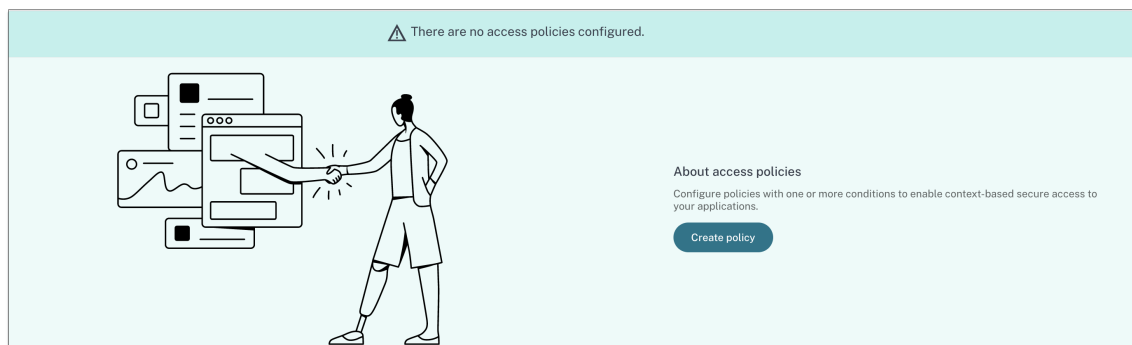
You can create multiple access rules and configure different access conditions for different users or user groups within a single policy. These rules can be applied separately for both HTTP/HTTPS and TCP/UDP applications, all within a single policy.

Access policies within Secure Private Access allow you to enable or disable access to the apps based on the context of the user or user's device. In addition, you can enable restricted access to the apps by adding security restrictions. For details, see [Security controls for Citrix Enterprise Browser](#).

Ensure that you have completed the following tasks before configuring an access policy.

- [Set up identity and authentication](#)
- [Configured applications](#)

1. On the navigation pane, click **Access Policies** and then click **Create policy**.



For the first-time users, the **Access Policies** landing page does not display any policies. Once you create a policy, you can see it listed here.

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.

Step 3: Access Policies

Create policies to enforce application access rules based on user context.

←

Create policy

Create a policy to enforce application access rules based on application context.

Policy name \*

policy-test

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

10000ft Demo Test

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
----------------	-----------	------------	-----------	-------------	--------	--------

Showing 1-0 of 0 itemsPage 1 of 010 rows

☐ Enable policy on save

Save

Cancel

5. Enter the rule name and a brief description of the rule, and then click **Next**.

1 Rule details

2 Conditions

3 Actions

4 Summary

Step 1: Rule details

Selected applications for this rule

DNS Suffix TestingBitBucket

Rule name \*

Allow with restrictions

Rule description

Enable access with restrictions

Cancel

Next

6. Select the users' conditions. The **Users** condition is a mandatory condition to be met to grant

access to the applications for the 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.

**Create new rule**

Step 2: Conditions

**Rule Scope**

Select the rule scope from the following options.

☒ **User**  
Applicable to both HTTP/HTTPS and TCP/UDP apps

☐ **Machine**  
Applicable to only TCP/UDP apps

User\*

Matches any of ▼ \* Ad ▼ aaa.local ▼

ak1-ak1@gmail.com 🔍

+ Add condition

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

When you add conditions based on a context, an AND operation is applied on the conditions wherein 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.

- **Desktop or Mobile device** –Select the device for which you want to enable access to the apps.
- **Geo location** –Select the condition and the geographic location from where the users are accessing the apps.
- **Network location** –Select the condition and the network using which the users are accessing the apps.
- **Device posture check** –Select the conditions that the user device must pass to access the application.
- **User risk score** –Select the risk score categories based on which the users must be provided access to the application.

8. Click **Next**.

9. Select the actions that must be applied based on the condition evaluation.

- For HTTP/HTTPS apps, you can select the following:

- **Allow access**
- **Allow access with restrictions**
- **Deny access**

**Note:**

If you select **Allow access with restrictions**, then you must select the restrictions that you want to enforce on the apps. For details on the restrictions, see [Available access restrictions options](#). You can also specify if you want the app to open in a remote browser or in Citrix Secure Browser.

- For TCP/UDP access, you can select the following:
  - **Allow access**
  - **Deny access**

✓ Rule details

✓ Conditions

3 Actions

4 Summary

Step 3: Action

Action for HTTP/HTTPS apps \*

☐ Allow access

☒ Allow access with restrictions

☐ Deny access

0 selected

☐ View selected only

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

Advanced options:

☒ Open in remote browser ?

Action for TCP/UDP apps \*

☐ Allow access

☒ Deny access

10. Click **Next**. The Summary page displays the policy details.
11. You can verify the details and click **Finish**.



**Zero Trust Network Access to all enterprise applications**  
Secure access to all enterprise applications based on adaptive authentication and access policies

Device Posture  
Applications  
Access Policies  
Review

**Step 4: Review**  
The following is a high-level summary of your ZTNA setup.

**Identity and authentication**  
Your current authentication method is: Active Directory ✓ Configured

For more information, please visit [Identity and Access Management](#).

**Device posture**

Integrations

Name	ID	Status
Microsoft Intune		Pending
CrowdStrike Falcon® Insight XDR		Not Configured

Showing 1-2 of 2 items Page 1 of 1

Device scans - Windows

Priority	Policy Name	Result	Status
12	windows-os	Non-Compliant	Enabled

No device scans configured

Device scans - Linux

No device scans configured

**App configuration**

App	SSO Settings	App Access	Policies
10000ft Demo Test <a href="https://app.10000ft.com/me/*_app.10000ft.com">https://app.10000ft.com/me/*_app.10000ft.com</a>	No SSO	Always	1

Showing 1-1 of 1 items Page 1 of 1 5 rows

**Access policies**

Priority	Name	Status	Modified
1	policy-test	<input checked="" type="checkbox"/>	2/6/2025

Showing 1-1 of 1 items Page 1 of 1 5 rows

[Back](#) [Close](#)

## 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:

Assume 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.

Assume 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.

### Note:

If none of the rules are evaluated, then the app is not enumerated to the users.

## Available access restrictions options

When you select the action **Allow access with restrictions**, you must select at least one of the security restrictions. These security restrictions are predefined in the system. Admins cannot modify or add other combinations. For details, see [Available access restrictions options](#)

## 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, use the [Create an adaptive access policy with multiple rules](#) procedure with the following changes.

- In **Step2: Conditions** page, click **Add condition**.
- Select **Desktop** or **Mobile device**.
- Complete the policy configuration.

**Step 2: Conditions**

**Rule Scope**  
Select the rule scope from the following options.

☒ User  
Applicable to both HTTP/HTTPS and TCP/UDP apps

☐ Machine  
Applicable to only TCP/UDP apps

**User\***

Matches any of ▼

aaa.local ▼

admin × ▼

**AND**

Desktop ▼

+ Add condition

Cancel Back Next

## 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 > Citrix Workspace > Access > Adaptive Access**. If not, you cannot add the location tags. For details, see [Enable Adaptive Access](#).
- You can also create a network location from the Citrix Cloud console. For details, see [Citrix Cloud network location configuration](#).

- 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 Citrix DaaS™ service and Citrix Secure Private Access service and is used to provide contextual access based on device posture.

For complete details on 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.

**Step 2: Conditions**

**Rule Scope**  
Select the rule scope from the following options.

☒ User  
Applicable to both HTTP/HTTPS and TCP/UDP apps

☐ Machine  
Applicable to only TCP/UDP apps

**User\***

Matches any of ▼ aaa.local ▼ admin X ▼

**AND**

Device posture check ▼ Matches all of ▼ Compliant X ▼

+ Add condition

Cancel Back Next

## Adaptive access based on user risk score

### Important:

This feature is available to the customers only if they have the Security Analytics entitlement.

User risk score is a scoring system to determine the risks associated with the user activities in your enterprise. Risk indicators are assigned to user activities that look suspicious or can pose a security threat to your organization. The risk indicators are triggered when the user's behavior deviates from the normal. Each risk indicator can have one or more risk factors associated with it. These risk factors help you to determine the type of anomalies in the user events. The risk indicators and their associated risk factors determine the risk score of a user. The risk score is calculated periodically and there is a delay between the action and the update in the risk score. For details, see [Citrix user risk indicators](#).

To configure an adaptive access policy with risk score, use the [Create an adaptive access policy with multiple rules](#) procedure with the following changes.

- In **Step2: Conditions** page, click **Add condition**.
- Select **User risk score** and then select the risk condition.
  - Preset tags fetched from the CAS service

- \* **LOW** 1–69
- \* **MEDIUM** 70–89
- \* **HIGH** 90–100

**Note:**

A risk score of 0 is not considered to have a risk level “Low.”

- Threshold types
  - \* **Greater than or equal to**
  - \* **Less than or equal to**
- A number range
  - \* **Range**

**Step 2: Conditions**

**Rule Scope**  
Select the rule scope from the following options.

☒ **User**  
Applicable to both HTTP/HTTPS and TCP/UDP apps

☐ **Machine**  
Applicable to only TCP/UDP apps

**User\***

Matches any of

**AND**

User risk score

## Access restriction options

September 6, 2025

When you select the action **Allow access with restrictions** while creating an access policy, you can select the access restrictions. These restrictions are predefined in the system. Admins cannot modify or add other combinations. For details on creating an access policy and enabling access restrictions, see [Configure an access policy](#).

✓ Rule details

✓ Conditions

3 Actions

4 Summary

Step 3: Action

Action for HTTP/HTTPS apps \*

Allow access

Allow access with restrictions

Deny access

0 selected

View selected only

Search

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

Action for TCP/UDP apps \*

Allow access

Deny access

Cancel

Back

Next

Clipboard

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

© 1997–2025 Citrix Systems, Inc. All rights reserved.

178

## Copy

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

### Note:

- If both **Clipboard** and **Copy** restrictions are enabled in a policy, the **Clipboard** restriction takes precedence over the **Copy** restriction.
- End users must use Citrix Enterprise Browser™ version 2405 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.
- For granular control of copy operation within the apps, admins can use the **Security groups** restriction. For details, see [Clipboard restriction for security groups](#).

## Download restriction by file type

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

### Note:

- The **Download restriction by file type** restriction is available in addition to the **Download** restriction.
- If both **Downloads** and **Download restriction by file type** restrictions are enabled in a policy, the **Downloads** restriction takes precedence over the **Download restriction by file type** restriction.
- End users must use Citrix Enterprise Browser version 2405 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.

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

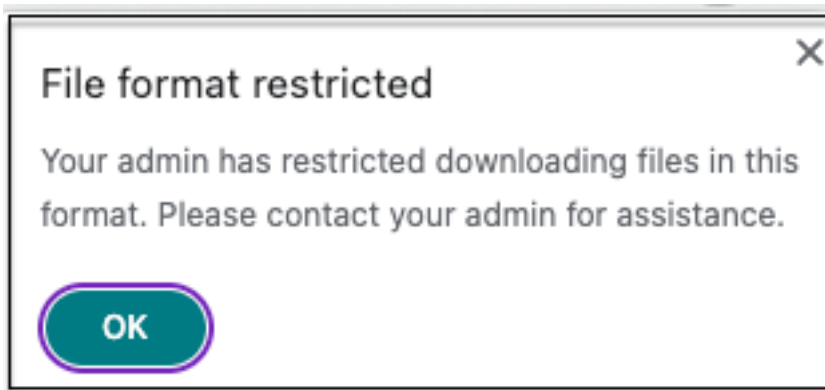
1. Create or edit an access policy. For details, see [Create access policies](#).
2. In the **Step 3: Action** page, select **Allow with restrictions**.
3. Click **Download restriction by file type** and then click **Edit**.
4. In the **Download restriction by file type settings** page, select one of the following:
  - **Allow all downloads with exceptions** –Select the types that must be blocked and allow all other types.
  - **Block all downloads with exceptions** –Select only the types that can be uploaded and block all other types.
5. If the file type does not exist in the list, then do the following:



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

The MIME type now appears in the list of exceptions.

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



## Downloads

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

### Note:

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

## Insecure content

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

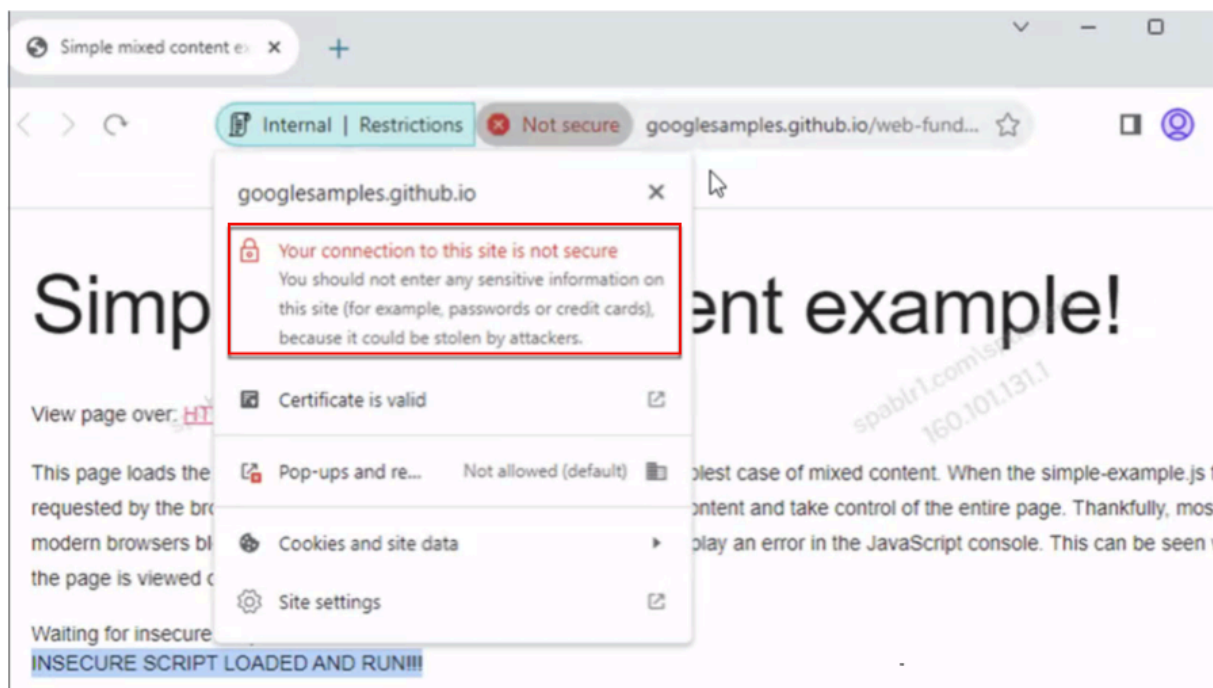
End users must use Citrix Enterprise Browser version 126 or later for disabling accessing insecure content.

To enable accessing insecure content, perform the following steps:

1. Create or edit an access policy. For details, see [Create access policies](#).

2. In the **Step 3: Action** page, select **Allow with restrictions**.
3. Select **Insecure content**.
4. Click **Next** and then click **Finish**.

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



## Keylogging protection

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

## Microphone

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

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

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

1. Create or edit an access policy. For details, see [Create access policies](#).
2. In the **Step 3: Action** page, select **Allow with restrictions**.
3. Click **Microphone** and then click **Edit**.

4. In the **Microphone settings** page, click **Always allow access**.
5. Click **Save**.
6. Click **Next** and then click **Finish**.

**Note:**

- If the **Microphone** restriction is enabled in the Secure Private Access policy, then Citrix Enterprise Browser displays the settings **Allow**.
- If the option **Prompt every time** in Secure Private Access policy, then the setting applied on Citrix Enterprise Browser varies depending on whether the Global App Configuration service (GACS) is used to manage Citrix Enterprise Browser.
  - If GACS is used, then the GACS setting is applied on Citrix Enterprise Browser.
  - If GACS is not used, then Citrix Enterprise Browser displays the setting **Ask**.

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

## Notifications

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

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

To block notifications without prompting, perform the following steps.

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

## Paste

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

**Note:**

- If both **Clipboard** and **Paste** restrictions are enabled in a policy, the **Clipboard** restriction takes precedence over the **Paste** restriction.
- End users must use Citrix Enterprise Browser version 126 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.
- For granular control of paste operation within the apps, admins can use the **Security groups** restriction. For details, see [Clipboard restriction for security groups](#).

## Personal data masking

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

**Note:**

End users must use Citrix Enterprise Browser version 2405 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.

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

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

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

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

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

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

6. Click **Save** and then click **Done**.
7. Click **Next** and then click **Finish**.

### Add custom information type

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

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

Personal data masking settings

Select information type

Select...

Add

Custom 1

Field name

Visa1

Number of characters

12

Regular expression (RE2 library)

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

Select masking type

☐ Full masking

☒ Partial masking

First masked characters

3

Last masked characters

3

i

No preview available

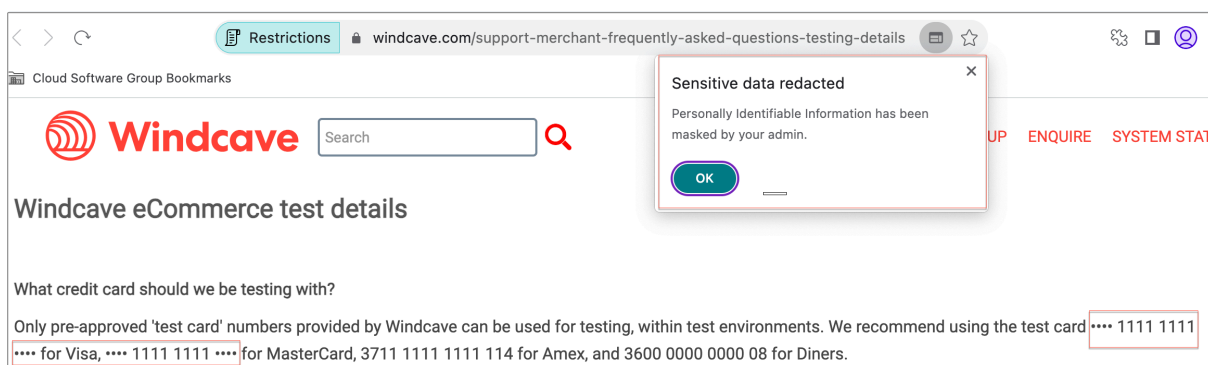
Cancel

Save

Done

Cancel

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



## Popups

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

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

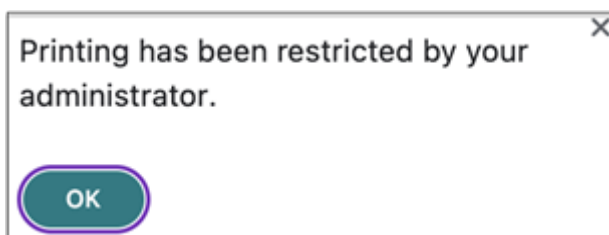
To enable display of popups, perform the following steps:

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

## Printing

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

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



**Note:**

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

## Printer management

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

**Note:**

- The **Printer management** restriction is available in addition to the **Printing** restriction where printing is either enabled or disabled.  
If both **Printing** and **Printer management** restrictions are enabled in an access policy, the **Printing** restriction takes precedence over the **Printer management** restriction.
- End users must use Citrix Enterprise Browser version 2405 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.

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

1. Create or edit an access policy. For details, see [Create access policies](#).
2. In the **Step 3: Action** page, select **Allow with restrictions**.
3. Click **Printer management** and then click **Edit**.



**Printer management settings**

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

**Network printers**

☐ Disabled

☒ Enabled

Enable printers by hostname

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

+

**Local printers**

☐ Disabled

☒ Enabled

**Print using Save as PDF**

☒ Disabled

☐ Enabled

**Save** **Cancel**

1. Select the exceptions as per your requirement.

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

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

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

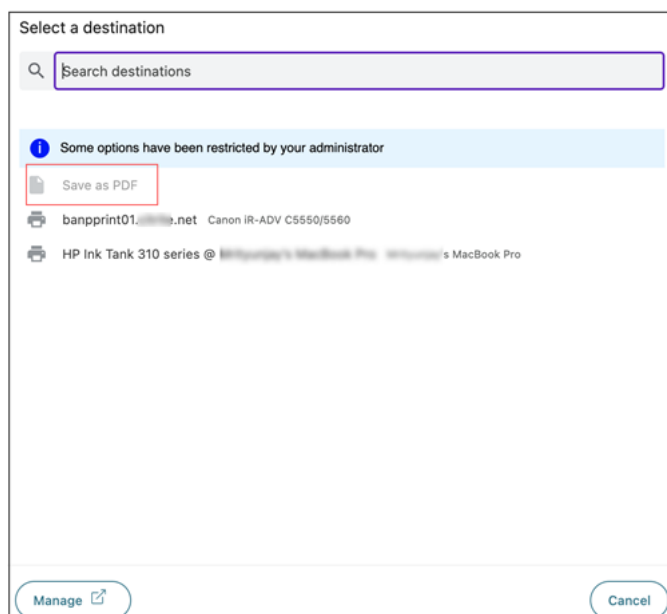
2. Click **Save**.

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

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

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

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



## Screen capture

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

## Upload restriction by file type

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

### Note:

- The **Upload restriction by file type** restriction is available in addition to the **Upload** restriction.
- If both **Upload** and **Upload restriction by file type** restrictions are enabled in a policy, the **Uploads** restriction takes precedence over the **Upload restriction by file type** restriction.

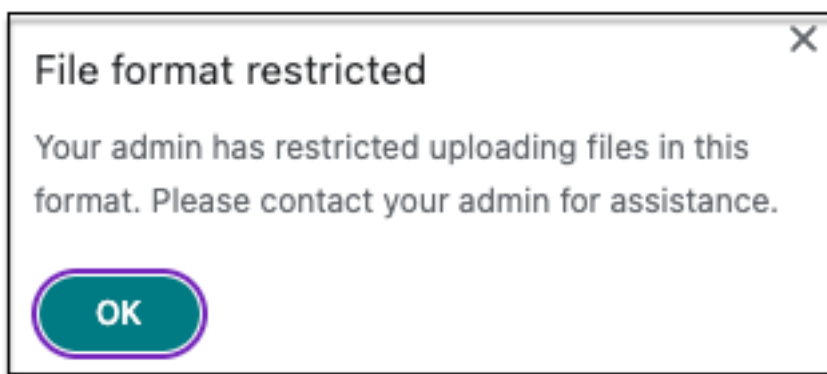
- End users must use Citrix Enterprise Browser version 2405 or later for accessing applications for which this restriction is enabled. Else, the application access is restricted.

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

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

The MIME type now appears in the list of exceptions.

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



## Uploads

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

**Note:**

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

**Watermark**

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

**Webcam**

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

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

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

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

**Note:**

- If the **Webcam** restriction is enabled in the Secure Private Access policy, then Citrix Enterprise Browser displays the settings **Allow**.
- If the option **Prompt every time** is enabled in the Secure Private Access policy, then the setting applied on Citrix Enterprise Browser varies depending on whether the Global App Configuration service (GACS) is used to manage Citrix Enterprise Browser.
  - If GACS is used, then the GACS setting is applied on Citrix Enterprise Browser.
  - If GACS is not used, then Citrix Enterprise Browser displays the setting **Ask**.

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

## Clipboard restriction for security groups

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

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

### Note:

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

To create a security group, perform the following steps:

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

Security group name

sec-group-1

Add web or SaaS applications

dribbble X Wikipedia X Pinterest X

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

> Advanced clipboard settings ?

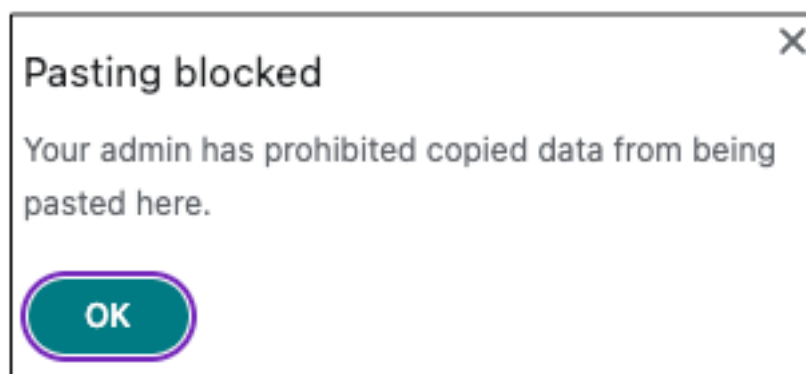
Cancel Save

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

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

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

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



**Note:**

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

### Enable granular level clipboard access

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

**Note:**

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

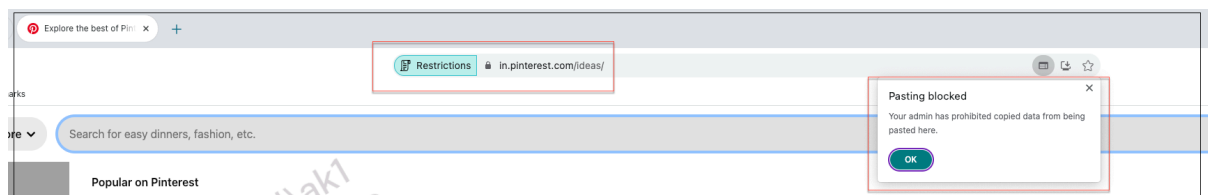
**Example:**

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

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

1. Create or edit an access policy assigned for the application **Pinterest**. For details on creating an access policy, see [Create access policies](#).
2. In the **Step 3: Action** page, select **Allow with restrictions**.
3. Select **Paste**.

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



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

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

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

Advanced clipboard settings ?

**Data out of the security group**

☐ Allow copying data from the security group to unpublished domains ?  
End users can copy data from apps within the security group and paste it into other Enterprise Browser apps.

☐ Allow copying data from the security group to native apps  
End users can copy data from apps in the security group and paste it into a local app on their machine.

**Data into the security group**

☐ Allow copying data from unpublished domains to the security group ?  
End users can copy data from other Enterprise Browser apps and paste it into apps within the security group.

☐ Allow copying data from native apps operating system apps to the security group  
End users can copy data from a local app on their machine and paste it into apps within the security group.

Cancel Save

3. Select any of the following options as per your requirement:
  - **Allow copying of data from the security group to unpublished domains**—Enable copying of data from applications in the security groups to the apps that are not published in Secure Private Access.

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

### Known issues

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

For example, assume the following scenario:

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

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

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

## Connector Appliance for Secure Private Access

September 6, 2025

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.

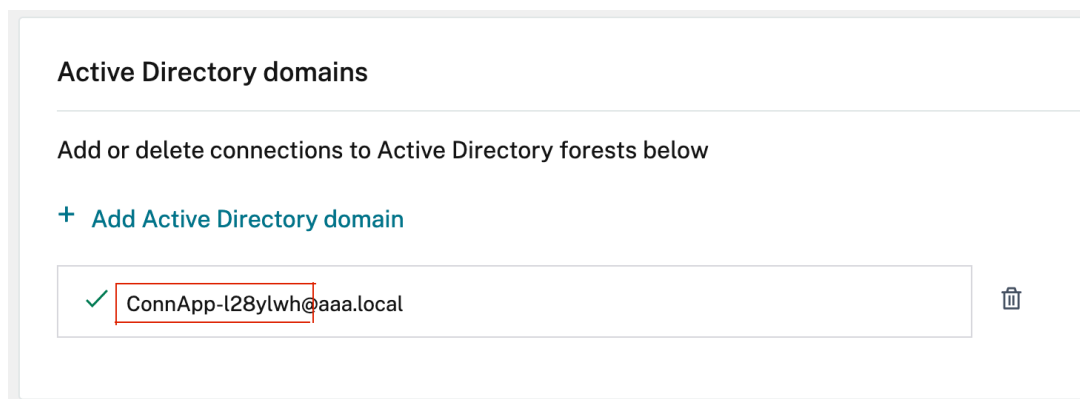
- Connect to the Connector Appliance administration webpage in your browser by using the IP address provided in the Connector Appliance console.
- In the **Active Directory domains** section, click **+ Add Active Directory** domain.  
If you don't have an **Active Directory domains** section in your 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.

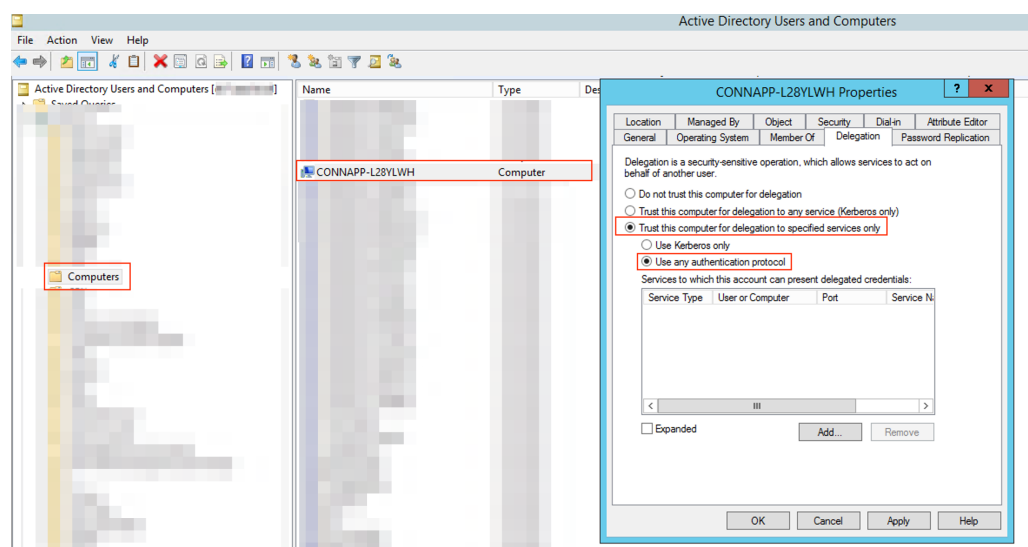
This machine name is created in the Active Directory domain when the Connector Appliance joins it.

- Click **Join**.

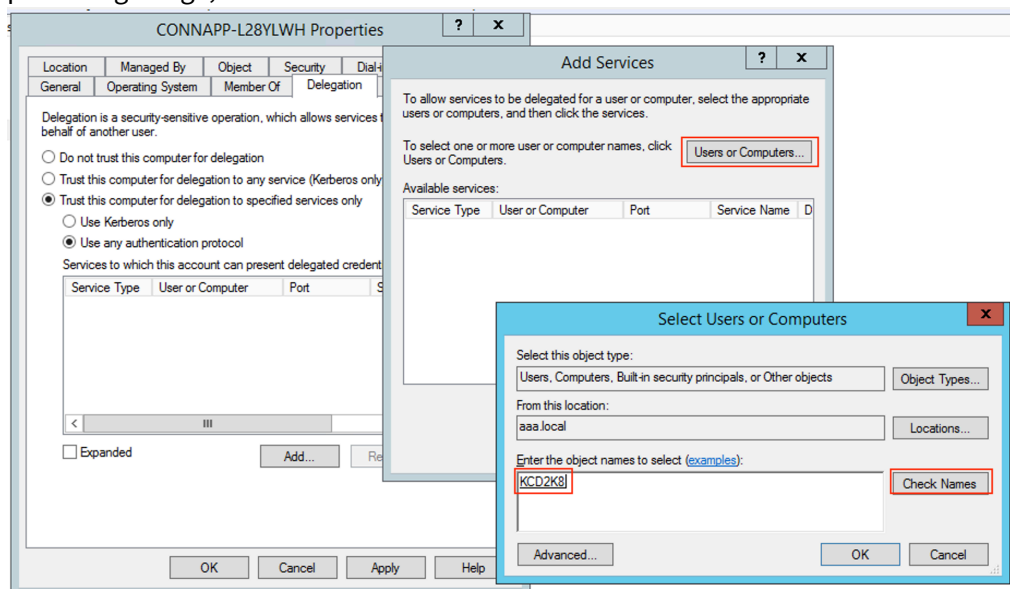
b) Configure Kerberos Constraint Delegation for web server without a load balancer.



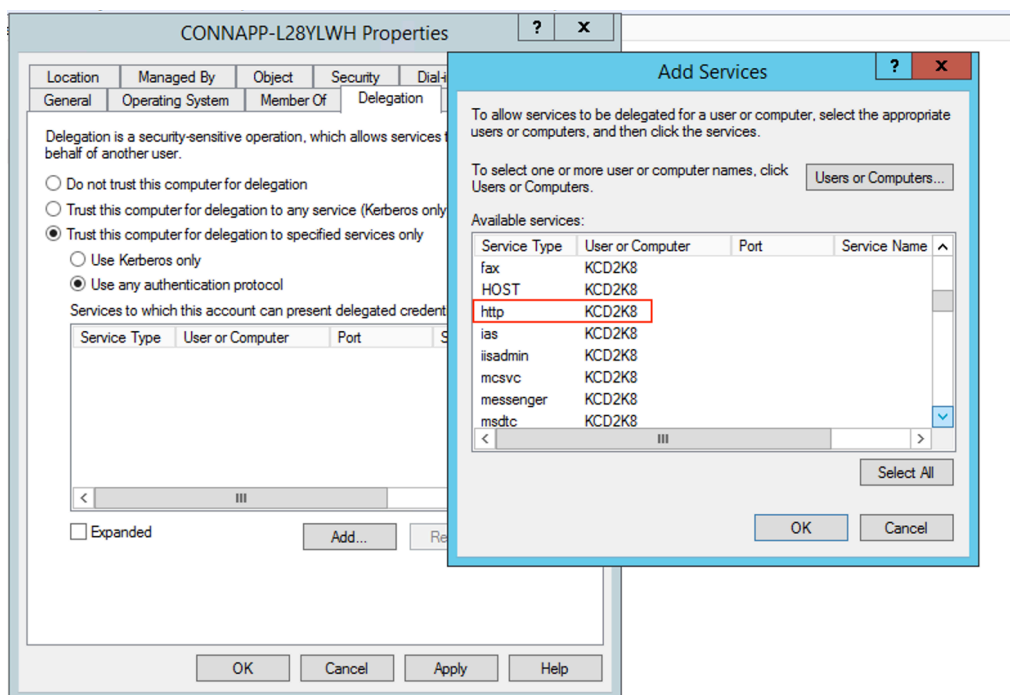
- Identify the connector appliance computer name. You can get this name either from the place where you hosted or simply from the connector UI.
- On your Active Directory controller, look for the connector appliance computer.
- Go to the properties of the Connector Appliance computer account, and navigate 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.

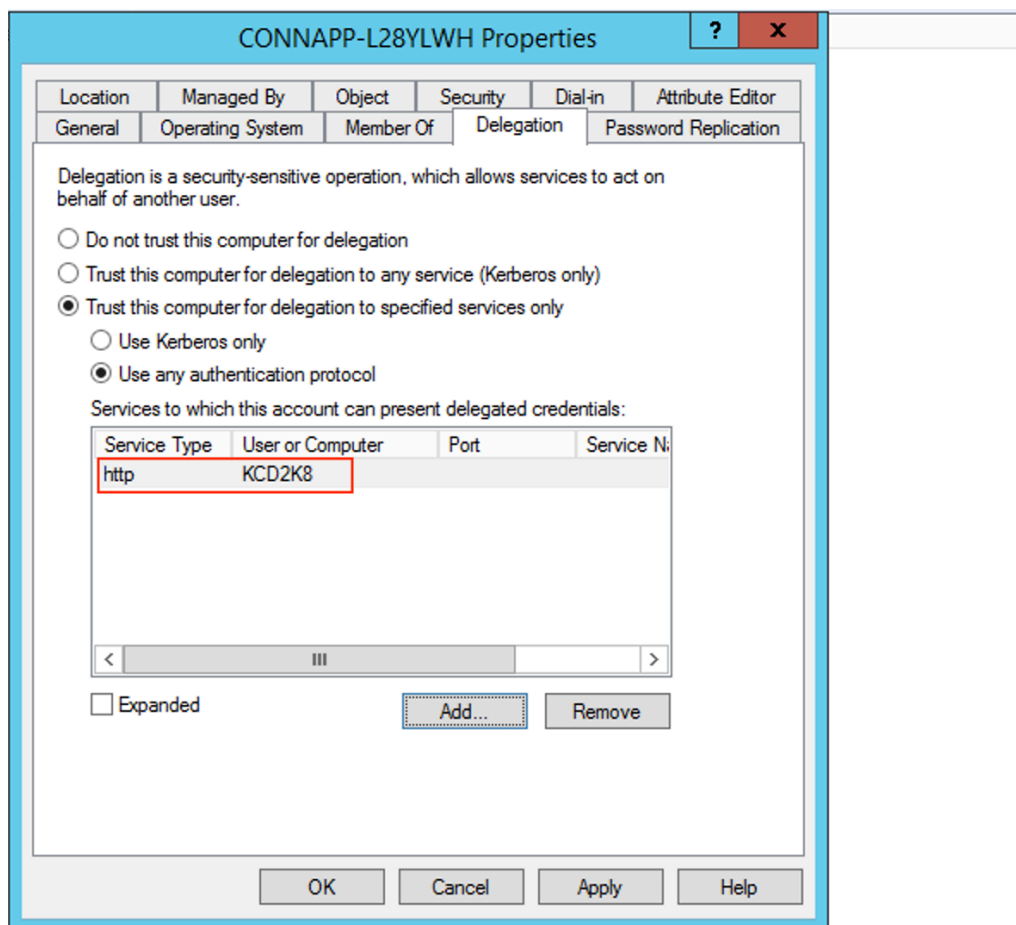


- click **OK**.
- Select the service type **http**.



- 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.

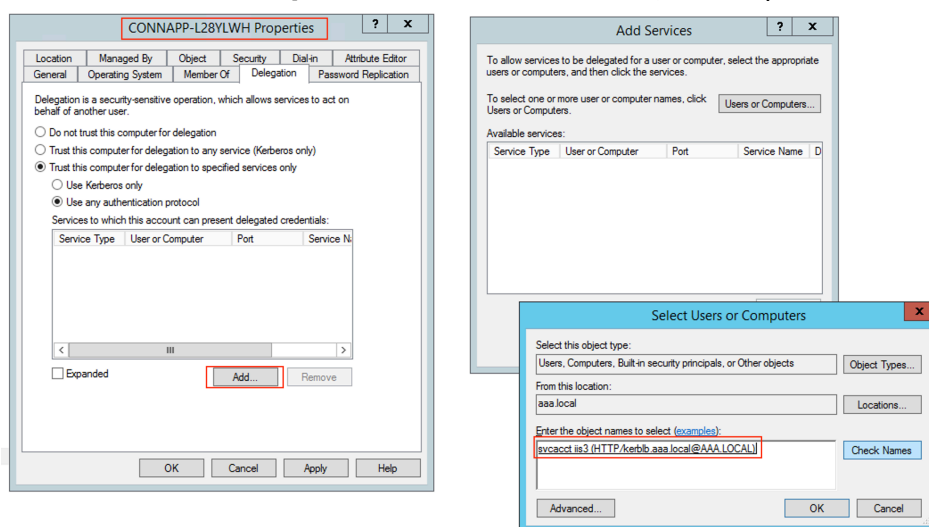
```
setspn -S HTTP/<web_server_fqdn> <service_account>
```

```
C:\Windows\system32>setspn -s HTTP/kcd-lb.aaa.local aaa\svc_iis3
Checking domain DC=aaa,DC=local
Registering ServicePrincipalNames for CN=svcacct iis3,OU=Users,OU=KCD,DC=aaa,DC=local
HTTP/kcd-lb.aaa.local
Updated object
C:\Windows\system32>_
```

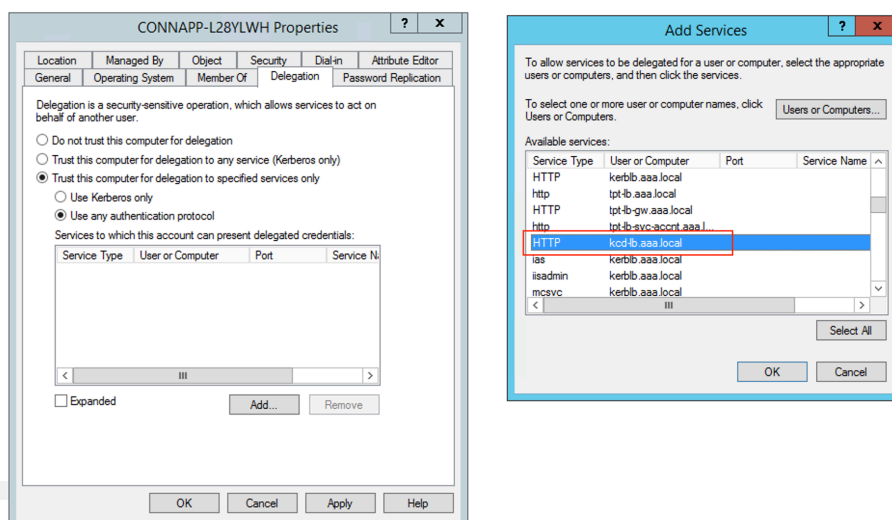
- Confirm the SPNs for the service account using the following command.
- ```
setspn -l <service_account>
```

```
C:\Windows\system32>setspn -l aaa\svc_iis3
Registered ServicePrincipalNames for CN=svcacct iis3,OU=Users,OU=KCD,DC=aaa,DC=1
local:
HTTP/kcd-lb.aaa.local
http/ntlm-lb.aaa.local
C:\Windows\system32>
```

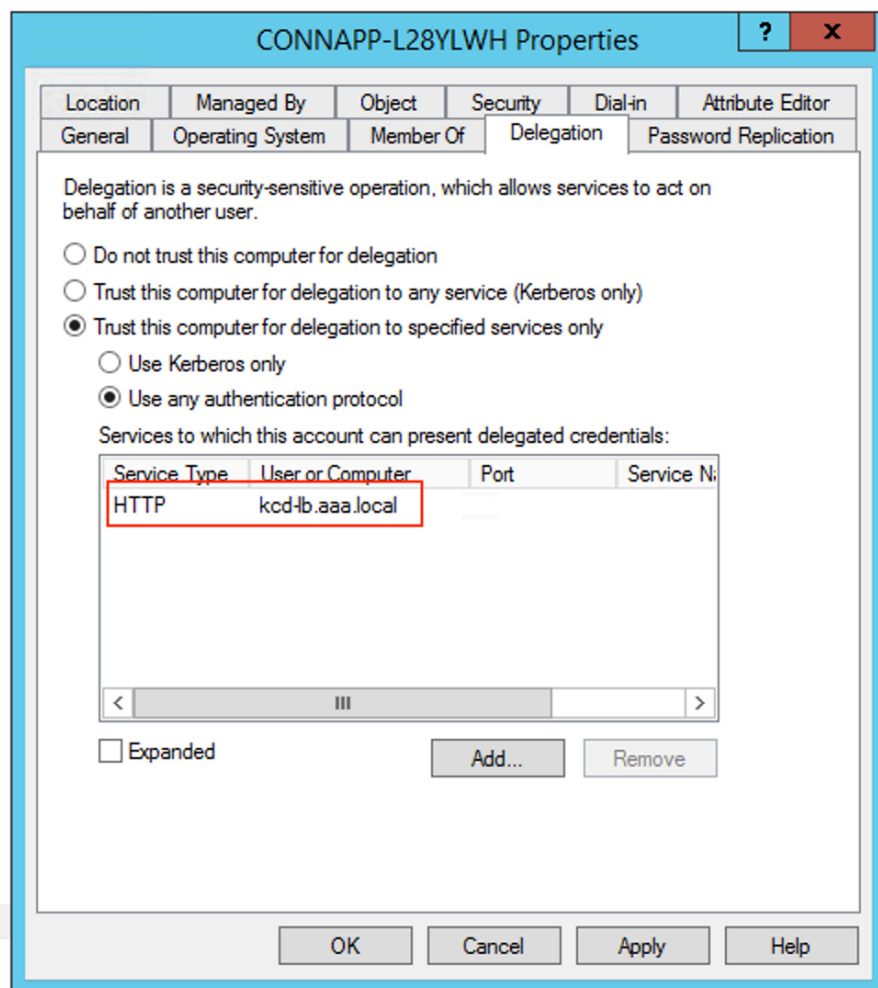
- Create a delegation for the connector appliance computer account.
  - Follow the steps to *Configure Kerberos Constraint Delegation for the webserver* without a load balancer to identify the CA machine and navigate to the Delegation UI.
  - In select **Users and Computers**, select service account (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**.



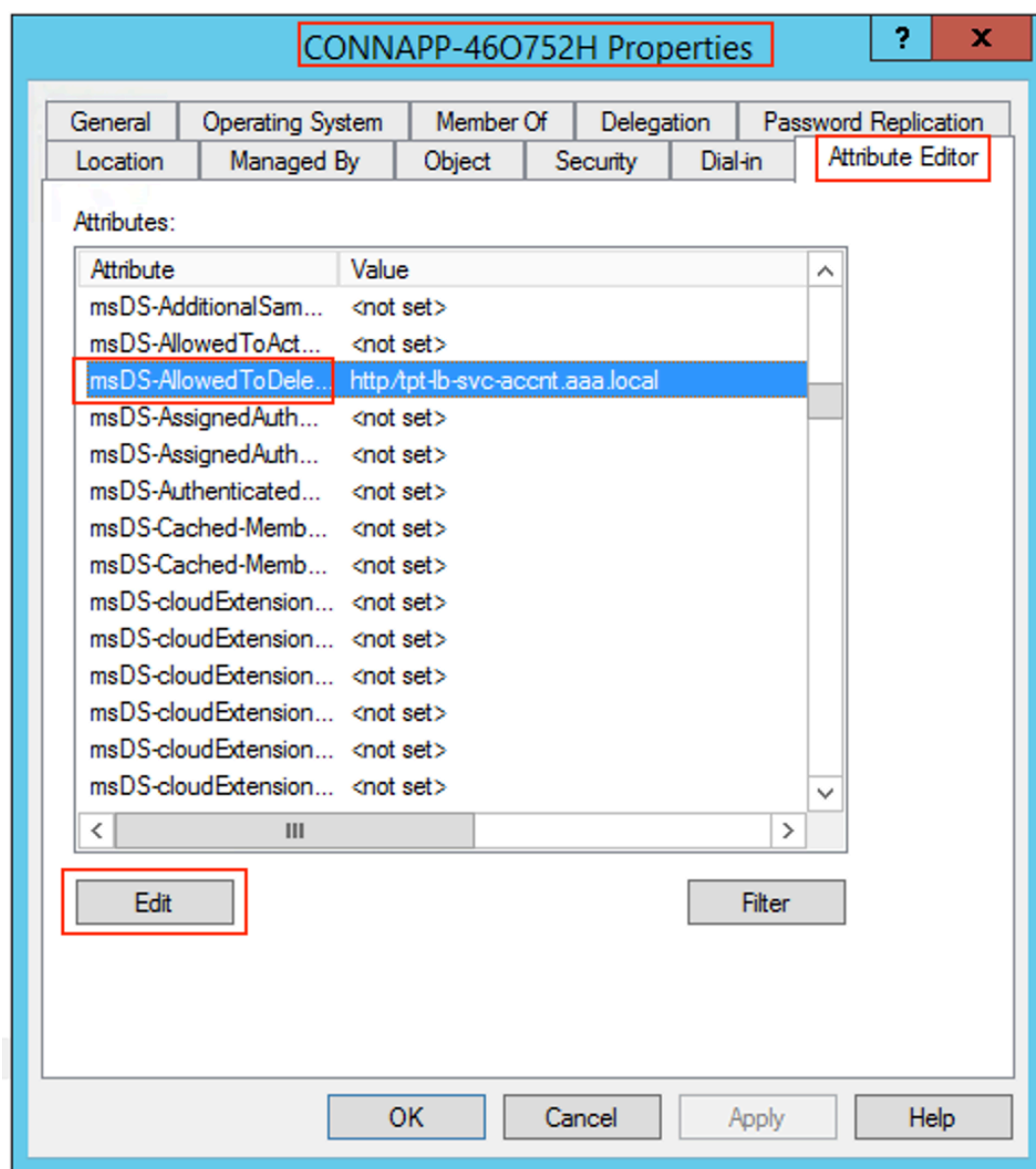
- d) Configure Kerberos Constrained Delegation (KCD) for a group managed service account.
- Add SPN to the group managed service account if not already done.  
`setspn -S HTTP/<web_server_fqdn> <group_managed_service_account>`
  - Confirm the SPN using following command.  
`setspn -l <group_managed_service_account>`

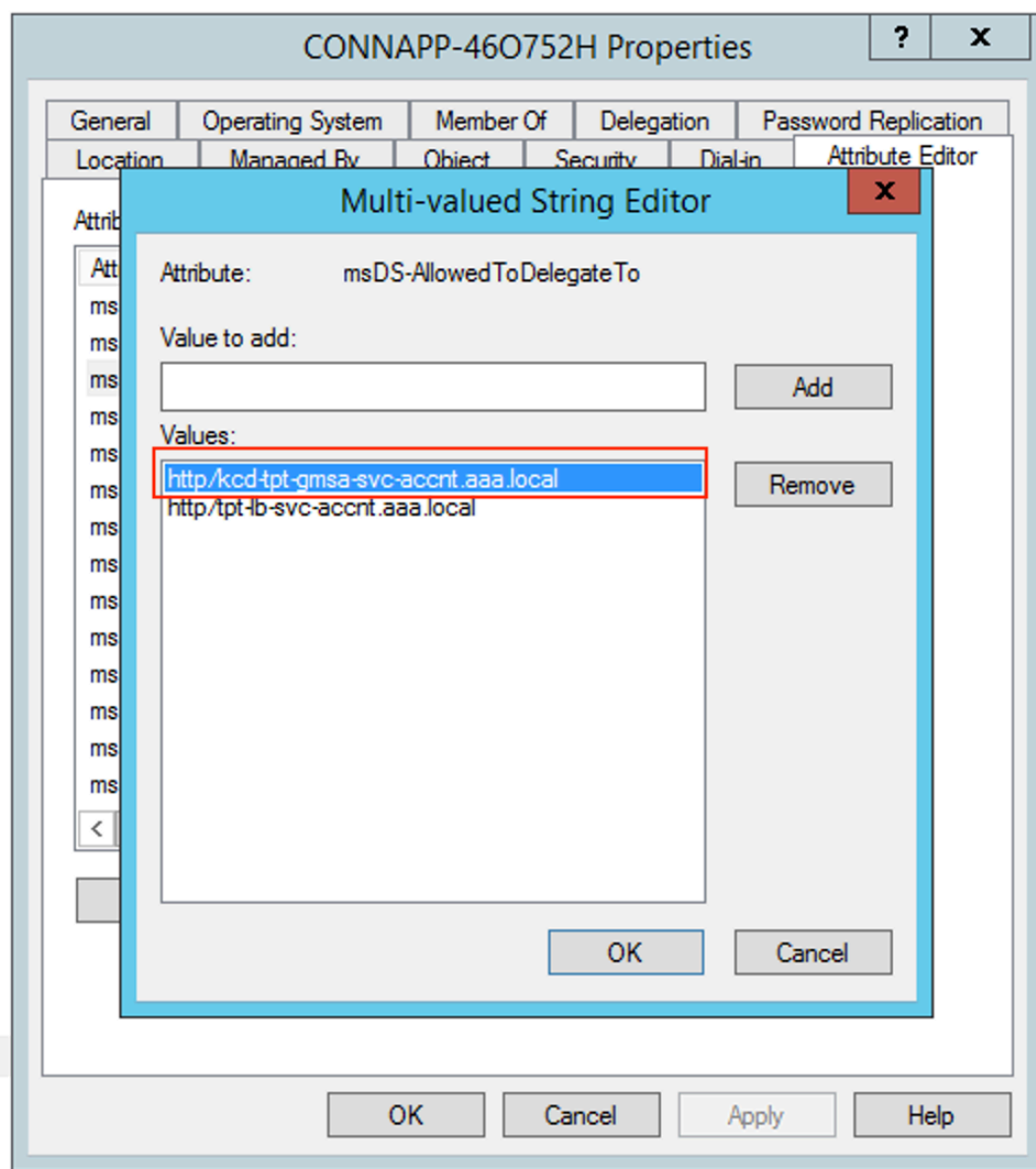
Because the group managed service account cannot be shown in **Users and Computers** search while adding the delegation entry for the computer account, you cannot add the delegation for a computer account using the usual method. Therefore, you can add this SPN as being delegated entry to the CA computer 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>
```



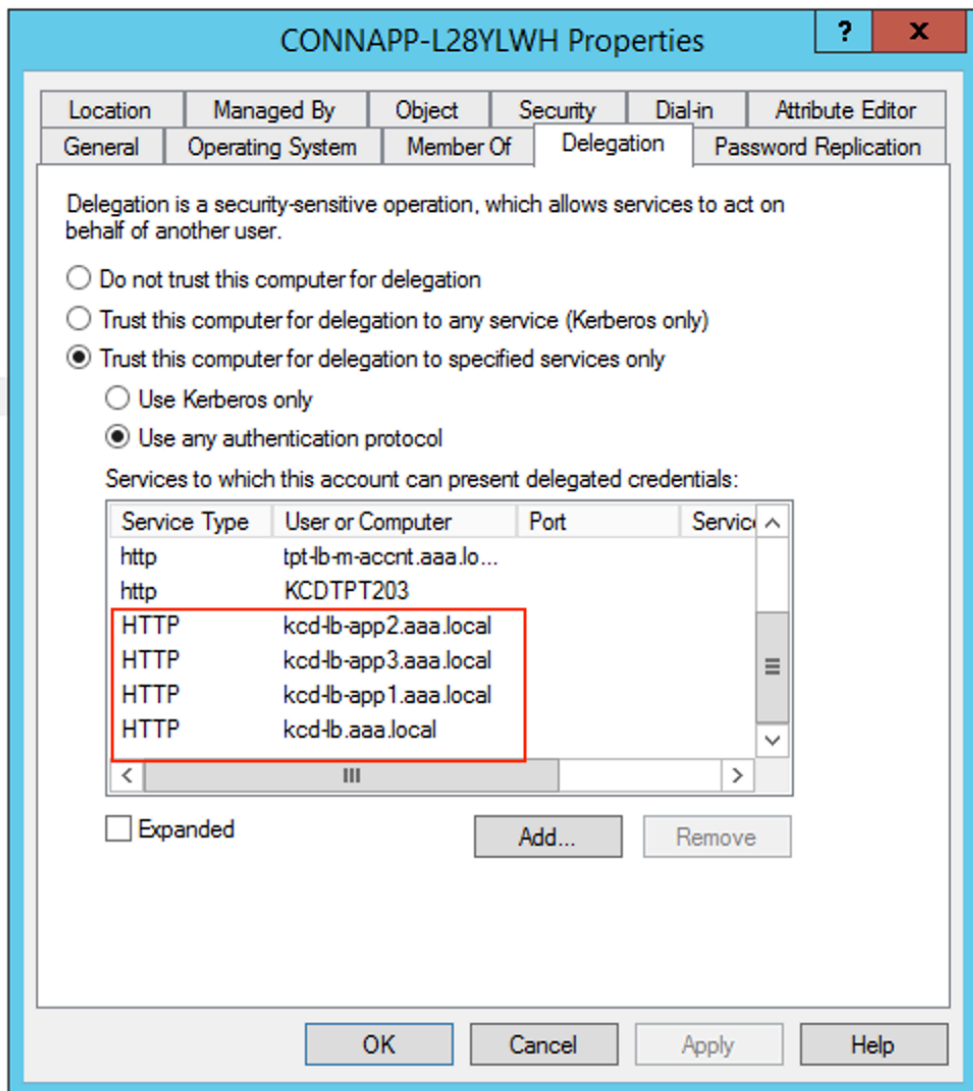
```

C:\Windows\system32>setspn -l aaa\svc_iis3
Registered ServicePrincipalNames for CN=svcacct iis3,OU=Users,OU=KCD,DC=aaa,DC=1
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 entries 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 entries 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

September 6, 2025

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](#).

## Advanced Secure Private Access features

September 6, 2025

The following are some of the advanced features supported by Secure Private Access:

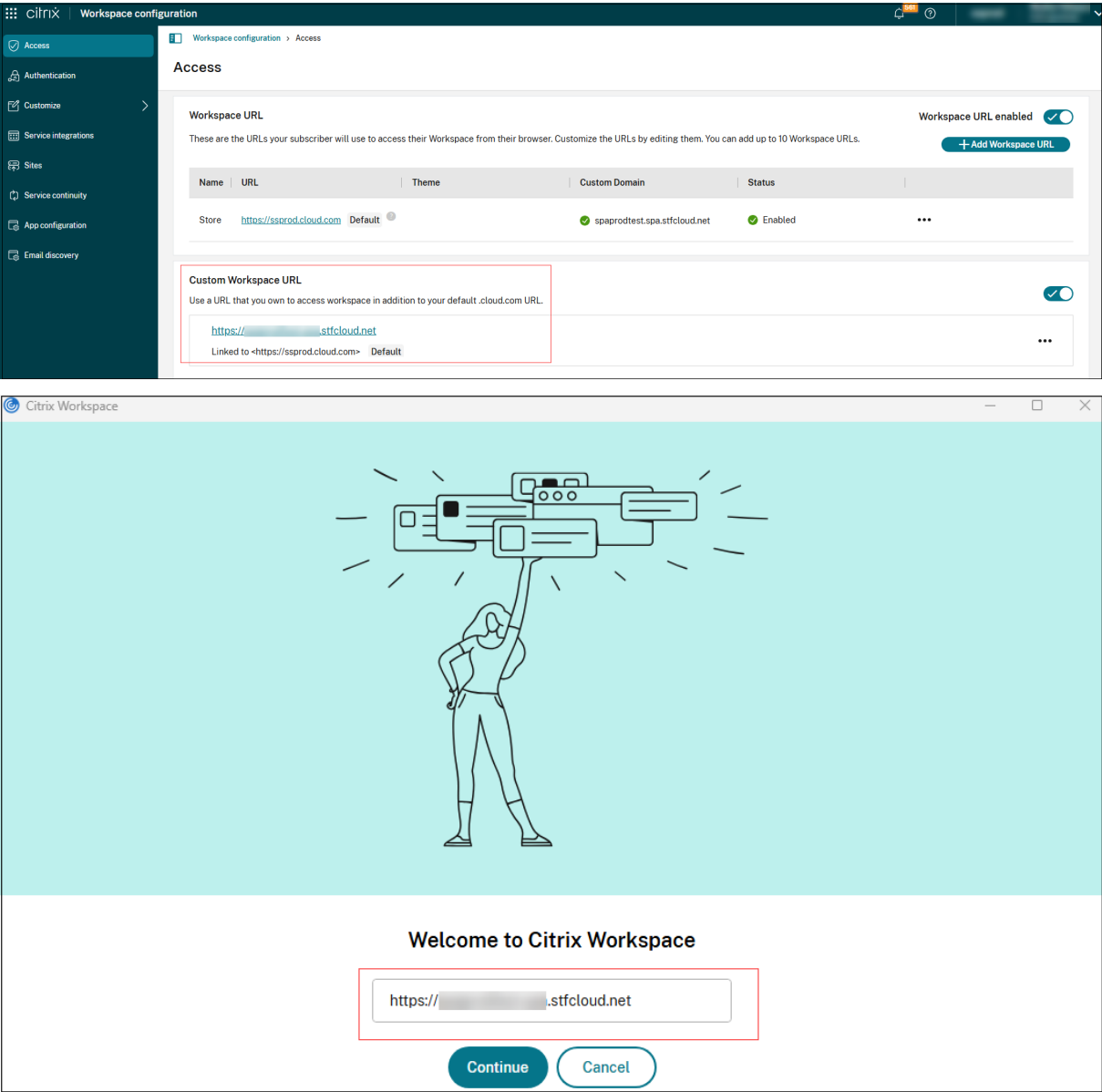
- **Custom workspace domains for accessing apps via Citrix Enterprise Browser:** The custom workspace domain feature allows organizations to provide users with access to SaaS and private web applications through a branded, organization-owned domain (for example, workspace.company.com) instead of the default \*.cloud.com domain. For details, see Custom workspace domains for accessing apps via Citrix Enterprise Browser. For details, see [Custom workspace domains for accessing apps via Citrix Enterprise Browser](#).
- **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, user risk score, 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](#).

## Custom workspace domains for accessing apps via Citrix Enterprise Browser™

September 6, 2025

Custom workspace domain support 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. Admins can configure a custom domain as the authentication and access endpoint for browser-based applications delivered via Citrix Enterprise Browser and Citrix Secure Private Access. End users benefit from a seamless, branded experience while organizations gain greater control over access and security.



Previously, custom workspace domains were only available for virtual apps and desktops. With the introduction of this feature, web-based applications accessed via Citrix Enterprise Browser and Secure Private Access also benefit from the same branding and security advantages. This ensures a cohesive and consistent domain experience across all Citrix Workspace™ services.

**Note:**

Currently, the custom workspace domains feature is disabled by default. Reach out to Citrix Support to get this feature enabled. This feature will be enabled by default to all customers soon.

## **Benefits of using a custom domain**

The following are some of the benefits of using a custom domain:

- Direct users to a familiar, branded URL for all web and SaaS app access.
- Use a privately owned domain as the authentication and access endpoint.
- Reduce the risk of impersonation and phishing attacks.

Custom domains feature help address the following limitations:

- Undermine corporate branding and user trust.
- Complicate regulatory compliance for organizations requiring access through company-owned domains.
- Increase the risk of phishing or impersonation attacks.
- Limit the ability to enforce access restrictions based on domain.

## **Applicability**

- The custom workspace domains feature is applicable only to the following:
  - Private web apps and SaaS apps accessed via Citrix Enterprise Browser.
  - Agentless access to web apps via Citrix Secure Private Access.
- The custom workspace domains are not supported for the TCP/UDP apps accessed via Citrix Secure Access.

**Note:**

Access to \*.cloud.com domain must be allowed from end-user devices to ensure proper functionality of web and SaaS applications within the custom workspace.

## **Prerequisites to configure custom domains**

Ensure that the following prerequisites are met to use custom domains.

- Custom domain settings must be configured in Citrix Workspace. For details, see [Configure a custom domain](#).
- The client versions support the custom domain feature.

- Citrix Workspace app for Windows: 2503.10 or later
- Citrix Workspace app for Mac: 2505.10 or later

## Hybrid data path for Secure Private Access service

September 6, 2025

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

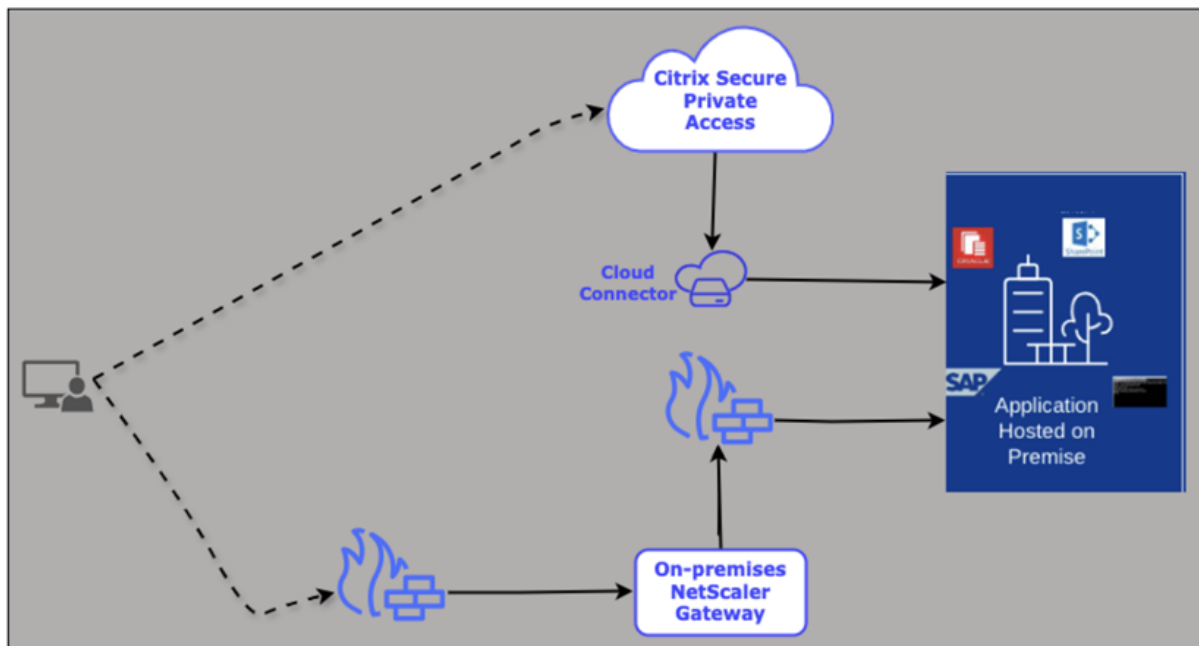
The following are some of the key advantages of using the hybrid data path:

- 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.

## **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.

## Connect to Gateway

×

Connect to a Gateway and select the Gateway type to provide access to the services available in the resource location. Gateways for DaaS and Secure Private Access can be added to the same resource location.  
[Learn more](#)

---

### Choose Gateway type

#### Gateway for DaaS

Use a Citrix-managed Gateway for external connectivity to virtual apps and desktops in Citrix DaaS. HDX connections between clients and VDAs are proxied through the Gateway service.

#### Gateway for Secure Private Access

Use an on-premises Gateway to connect to Secure Private Access services in the resource location.

Cancel

- **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. For details, see [Connectivity to resources](#).

- **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**.

## Connect to Gateway

Secure Private Access

Connect to an on-premises Gateway to use Secure Private Access services available in the resource location.  
[Learn more](#)

1. Enter the Gateway FQDN

spa.test.com
Edit

2. Generate metadata

Copy the metadata, remote into your Gateway, and paste the copied metadata into the required script to receive an 8-digit registration code. [Learn more](#)

Metadata
eyJnYXRld2F5RnFkbil6ICJzcGEudGVzdC5jb20iLCAiaW5zdGFuY2VJ

Regenerate metadata

3. Register with Citrix Cloud

Enter the 8-digit code you received from the Gateway to validate and then register the Gateway with Citrix Cloud.

A N Z K — 3 F T 1
Validate

Back
Cancel

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.

App Connectivity

URL \*

https://developer-docs.citrix.com

Routing Type \*

Internal via NetScaler Gateway

Primary Resource Location \* ⓘ



AAA-ConnApp

1 Gateway FQDN is available [Refresh](#)

Related Domains

www.example.org or \*.example.org

Add

| Related Domains             | Routing Type                   | Primary Resource Location | Available Connectors/Gateways | Actions                                                                                                                                                                 |
|-----------------------------|--------------------------------|---------------------------|-------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| *.developer-docs.citrix.com | Internal via NetScaler Gateway | AAA-ConnApp               | 1                             |   |

Showing 1-1 of 1 items

Page 1 of 1

5 rows

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](#).

**Step 3: Action**

**Action for HTTP/HTTPS apps \***

☒ Allow access

☐ Allow access with restrictions

☐ Deny access

**Action for TCP/UDP apps \* ?**

☒ Allow access

☐ Deny access

**Routing exceptions ? ☒**

Changing the routing type or resource location for these domains will create a routing exception. Routing exceptions will apply to all users in this access policy only. [Learn more](#)

Search for a domain

| FQDN/IP             | Routing Type           | Primary Resource Location | Actions |
|---------------------|------------------------|---------------------------|---------|
| www.nature.org      | Internal via Connector | AAA RL 01                 |         |
| *.nature.org        | Internal via Connector | AAA RL 01                 |         |
| *.fonts.gstatic.com | Internal via Connector | Azure_A2V2                |         |

Showing 1-3 of 3 items Page 1 of 1 10 rows

**Change routing details**

Changing the routing type or resource location for this domain will create a routing exception. This routing exception will apply to all users in the access policy.

URL \*  
www.nature.org

Routing type \*  
Internal via NetScaler Gateway

Primary resource location \*  
spaopdev/local RL1

1 Gateway FQDN is available [Refresh](#)

- 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.
- Click the edit icon next to the domain for which you want to modify the routing type.
- In **Routing type**, select **Internal via NetScaler Gateway**.
- Click **Save**.

### Points to note

- 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](#)

## Discover applications, domains, or IP addresses within your network

September 6, 2025

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

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

- Provides visibility into both internal or external domains/IPs addresses accessed by the end users.
- Provides a comprehensive visibility into all types of applications accessed (HTTP, HTTPS, TCP, and UDP). All access methods are supported, that is access via Citrix Enterprise Browser™, Secure Access Agent, Direct Access, or Workspace for Web.
- 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.

Secure Private Access > Applications > App Discovery

Configure and secure enterprise applications from unwanted access.

All protocols Last 1 Week Add filter

App discovery shows list of domains visited by end-users. Select one or more domains to add them to a new or existing application. Click on dropdown button to see related domains of the main app domain.

3 Selected View selected only Create application Add to an existing application

|   | Domain/IP                   | Port | Protocol | Total Visits | Unique Users | Most Recent Visit   | Assigned To App(S) |
|---|-----------------------------|------|----------|--------------|--------------|---------------------|--------------------|
| ✓ | pg-dev-ed.my.salesforce.com | 443  | HTTPS    | 11           | 2            | 2024-07-26 21:18:51 | 2                  |
| ✓ | a.sfdcstatic.com            | 443  | HTTPS    | 11           | 2            | 2024-07-30 11:37:16 | 0                  |
| ✓ | c.salesforce.com            | 443  | HTTPS    | 11           | 2            | 2024-07-30 11:37:16 | 0                  |
| ✓ | geolocation.onetrust.com    | 443  | HTTPS    | 11           | 2            | 2024-07-30 11:37:16 | 0                  |
|   | login.salesforce.com        | 443  | HTTPS    | 11           | 2            | 2024-07-30 11:37:16 | 0                  |
|   | www.google-analytics.com    | 443  | HTTPS    | 11           | 2            | 2024-07-30 11:37:16 | 0                  |
|   | www.googletagmanager.com    | 443  | HTTPS    | 11           | 2            | 2024-07-30 11:37:16 | 0                  |
|   | www.salesforce.com          | 443  | HTTPS    | 11           | 2            | 2024-07-30 11:37:16 | 0                  |

#### 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.

|                                                                                                            |                                                                                                                                                                                                        |
|------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>App type *</b><br><input type="text" value="HTTP/HTTPS"/>                                               | <b>App icon</b><br> <a href="#">Change icon</a> <a href="#">Use default icon</a><br><small>(128 KB max, PNG)</small> |
| <b>App name *</b><br><input type="text" value="Discover_app1"/>                                            | <input type="checkbox"/> Do not display application icon in Workspace app                                                                                                                              |
| <b>App description</b><br><input type="text"/>                                                             | <input type="checkbox"/> Add application to favorites in Workspace app                                                                                                                                 |
| <b>App category ?</b><br><input type="text" value="Ex.: Category\SubCategory\SubCategory"/>                | <input type="radio"/> Allow user to remove from favorites<br><input type="radio"/> Do not allow user to remove from favorites                                                                          |
| <input type="checkbox"/> Direct Access<br>Enable direct browser-based access to internal web applications. |                                                                                                                                                                                                        |
| <b>URL *</b><br><input type="text" value="https://test.citrix.com"/>                                       |                                                                                                                                                                                                        |
| <b>Related Domains * ?</b><br><input type="text" value="*.docs.citrix.com"/>                               |                                                                                                                                                                                                        |

Web app URL: <https://test.citrix.com/>

Related domain: \*.[citrix.com](https://test.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

The screenshot shows a web form for configuring an application. It is divided into two main sections: 'App details' and 'Destinations'.

**App details section:**

- App type \***: A dropdown menu with 'TCP/UDP' selected.
- App name \***: A text input field containing 'Discover\_app2'.
- App description**: An empty text area.
- App icon**: A section with an icon placeholder, a 'Change icon' link (with '(128 KB max, PNG)' below it), and a 'Use default icon' link. Below these are two links: 'Citrix Secure Access Client for Windows' and 'Citrix Secure Access Client for macOS'.

**Destinations section:**

This section contains three input fields:

- Destination \***: A text input field containing '10.0.0.0/8'.
- Port \***: A text input field containing '443'.
- Protocol \***: A dropdown menu with 'TCP' selected.

- 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)].

## 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**.

The screenshot shows the Citrix Secure Private Access console. The left sidebar contains navigation options: App Configuration, App Discovery (selected), and Security Groups. The main area is titled 'Secure Private Access > Applications > App Discovery' and contains a table of discovered domains. The table has columns for Domain/IP, Port, Protocol, Total Visits, Unique Users, Most Recent Visit, and Assigned To App. Four domains are selected, indicated by checkboxes. To the right, the 'Edit app' panel is open, showing fields for App category (saas), URL (https://rapido.com), and Related Domains. The Related Domains field is populated with a list of domains, including \*.rapido.com, \*.7bas813.webbengage.co, \*.a.quora.com, \*.c.webbengage.com, \*.cdn.taboola.com, \*.cdnjs.cloudflare.com, \*.code.lavex.com, \*.connect.facebook.net, \*.eosafe.com, and \*.eosafeads.g.doubleclick.net.

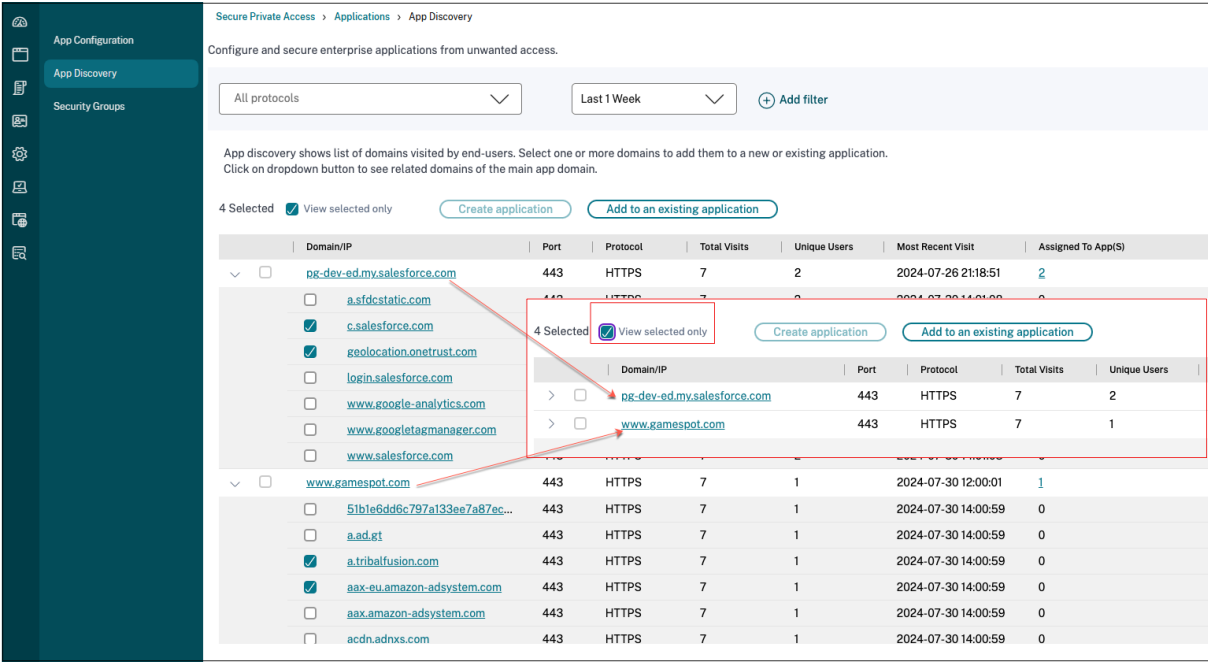
| Domain/IP                                                 | Port | Protocol | Total Visits | Unique Users | Most Recent Visit   | Assigned To App |
|-----------------------------------------------------------|------|----------|--------------|--------------|---------------------|-----------------|
| <input type="checkbox"/> 10.222.102.178                   | 3389 | TCP      | 10           | 1            | 2024-07-25 10:30:48 | 0               |
| <input type="checkbox"/> fonts.gstatic.com                | 443  | HTTPS    | 10           | 1            | 2024-07-23 15:22:13 | 1               |
| <input type="checkbox"/> 10.221.40.139                    | 3389 | TCP      | 8            | 1            | 2024-07-29 12:26:54 | 0               |
| <input type="checkbox"/> www.designsafe.com               | 443  | HTTPS    | 8            | 3            | 2024-07-24 17:55:09 | 0               |
| <input checked="" type="checkbox"/> 7bas813.webbengage.co | 443  | HTTPS    | 8            | 3            | 2024-07-30 11:44:48 | 0               |
| <input checked="" type="checkbox"/> a.quora.com           | 443  | HTTPS    | 8            | 3            | 2024-07-30 11:44:48 | 0               |
| <input type="checkbox"/> analytics.eosafe.com             | 443  | HTTPS    | 8            | 3            | 2024-07-30 11:44:48 | 0               |
| <input type="checkbox"/> bust.bing.com                    | 443  | HTTPS    | 8            | 3            | 2024-07-30 11:44:48 | 0               |
| <input checked="" type="checkbox"/> c.webbengage.com      | 443  | HTTPS    | 8            | 3            | 2024-07-30 11:44:48 | 0               |
| <input type="checkbox"/> cdn.taboola.com                  | 443  | HTTPS    | 8            | 3            | 2024-07-30 11:44:48 | 0               |
| <input checked="" type="checkbox"/> cdnjs.cloudflare.com  | 443  | HTTPS    | 8            | 3            | 2024-07-30 11:44:48 | 0               |
| <input type="checkbox"/> cdn.taboola.com                  | 443  | HTTPS    | 8            | 3            | 2024-07-30 11:44:48 | 0               |
| <input type="checkbox"/> code.lavex.com                   | 443  | HTTPS    | 8            | 3            | 2024-07-30 11:44:48 | 0               |
| <input type="checkbox"/> connect.facebook.net             | 443  | HTTPS    | 8            | 3            | 2024-07-30 11:44:48 | 0               |
| <input type="checkbox"/> eosafe.com                       | 443  | HTTPS    | 8            | 3            | 2024-07-30 11:44:48 | 2               |
| <input type="checkbox"/> eosafeads.g.doubleclick.net      | 443  | HTTPS    | 8            | 3            | 2024-07-30 11:44:48 | 0               |

#### 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 locations selection

September 6, 2025

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 re-

source 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 Access Policies using the **Routing Exceptions** feature. 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.

**Step 3: Action**

**Action for HTTP/HTTPS apps \***

☒ Allow access  
☐ Allow access with restrictions  
☐ Deny access

**Action for TCP/UDP apps \***

☒ Allow access  
☐ Deny access

**Routing exceptions** ☒

Changing the routing type or resource location for these domains will create a routing exception. Routing exceptions will to all users in this access policy only. [Learn more](#)

Search for a domain

| FQDN/IP                       | Routing Type | Resource Location | Actions |
|-------------------------------|--------------|-------------------|---------|
| ak1.mgmt.netscalergateway...  | Internal     | AAA-ConnApp       |         |
| pki-google.l.google.com       | Internal     | AAA-ConnApp       |         |
| *.ak1.mgmt.netscalergatewa... | Internal     | AAA-ConnApp       |         |
| ven01955.service-now.com      | External     |                   |         |
| *.service-now.com             | External     |                   |         |

**Change routing details**

Changing the routing type or resource location for this domain will create a routing exception. This routing exception will apply to all users in the access policy.

URL \*  
ak1.mgmt.netscalergatewaydev.net

Routing type \*  
Internal

Resource location \*  
AAA-ConnApp

Back Next

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.

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.

**Routing exceptions** ? ☒

Changing the routing type or resource location for these domains will create a routing exception that will apply to all users in the access policy only. [Learn more](#)

Search for a domain

| FQDN/IP        | Routing Type           | Resource Location |
|----------------|------------------------|-------------------|
| 12.11.13.29/32 | Internal via Connector | Sandy             |
| 12.11.13.27    | Internal via Connector | Sandy             |
| 12.11.13.28/32 | Internal via Connector | NewConnectApp-2   |

URL \*  
12.11.13.29/32

Routing type \*  
Internal via Connector  
Internal via Connector  
Sandy

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.

### 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 Connector**.
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**.

Secure Private Access > Policies > Create/Edit Session Policy

### Create session policy

Policy name  
session

Description (optional)  
Enter a description

**Conditions**  
Add the user conditions to which you would like to apply the settings below.

User:  
All users

AND

Geo-location Matches any of India

AND

Network location Matches any of hyd\_ip

+ Add condition

**Settings**  
Choose at least one setting to add to this policy.

Direct routing  
Route all users externally for all applications.

**Policy enablement**  
☒ Enable policy after creation

Cancel Save

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.
  5. (Optional) Click + to add multiple conditions based on the context.
  6. 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](#).
7. Select **Direct routing** to route all users externally to the back-end applications.
  8. 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.

9. 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.

## 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/SaaS 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](#).

## Policy modeling tool

September 6, 2025

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, user risk score, and workspace 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 Workspace 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:

Secure Private Access > Policies > Policy Modeling

Model user or machine access outcomes, given various contexts and conditions.

All Apps

URL

IP/Port

Users

Machines

Device type

Select IDP

Domain

Username or user group

Desktop

\* Ad

aaa.local

ak4

+

 Simulate conditions

User information

Account name: ak4

Email address:

Display name: ak4 test

Domain name: aaa.local

Application access

Filter by app name

| Application Name   | Result                                    | Access Policy Name | Rule Name          | Actions |
|--------------------|-------------------------------------------|--------------------|--------------------|---------|
| saasapps-totb-itr3 | No policy matched - Access will be denied | N/A                | N/A                |         |
| Salesforce-staging | Access will be allowed                    | Salesforce-staging | Salesforce-staging |         |
| BingTest           | Access will be allowed with restrictions  | OpenInRBI          | OpenInRBI          |         |
| sss_web-1          | No policy matched - Access will be denied | N/A                | N/A                |         |
| test_saasapp2      | No access policy found                    | N/A                | N/A                |         |

The following figure displays the policy analyzer for a web app:

Secure Private Access > Policies > Policy Modeling

Model user or machine access outcomes, given various contexts and conditions.

All Apps

URL

IP/Port

Users

Machines

Device type

Select IDP

Domain

Username or user group

Desktop

\* Ad

aaa.local

dkr

URL

https://textbook. .netscalergatewayde

Apply

+

 Simulate conditions

User information

Account name: dkr

Email address:

Display name:

Domain name: aaa.local

Application access

Filter by app name

| Application Name    | Result                                   | Access Policy Name  | Rule Name       | Actions |
|---------------------|------------------------------------------|---------------------|-----------------|---------|
| app-policy-modeling | Access will be allowed with restrictions | Policy-modeling-123 | Policy-modeling |         |

Showing 1-1 of 1 itemsPage 1 of 125 rows

The following figure displays the policy analyzer for a TCP app:

Secure Private Access > Policies > Policy Modeling

Model user or machine access outcomes, given various contexts and conditions.

All Apps

URL

IP/Port

Users

Machines

Device type

Desktop

Select IDP

\* Ad

Domain

aaa.local

Username or user group

as1

Type

TCP

IP:Port

10.10.10.1:443

Apply

Simulate conditions

User information

Account name: as1

Email address:

Display name: as1

Domain name: aaa.local

Application access

Filter by app name

| Application Name | Result                 | Access Policy Name | Rule Name | Actions |
|------------------|------------------------|--------------------|-----------|---------|
| 2025-TCP-Test    | Access will be allowed | 2025-PolicyTest    | rule1     |         |

Showing 1-1 of 1 itemsPage 1 of 125 rows

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.                                                                                                                                                                                                                                                                     |
| 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.<br>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). |

| Field                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Routing Type              | <p>The routing type details the path a user's request takes through the Secure Private Access service.</p> <p><b>External</b> Requests are routed directly to the intended destination.</p> <p><b>Internal via Connector</b> Requests are routed through a Connector.</p> <p><b>Internal via Gateway</b> 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 <a href="#">Hybrid data path for Secure Private Access services</a>.</p> |
| Primary Resource Location | Name associated with the primary location of the application.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| 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.

Access and routing details for 2025-TCP-Test

Application: 2025-TCP-Test  
Matching Access policy: 2025-PolicyTest  
Rule name: rule1  
Projected result: Access will be allowed  
Restrictions applied: Browser: Embedded, Clipboard: Disabled, Printing: Disabled, Watermark: Enabled  
Applied Route Policy Type: Access Policy

Routing type: Internal via Connector  
Primary resource location: [First Available](#)  
Backup resource location: N/A

Policy execution order

| Priority | Access Policy Name | Rule Name | Result                 |
|----------|--------------------|-----------|------------------------|
| 1        | 2025-PolicyTest    | rule1     | Access will be allowed |

Showing 1-1 of 1 items    Page 1 of 1    25 rows

The following figure displays the policy drill-down results for a web app for which access is allowed with restrictions.

Access and routing details for app-policy-modeling

Application: app-policy-modeling

Routing type: Internal via NetScaler Gateway

Matching Access policy: Policy-modeling-123

Primary resource location: [AAA-ConnApp 2](#)

Rule name: Policy-modeling

Backup resource location: N/A

Projected result: ✔ Access will be allowed with restrictions

Restrictions applied: Browser: Embedded,  
Keylogging protection: Disabled,  
Watermark: Enabled

Applied Route Policy Type: Application Domain

Policy execution order

| Priority | Access Policy Name  | Rule Name       | Result                                                  |
|----------|---------------------|-----------------|---------------------------------------------------------|
| 1        | Policy-modeling-123 | Policy-modeling | <span>✔</span> Access will be allowed with restrictions |

Showing 1-1 of 1 items    Page 1 of 1    25 rows

The following figure displays the policy drill-down results for a web app for which access is denied:

Access and routing details for Webapp-Test

Application: Webapp-Test

Routing type: N/A

Matching Access policy: N/A

Primary resource location: N/A

Rule name: N/A

Backup resource location: N/A

Projected result: ✘ No policy matched - Access will be denied

Restrictions applied: N/A

Applied Route Policy Type: N/A

Policy execution order

| Priority | Access Policy Name | Rule Name | Result                                                 |
|----------|--------------------|-----------|--------------------------------------------------------|
| 1        | 29policy           | test      | <span>!</span> No rule matched - Access will be denied |

Showing 1-1 of 1 items    Page 1 of 1    25 rows

## Applications import tool - Preview

September 6, 2025

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.
- **nsconfig file:** The nsconfig file can be directly imported into the Secure Private Admin console. This import automatically generates applications associated with the different virtual server types and the VPN URL. The following commands are used for creating the applications.
  - VPN intranet application - `add vpn intranetApplication`
  - Load balancing virtual server - `add lb vserver`
  - Content switching virtual server - `add cs vserver`
  - VPN URL - `add vpn url`

All other commands in the nsconfig file are ignored.

The following information is extracted from the commands for creating the applications.

- \* Application name
- \* URL/destinations
- \* Related domains
- \* Port
- \* Protocol

## 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/validate the nsconfig file:

- If using the CSV file - Populate the application details in the CSV file.
- If using nsconfig file - Ensure to use a valid nsconfig 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.

## Mapping of command parameters in nsconfig file to application details

The following sections provide information about the mapping of command parameters in the nsconfig file to application details and also some points to note related to the commands.

### VPN intranet applications

#### Example command:

```
add vpn intranetApplication IT_test.com ANY "*.test.com"-destPort 1-65535 -interception TRANSPARENT
```

#### Extracted application:

The following table captures the application details extracted from the command.

| Details required for application creation | Mapping of command parameters to application details | Description                                                                |
|-------------------------------------------|------------------------------------------------------|----------------------------------------------------------------------------|
| Application name                          | IT_test.com                                          | Name of the intranet application.                                          |
| URL/destinations                          | "*.test.com"                                         | Destination IP address, IP range, or host name of the intranet.            |
| Related domains                           | Not applicable                                       | Not Applicable                                                             |
| Port                                      | 1-65535                                              | Destination port number for the intranet application.                      |
| Protocol                                  | ANY                                                  | The protocol used by the intranet application. It can be TCP, UDP, or ANY. |

#### Note:

- If the protocol is ANY, the import process creates two separate applications, one with the protocol set to TCP and another with the protocol set to UDP.
- If the VPN application command explicitly states the protocol as either TCP or UDP, only one application is created using the specified protocol.

## Load balancing virtual server applications

### Example command:

```
add lb vserver vs-STOREFRONT SSL 192.0.2.143 443 -persistenceType SOURCEIP -timeout 480 -state DISABLED -cltTimeout 180
```

### Extracted application:

The following table captures the application details extracted from the command.

| Details required for application creation | Mapping of command parameters to application details |                                                                                                                    |
|-------------------------------------------|------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
|                                           |                                                      | Description                                                                                                        |
| Application name                          | <code>vs-STOREFRONT™</code>                          | Name of the load balancing virtual server.                                                                         |
| URL/destinations                          | <code>https://192.0.2.143</code>                     | IPv4 or IPv6 address to assign to the virtual server.                                                              |
| Related domains                           | <code>192.0.2.143</code>                             | IP address                                                                                                         |
| Port                                      | <code>443</code>                                     | The port number for the virtual server.                                                                            |
| Protocol                                  | <code>HTTPS</code>                                   | The protocol used by the virtual server. The protocol in the example is SSL and port 443, which is used for HTTPS. |

### Note:

- **Redirect URL:** If the `add lb vserver` command includes either the `-httpsRedirectUrl` or `-redirectUrl` argument, the application's URL is set to the specified redirect URL instead of the load balancing virtual server's IP address.

For example, consider the command `add lb vserver "vs - secured.test.net - REDIRECT"HTTP 192.0.2.51 80 -persistenceType NONE - redirectURL <"https://secured.test.net"> -cltTimeout 180`

After the migration, the URL becomes `https://secured.test.net` instead of `https://192.0.2.51`

- **Non-existent virtual server with redirect URL:** If the load balancing virtual server IP address is 0.0.0.0 and the `'add'` command includes a redirect URL argument, the application is created using that redirect URL.

For example, consider the command `add lb vserver "vs - secured.test.`



```
net - REDIRECT"HTTP 0.0.0.0 -persistenceType NONE -redirectURL
<"https://secured.test.net"> -cltTimeout 180
```

After the migration, the URL becomes `https://secured.test.net`.

## Content switching virtual server applications

### Example command:

- `add cs vserver Test-CS-HTTPS SSL 192.0.2.150 443 -cltTimeout 180 -persistenceType NONE`
- `add cs policy Test-Lab-Policy -rule "HTTP.REQ.HOSTNAME.eq(\"test.co.il\") || HTTP.REQ.HOSTNAME.eq(\"test\")"-action Test-Lab-Action`
- `bind cs vserver Test-CS-HTTPS -policyName Test-Lab-Policy -priority 100`

### Extracted application:

The following table captures the application details extracted from the command.

| Details required for application creation | Mapping of command parameters to application details |                                                                    |
|-------------------------------------------|------------------------------------------------------|--------------------------------------------------------------------|
|                                           |                                                      | Description                                                        |
| Application name                          | Test-CS-HTTPS                                        | Name of the content switching virtual server.                      |
| URL/destinations                          | <code>https://test.co.il</code>                      | First occurrence of <code>HTTP.REQ.HOSTNAME.eq</code> in the rule. |
| Related domains                           | <code>*.test.co.il, *.test</code>                    | All occurrences of <code>HTTP.REQ.HOSTNAME.eq</code> in the rule.  |
| Port                                      | 443                                                  | The port number in the <code>add cs vserver</code> command.        |
| Protocol                                  | HTTPS                                                | The protocol in the <code>add cs vserver</code> command.           |

### Note:

- **No content switching policy:** If the content switching virtual server does not have a content switching policy associated with it, then the import does not create the application.
- **Content switching virtual server app creation:** All content switching policies containing rule `HTTP.REQ.HOSTNAME` bound to a single content switching virtual server forms one

application.

- **Rules priority and related domains:** If both `.EQ/.eq/.EQUALS_ANY` and `.CONTAINS/.CONTAINS_ANY` rules are present, the `.EQ/.eq/.EQUALS_ANY` rule takes precedence. The application is created with the `.EQ/.eq/.EQUALS_ANYURL`, and the `.CONTAINS/.CONTAINS_ANY` URLs are added as related domains.
- **Multiple `.EQ/.eq/.EQUALS_ANY` rules:** If multiple `.EQ/.eq/.EQUALS_ANY` rules are present, the application is created using the first parsed `.EQ/.eq/.EQUALS_ANY` URL. All other URLs are added as related domains.
- **Only `.CONTAINS/.CONTAINS_ANY` rules:** If the command includes only `.CONTAINS/.CONTAINS_ANY` rules, the application is created with the first occurrence of the rule.
- **Port and protocol:** The port and protocol is extracted from the `add cs vserver` command.
- **Bind command:** The command relation between `add cs policy` and `add csvserver` is determined by the `bind csvserver` command.

## VPN URL applications

### Example command:

```
add vpn url XenApp XenApp "https://test.eportal.com/Citrix/Eportal-CitrixWeb/"-clientlessAccess ON -applicationtype CVPN
```

### Extracted application:

The following table captures the application details extracted from the command.

| Details required for application creation | Mapping of command parameters to application details            | Description                                                 |
|-------------------------------------------|-----------------------------------------------------------------|-------------------------------------------------------------|
| Application name                          | XenApp®                                                         | Name of the bookmark link.                                  |
| URL/destinations                          | <code>https://test.eportal.com/Citrix/Eportal-CitrixWeb/</code> | Web address for the bookmark link.                          |
| Related domains                           | <code>*.test.eportal.com</code>                                 | Extracted from the bookmark link.                           |
| Port                                      | 443                                                             | Default port for the protocol mentioned in the web address. |
| Protocol                                  | HTTPS                                                           | Protocol mentioned in the web address.                      |

## 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:**, click the **CSV** icon.

The **Import using CSV** page appears.

4. 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.

Click **Download examples** to view a sample CSV file with the data.

Note the following points when preparing the CSV file:

- The **App Location** must be one of the following values:
  - **Inside Corporate Network**
  - **Outside Corporate Network**
- The **App Type** can be one of the following values:
  - **SaaS**
  - **HTTP/HTTPS**
  - **TCP/UDP**
- The **Routing Type** must be one of the following values based on the app type.
  - **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 but the traffic must flow through the Connector Appliance to the outside network.
  - **External** - The traffic flows directly to the internet.
- Mandatory fields:
  - SaaS and HTTP/HTTPS - App Name, App Location, App Type, URL, Related Domains, Routing Type, and Resource Location.
  - TCP/UDP - App Name, App Location, App Type, Destination/Port/Protocol, Routing Type, and Resource Location.
  - The destination, port, and protocol must be formatted as:
    - \* **Destination:Port:Protocol**. Example: 192.0.2.254:5050:PROTOCOL\_TCP

- ★ If there are multiple destinations, ports, and protocols, separate them with commas.  
Example: 192.0.2.254:5050:PROTOCOL\_TCP, 2.2.2.2:1-65535: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 1-65535).
- ★ The protocol must be specified in the format PROTOCOL\_TCP or PROTOCOL\_UDP.

- Optional fields: **Description**, **Category**.

**Important:**

- The column names are case sensitive and must not be modified/edited.
- The columns must not be interchanged or deleted.

**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 Citrix Workspace. 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 Applications**.

**Note:**

- For import using a CSV file, the **Next: Review Applications** button is enabled only if the file contains no errors.
- When importing a nsconfig file, the **Next: Review Applications** button is disabled if the nsconfig file does not contain the commands required for application creation.
- 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.

If an application with the same domain or wildcard domain already exists, that application is disabled for import. You cannot select those applications.

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.

**Note:**

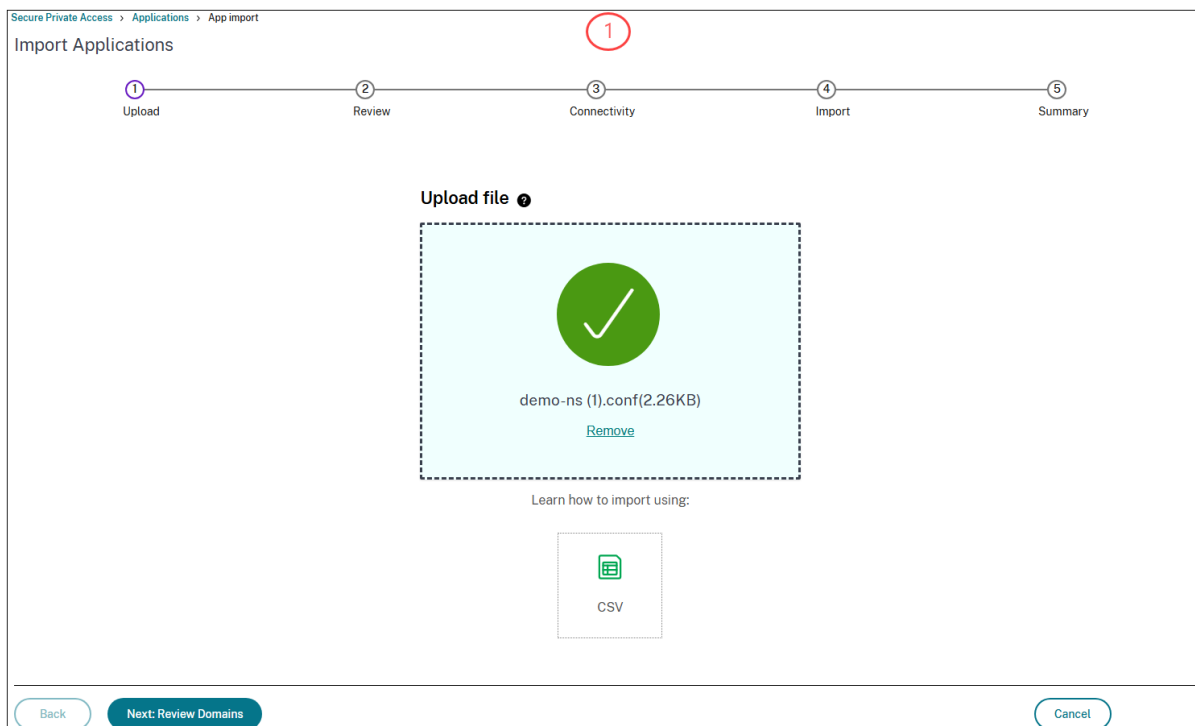
- If the specified resource location does not exist, the first resource location available in the list of resource locations associated with the customer is selected by default. if the Connector Appliance in the specified resource location is not up, the application creation fails.

11. Click: **Next: Import**.

The Summary page displays the imported application details. These applications are also added to the list of applications in the **Applications** page.

12. Click **Go to Applications** to view the imported applications in the **Applications** page.

The following images capture the migration workflow:



Secure Private Access > Applications > App import

2

Upload

Review

Connectivity

Import

Summary

Import Applications

Applications Found: 11

Select the application you wish to import, Any application that have missing details cannot be imported.

| Application                                         | Port    | Protocol     | Related Domains |
|-----------------------------------------------------|---------|--------------|-----------------|
| <input checked="" type="checkbox"/> iT_test.com_TCP | 1-65535 | PROTOCOL_TCP | 0               |
| <input type="checkbox"/> iT_test.com_UDP            | 1-65535 | PROTOCOL_UDP | 0               |
| <input type="checkbox"/> CMIS_Test-Hostname_443     |         |              | 0               |
| <input type="checkbox"/> vs-STOREFRONT              | 443     | HTTPS        | 1               |
| <input checked="" type="checkbox"/> XenApp          | 443     | HTTPS        | 1               |
| <input type="checkbox"/> IT-Remote                  | 3389    | PROTOCOL_TCP | 0               |
| <input checked="" type="checkbox"/> Sharefile       | 443     | HTTPS        | 1               |
| <input checked="" type="checkbox"/> File Transfer   | 443     | HTTPS        | 1               |
| <input checked="" type="checkbox"/> S4B_Intranet    | 80      | HTTP         | 1               |
| <input type="checkbox"/> HybriT_PISMS               | 80      | HTTP         | 1               |
| <input type="checkbox"/> external_cs_egov_ssl       | 443     | HTTPS        | 0               |

Showing 1-11 of 11 itemsPage 1 of 150 rows

Back

Next: Review connectivity

Cancel

Secure Private Access > Applications > App import

3

Upload

Review

Connectivity

Import

Summary

Import Applications

Review the connectivity details and update if needed

| Application     | Domain/IP Range                               | Routing Type           | Resource Location |
|-----------------|-----------------------------------------------|------------------------|-------------------|
| iT_test.com_TCP | *.test.com                                    | Internal bypass proxy  | AAA RL 01         |
| XenApp          | https://test.eportal.com/Citrix/Sg-CitrixWeb/ | Internal via connector | pasdev.net II     |
| Sharefile       | https://telephone.sharefile.com               | Internal bypass proxy  | pasdev.net        |
| File Transfer   | https://www.telephone.co.kl                   | Internal via connector | pasdev.net II     |
| S4B_Intranet    | http://200.0.0.13/                            | Internal via connector | AAA RL 01         |

Showing 1-5 of 5 itemsPage 1 of 150 rows

Back

Next: Import

Cancel

Secure Private Access > Applications > App import

Upload

Review

Connectivity

Import

Summary

4

Import in progress

20%

Creating applications...

Back

Cancel

Secure Private Access > Applications > App import

Upload

Review

Connectivity

Import

Summary

5

Import complete

Your Applications have been successfully imported to Secure Private Access.

Recommendation:

Review the imported applications

Create access policies

Apps import failed 3

Apps imported successfully 2

| Application     | Domain/IP Range 1   | Port 1  | Protocol 1 |
|-----------------|---------------------|---------|------------|
| iT_test.com_TCP | *.test.com          | 1-65535 | TCP/UDP    |
| S4B_Intranet    | http://192.0.2.150/ | 80      | HTTP/HTTPS |

Showing 1-2 of 2 itemsPage 1 of 150 rows

Import More Applications

Go to Applications

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.

## 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

September 6, 2025

The client internal IP address pools contain IP address ranges that can be allocated to each of the logged-in clients. The client internal IP address is required to assign a unique IP address to a user and their device. The client IP address is internal for Secure Private Access and is only available to the customer resource location. 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, initiating a server-to-client connection. The client internal IP address can also support source IP stickiness for existing client-to-server tunnel traffic to maintain consistent connections.

### Use cases of client internal IP address pools

- **Enable server-to-client connections:** A server must initiate a connection with the client devices for tasks such as push configurations, remote assistance, and software installation. The client internal IP address pools enable achieve these tasks by designating a range of IP addresses for client identification. These client internal IP address pools are allocated based on the user context and location. For example, specific IP address ranges can be assigned for user groups such as the HR team.

To enable server-to-client communication, you must create a server-to-client app and then provide the client machine port and protocol details in addition to the back-end IP address range that is used to connect to 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 details, see [Client IP address stickiness](#).

For enabling client IP address persistence, see [Enable client IP address stickiness for TCP/UDP applications](#).

**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.
- If a user's assigned resource pool is deleted, the user is not allocated an internal IP address from other pools until the original pool is completely deleted from the system.

## Create an intranet IP address pool

1. Navigate to **Settings > IP Pools** and then click **Create IP Pool**.

**Create IP Pool**

IP Pool name \*

ftp-pool

IP Range or CIDR \*

10.102.124.160/24

Connector Appliance Netmask (Optional)

Enter connector appliance mask

Resource Location \*

ResourceLoc5-SIC

⚠ Only 1 Connector is up. [Install Connector Appliance](#)

Allocation type

☒ User

☐ Machine

User \*

Matches any of

spaztnablr.net

Administrator

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.

| Name                    | IP Range Or CIDR              | Connector Appliance Netmask | Resource Location       | Actions |
|-------------------------|-------------------------------|-----------------------------|-------------------------|---------|
| IP_POOL_MACHINE_aalocal | 10.102.124.234-10.102.124.236 |                             | ResourceLoc4-Regression | ...     |
| ram_pool_2              | 10.102.124.240-10.102.124.242 |                             | ResourceLoc4-Regression | ...     |
| rampl_user_tunnel       | 10.102.124.243-10.102.124.244 |                             | ResourceLoc5-SIC        | ...     |
| ram_r15_machine_pool    | 10.102.124.249-10.102.124.250 |                             | ResourceLoc5-SIC        | ...     |

Once the client login is successful, an intranet IP address is assigned to the user from the client internal IP address pool.

## 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**.

Secure Private Access > Settings > IP Pools

Search for IP pool or IP range

Create IP Pool

| Name            | IP Range Or CIDR              | Connector Appliance Netmask | Resource Location | Actions |
|-----------------|-------------------------------|-----------------------------|-------------------|---------|
| mathi_testpool2 | 10.2.0.31-10.2.0.35           |                             | ResourceLoc5-SIC  | ...     |
| mathi_mockpool  | 10.2.0.21-10.2.0.25           |                             | ResourceLoc5-SIC  | ...     |
| AjayTestPoolSIC | 10.102.124.245-10.102.124.246 |                             | DeepakSIC         | ...     |

Showing 1-3 of 3 items Page 1 of 1

View IP Utilization

Delete IP pool by force

Delete IP pool over time

## 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.

Admins 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

September 6, 2025

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](#)

**Add an app**

Related Domains \* ⓘ

[+ Add another related domain](#)

☒ **Maintain consistent connection** ⓘ  
Use the same connector appliance for the entire length of the session while accessing the application.

**Next**

## 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.

Destinations and connectivity

Destination \* ⓘ

192.0.2.125

Port \* ⓘ

443

Protocol \*

TCP

⊖

Routing Type \*

Internal via Connector

Primary Resource Location \* ⓘ

AAA RL 01

Secondary Resource Location (optional) ⓘ

AAA RL 02

1 connector is available [Refresh](#)

⚠ Add another for high availability [Add](#)

1 connector is available [Refresh](#)

⚠ Add another for high availability [Add](#)

Destination \* ⓘ

192.0.2.150

Port \* ⓘ

1024

Protocol \*

UDP

⊖

Routing Type \*

Internal via Connector

Primary Resource Location \* ⓘ

AAA RL 01

Secondary Resource Location (optional) ⓘ

None

1 connector is available [Refresh](#)

⚠ Add another for high availability [Add](#)

⊕ [Add another destination](#)

Maintain consistent connection ⓘ

Use the same connector appliance (Connector ID) or end user device IP (Client IP) for the entire length of the session while accessing the application.

Client IP

⌵

Save

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

September 6, 2025

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 Citrix Enterprise Browser, direct access, CWA 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.

**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.
- Only the access to published Secure Private Access applications is blocked. Internet access via Citrix Enterprise Browser is allowed or denied even after a user/machine is added to the block list based on your [web filtering configuration](#).

**Use cases**

You can use this feature in the following scenarios.

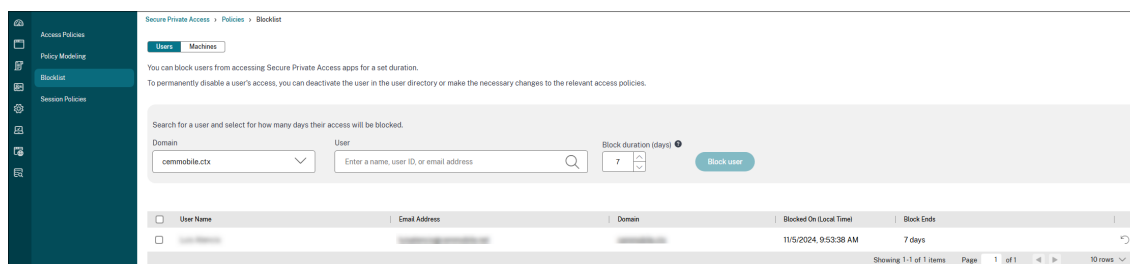
- An employee quits the organization or is terminated from the organization. In this case, the admin revokes all Secure Private Access app access by terminating active Secure Private Access sessions and blocking any future app access.
- A device is lost or stolen. In this case, the access is blocked 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.

**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:**

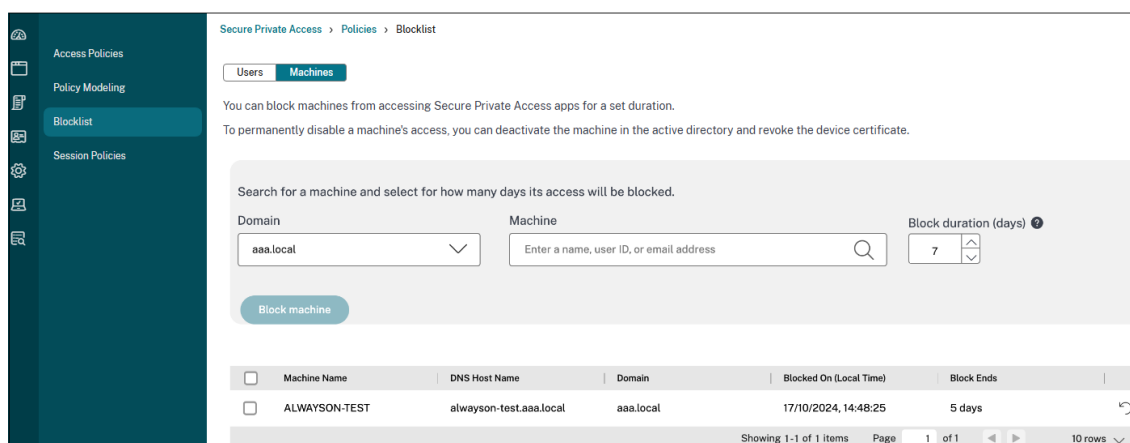
The **User** field appears only if the **Users** tab is selected.



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 Workspace, 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**

### **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 Citrix Enterprise 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**

September 6, 2025

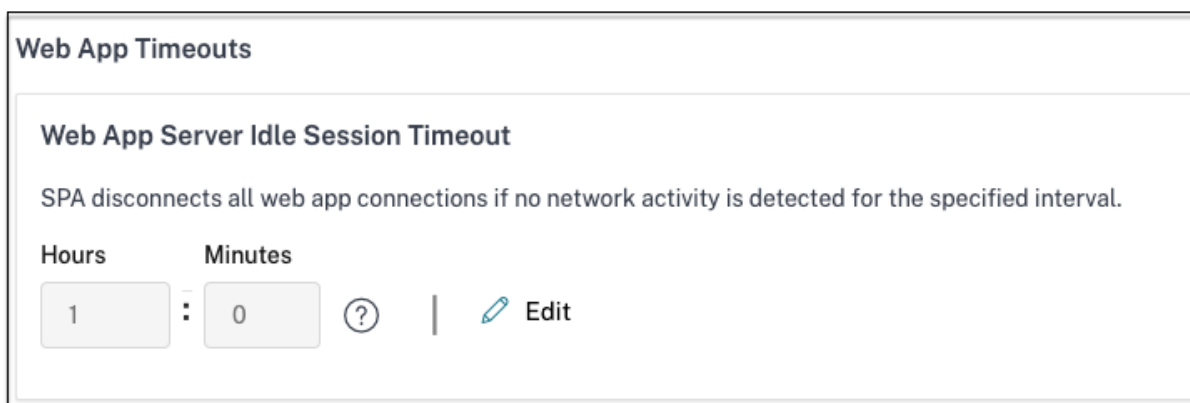
You can configure a timeout period for the Web apps and the Citrix Secure Access™ client to end user sessions if there is no network activity for the specified time period.

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.



The screenshot shows a configuration window titled "Web App Timeouts". Inside, there is a section titled "Web App Server Idle Session Timeout" with a descriptive text: "SPA disconnects all web app connections if no network activity is detected for the specified interval." Below this, there are two input fields: "Hours" with the value "1" and "Minutes" with the value "0". To the right of these fields is a question mark icon and an "Edit" button with a pencil icon.

## 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

September 6, 2025

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 Citrix Workspace™ 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.

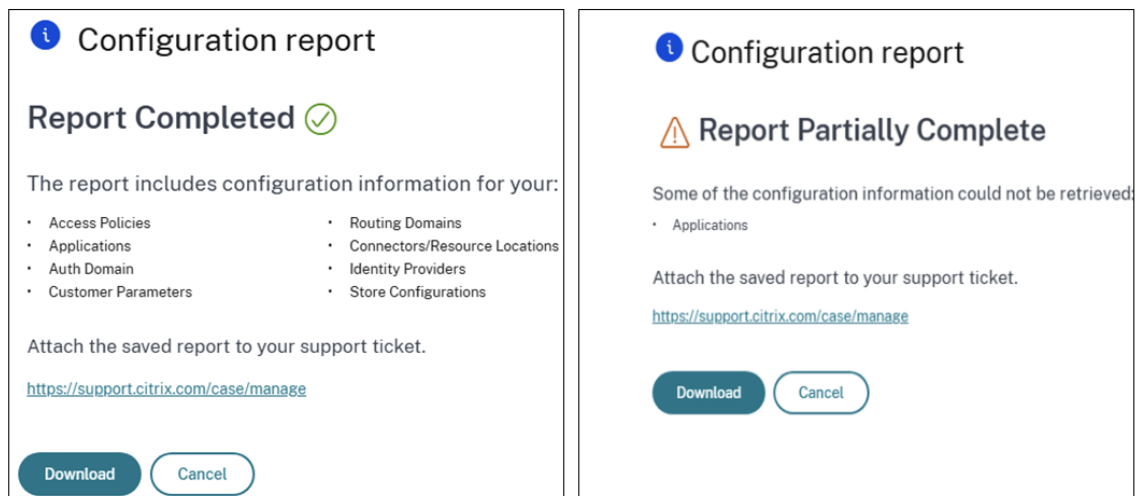
1. In the Secure Private Access admin console, go to **Settings > Global Configuration**.
2. Click **Create report** to initiate the report generation process.

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

September 6, 2025

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](#).

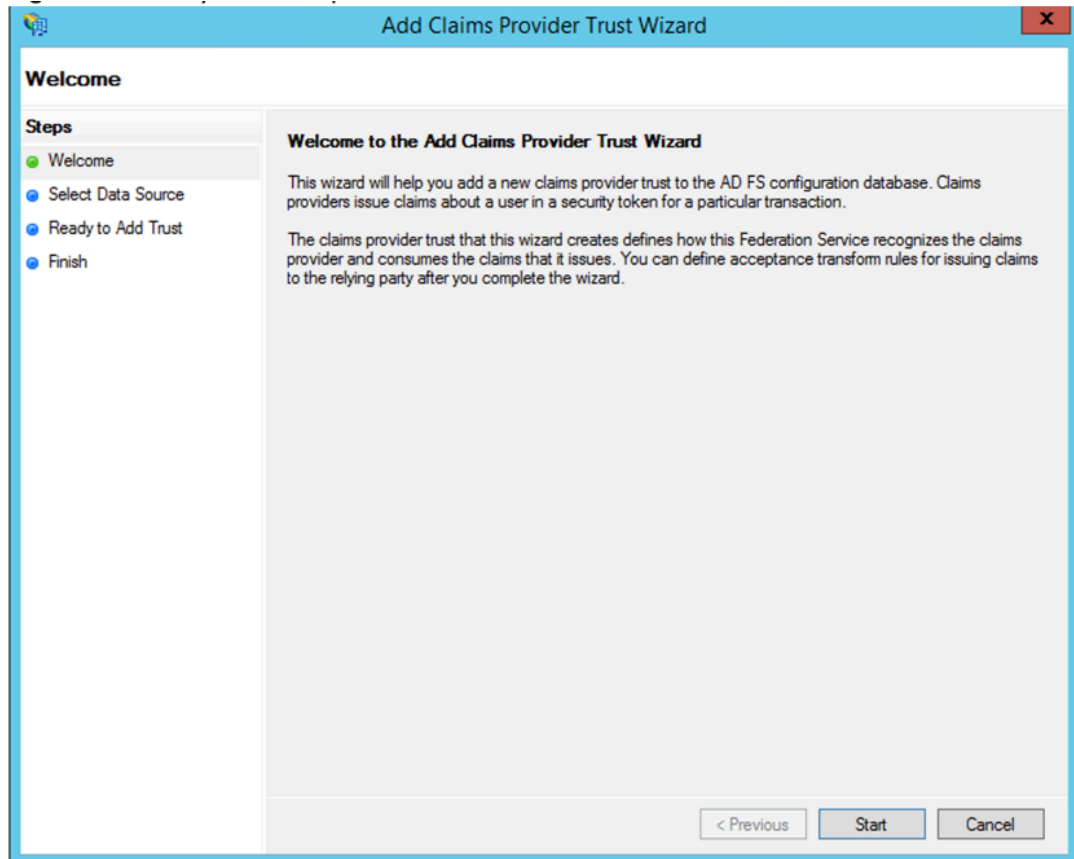
To set up ADFS to accept claims from Citrix Secure Private Access™, you must perform the following steps:

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](#).

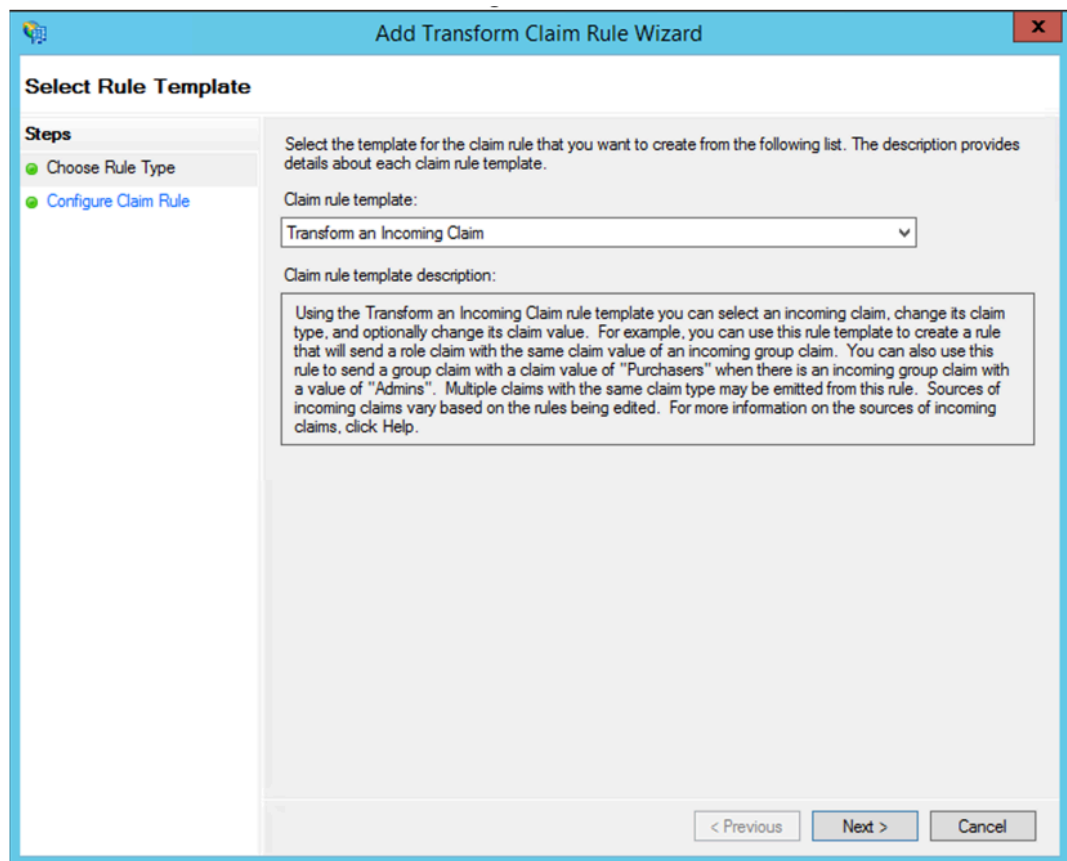
### Note:

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.



The screenshot shows the 'Add Claims Provider Trust Wizard' window. The title bar is blue with the text 'Add Claims Provider Trust Wizard' and a close button. The window is divided into two main sections. On the left is a 'Steps' pane with a list of steps: 'Welcome', 'Select Data Source' (which is highlighted with a green dot and a grey background), 'Ready to Add Trust', and 'Finish'. The main area on the right is titled 'Select Data Source' and contains the following text: 'Select an option that this wizard will use to obtain data about this claims provider:'. There are three radio button options. The first option is 'Import data about the claims provider published online or on a local network', which is currently unselected. Below it is a text box for 'Federation metadata address (host name or URL):' with an example: 'fs.fabrikam.com or https://fs.fabrikam.com/'. The second option is 'Import data about the claims provider from a file', which is selected with a black dot. Below it is a text box for 'Federation metadata file location:' containing the path 'C:\Users\Administrator\Downloads\idp\_metadata (1).xml' and a 'Browse...' button. The third option is 'Enter claims provider trust data manually', which is unselected. At the bottom right of the window are three buttons: '< Previous', 'Next >', and 'Cancel'.

- 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**.



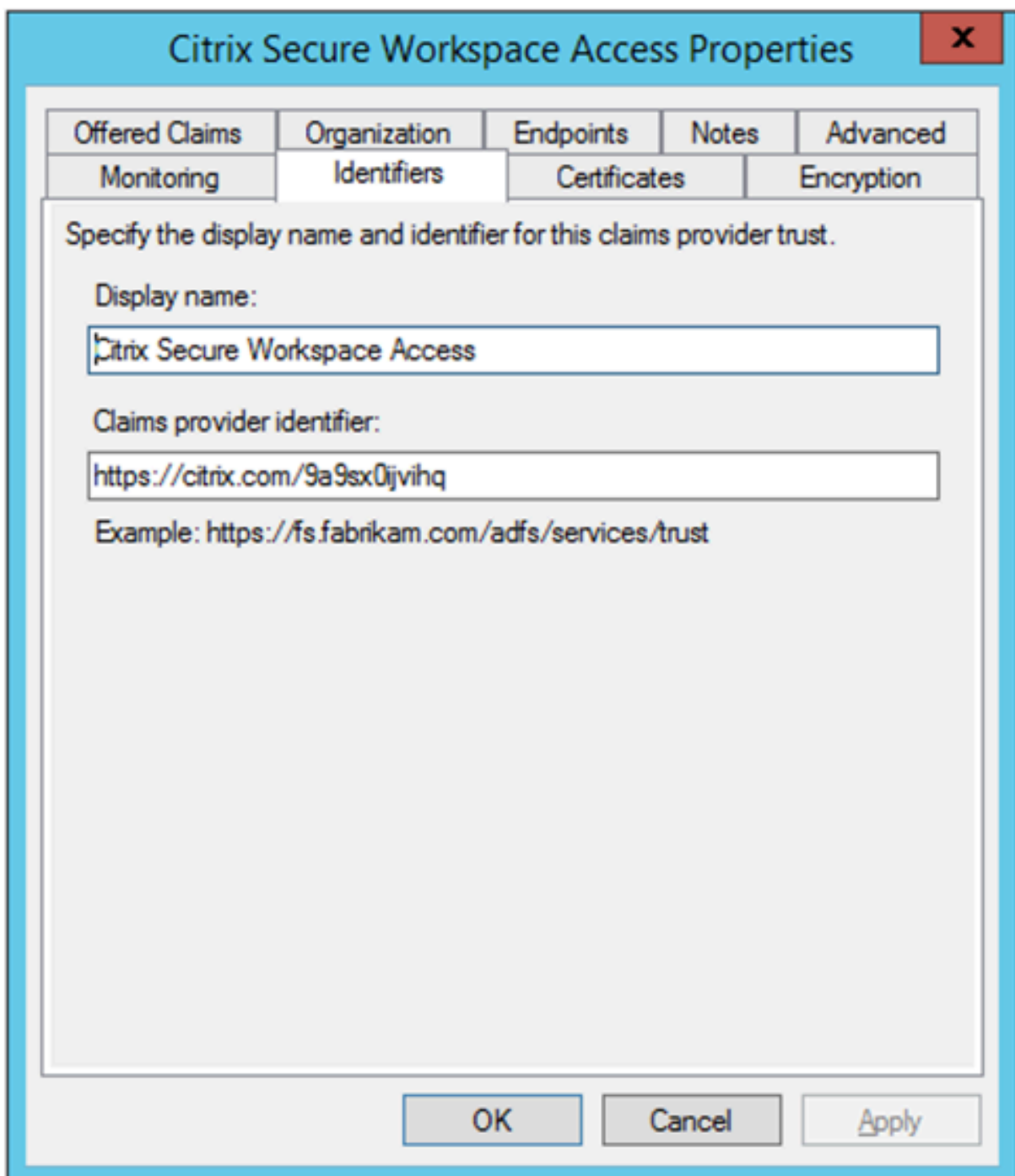
- c) Complete the settings as shown in the following figure. If your ADFS accepts other claims, then use those claims and configure SSO in Secure Private Access also accordingly.

The screenshot shows the 'Add Transform Claim Rule Wizard' window, specifically the 'Configure Rule' step. The window has a blue title bar with the text 'Add Transform Claim Rule Wizard' and a close button. On the left, there is a 'Steps' pane with two items: 'Choose Rule Type' (highlighted with a green dot) and 'Configure Claim Rule' (also with a green dot). The main area contains a text box for 'Claim rule name' with the value 'nameid to email'. Below this is a section titled 'Rule template: Transform an Incoming Claim'. It contains four dropdown menus: 'Incoming claim type' (set to 'Name ID'), 'Incoming name ID format' (set to 'Email'), 'Outgoing claim type' (set to 'E-Mail Address'), and 'Outgoing name ID format' (set to 'Unspecified'). There are three radio button options: 'Pass through all claim values' (selected), 'Replace an incoming claim value with a different outgoing claim value', and 'Replace incoming e-mail suffix claims with a new e-mail suffix'. The second option has input fields for 'Incoming claim value' and 'Outgoing claim value' with a 'Browse...' button. The third option has a 'New e-mail suffix' input field with an example 'fabrikam.com' below it. At the bottom right are three buttons: '< Previous', 'Finish', and 'Cancel'.

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.



The image shows a Windows-style dialog box titled "Citrix Secure Workspace Access Properties". It has a blue title bar with a close button (X) in the top right corner. Below the title bar is a tabbed interface with five tabs: "Offered Claims", "Organization", "Endpoints", "Notes", and "Advanced". The "Offered Claims" tab is currently selected. Below the tabs, there is a section titled "Specify the display name and identifier for this claims provider trust." This section contains two text input fields. The first field is labeled "Display name:" and contains the text "Citrix Secure Workspace Access". The second field is labeled "Claims provider identifier:" and contains the text "https://citrix.com/9a9sx0jviahq". Below the second field, there is an example text: "Example: https://fs.fabrikam.com/adfs/services/trust". At the bottom of the dialog box, there are three buttons: "OK", "Cancel", and "Apply".

| Offered Claims | Organization | Endpoints    | Notes | Advanced   |
|----------------|--------------|--------------|-------|------------|
| Monitoring     | Identifiers  | Certificates |       | Encryption |

Specify the display name and identifier for this claims provider trust.

Display name:

Claims provider identifier:

Example: https://fs.fabrikam.com/adfs/services/trust

OK Cancel Apply

### 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.

The screenshot shows a Windows-style dialog box titled "service now Properties" with a red close button (X) in the top right corner. The dialog has a tabbed interface with the following tabs: "Organization", "Endpoints", "Proxy Endpoints", "Notes", "Advanced", "Monitoring", "Identifiers" (selected), "Encryption", "Signature", and "Accepted Claims". The "Identifiers" tab contains the following content:

Specify the display name and identifiers for this relying party trust.

Display name:

Relying party identifier:  
  
Example: `https://fs.contoso.com/adfs/services/trust`

Relying party identifiers:  

`https://dev98714.service-now.com`  
`servicenow`

Buttons: "Add" (next to the empty identifier input), "Remove" (next to the identifier list), "OK", "Cancel", and "Apply" (at the bottom).

### 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\ads\ls\web.config
- For ADFS 3.0, enter the following file in Notepad: %systemroot%\ADFS\Microsoft.IdentityServer.Service

2. In the microsoft.identityServer.web section, add a line for useRelyStateForIdpInitiatedSignOn as follows, and save the change:

```
<microsoft.identityServer.web> ... <useRelyStateForIdpInitiatedSignOn  
enabled="true"/> ...</microsoft.identityServer.web>
```

- For ADFS 2.0, run `IISReset` to restart IIS.

3. For both platforms, restart the Active Directory Federation Services (`adfsrv`) 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\(v=ws.10\)](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, [Support for SaaS apps](#).

Which single sign on type would you like to use for your SaaS app setup?

☒ SAML
 ☐ Don't use SSO

Sign Assertion \*

Assertion

Assertion URL \*

<https://adfs1.workspacesecurity.com/adfs/ls/>

Relay State \*

RPID=https%3A%2F%2Fdev98714.service-now.c

Audience

<http://adfs1.workspacesecurity.com/adfs/servi>

Name ID Format \*

Email Address

Name ID \*

Email

☐ Launch the app using the specified URL (SP initiated)

Advanced attributes (optional)

An attribute is additional information about the user that is sent to the application for access control decisions. Make sure these values are consistent with the settings in the SaaS vendor.

| Attribute Name | Attribute Format | Attribute Value |
|----------------|------------------|-----------------|
|                |                  |                 |

[Add another attribute](#)

**What does this form do?**  
This form generates the XML needed for the application's SAML request.

**Where do I find the information this form needs?**  
The application you're integrating with should have its own documentation on using S/

**SAML Metadata**  
Provide this metadata to your Service Provider (application)  
<https://ctxaccess.mgmt.netscalergatewaydev.net/ldp/saml/9a9sx0ijvihq/4b2f73ed-5fa>

**Login URL**  
<https://apo.ctxa.netscalergatewaydev.net/ngs/9a9sx0ijvihq/saml/login?APPID=4b2f73e>

**Certificate**  
Select download type \*  
PEM Download

## 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.

## Secure Private Access dashboard

September 6, 2025

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.

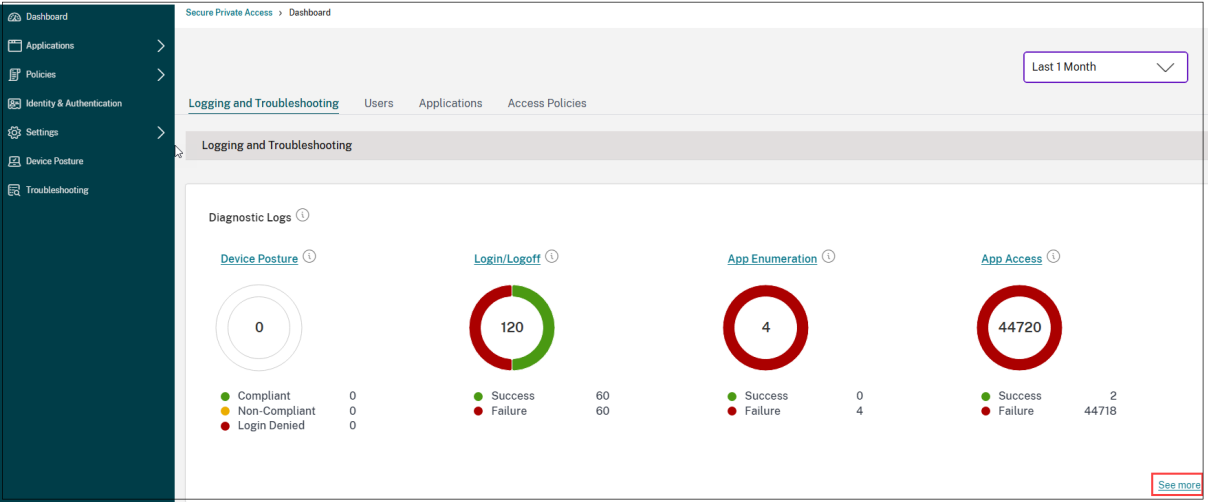
- You can use the **Add Filter** option to refine your search based on the various criteria such as app type, category, description. For example, in the search fields, you can select **Transaction ID**, **= (equals to some value)**, and enter **7456c0fb-a60d-4bb9-a2a2-edab8340bb15** in this sequence, 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](#).

The screenshot shows the 'Diagnostic Logs' section of the Citrix Secure Private Access dashboard. It features a filter bar at the top with a dropdown for 'Last 1 Week' and an 'Add filter' button. A filter is applied: 'Transaction-ID = 3f37fcfa-f880-1655-9678-6045bdc2f9dc'. Below the filter bar, a table displays log results. The table has columns: Time, App Access, N/A, Transaction-ID, Secure Access, Info code, User name, and Status. One row is visible with a status of 'Failure'. At the bottom, it says 'Showing 1-1 of 1 items', 'Page 1 of 1', and '20 rows'.

- **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.

The screenshot shows the 'Diagnostic Logs' page. It has a filter for 'Last 1 Week' and an 'Add filter' button. Below the filter, there's a note: 'Results are limited to the first 10000 records. Narrow your search criteria for more relevant results.' The table has columns: Time, Category, App name, App type, App FQDN, Transaction ID, Mode of access, Info code, User name, and Status. The table shows 11 rows of log entries. The first row is a success for 'aaa.local\ak2' at 2024-10-31 20:16:28. The second row is a failure for 'aaa.local\ak2' at 2024-10-31 20:15:31. The third row is a success for 'aaa.local\ak2' at 2024-10-31 20:15:28. The fourth row is a success for 'aaa.local\ak2' at 2024-10-31 20:14:29. The fifth row is a failure for 'adg8a4thridnb\565...' at 2024-10-30 09:37:25. The sixth row is a success for 'adg8a4thridnb\565...' at 2024-10-30 09:37:13. The seventh row is a failure for 'adg8a4thridnb\565...' at 2024-10-30 07:18:11. The eighth row is a success for 'adg8a4thridnb\565...' at 2024-10-29 13:32:38. The ninth row is a success for 'adg8a4thridnb\565...' at 2024-10-29 13:31:44. The table is paginated, showing 1-11 of 11 items, Page 1 of 1, and 20 rows.

| Time                  | Category     | App name | App type | App FQDN     | Transaction ID                   | Mode of access | Info code  | User name            | Status  |
|-----------------------|--------------|----------|----------|--------------|----------------------------------|----------------|------------|----------------------|---------|
| > 2024-10-31 20:16:28 | N/A          | N/A      | SaaS     | N/A          | 21196A21-F44B-46DB-A6CB-A89...   | N/A            | N/A        | aaa.local\ak2        | Success |
| > 2024-10-31 20:16:28 | N/A          | N/A      | SaaS     | N/A          | 21196A21-F44B-46DB-A6CB-A89...   | N/A            | N/A        | aaa.local\ak2        | Success |
| > 2024-10-31 20:15:31 | App Access   | N/A      | UDP      | 173.16.255.1 | 387F5E03-C316-4197-B6FF-FBB...   | N/A            | 0x10000409 | aaa.local\ak2        | Failure |
| > 2024-10-31 20:15:28 | Login/Logoff | N/A      | SaaS     | N/A          | A2988309-2E22-419E-A44F-B2...    | N/A            | N/A        | aaa.local\ak2        | Success |
| > 2024-10-31 20:14:29 | Login/Logoff | N/A      | N/A      | N/A          | a956311d-0a6b-4509-b6ed-40b...   | N/A            | N/A        | aaa.local\ak2        | Success |
| > 2024-10-30 09:37:25 | Login/Logoff | N/A      | SaaS     | N/A          | 15c3b70e-b0f2-1721-9678-9022...  | N/A            | 0x180003   | adg8a4thridnb\565... | Failure |
| > 2024-10-30 09:37:13 | Login/Logoff | N/A      | N/A      | N/A          | 721711e1-d9f2-4b77-9887-6e38a... | N/A            | N/A        | N/A                  | Success |
| > 2024-10-30 07:18:11 | Login/Logoff | N/A      | SaaS     | N/A          | 01606a6d-905d-1721-9678-000d...  | N/A            | 0x180003   | adg8a4thridnb\565... | Failure |
| > 2024-10-30 07:18:11 | Login/Logoff | N/A      | N/A      | N/A          | ea7b92ee-54b8-4521-a70d-93fa...  | N/A            | N/A        | N/A                  | Success |
| > 2024-10-29 13:32:38 | Login/Logoff | N/A      | SaaS     | N/A          | 2d8a1285-9669-1720-9678-000d...  | N/A            | 0x180003   | adg8a4thridnb\565... | Failure |
| > 2024-10-29 13:31:44 | Login/Logoff | N/A      | N/A      | N/A          | d199cf38-adff-4611-a827-d4224... | N/A            | N/A        | N/A                  | Success |

**Note:**

- 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.

**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.

Connector insights

Filter

Clear all

Status

☐ Active

☐ Down

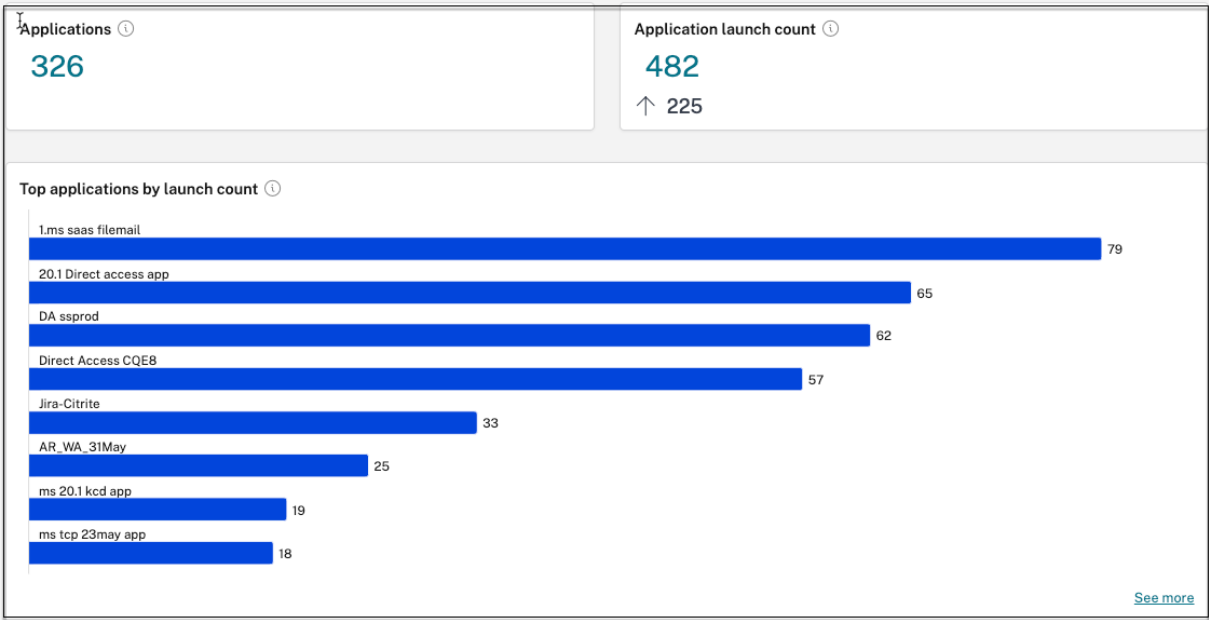
Connectors

| NAME                             | RESOURCE LOCATION | STATUS |
|----------------------------------|-------------------|--------|
| tpt-10-222-102-236.ca.net        | Tirupati_CA01     | Active |
| varunt-10-222-102-198.com        | VarunIT-ssprod    | Active |
| pasdev-ssprod-ca.pasdev.net      | PasDev AAD        | Down   |
| tpt-ssprod-10-222-102-200.ca.net | Demo_CA           | Active |
| ssprod-10-222-102-171.aaa.local  | AAA               | Active |
| ca-10-222-102-251.ca.net         | Tirupati_CA02     | Active |

Showing 1-6 of 6 itemsPage 1 of 110 rows

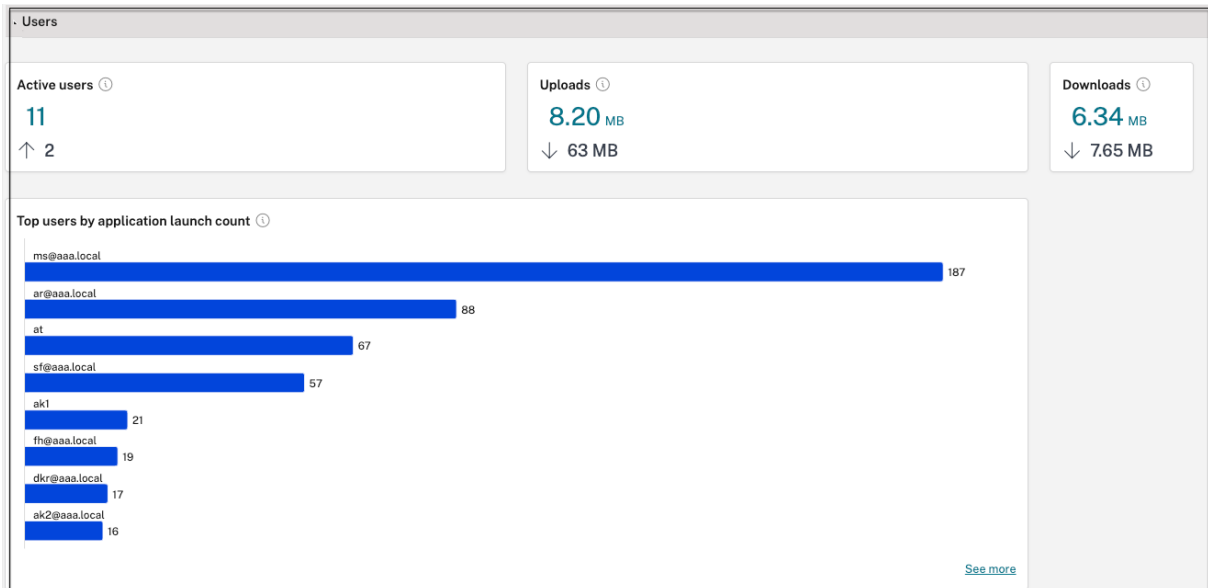
Top applications by launch count

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.

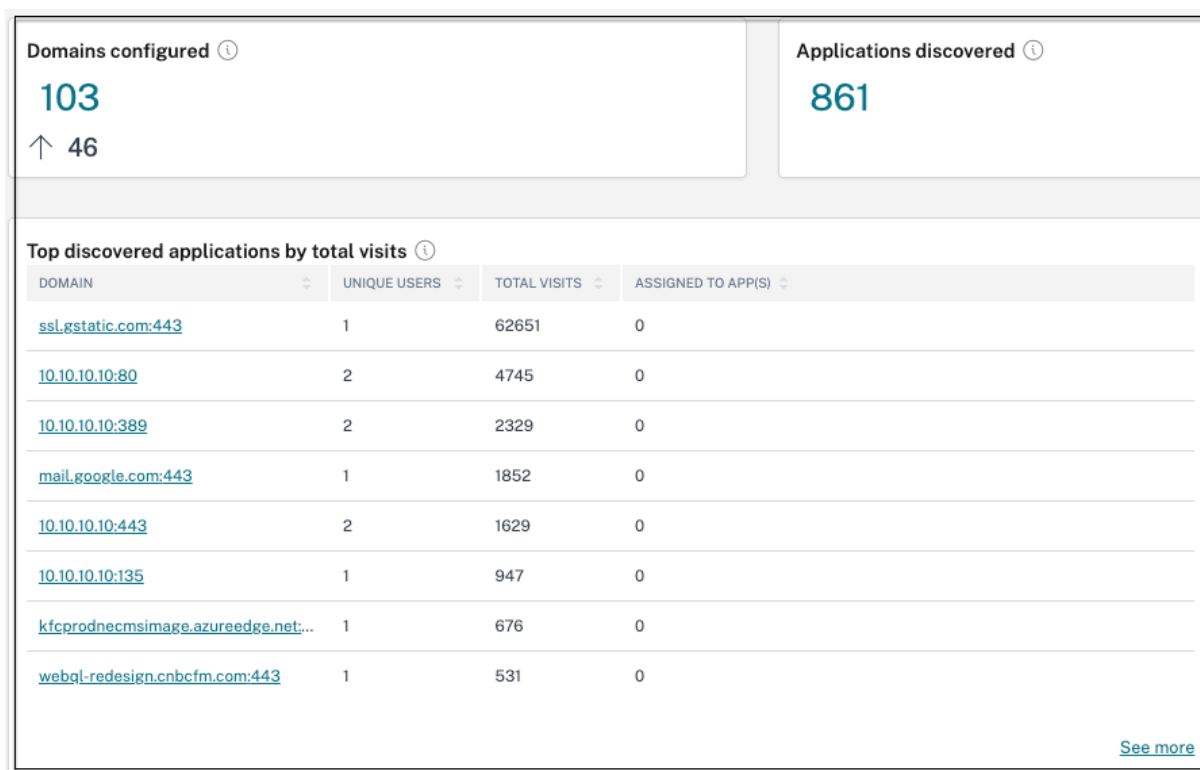


## Top access policies by enforcement

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.

← Discovered applications

Domain - ✕ Last 1 Week ▾ Search

Select a domain or multiple domains to create an application. Protocols cannot be mixed.  
Results are limited to the first 10000 records. Narrow your search criteria for more relevant results.

Create application

| <input type="checkbox"/> | DOMAIN                        | PORT  | PROTOCOL | TOTAL VISITS | UNIQUE USERS | MOST RECENT VISIT    | ASSIGNED TO APP(S) | CREATE APP |
|--------------------------|-------------------------------|-------|----------|--------------|--------------|----------------------|--------------------|------------|
| <input type="checkbox"/> | 10.10.10.10                   | 50000 | UDP      | 13           | 1            | 2023-03-28T05:47:36Z | 1                  |            |
| <input type="checkbox"/> | 10.10.10.10                   | 3389  | TCP      | 11           | 1            | 2023-03-29T05:13:23Z | 0                  |            |
| <input type="checkbox"/> | 10.10.10.10                   | 3389  | UDP      | 5            | 1            | 2023-03-29T05:13:29Z | 0                  |            |
| <input type="checkbox"/> | 172.16.17.17                  | 137   | UDP      | 5            | 2            | 2023-03-28T21:12:57Z | 0                  |            |
| <input type="checkbox"/> | 10.10.10.10                   | 23    | TCP      | 3            | 1            | 2023-03-27T07:06:33Z | 0                  |            |
| <input type="checkbox"/> | windows1.ztnacloud.local      | 8080  | TCP      | 3            | 1            | 2023-03-29T10:05:06Z | 1                  |            |
| <input type="checkbox"/> | ztna_conn_app.ztnacloud.local | 3389  | TCP      | 3            | 1            | 2023-03-29T09:59:54Z | 0                  |            |

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](#)  
(128 kb max, PNG)

[Use default icon](#)

☐ 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

App Details

Where is the application located? \*


Outside my corporate network

☒ Inside my corporate network

App type \*

TCP/UDP

App icon

 [Change icon](#) [Use default icon](#)  
(128 kb max, PNG)

[Citrix Secure Access Client for Windows](#)  
[Citrix Secure Access Client for macOS](#)

App name \*

Discovery tcp apps by IP

App description

Destinations ?

Destination \*

windows.ztnaaccess.cloud

Port \*

8080

Protocol \*

TCP

+ Add another destination

Save

App Connectivity

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.

ztna\_conn\_app.ztnacloud.local:3389

Create application

Filters

Clear All

Access Outcome

☐ ACCESS\_ALLOW

☐ ACCESS\_DENY

User - "" AND Access\_Outcome - ""

Last 1 Week

Search

| TIMESTAMP             | USER | ACCESS OUTCOME |
|-----------------------|------|----------------|
| Mar 29, 2023 15:29:57 |      | ACCESS_DENY    |
| Mar 29, 2023 15:29:54 |      | ACCESS_ALLOW   |
| Mar 29, 2023 15:29:50 |      | ACCESS_ALLOW   |
| Mar 29, 2023 15:28:58 |      | ACCESS_ALLOW   |

Showing 1-4 of 4 items Page 1 of 1 20 rows

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.

## Logging and troubleshooting

September 6, 2025

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.

### FAQs?

[What are Secure Private Access diagnostic logs?](#)

[Where do I find Secure Private Access logs?](#)

[Which widget displays the Secure Private Access diagnostic logs?](#)

[What details can I find in the Secure Private Access diagnostic logs?](#)

[What events are captured in the Secure Private Access diagnostic logs?](#)

[How do I filter the diagnostic logs?](#)

[How do I use the Secure Private Access troubleshooting topic to resolve a failure that I have encountered?](#)

[What is an info code? Where do I find them?](#)

[What is a transaction ID? How do I use it?](#)

[What are all the Secure Private Access PoP locations?](#)

[What do I do if I am unable to resolve my failure using the info code and the error lookup table?](#)

### Info code lookup table

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                                                                                                                                                                             | <a href="#">App launch failed because app FQDN length exceeded</a>                                                |
| 0x180022                                                                                                                                                       | App launch failed as Authentication Service is down                                                                                                                                                                            | <a href="#">App launch failed as authentication service is down</a>                                               |
| 0x180001, 0x18001A, 0x18001B, 0x18008A, 0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3, 0x180048 | Single sign-on errors, Connection establishment failure between Citrix Cloud and on-premises connectors, SAML SSO failure, Invalid app FQDN                                                                                    | <a href="#">App access is denied</a>                                                                              |
| 0x1800EF                                                                                                                                                       | Problem connecting to Connector Appliance                                                                                                                                                                                      | <a href="#">Problem connecting to Connector Appliance</a>                                                         |
| 0x18009D                                                                                                                                                       | DNS lookup/Connection failed                                                                                                                                                                                                   | <a href="#">Secure Browser Service - DNS lookup/connection errors</a>                                             |
| 0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7                                                                                                     | Web app launch failed as unable to connect to back end web app                                                                                                                                                                 | <a href="#">Web app launch failed as unable to connect to back-end web app</a>                                    |
| 0x1800BC, 0x1800BF                                                                                                                                             | User is not entitled to access the Web/SaaS app                                                                                                                                                                                | <a href="#">User is not entitled to access the Web/SaaS app</a>                                                   |
| 0x1800BD                                                                                                                                                       | User is not entitled to access the Web/SaaS app for DirectAccess                                                                                                                                                               | <a href="#">User is not entitled to access the Web/SaaS app for DirectAccess</a>                                  |
| 0x1800D0                                                                                                                                                       | Citrix Secure Access agent Session launch has failed while fetching the application configuration                                                                                                                              | <a href="#">Citrix Secure Access agent Session launch has failed while fetching the application configuration</a> |
| 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 | <a href="#">Malformed client requests</a>                                                                         |

| Info code                                      | Description                                                                      | Resolution                                                                                 |
|------------------------------------------------|----------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 0x1800DE                                       | Citrix Secure Access agent App launch has failed during Policy evaluation        | <a href="#">Citrix Secure Access agent App launch has failed during Policy evaluation</a>  |
| 0x180055, 0x1800DF, 0x1800E3                   | Apps restricted by contextual policy, Access denied due to policy configuration  | <a href="#">One or more apps not listed in the user dashboard</a>                          |
| 0x1800EB                                       | Citrix Secure Access agent app launch has failed as IPv6 is not supported        | <a href="#">Citrix Secure Access agent app launch has failed as IPv6 is not supported</a>  |
| 0x1800EC, 0x1800ED                             | Citrix Secure Access agent App launch has failed due to invalid IP address       | <a href="#">Citrix Secure Access agent App launch has failed due to invalid IP address</a> |
| 0x10000001, 0x10000002, 0x10000003, 0x10000004 | Citrix Secure Access client login failure due to network issue                   | <a href="#">Network connectivity reachability issue with Citrix Secure Access client</a>   |
| 0x10000006                                     | Citrix Secure Access client login failure due to proxy in the middle             | <a href="#">Proxy server interfering client connectivity with service</a>                  |
| 0x10000007                                     | Citrix Secure Access client login failure due to untrusted certificate authority | <a href="#">Untrusted server certificate issue is observed</a>                             |
| 0x10000008                                     | Citrix Secure Access client login failure due to invalid certificate             | <a href="#">Invalid server certificate issue is observed</a>                               |
| 0x1000000A                                     | Citrix Secure Access client login failure due to configuration issue             | <a href="#">Login failed as configuration is empty for the user</a>                        |
| 0x1000000B                                     | Citrix Secure Access client login failure due to connection failure              | <a href="#">Connection terminated by the network or end user</a>                           |
| 0x10000010                                     | Citrix Secure Access client login failure due to expired session                 | <a href="#">Configuration download failed as session is expired</a>                        |
| 0x10000013                                     | Citrix Secure Access client login failure due huge configuration list            | <a href="#">Citrix Secure Access client failed to log in</a>                               |

| Info code                          | Description                                                                       | Resolution                                                                                  |
|------------------------------------|-----------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| 0x11000003                         | Citrix Secure Access client login failure due to control channel creation failure | <a href="#">Control channel establishment failed as the session expired</a>                 |
| 0x11000004                         | Citrix Secure Access client login failure due control channel creation failure    | <a href="#">Control channel establishment failed</a>                                        |
| 0x11000005                         | Citrix Secure Access client login failure due control channel creation failure    | <a href="#">Control channel establishment failed</a>                                        |
| 0x11000006                         | Citrix Secure Access client login failure due control channel creation failure    | <a href="#">Control channel establishment failed because of network issue</a>               |
| 0x12000001                         | Citrix Secure Access client logout failure as session already expired             | <a href="#">Unable to logoff as session is terminated</a>                                   |
| 0x12000002                         | Citrix Secure Access client logout failure as session already timed out           | <a href="#">Session is forcefully terminated</a>                                            |
| 0x13000001                         | App access failed as the session expired                                          | <a href="#">Application launch failed as session is expired</a>                             |
| 0x13000002                         | App access failed as inadequate license                                           | <a href="#">Application Launch failed because of license issue</a>                          |
| 0x13000003, 0x13000008, 0x001800DF | App access failed as access forbidden, TCP/UDP app launch is denied as per Policy | <a href="#">Application launch failed as access is denied by service</a>                    |
| 0x13000004, 0x13000005             | App access failed as the server is unavailable                                    | <a href="#">Application launch failed as the client is unable to reach the service</a>      |
| 0x13000007                         | App access failed as the access policy is disabled or the user is not subscribed  | <a href="#">Application launch failed as policy evaluation and config validation failed</a> |
| 0x13000009                         | App access failed as the routing entry is missing                                 | <a href="#">Application launch failed because of issues in application domain table</a>     |

| Info code                          | Description                                                                                                                                                                                          | Resolution                                                                      |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| 0x1300000B                         | The client closed the connection                                                                                                                                                                     | <a href="#">Client closed the connection with Secure Private Access service</a> |
| 0x1300000C                         | The FQDN resolution over ZTNA failed                                                                                                                                                                 | <a href="#">Unable to resolve FQDN by the DNS server</a>                        |
| 0x1300000E                         | App launch failed due to use of non-Chrome browser                                                                                                                                                   | <a href="#">App launch failed due to use of a non-Chrome browser</a>            |
| 0x001800D3                         | Applications configuration download failure while login                                                                                                                                              | <a href="#">Failed to fetch configured application destinations list</a>        |
| 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                                                  | <a href="#">Application configuration issue</a>                                 |
| 0x001800DB                         | TCP/UDP app launch has failed with invalid resource location configuration                                                                                                                           | <a href="#">Issue with resource location</a>                                    |
| 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 | <a href="#">Enhanced security policy is bound to the HTTP application</a>       |
| 0x001800DE                         | TCP/UDP app launch has failed as there is no application configuration found for the destination                                                                                                     | <a href="#">Unable to locate the application</a>                                |
| 0x001800EA                         | TCP app launch has failed due to destination FQDN is too long                                                                                                                                        | <a href="#">Host name length exceeds 256 characters</a>                         |
| 0x001800ED                         | TCP app launch has failed because of invalid destination IP                                                                                                                                          | <a href="#">Invalid IP address</a>                                              |

| Info code                                                                          | Description                                                                                                                                                | Resolution                                                                                        |
|------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| 0x001800EF                                                                         | TCP app launch has failed during connection establishment to private TCP server                                                                            | <a href="#">Unable to establish end-to-end connection</a>                                         |
| 0x001800F5                                                                         | UDP app launch failed because of IPV6 address                                                                                                              | <a href="#">IPv6 received in the app request</a>                                                  |
| 0x001800F9                                                                         | UDP Traffic failed to deliver as client connection is lost                                                                                                 | <a href="#">UDP traffic failed to deliver</a>                                                     |
| 0x001800FF                                                                         | UDP Data traffic delivery failed                                                                                                                           | <a href="#">UDP data traffic delivery failed</a>                                                  |
| 0x10000401                                                                         | Citrix rendezvous server dial failed                                                                                                                       | <a href="#">Application launch failed because of network connectivity issues</a>                  |
| 0x10000402, 0x1000040C                                                             | Unable to register the Connector Appliance, UDP network connection initialization failure                                                                  | <a href="#">Connector appliance failed to register to Secure Private Access service</a>           |
| 0x10000403, 0x10000404, 0x10000407, 0x1000040A, 0x1000040B, 0x1000040F, 0x10000410 | Connection error, Control packet transmission failure, Error on reading Gateway service, Control packet parsing failure, Error on reaching gateway service | <a href="#">Connectivity issue with Connector Appliance</a>                                       |
| 0x10000405, 0x10000408, 0x10000409, 0x1000040D, 0x1000040E, 0x10000412             | UDP packet transmission failure, UDP packet receiving failure, Error on writing back-end, DNS resolution failed                                            | <a href="#">Connectivity issues with Connector Appliance and back-end private TCP/UDP servers</a> |
| 0x10000406                                                                         | back-end closed the connection                                                                                                                             | <a href="#">Connector appliance fails to resolve DNS for FQDNs</a>                                |
| 0x10000411                                                                         | Gateway service closed the connection                                                                                                                      | <a href="#">Private server connection terminated</a>                                              |
| 0x10000413                                                                         | Error in determining connection teardown reason                                                                                                            | <a href="#">Failed to connect or send data to the private service IP or FQDN</a>                  |
| 0x100508                                                                           | User context does not match the access rule conditions                                                                                                     | <a href="#">No matching policy condition</a>                                                      |
| 0x100509                                                                           | Access policy not associated with the application                                                                                                          | <a href="#">No access policy associated with the application</a>                                  |

| Info code  | Description                                                                           | Resolution                                                                                        |
|------------|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| 0x10050C   | Policy evaluation results of multiple applications that the user might be entitled to | <a href="#">App enumeration information</a>                                                       |
| 0x00180101 | TCP/UDP app launch failed as routing entry is missing in application domain table     | <a href="#">TCP/UDP app launch failed as routing entry is missing in application domain table</a> |
| 0x00180102 | TCP/UDP app launch failed as connectors are not healthy                               | <a href="#">TCP/UDP app launch failed as connectors are not healthy</a>                           |
| 0x00180103 | UDP/DNS request failed, as Connector is unreachable                                   | <a href="#">UDP/DNS request failed, as Connector is unreachable</a>                               |
| 0x20580001 | Failed to load the page as NGS Cookie is expired                                      | <a href="#">Failed to load the page as NGS Cookie is expired</a>                                  |
| 0x20580002 | Access policy fetch failed because of network failure                                 | <a href="#">Access policy fetch failed because of network failure</a>                             |
| 0x20580003 | Access policy fetch failed while parsing the JSON web token                           | <a href="#">Access policy fetch failed while parsing the JSON web token</a>                       |
| 0x20580004 | Network failure to fetch Access Policy details                                        | <a href="#">Network failure to fetch Access Policy details</a>                                    |
| 0x20580005 | Policy fetch failed while fetching public certificate                                 | <a href="#">Policy fetch failed while fetching public certificate</a>                             |
| 0x20580007 | Policy fetch failed while validating signature of JWT                                 | <a href="#">Policy fetch failed while validating signature of JWT</a>                             |
| 0x20580008 | Policy fetch failed while validating the public certificate                           | <a href="#">Policy fetch failed while validating the public certificate</a>                       |
| 0x2058000A | Failed to determine store environment to form a policy URL                            | <a href="#">Failed to determine store environment to form a policy URL</a>                        |
| 0x2058000B | Failed to get response of access policy fetch request                                 | <a href="#">Failed to get response of access policy fetch request</a>                             |
| 0x2058000C | Access policy fetch failed due to an expired secondary DS auth token                  | <a href="#">Access Policy fetch failed due to an expired secondary DS auth token</a>              |

| Info code                                      | Description                                                                    | Resolution                                                                                 |
|------------------------------------------------|--------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 0x10200002                                     | Connector appliance is not registered                                          | <a href="#">Connector appliance is not registered</a>                                      |
| 0x10200003                                     | Unable to connect to connector appliance                                       | <a href="#">Unable to connect to connector appliance</a>                                   |
| 0x10000301                                     | Connection to Citrix SPA service failed                                        | <a href="#">Connection to Citrix Secure Private Access service failed</a>                  |
| 0x10000303, 0x10000304                         | The proxy server is not reachable                                              | <a href="#">Proxy server is not reachable</a>                                              |
| 0x10000305                                     | Proxy server authentication failed                                             | <a href="#">Proxy server authentication failed</a>                                         |
| 0x10000306                                     | Configured proxy servers are not reachable                                     | <a href="#">Configured proxy servers are not reachable</a>                                 |
| 0x10000307                                     | Received error response from backend server                                    | <a href="#">Received error response from backend server</a>                                |
| 0x10000005                                     | Unable to send request to the target URL                                       | <a href="#">Unable to send request to the target URL</a>                                   |
| 0x10000107                                     | Failed to process SSO                                                          | <a href="#">Failed to process SSO</a>                                                      |
| 0x10000108, 0x1000010B                         | Failed to process SSO, unable to determine SSO settings                        | <a href="#">Failed to process SSO, unable to determine SSO settings</a>                    |
| 0x10000101, 0x10000102, 0x10000103, 0x10000104 | FormFill SSO failed, incorrect form app configuration                          | <a href="#">FormFill SSO failed, incorrect form app configuration</a>                      |
| 0x1000010A                                     | FormFill SSO failed, incorrect form app configuration                          | <a href="#">FormFill SSO failed, incorrect form app configuration</a>                      |
| 0x10000202                                     | Kerberos SSO failed                                                            | <a href="#">Kerberos SSO failed</a>                                                        |
| 0x10000203                                     | Failed to process SSO for auth type                                            | <a href="#">Failed to process SSO for auth type</a>                                        |
| 0x10000204                                     | Kerberos SSO failed but falling back to NTLM                                   | <a href="#">Kerberos SSO failed but falling back to NTLM</a>                               |
| 0x14000001                                     | Multiple ZTNA entitled accounts configured in the Citrix Workspace application | <a href="#">Multiple ZTNA entitled accounts configured in Citrix Workspace application</a> |



## 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 **Workspace Configuration** 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 `WebAppUnsupportedAuth` 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 `FailedToConstructFormL` 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 is 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.
  1. In the Citrix Cloud hamburger menu, select **Resource Location**.
  2. 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™ application

**Info code:** 0x14000001

Configure only one ZTNA entitled account in the Citrix Workspace application.

## How to collect client logs

### • Windows client:

1. Open the app and ensure that logging is enabled.
2. Now connect to the Secure Private Access service and duplicate the issue you are facing.
3. In the app, go to **Logging** and click **Collect Log Files**. This generates the log file.
4. Save the log file on the client machine's desktop.

### • Mac client:

1. Open the app and go to **Logs > Verbose**.
2. Clear the logs and proceed to reproduce the issue.
3. Go back to **Logs > Export logs**. This creates a zip file that contains log files.

## Answers to FAQs

### What are Secure Private Access diagnostic logs?

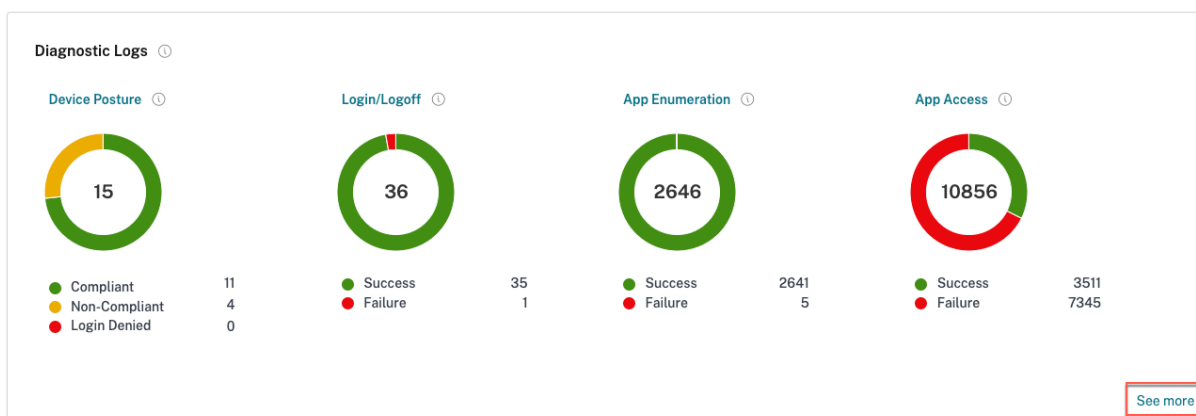
Secure Private Access diagnostic logs capture all events that occur when a user accesses any application (Web/SaaS/TCP/UDP). These logs capture device posture, app authentication, app enumeration, and app access logs. The details are presented in a tabular format. You can view the logs for the pre-set 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** widgets 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 fetches 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.



Diagnostic Logs

Diagnostic Logs 92338

Device Posture Logs 15

Last 1 Week

Add filter

Results are limited to the first 10000 records. Narrow your search criteria for more relevant results.

Export to CSV format

| Time                  | Category        | App name                  | App type | App FQDN                   | Transaction ID                        | Mode of access            | Info code  | User name             | Status  |  |
|-----------------------|-----------------|---------------------------|----------|----------------------------|---------------------------------------|---------------------------|------------|-----------------------|---------|--|
| > 2024-07-10 15:33:48 | App Access      | N/A                       | N/A      | ssprodt.ngsautomation.n... | 3141f1601-4934-4aca-865b-d21ca369...  | N/A                       | 0x10000000 | aaa.local\smi         | Failure |  |
| > 2024-07-10 15:33:48 | App Access      | DA_app                    | N/A      | ssprodt.ngsautomation.n... | 3141f1601-4934-4aca-865b-d21ca369...  | N/A                       | 0x10000005 | aaa.local\smi         | Failure |  |
| > 2024-07-10 15:33:28 | App Enumeration | SRK_Form Base SSO.mb...   | Web/SaaS | N/A                        | 4b28d126-16da-4957-829b-bae171e47...  | Citrix Enterprise Browser | 0x10050c   | aaa.local\sssl        | Success |  |
| > 2024-07-10 15:33:25 | App Enumeration | SRK_Form Base SSO.Par...  | Web/SaaS | N/A                        | 54614d25-3023-4315-8663-2a001a22...   | Citrix Enterprise Browser | 0x10050c   | aaa.local\sssl        | Success |  |
| > 2024-07-10 15:32:05 | App Enumeration | Web115_sasr_166_etrod...  | Web/SaaS | N/A                        | cc1d5e21-87b8-4567-8a5d-479f1adde4... | Citrix Enterprise Browser | 0x10050c   | aaa.local\sssl        | Success |  |
| > 2024-07-10 15:32:03 | App Enumeration | saas_166_prod/Web116...   | Web/SaaS | N/A                        | 71541fb9-8674-486c-a282-5ea781a70...  | Citrix Enterprise Browser | 0x10050c   | aaa.local\sssl        | Success |  |
| > 2024-07-10 15:32:02 | App Access      | DA_app                    | N/A      | ssprodt.ngsautomation.n... | 7b6f6e404-5e43-4b21-84ae-128184c1...  | N/A                       | N/A        | aaa.local\smi         | Success |  |
| > 2024-07-10 15:31:37 | App Access      | N/A                       | N/A      | ssprodt.ngsautomation.n... | 7b6f6e404-5e43-4b21-84ae-128184c1...  | N/A                       | 0x10000000 | aaa.local\smi         | Failure |  |
| > 2024-07-10 15:31:37 | App Access      | SRK-WebApp                | N/A      | ssprodt.ngsautomation.n... | 7b6f6e404-5e43-4b21-84ae-128184c1...  | N/A                       | 0x10000005 | aaa.local\smi         | Failure |  |
| > 2024-07-10 15:30:10 | App Access      | DA_app                    | Web      | https://ssprodt.ngsauto... | c46c310f-9336-4821-9302-88614a774...  | N/A                       | N/A        | aaa.local\smi         | Success |  |
| > 2024-07-10 15:29:53 | App Access      | DA_app                    | Web      | ssprodt.ngsautomation.n... | 7b6f6e404-5e43-4b21-84ae-128184c1...  | Citrix Enterprise Browser | N/A        | aaa.local\smi         | Success |  |
| > 2024-07-10 15:29:52 | App Access      | DA_app                    | N/A      | N/A                        | 67aab9f5-23a5-4b95-a87b-4f1010991...  | N/A                       | N/A        | aaa.local\smi         | Success |  |
| > 2024-07-10 15:29:49 | App Access      | N/A                       | SaaS     | N/A                        | 67aab9f5-23a5-4b95-a87b-4f1010991...  | N/A                       | N/A        | aaa.local\smi         | Success |  |
| > 2024-07-10 15:29:46 | App Access      | DA_app                    | Web      | N/A                        | 67aab9f5-23a5-4b95-a87b-4f1010991...  | Citrix Enterprise Browser | N/A        | aaa.local\smi         | Success |  |
| > 2024-07-10 15:29:40 | App Enumeration | SM Kerberos.SM SaaS S...  | Web/SaaS | N/A                        | 7dbabacf-abc8-47a2-aabc-8adceead6...  | Citrix Enterprise Browser | 0x10050c   | aaa.local\smi         | Success |  |
| > 2024-07-10 15:29:35 | App Enumeration | SM Kerberos.test-uploa... | Web/SaaS | N/A                        | 7b2d5689-cab4-436f-ac18-2ac15e411...  | Citrix Enterprise Browser | 0x10050c   | aaa.local\smi         | Success |  |
| > 2024-07-10 15:28:45 | App Enumeration | Perf WA Google Drive.N... | Web/SaaS | N/A                        | a8713ba6-50c2-46b4-87ab-4c1bc668...   | Citrix Enterprise Browser | 0x10050c   | aaa.local\spausser001 | Success |  |
| > 2024-07-10 15:27:01 | App Access      | SRK-WebApp                | Web      | https://www.naresht.in/    | a34c101c-942b-4f95-b633-9d44b1228...  | N/A                       | N/A        | aaa.local\sssl        | Success |  |
| > 2024-07-10 15:27:01 | App Access      | SRK-WebApp                | N/A      | www.naresht.in             | 81fa2602-84a8-4a55-bdaf-83bcc4b0...   | N/A                       | N/A        | aaa.local\sssl        | Success |  |
| > 2024-07-10 15:26:59 | App Access      | N/A                       | SaaS     | N/A                        | ac9122ae-f316-434a-bba8-757c56e8b...  | N/A                       | N/A        | aaa.local\sssl        | Success |  |

Showing 1,201 of 10000 Items

Page 1 of 600

20 Pages

## 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** - Displays the name of the access policy or policies that were triggered during the event.
- **Status** - Displays the status of the event, success, or failure.
- **Info Code** - Every failure event within the Secure Private Access diagnostic logs dashboard has an associated info code. [See more information on info code.](#)
- **Description** - Displays the reason for the failure or more details about the event.
- **APP FQDN** - FQDN of the application accessed
- **Event type** - Displays the event type associated with the operation performed.
- **Operation type** - Displays the operation for which the log is generated.
- **Category** - Three categories are available depending on the type of event. That is 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** - Displays the 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 your 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](#).

Diagnostic Logs

Diagnostic Logs 5 Device Posture Logs 15

Last 1 Week Add Filter Transaction-ID = 21538289-0c88-414a-9de2-7f3e32a1470b

Results are limited to the first 10000 records. Narrow your search criteria for more relevant results.

Export to CSV format

| Time                | Category   | App name         | App type | App FQDN       | Transaction ID                       | Mode of access      | Info code  | User name     | Status  |
|---------------------|------------|------------------|----------|----------------|--------------------------------------|---------------------|------------|---------------|---------|
| 2024-07-10 12:20:25 | App Access | AR TCP 30 Nov 21 | TCP      | 10.220.177.102 | 21538289-0c88-414a-9de2-7f3e32a1470b | N/A                 | N/A        | aaa.local\sm1 | Success |
| 2024-07-10 12:20:25 | App Access | AR TCP 30 Nov 21 | TCP      | 10.220.177.102 | 21538289-0c88-414a-9de2-7f3e32a1470b | N/A                 | N/A        | aaa.local\sm1 | Success |
| 2024-07-10 12:19:51 | App Access | N/A              | TCP      | N/A            | 21538289-0c88-414a-9de2-7f3e32a1470b | N/A                 | 0x13000010 | aaa.local\sm1 | Success |
| 2024-07-10 12:19:51 | App Access | N/A              | TCP      | N/A            | 21538289-0c88-414a-9de2-7f3e32a1470b | N/A                 | 0x1300000b | aaa.local\sm1 | Failure |
| 2024-07-10 12:19:41 | App Access | AR TCP 30 Nov 21 | TCP      | 10.220.177.102 | 21538289-0c88-414a-9de2-7f3e32a1470b | Secure Access Agent | N/A        | aaa.local\sm1 | Success |

Showing 1-5 of 5 items Page 1 of 1 20 rows

Diagnostic Logs

Diagnostic Logs 682 Device Posture Logs 15

Last 1 Week Add Filter User-Name = aaa.local\sm1

Results are limited to the first 10000 records. Narrow your search criteria for more relevant results.

Export to CSV format

| Time                | Category     | App name         | App type | App FQDN       | Transaction ID                       | Mode of access | Info code  | User name     | Status  |
|---------------------|--------------|------------------|----------|----------------|--------------------------------------|----------------|------------|---------------|---------|
| 2024-07-10 12:28:56 | N/A          | N/A              | TCP      | N/A            | c1fa1144-b352-4c85-b0ba-8256dea74... | N/A            | N/A        | aaa.local\sm1 | Success |
| 2024-07-10 12:20:25 | App Access   | AR TCP 30 Nov 21 | TCP      | 10.220.177.102 | 21538289-0c88-414a-9de2-7f3e32a14... | N/A            | N/A        | aaa.local\sm1 | Success |
| 2024-07-10 12:20:25 | App Access   | AR TCP 30 Nov 21 | TCP      | 10.220.177.102 | 21538289-0c88-414a-9de2-7f3e32a14... | N/A            | N/A        | aaa.local\sm1 | Success |
| 2024-07-10 12:19:57 | Login/Logout | N/A              | TCP      | N/A            | 473e058d-5580-4588-883c-60d420c...   | N/A            | N/A        | aaa.local\sm1 | Success |
| 2024-07-10 12:19:51 | App Access   | N/A              | TCP      | N/A            | 21538289-0c88-414a-9de2-7f3e32a14... | N/A            | 0x13000010 | aaa.local\sm1 | Success |
| 2024-07-10 12:19:51 | App Access   | N/A              | TCP      | N/A            | 21538289-0c88-414a-9de2-7f3e32a14... | N/A            | 0x1300000b | aaa.local\sm1 | Failure |

You can also use the various filter options to refine your search on the Device Posture logs.

Diagnostic Logs

Diagnostic Logs 5 Device Posture Logs 12

Last 1 Week Add Filter Policy-Result = Non-Compliant

Results are limited to the first 10000 records. Narrow your search criteria for more relevant results.

Export to CSV format

| Time                | Policy info      | Policy result | Operating system | Info code | User name     | Status  |
|---------------------|------------------|---------------|------------------|-----------|---------------|---------|
| 2024-07-09 19:01:52 | NoMatchingPolicy | Non-Compliant | Windows          | N/A       | aaa.local\sm1 | Success |
| 2024-07-09 18:53:01 | NoMatchingPolicy | Non-Compliant | Windows          | N/A       | aaa.local\sm1 | Success |
| 2024-07-09 18:52:04 | NoMatchingPolicy | Non-Compliant | Windows          | N/A       | aaa.local\sm1 | Success |
| 2024-07-09 18:33:01 | NoMatchingPolicy | Non-Compliant | Windows          | N/A       | aaa.local\sm1 | Success |
| 2024-07-09 18:30:05 | NoMatchingPolicy | Non-Compliant | Windows          | N/A       | aaa.local\sm1 | Success |
| 2024-07-09 18:10:51 | NoMatchingPolicy | Non-Compliant | Windows          | N/A       | aaa.local\sm1 | Success |
| 2024-07-09 18:01:01 | NoMatchingPolicy | Non-Compliant | Windows          | N/A       | aaa.local\sm1 | Success |
| 2024-07-09 17:52:29 | NoMatchingPolicy | Non-Compliant | Windows          | N/A       | aaa.local\sm1 | Success |
| 2024-07-09 17:42:11 | NoMatchingPolicy | Non-Compliant | Windows          | N/A       | N/A           | Success |
| 2024-07-09 17:25:31 | NoMatchingPolicy | Non-Compliant | Windows          | N/A       | N/A           | Success |
| 2024-07-09 16:25:37 | NoMatchingPolicy | Non-Compliant | Windows          | N/A       | aaa.local\sm1 | Success |
| 2024-07-09 16:41:23 | NoMatchingPolicy | Non-Compliant | Windows          | N/A       | N/A           | Success |

Showing 1-12 of 12 items Page 1 of 1 20 rows

## 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 about end-user logon or logoff status to the Citrix Secure Access client and authentication to workspace (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.

### **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  |
| 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](#)

## Integration with DaaS Monitor

September 6, 2025

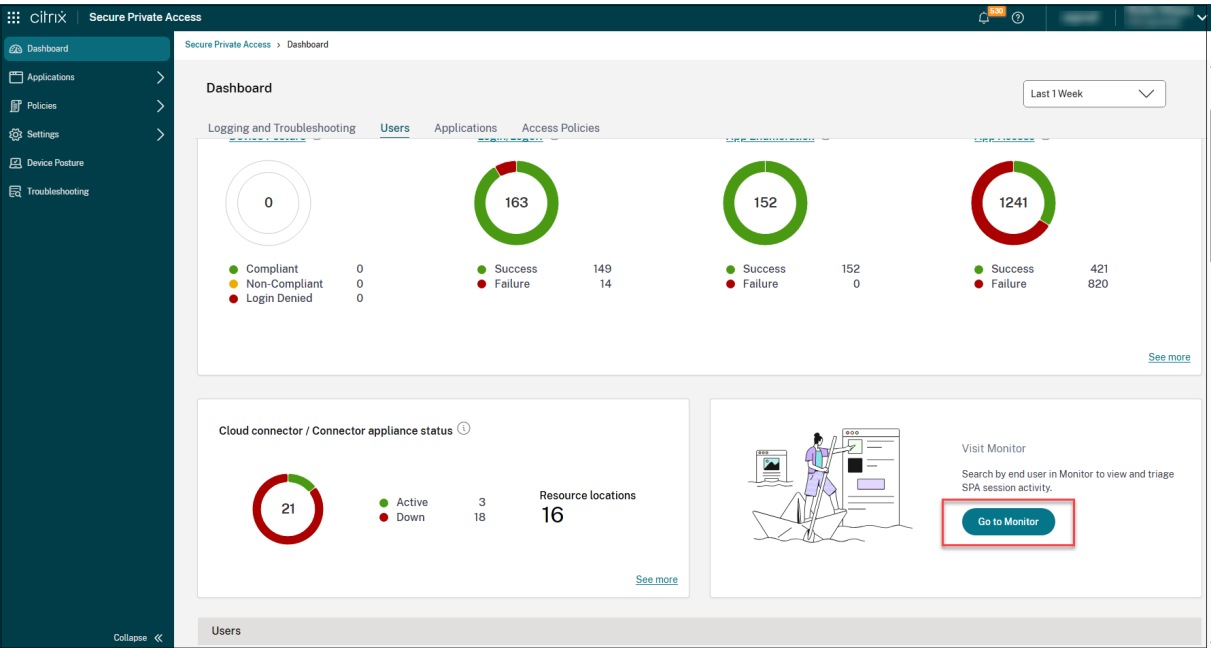
Secure Private Access is integrated with Monitor, the monitoring and troubleshooting console for Citrix DaaS. Administrators and help-desk personnel can monitor and troubleshoot Web/SaaS, agentless, and TCP/UDP app sessions and events from the DaaS Monitor, in addition to the Secure Private Access dashboard.

### How to access Monitor

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

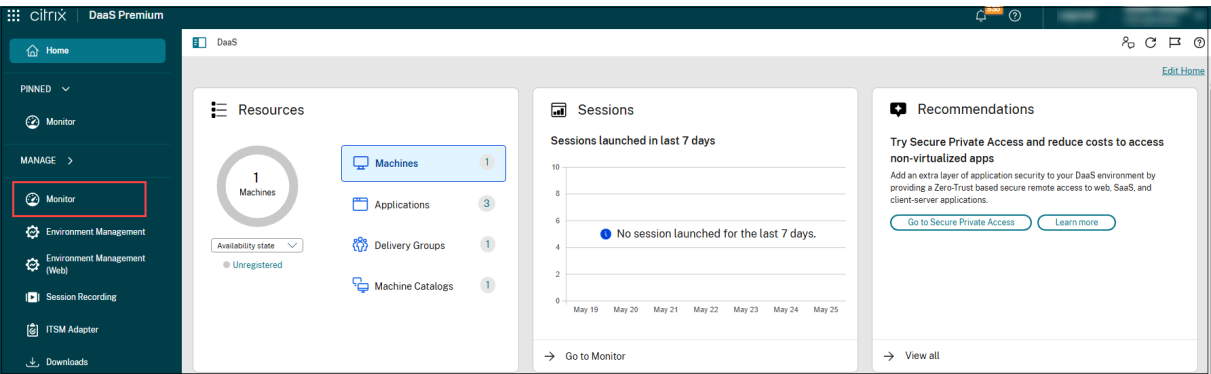
#### Access monitor from Secure Private Access dashboard:

The following figure displays a sample Secure Private Access dashboard with **Go to Monitor** link.



**Access monitor from Citrix DaaS:**

The following figure displays a Citrix DaaS landing page.



In the Monitor page, you can search a Secure Private Access session by using the **Search** field or from the **Filters** page.

**Reference**

For complete details on the Secure Private Access and Monitor integration, see [Secure Private Access integration with Monitor](#).

## Secure Private Access sessions codes in DaaS Monitor

September 6, 2025

The following tables provide a list of error codes related to application enumeration, application launch, and sessions in Citrix Monitor.

For related information, see the following topics:

- [Integration with DaaS monitor](#)
- [DaaS Monitor](#)

### Info code lookup table

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 and the corresponding resolution.

| Info code                                                  | Description                                                                                    | Resolution                                                                                       |
|------------------------------------------------------------|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
| 0x180022                                                   | App launch failed as authentication service is down                                            | <a href="#">App launch failed as the authentication service is down</a>                          |
| 0x1800B7                                                   | App launch failed because App FQDN length exceeded                                             | <a href="#">App launch failed because App FQDN length exceeded</a>                               |
| 0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5, 0x1800A6, 0x1800A7 | Web app launch failed as unable to connect to back end web app                                 | <a href="#">Web app launch failed as unable to connect to back end web app</a>                   |
| 0x18001A, 0x18001B                                         | User details not found                                                                         | <a href="#">User details not found</a>                                                           |
| 0x1800AA                                                   | Web/SaaS app launch has failed due to user attributes not found while preparing the SAML token | <a href="#">Web/SaaS app launch has failed</a>                                                   |
| 0x180010                                                   | Web/SaaS app launch has failed due to inability to identify the application FQDN               | <a href="#">Web/SaaS app launch has failed due to inability to identify the application FQDN</a> |
| 0x180040                                                   | Web/SaaS app launch has failed due to invalid appld provided by the SAML service provider      | <a href="#">App launch failed due to invalid appld provided by the SAML service provider</a>     |

| 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                                              | <a href="#">Web/SaaS app launch has failed due to invalid app access request</a>                                              |
| 0x1800D4, 0x1800E1, 0x180106, 0x180107, 0x1800EB, 0x1800EC                               | TCP/UDP app launch has failed during policy evaluation due to internal error                                  | <a href="#">TCP/UDP app launch has failed during policy evaluation due to internal error</a>                                  |
| 0x1800D9                                                                                 | TCP/UDP app launch has failed while parsing policy evaluation response                                        | <a href="#">TCP/UDP app launch has failed while parsing policy evaluation response</a>                                        |
| 0x1800DA                                                                                 | TCP/UDP app launch has failed with invalid result during policy evaluation                                    | <a href="#">TCP/UDP app launch has failed with invalid result during policy evaluation</a>                                    |
| 0x1800DB                                                                                 | TCP/UDP app launch has failed with invalid resource location configuration                                    | <a href="#">TCP/UDP app launch has failed with invalid resource location configuration</a>                                    |
| 0x1800E0                                                                                 | TCP/UDP app launch failed as the length of the app name is too long                                           | <a href="#">TCP/UDP app launch failed as the length of App Name is too long</a>                                               |
| 0x1800EE                                                                                 | TCP/UDP app launch has failed during connection establishment to the private TCP server due to invalid app ID | <a href="#">TCP/UDP app launch has failed during connection establishment to the private TCP server due to invalid app ID</a> |
| 0x1800E3                                                                                 | TCP/UDP app launch has been denied during policy evaluation                                                   | <a href="#">TCP/UDP app launch has been denied during policy evaluation</a>                                                   |
| 0x1800EA                                                                                 | TCP app launch has failed due to destination FQDN being too long                                              | <a href="#">TCP app launch has failed due to destination FQDN being too long</a>                                              |
| 0x1800ED                                                                                 | TCP app launch has failed due to invalid destination IP                                                       | <a href="#">TCP app launch has failed due to invalid destination IP</a>                                                       |
| 0x180102                                                                                 | TCP/UDP app launch failed as no response was received from the Connector Appliance                            | <a href="#">TCP/UDP app launch failed as no response was received from the Connector Appliance</a>                            |

| Info code                                      | Description                                                                                                | Resolution                                                                                                                 |
|------------------------------------------------|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------|
| 0x10000005                                     | Web/SaaS application launch failed due to a failure to establish a connection with the back-end app server | <a href="#">Web/SaaS application launch failed due to a failure to establish a connection with the back-end app server</a> |
| 0x10000101, 0x10000102, 0x10000103, 0x10000104 | Web/SaaS FormFill SSO failed due to invalid application configuration                                      | <a href="#">Web/SaaS FormFill SSO failed due to invalid application configuration</a>                                      |
| 0x10000202                                     | Kerberos SSO for Web/SaaS failed                                                                           | <a href="#">Kerberos SSO for Web/SaaS failed</a>                                                                           |
| 0x10000203                                     | Web/SaaS SSO failed due to internal server error                                                           | <a href="#">Web/SaaS SSO failed due to internal server error</a>                                                           |
| 0x10000303, 0x10000304                         | Web/SaaS app launch failed due to the configured proxy being unreachable                                   | <a href="#">Web/SaaS app launch failed due to the configured proxy being unreachable</a>                                   |
| 0x10000305                                     | Web/SaaS app launch failed due to a failure to authenticate with the configured proxy                      | <a href="#">Web/SaaS app launch failed due to a failure to authenticate with the configured proxy</a>                      |
| 0x10000414                                     | TCP/UDP application launch failed due to a request coming on an invalid IP/hostname or port                | <a href="#">TCP/UDP application launch failed due to a request coming on an invalid IP/hostname or port</a>                |
| 0x10000415                                     | TCP/UDP application launch failed as the destination server refused the connection                         | <a href="#">TCP/UDP application launch failed as the destination server refused the connection</a>                         |
| 0x10000416                                     | TCP/UDP application launch failed as the destination was not found                                         | <a href="#">TCP/UDP application launch failed as the destination was not found</a>                                         |
| 0x10000417                                     | TCP/UDP application launch failed as the destination network was not reachable                             | <a href="#">TCP/UDP application launch failed as the destination network was not reachable</a>                             |
| 0x10000405                                     | TCP/UDP application launch failed due to the inability to connect to the destination                       | <a href="#">TCP/UDP application launch failed due to the inability to connect to the destination</a>                       |

| Info code                          | Description                                                            | Resolution                                                                             |
|------------------------------------|------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| 0x10000302                         | Connector failed to read the proxy details                             | <a href="#">Connector failed to read the proxy details</a>                             |
| 0x10000306                         | Configured proxies are not reachable                                   | <a href="#">Configured proxies are not reachable</a>                                   |
| 0x10000403, 0x10000404, 0x10000407 | TCP/UDP application launch failed due to the internal connection error | <a href="#">TCP/UDP application launch failed due to the internal connection error</a> |
| 6003, 6007                         | Citrix Secure Access client failed to do SSO                           | <a href="#">Citrix Secure Access client failed to do SSO</a>                           |

### 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 cause 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 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

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.

### **TCP/UDP 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.

### **TCP/UDP 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.

### **TCP/UDP 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.

### **TCP/UDP 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.

### **TCP/UDP 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.

**TCP/UDP 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.

**TCP/UDP app launch has been denied during policy evaluation**

**Info code:** 0x1800E3

Contact Citrix support with the transaction ID and client collected debug logs.

**TCP app launch has failed due to destination FQDN being too long**

**Info code:** 0x1800EA

Ensure that the FQDN length is under 256 characters.

**TCP app launch has failed due to invalid destination IP**

**Info code:** 0x1800ED

Access only valid private IP addresses from the clients.

**TCP/UDP app launch failed as no response was received from the Connector Appliance**

**Info code:** 0x180102

Check the reachability of Connector Appliance.

**TCP/UDP 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.

**TCP/UDP application launch failed as the destination server refused the connection**

**Info code:** 0x10000415

Check the status of the destination server.

### **TCP/UDP application launch failed as the destination was not found**

**Info code:** 0x10000416

Check the destination server host name.

### **TCP/UDP 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 of 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.

### **TCP/UDP 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 of 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 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 of 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 of 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.

### **TCP/UDP 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 login 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 terminated/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              |

| Code | Status                      | Description                                                                                  |
|------|-----------------------------|----------------------------------------------------------------------------------------------|
| 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                                                  |
| 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 |



---

| Code | Status             | Description                                 |
|------|--------------------|---------------------------------------------|
| 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                         |
| 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                   |

---

## Audit logs

September 6, 2025

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**.

| Date & Time ↓             | Actor           | Service               | Event                          | Target                |
|---------------------------|-----------------|-----------------------|--------------------------------|-----------------------|
| Jan 28, 2025 05:44:26 UTC | admin@sun.ac.za | Secure Private Access | Updated HTTP/HTTPS application | Base CRM1             |
| Jan 28, 2025 05:44:24 UTC | admin@sun.ac.za | Secure Private Access | Updated application domain     | sufmprod.sun.ac.za    |
| Jan 28, 2025 05:44:24 UTC | admin@sun.ac.za | Secure Private Access | Updated application domain     | *.sufmprod.sun.ac.za  |
| Jan 28, 2025 05:44:08 UTC | admin@sun.ac.za | Secure Private Access | Updated HTTP/HTTPS application | Base CRM1             |
| Jan 28, 2025 05:44:03 UTC | admin@sun.ac.za | Secure Private Access | Updated application domain     | sufmprod.sun.ac.za    |
| Jan 28, 2025 05:44:03 UTC | admin@sun.ac.za | Secure Private Access | Updated application domain     | *.sufmprod.sun.ac.za  |
| Jan 28, 2025 05:43:17 UTC | admin@sun.ac.za | Secure Private Access | Deleted TCP/UDP application    | ING_Ingenieursbib_TCP |
| Jan 28, 2025 05:41:07 UTC | admin@sun.ac.za | Secure Private Access | Created application domain     | ING_Ingenieursbib_TCP |
| Jan 28, 2025 05:41:07 UTC | admin@sun.ac.za | Secure Private Access | Created TCP/UDP application    | ING_Ingenieursbib_TCP |
| Jan 28, 2025 05:40:54 UTC | admin@sun.ac.za | Secure Private Access | Updated application domain     | *.id.sun.ac.za        |
| Jan 28, 2025 05:40:51 UTC | admin@sun.ac.za | Secure Private Access | Updated application domain     | id.sun.ac.za          |
| Jan 28, 2025 05:40:50 UTC | admin@sun.ac.za | Secure Private Access | Created HTTP/HTTPS application | SunID                 |

For details such as exporting events, retrieving events for a specific time period, forwarding log events, and data retention, see [System Log](#).

## Citrix Enterprise Browser

September 6, 2025

Citrix Enterprise Browser (formerly known as Citrix Workspace™ Browser) is a native browser that runs on the client machine, allowing users to securely access web and SaaS applications directly from the Citrix Workspace app. It provides a consistent user interface across various applications, enhancing productivity and delivering excellent performance in rendering these apps.

Built on a Chromium foundation, the Enterprise Browser prioritizes security, protecting both your device and your organization's network from unintended user behaviors. It is available as part of the Citrix Workspace app for both Windows and Mac. When you open web or SaaS applications within the Workspace app, the Enterprise Browser is activated, launching these apps in a new window.

You can access the following types of web and SaaS apps that have the enhanced security feature enabled:

- Internal web apps that would otherwise require a VPN to access outside of the Citrix Workspace app framework, open in the Enterprise Browser.
- External SaaS apps open in the Enterprise Browser if Secure Private Access policies are applied while deploying the app. If the Secure Private Access policies aren't applied to the external SaaS app, they open in your native browser.

For more details, see [Citrix Enterprise Browser](#).

## Unsanctioned websites

September 6, 2025

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

For all other internet URLs or SaaS applications that do not have an app configured, admins can use the **Settings > Unsanctioned Websites** page from the admin console to allow or deny access via Citrix Enterprise Browser. Admins can also redirect access to a Remote Browser Isolated (RBI) environment to prevent browser-based attacks. If an admin has configured redirection of URLs to RBI, the following actions occur.

1. Secure Private Access converts the domains.
2. Citrix Enterprise Browser then sends these URLs back to Secure Private Access.

- Secure Private Access redirects those URLs to the Remote Browser Isolation service.

You can use wildcards, such as `*.example.com`, to control access to all the domains in that website and all the pages within that domain.

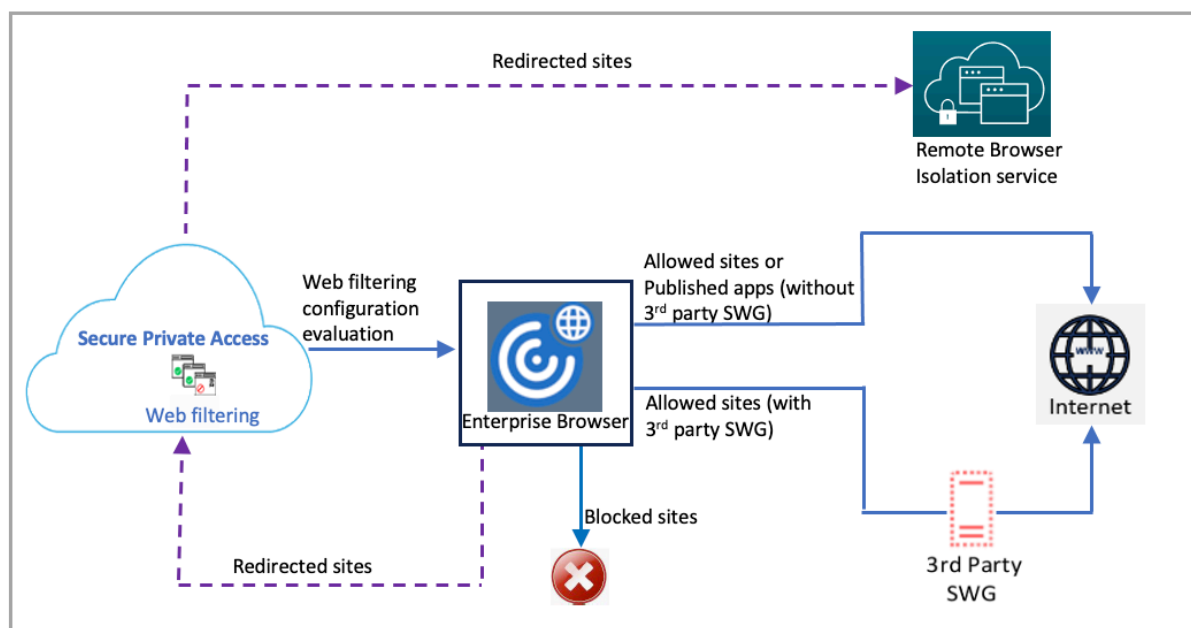
**Note:**

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

## How unsanctioned websites work

- URL analysis check is done to determine if the URL is a Citrix® service URL.
- The URL is then checked to determine if it is an Enterprise web or SaaS app URL.
- The URL is then checked to determine if it is identified as a blocked URL, or if it must be redirected to a secure browser session or if the URL can be allowed to be accessed.

The following illustration explains the end user traffic flow.



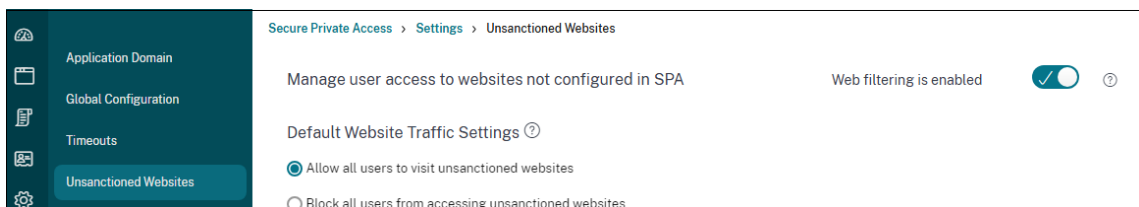
When a request arrives, the following checks are performed, and corresponding actions are taken:

- Does the request match the global allow list?
  - If it matches, the user can access the requested website.
  - If it does not match, website lists are checked.
- Does the request match the configured website list?

- a) If it matches, the following sequence determines the action.
  - i. Block
  - ii. Redirect
  - iii. Allow
- b) If it does not match, the default action (ALLOW) is applied. The default action cannot be changed.

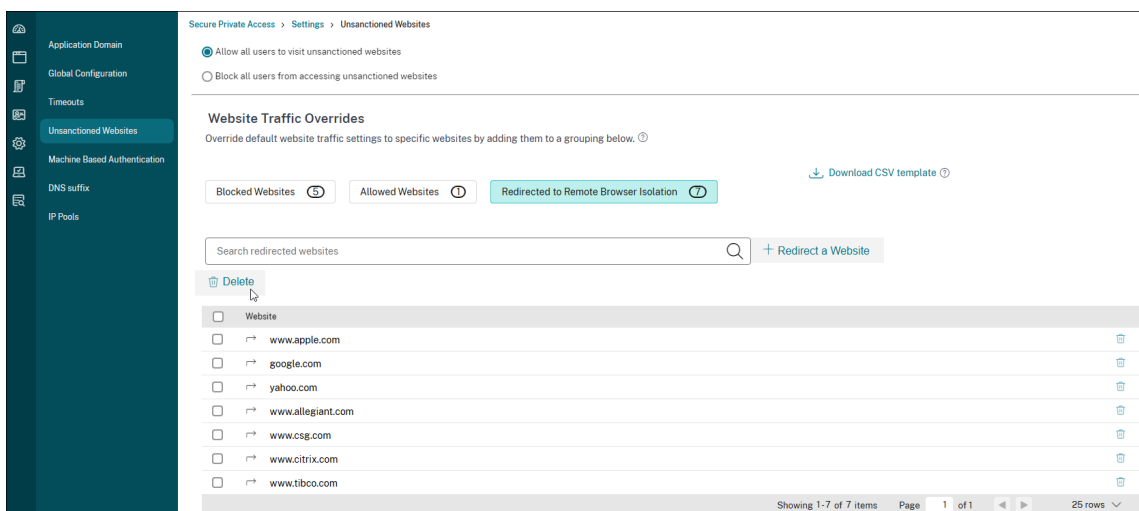
## Configure rules for unsanctioned websites

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



### Note:

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



You can also change settings for specific URLs by adding them to blocked websites, allowed websites, or redirected to the Remote Browser Isolation list.

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

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

The URL is added to the list of allowed websites.

**Note:**

A paid Remote Browser Isolation Standard service customer (organization) gets 5,000 hours of use per year by default. For more hours, they must buy the secure browser add-on packs. You can track the usage of the Remote Browser Isolation service. For more information, see the following topics:

- [Manage and monitor remote isolated browsers](#)
- [Remote Browser Isolation](#).

**Points to note**

If the users do not have access to a SaaS app, they cannot launch the application from Citrix Enterprise Browser. However, they might still be able to access the app by typing the URL directly in Citrix Enterprise Browser.

- If access to an app is denied by policy, the application URL is added to the blocked list if the **Web Filtering** feature is enabled. This ensures that any attempts to access the app, whether through Citrix Enterprise Browser or directly via URL, are blocked.
- For unpublished apps, even if routing is configured, access to these apps is denied. The URL of the unpublished app is added to the blocked list if the **Web Filtering** feature is enabled, preventing any access attempts.

**Role-based access control**

September 6, 2025

Secure Private Access uses a role-based access control model to manage user permissions and access levels. This means that each user is assigned a specific role, and that role determines what they can

and cannot do within the system. This model helps to ensure that users have the appropriate level of access to perform their tasks, while also preventing them from accessing sensitive data or functions that they must not have access to.

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

- Full Access Administrator
- Read Only Administrator
- Full Monitor Administrator
- Helpdesk Administrator

**Note:**

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

The following table provides a brief description of each role:

| Role                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Full Access Administrator | <p>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.</p> <p>Access to all Secure Private Access functionalities.</p> <p>Permissions to create, edit, and modify apps, policies, and settings within the Secure Private Access console.</p>                                                      |
| Read Only Administrator   | <p>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.</p> <p>Access to the Secure Private Access dashboard.</p> <p>Ability to view all Secure Private Access application configurations and settings.</p> <p>The Read Only Administrator does not have the privileges to any of the create/update/delete functionality.</p> |

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

## Roles and privileges

The following table summarizes the roles and privileges:



|                                                                                              | Full Access<br>Administrator | Read Only<br>Administrator | Full Monitor<br>Administrator | Helpdesk<br>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                   |
| 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                   |

|                        | Full Access Administrator | Read Only Administrator | Full Monitor Administrator | Helpdesk Administrator |
|------------------------|---------------------------|-------------------------|----------------------------|------------------------|
| Access reporting tools | Yes                       | No                      | Yes                        | Limited                |

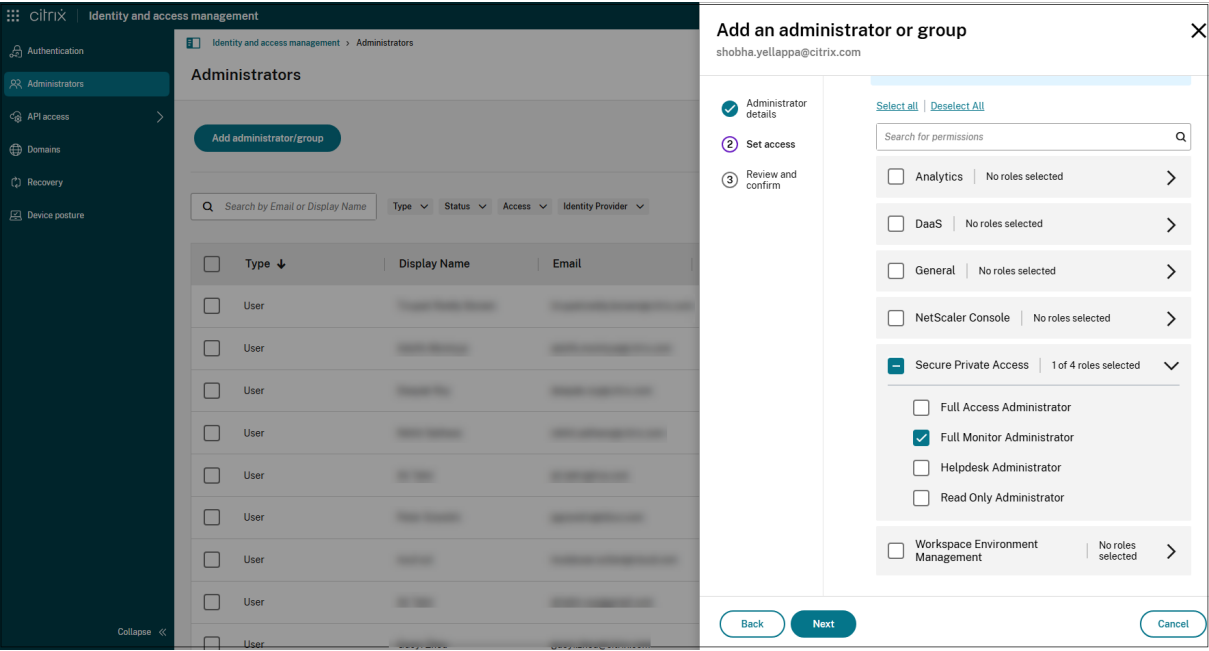
## Enable role-based access to admins

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:

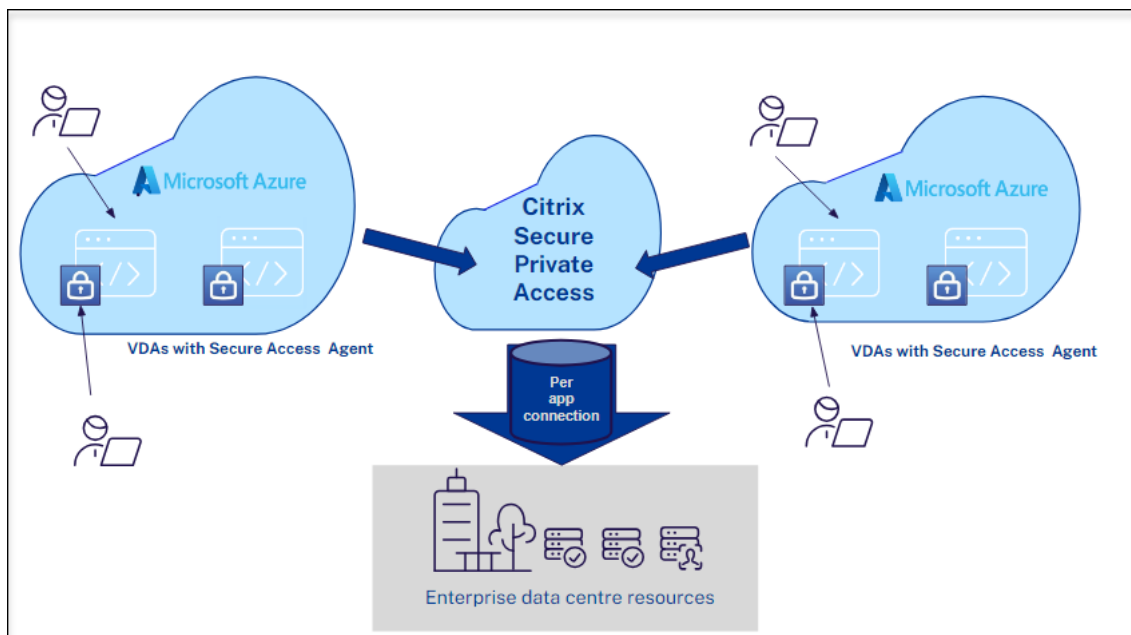
The **Analytics** and **General** services must be enabled for all Secure Private Access roles. The **Analytics** service is necessary for monitoring and reporting, while the **General** services are required for authentication, domains, authorization, traffic routing, and other functionalities.



Support for multi-session virtual desktop infrastructure

September 6, 2025

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).

## Feature deprecations

September 6, 2025

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 <a href="#">About deprecation of clientless VPN access for Web app access</a> .                       |
| 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 <a href="#">Migrate Gateway Connector to Connector Appliance</a> . |

## 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 Workspace for Web (Citrix Workspace™ app for HTML5).

**Note:**

Clientless VPN access method is only used when an internal app is accessed via Workspace for Web (Citrix Workspace app for HTML5). 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 Workspace for Web, then access to that application will be blocked.

It will not impact end-user accessing applications via Workspace Application, 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 Workspace for Web. 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 Workspace for Web or the HTML5 variant of Citrix Workspace app, then access to those applications will be blocked.

- Have more questions?

Reach out to [Citrix Support](#).





© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at <https://www.cloud.com/legal>. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (<https://www.cloud.com/legal>) for more information.