Citrix Secure Private Access

Contents

What's new

June 14, 2024

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. For details, see /en-us/citrix-secure-private-access/service/secure-private-access-for-on-premises-config-tool.html.

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. For details, see Troubleshoot Citrix Gateway Connector registration issues.

    [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. For details, see Log on and set up the Citrix Gateway Connector.

    [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]

Feature deprecations

June 12, 2024

This article gives you advanced notice of Secure Private Access service features that are being phased out, so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when features are withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality. For details about product lifecycle support, see Product Lifecycle Support Policy.

The following table lists the Secure Private Access service features that are deprecated or planned for deprecation.

Item	Deprecation announced in	Deprecation date	Alternative
Clientless VPN access method for Web app access	January 2023	October 17, 2023	Use Citrix Enterprise Browser or Direct Access as per your use case. For more details, see About deprecation of clientless VPN access for Web app access.
Category-based web filtering	December 2022	December 31, 2022	The allow, deny, or RBI redirection functionality per website in Secure Private Access will be retained to provide selective access to non-work related websites from Citrix Enterprise Browser.
Restrict navigation security control	April 2022	15 June 2022	NA
Citrix Gateway Connector	May 2022	30 September 2022	Connector Appliance. To migrate your Gateway Connector to Connector Appliance, see Migrate Gateway Connector to Connector Appliance.

About deprecation of clientless VPN access for Web app access

- What is Clientless VPN (clientless VPN) access method?

  Citrix Secure Private Access uses the CVPN-based access method when an internal web app, configured without any enhanced security restrictions, is accessed via 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. Secure Private Access for Citrix Workspace.
  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.

Get started with Citrix Secure Private Access

November 21, 2023

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

Functionality	Service/Component providing the functionality
Web filtering and categorization	Web filtering service
Enhanced security policies for SaaS	Cloud app control
Secure browsing	Remote Browser Isolation service
Visibility into website access and risky behavior	Citrix Analytics

Get started with 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.

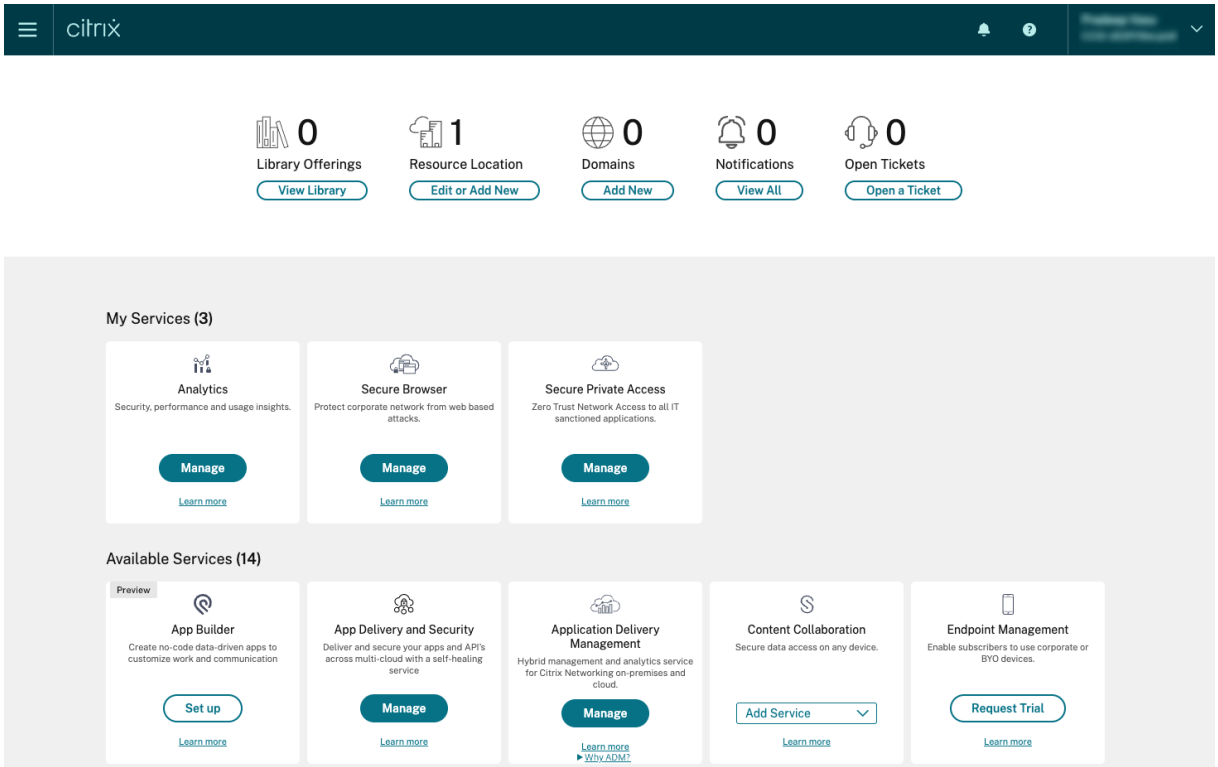
Step 1: **Sign Up for Citrix Cloud**

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.

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.

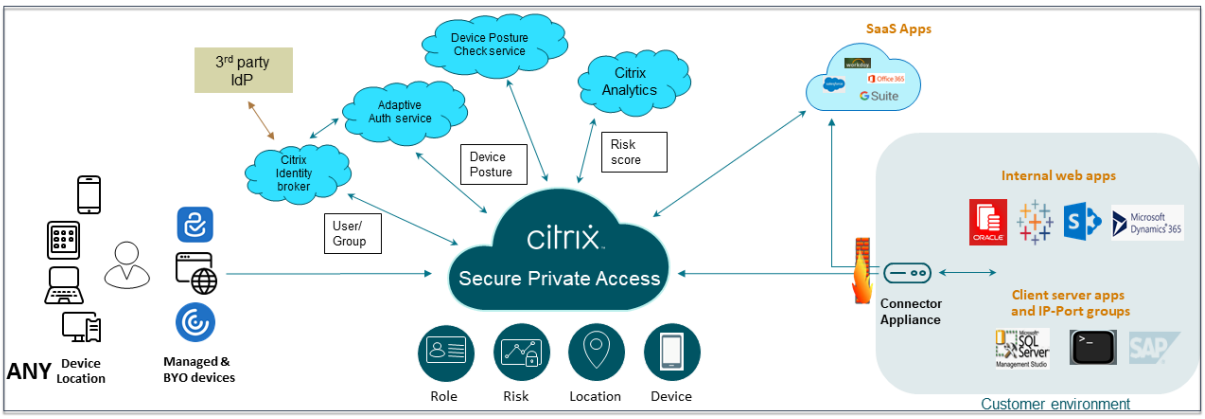
Secure Private Access service solution overview

November 21, 2023

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 poli-

cies 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-gateway/plug-ins/citrix-secure-access-client-for-windows.html.
- For macOS, the client version (22.02.3 and later) can be downloaded from the App Store.

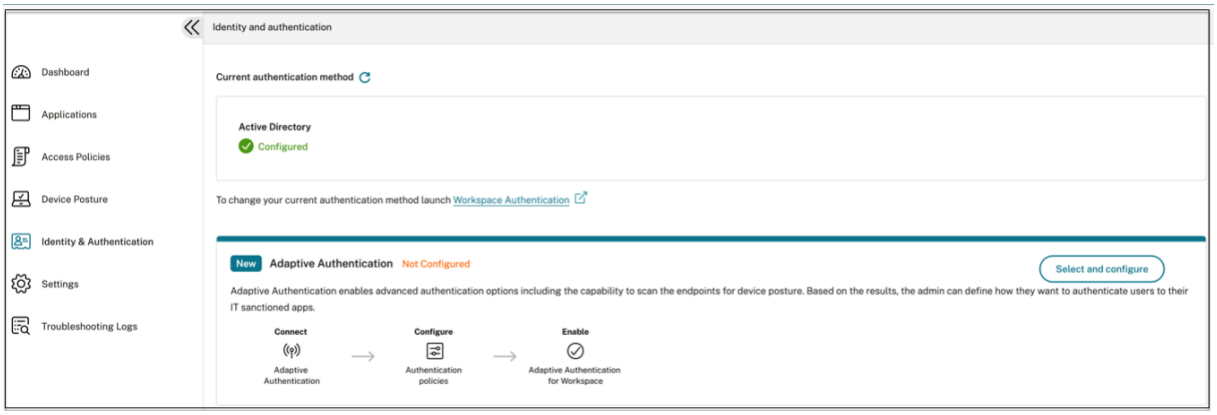
For details, see Support for client-server apps.

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.

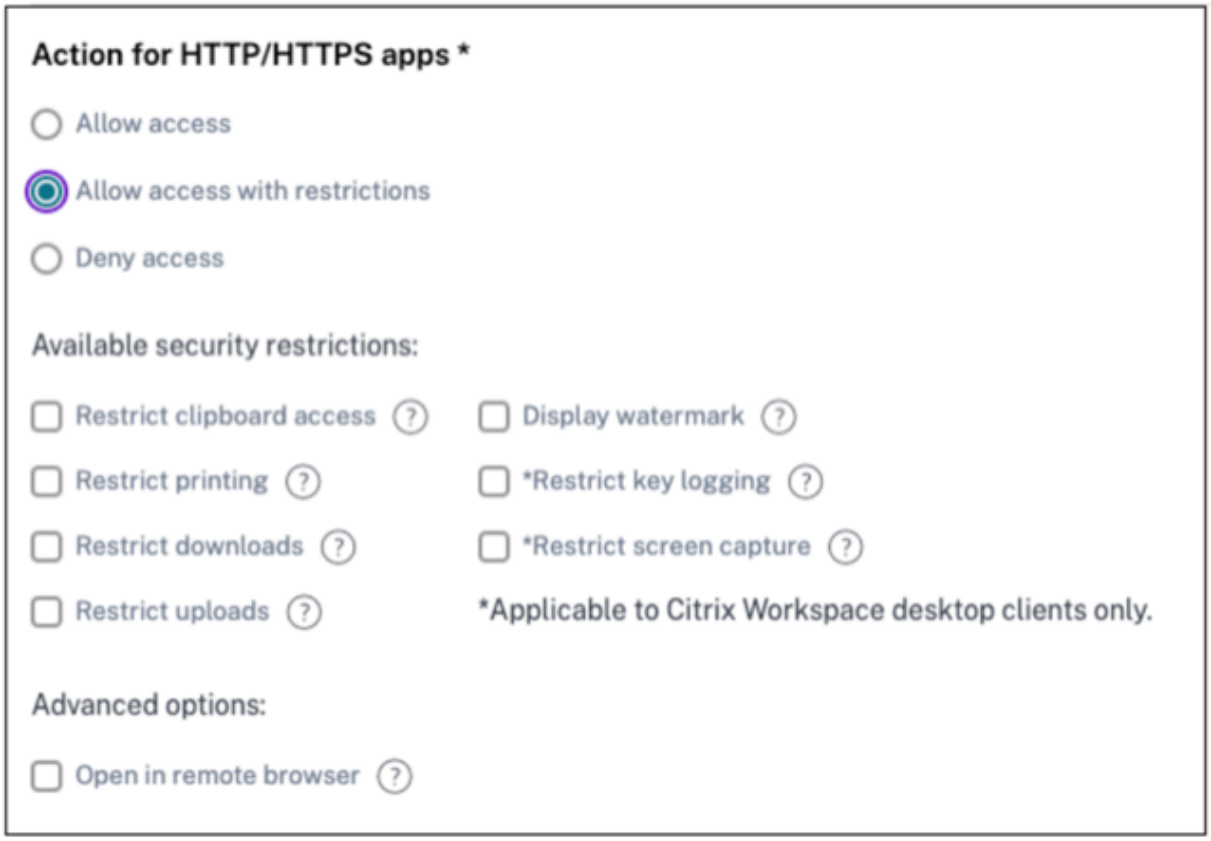
Enumerate and publish apps

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.



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 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:

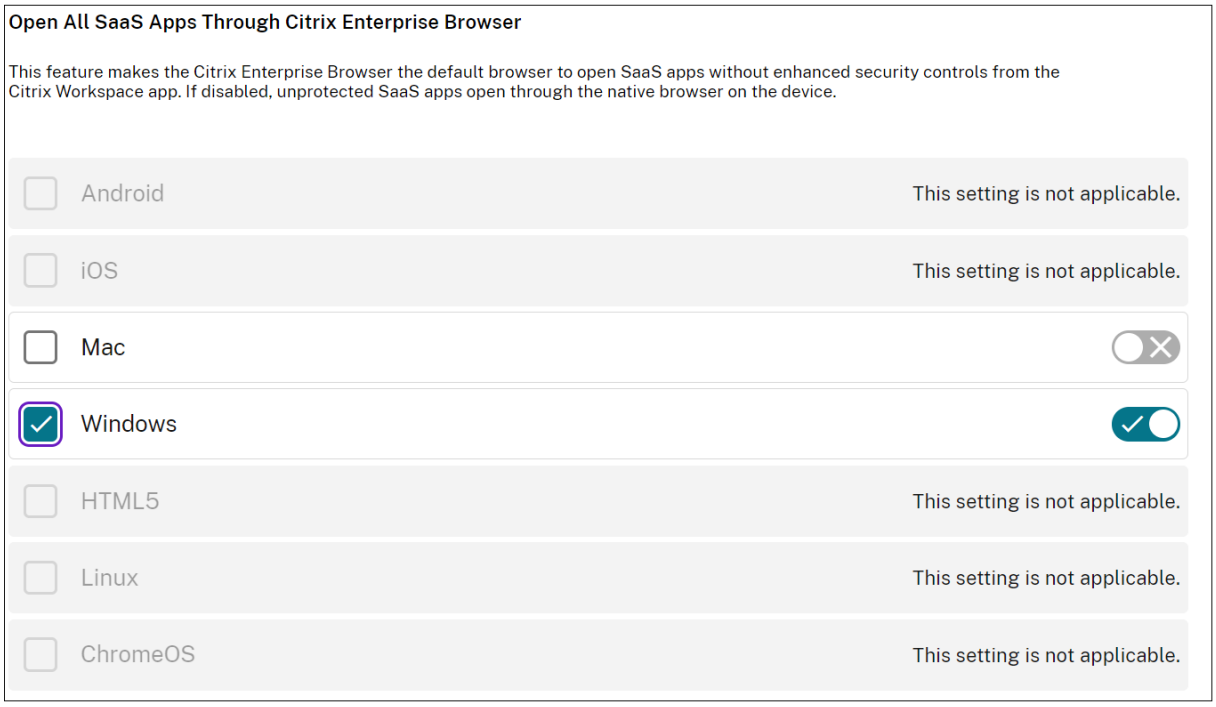
To configure, here is an example JSON file to enable Citrix Enterprise Browser for all apps, by default:


```
"settings": [
                    {

                       "name": "open all apps in ceb",
                       "value": "true"
                     }

                    ]
<!--NeedCopy-->
```

The default value is true.

Configuration through GUI:

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



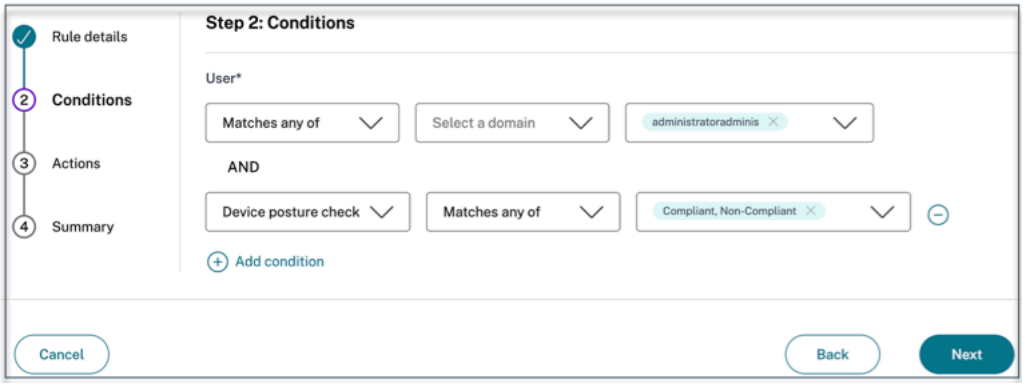
For details, see Manage Citrix Enterprise Browser through GACS.

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:



   - **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**.

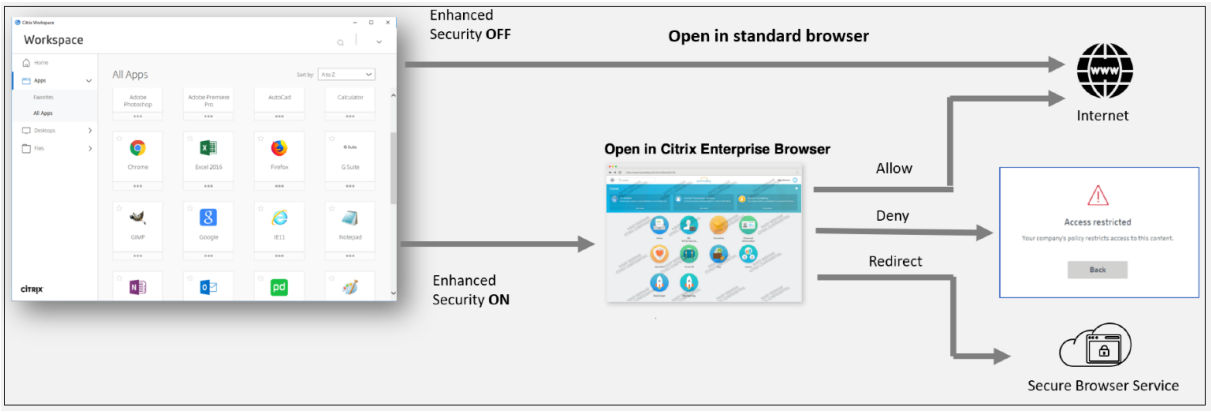
    The Summary page displays the policy details.
14. Verify the details and click **Finish**.

> **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.

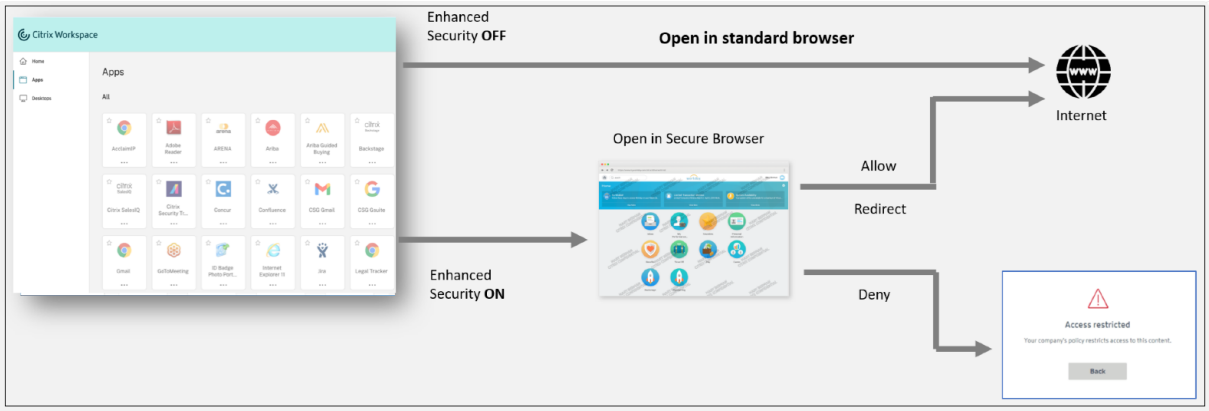
End-user experience

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 websites.

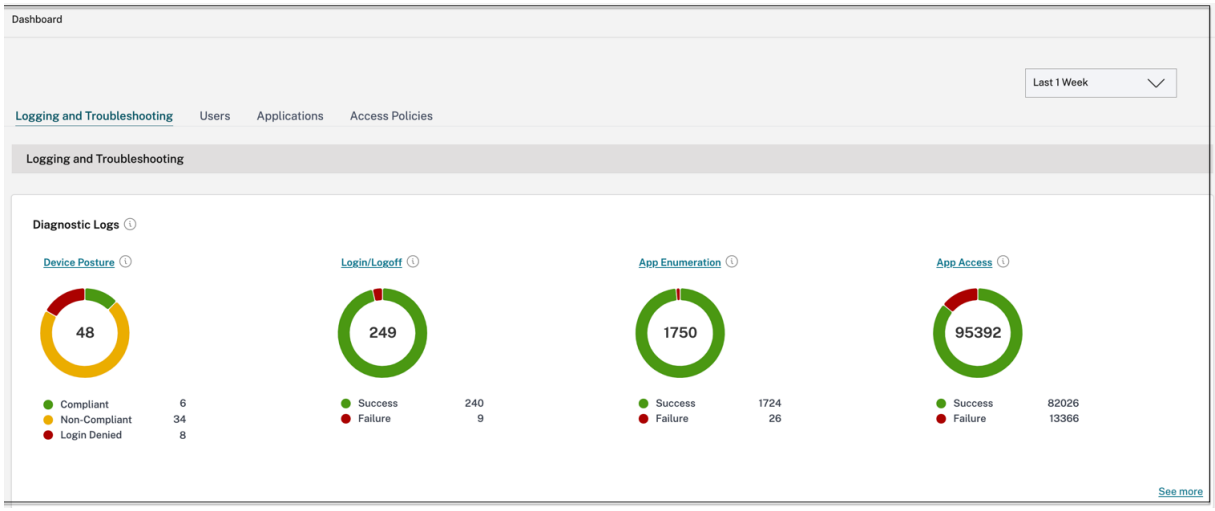
Analytics dashboard

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

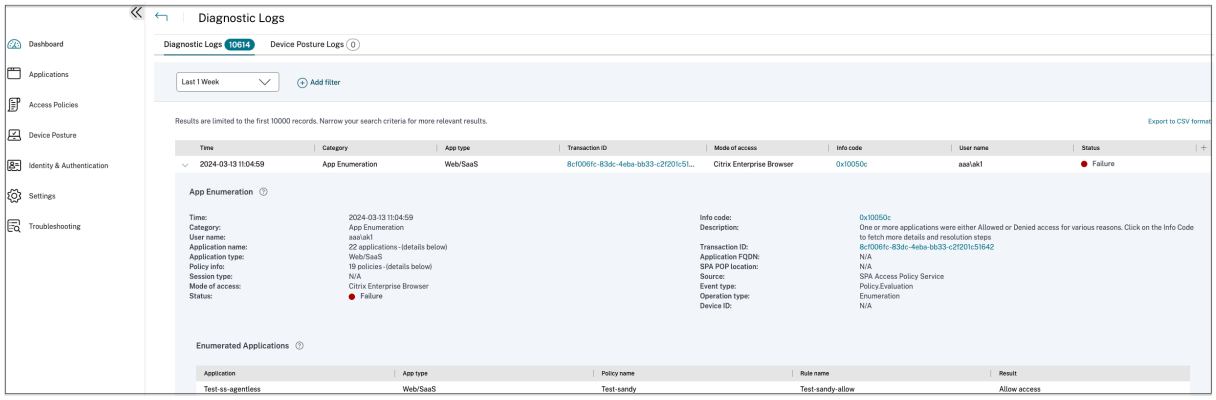
For details, see Dashboard.



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.



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

Admin-guided workflow for easy onboarding and set up

February 9, 2024

A new streamlined admin experience with step-by-step process to configure Zero Trust Network Access to SaaS apps, internal web apps, and TCP apps is available in the Secure Private Access service. It includes configuration of Adaptive Authentication, applications including user subscription, adaptive access policies, and others within a single admin console.

This wizard helps admins in achieving an error-free configuration either during onboarding or recurrent use. Also, a new dashboard is available with full visibility into the overall usage metrics and other key information.

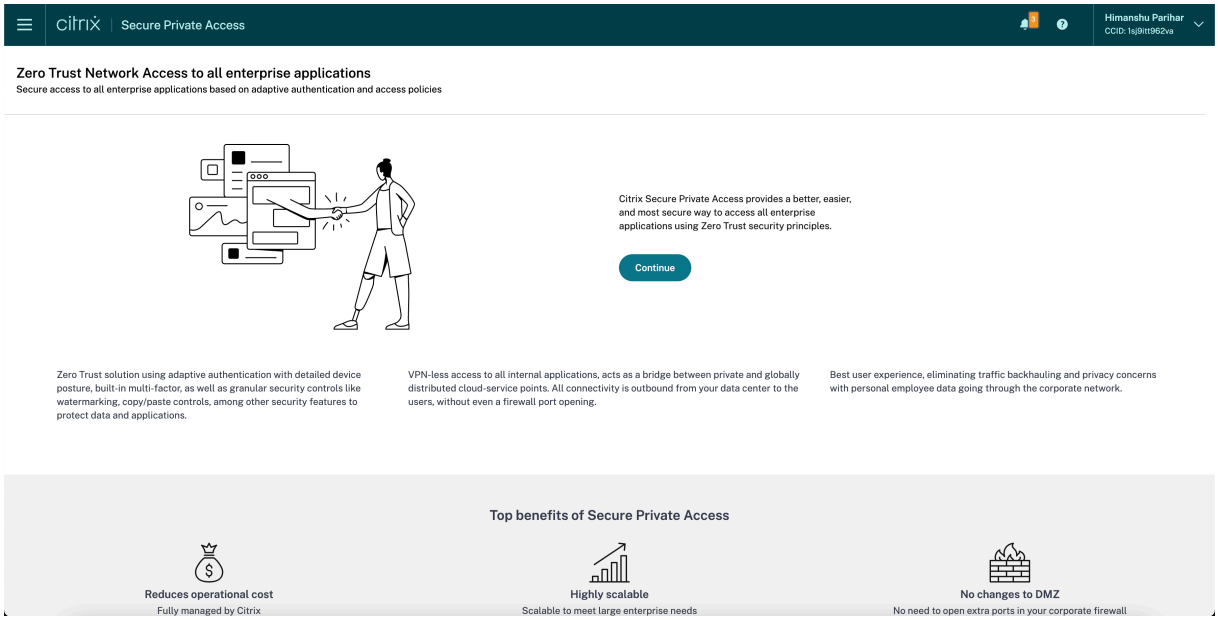
The high-level steps include the following:

1. Choose the authentication method for the subscribers to log in to Citrix Workspace.
2. Add applications 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.

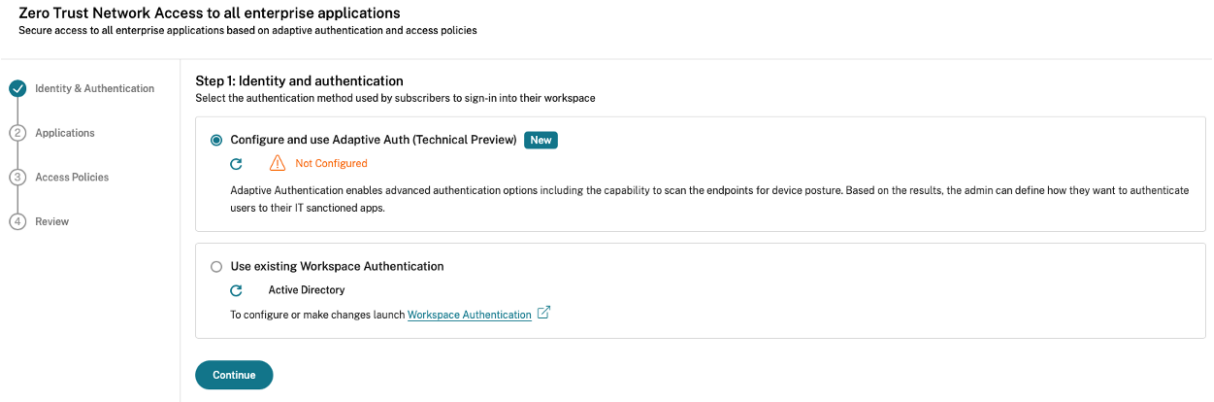
1. On the **Secure Private Access** service tile, click **Manage**.
2. In the Overview page, click **Continue**.



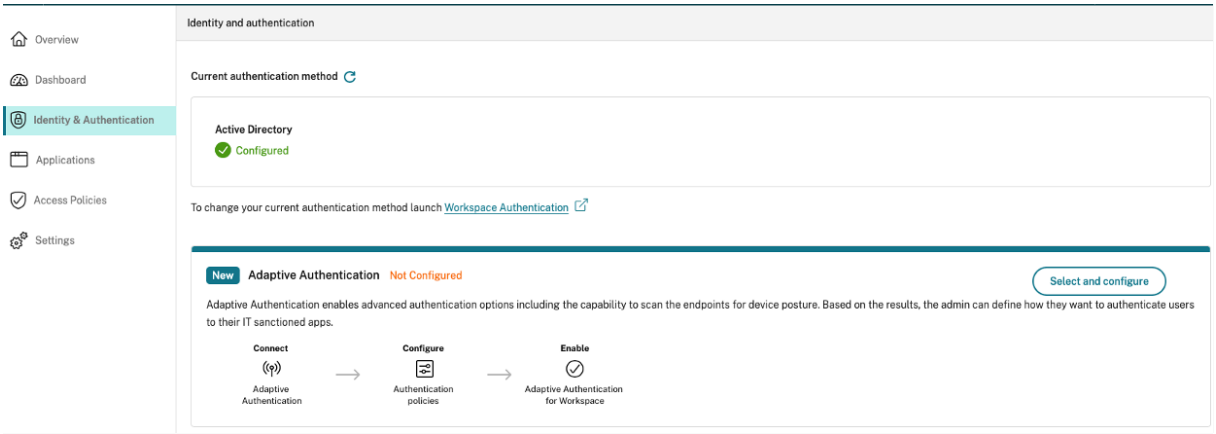
Step 1: Set up identity and authentication

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. Adaptive Authentication service is a Citrix hosted, Citrix managed, Cloud hosted Citrix ADC that provides all the advanced authentication capabilities such as the following.

- Multifactor authentication
- Device posture scans
- Conditional authentication
- Adaptive access to Citrix Virtual Apps and Desktops
- To configure Adaptive Authentication, select **Configure and use Adaptive Auth (Technical Preview)** and then complete the configuration. For more details on Adaptive Authentication, see Adaptive Authentication service. After you configure Adaptive Authentication, you can click **Manage** to modify the configuration, if necessary.



- If you have initially selected a different authentication method and to switch to Adaptive Authentication, click **Select and configure** and then complete the configuration.

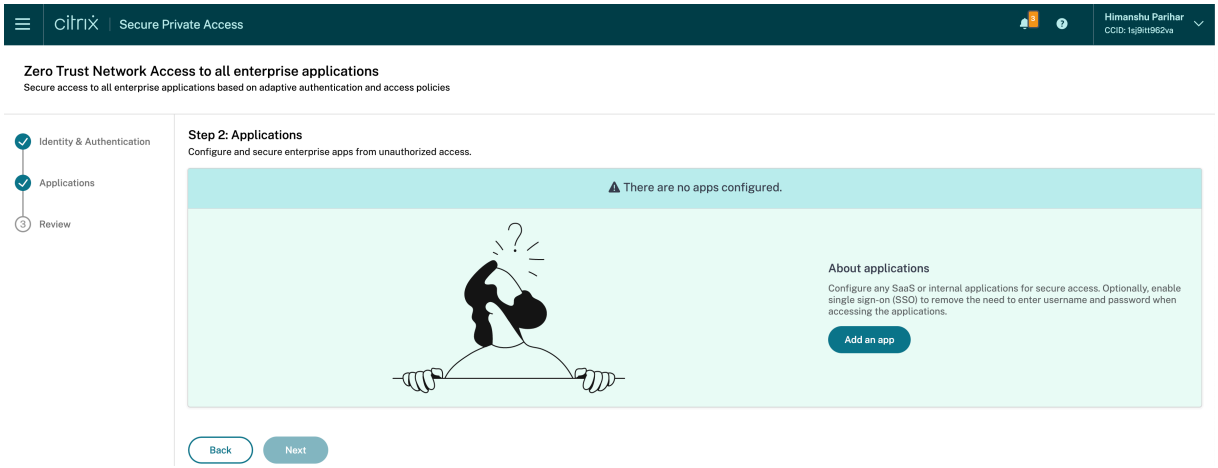


To change the existing authentication method or change the existing authentication method, click **Workspace Authentication**.

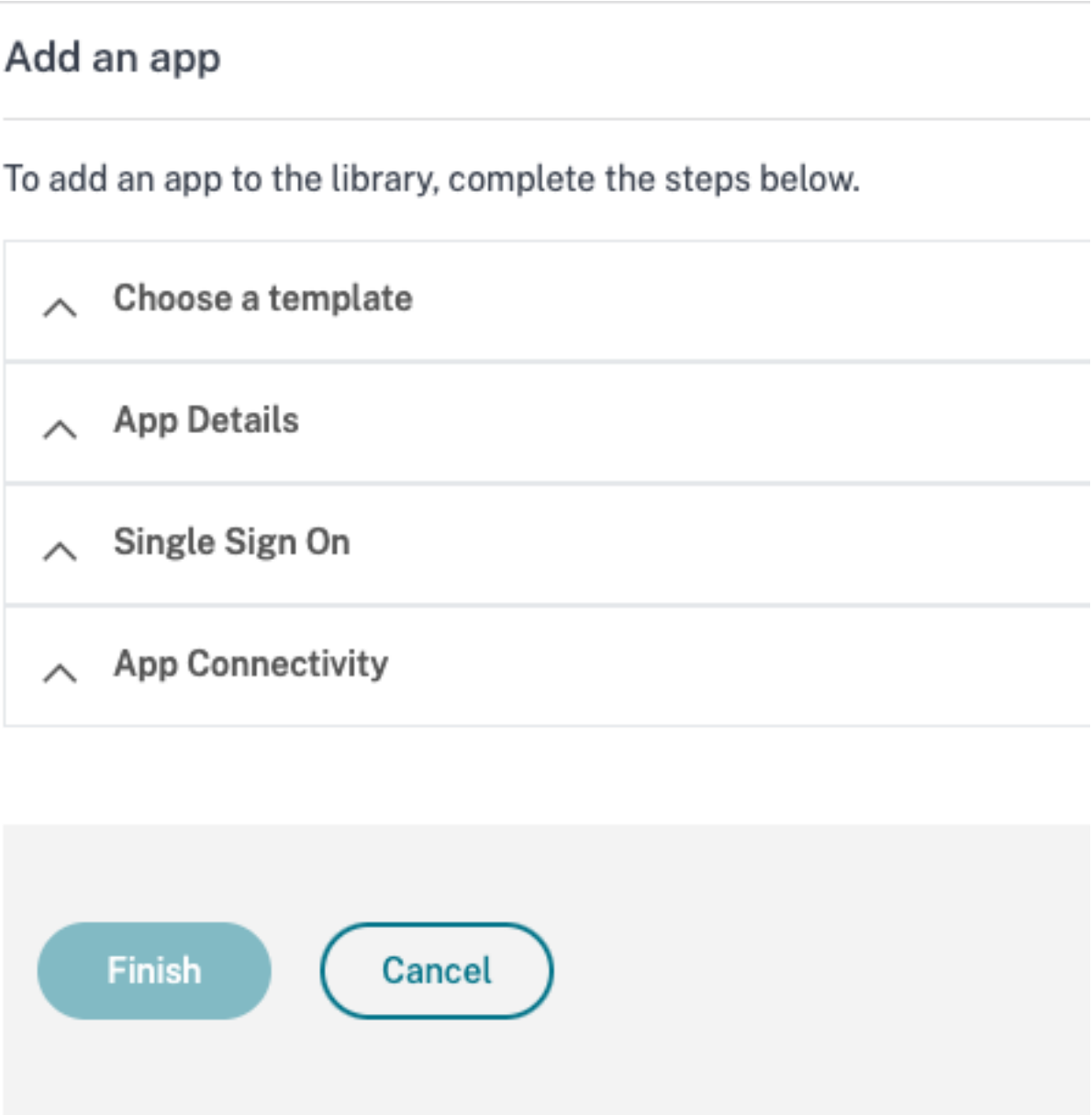
Step 2: Add and manage applications

After you have selected the authentication method, configure the applications. For the first-time users, the **Applications** landing page does not display any applications. 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**.

Once you add an app, you can see it listed here.



Complete the steps displayed in the following figure to add an app.



- **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
- **Enable read-only access to admins**
  - Read-only access for admins to SaaS and Web apps

Step 3: Configure an access policy with multiple rules

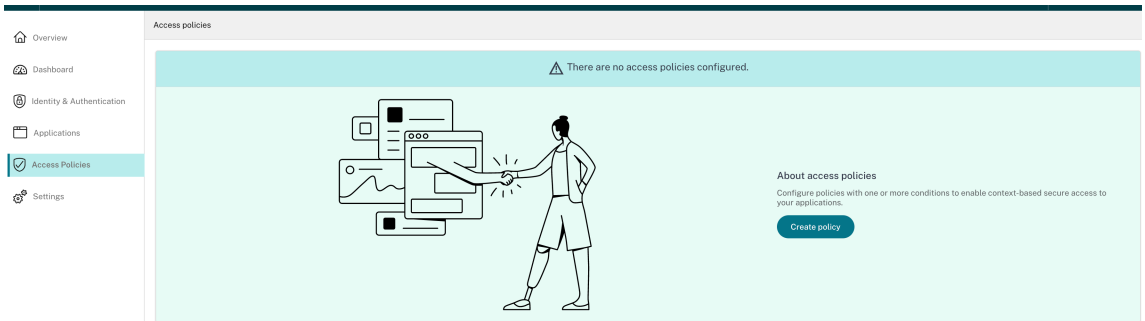
You can create multiple access rules and configure different access conditions for different users or user groups within a single policy. These rules can be applied separately for both HTTP/HTTPS and TCP/UDP applications, all within a single policy.

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 the following security restrictions:

- Restrict clipboard access
- Restrict printing
- Restrict downloads
- Restrict uploads
- Display watermark
- Restrict key logging
- Restrict screen capture

For more information on these restrictions, see Available access restrictions options.

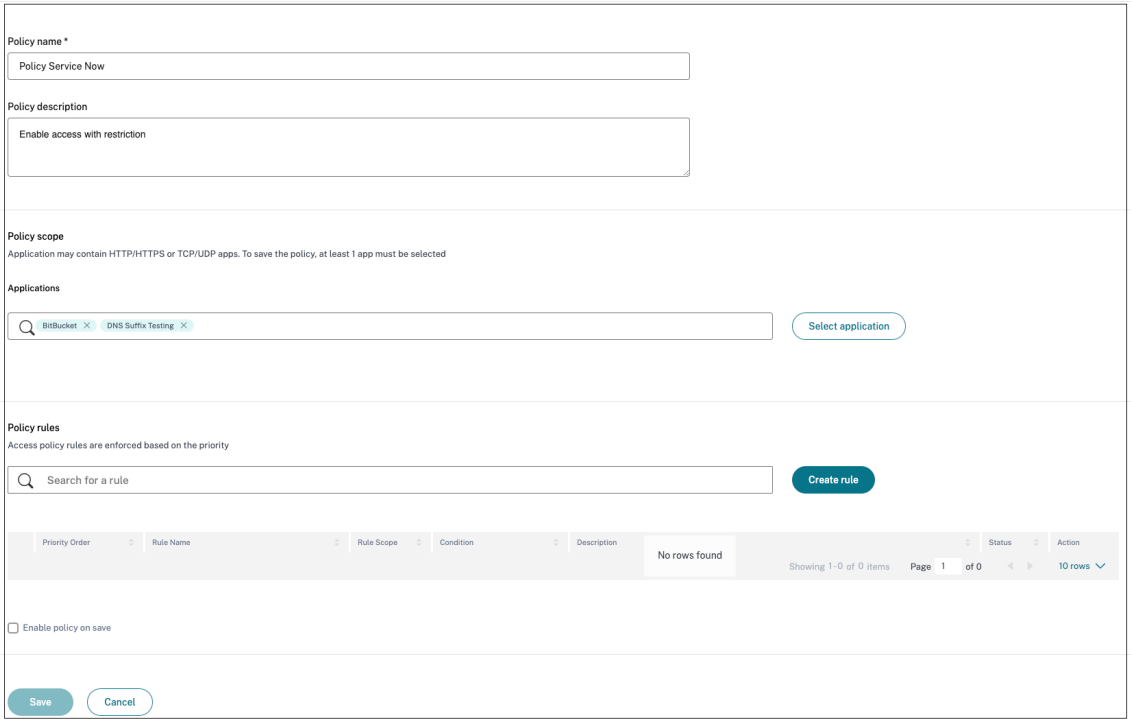
1. On the navigation pane, click **Access Policies** and then click **Create policy**.



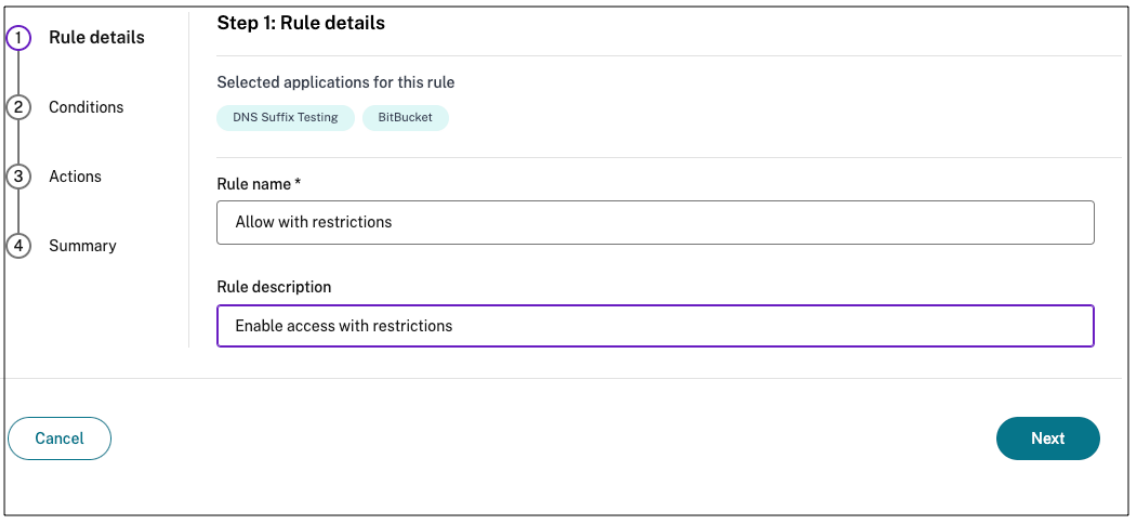
   For the first-time users, the **Access Policies** landing page does not display any policies. Once you create a policy, you can see it listed here.

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.

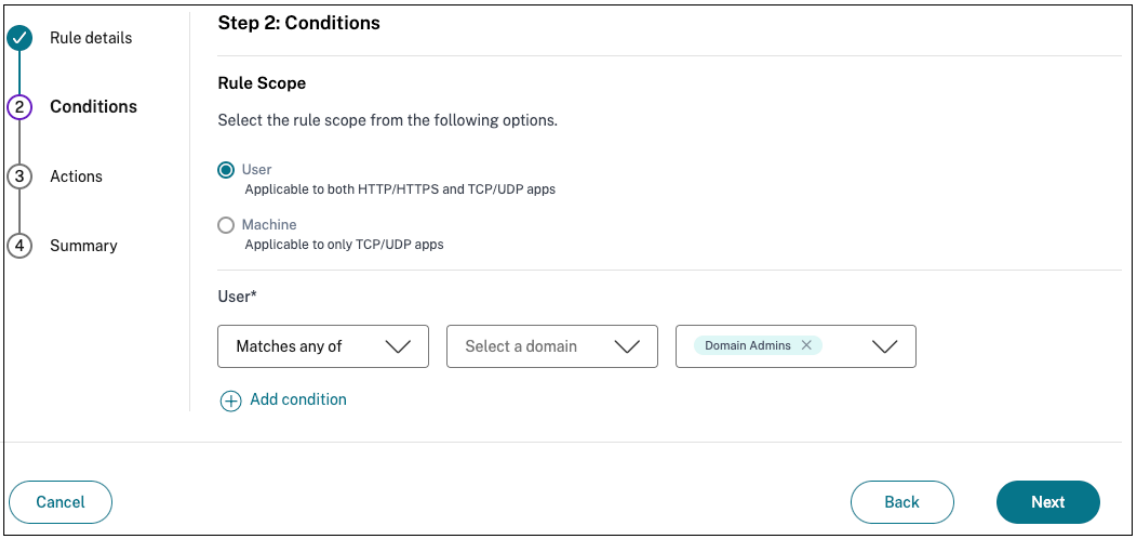


5. Enter the rule name and a brief description of the rule, and then click **Next**.



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



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.

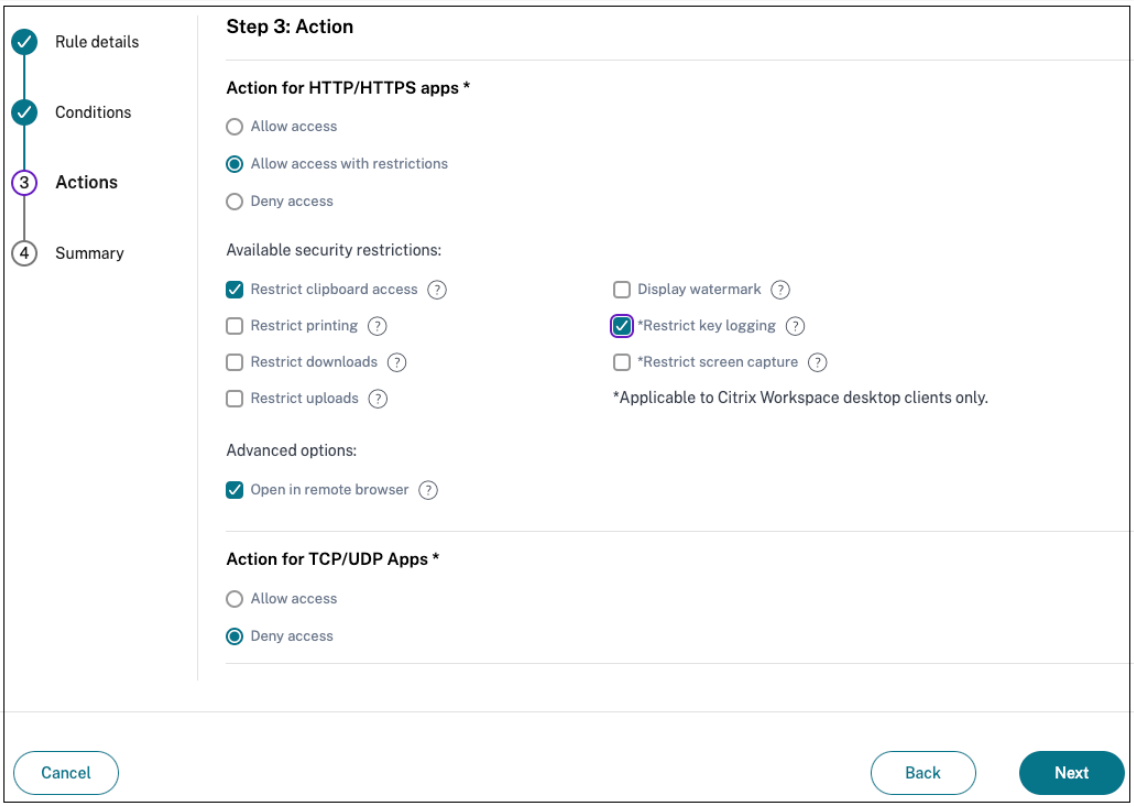
   - **Desktop** or **Mobile device** –Select the device for which you want to enable access to the apps.
   - **Geo location** –Select the condition and the geographic location from where the users are accessing the apps.
     - **Matches any of:** Only users or user groups accessing the apps from any of the geographic locations listed are enabled access to the apps.
     - **Does not match any:** All users or user groups other than those from the listed geographic locations are enabled access.
   - **Network location** –Select the condition and the network using which the users are accessing the apps.
     - **Matches any of:** Only users or user groups accessing the apps from any of the network locations listed are enabled access to the apps.
     - **Does not match any:** All users or user groups other than those from the listed network locations are enabled access.
   - **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.
   - **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.

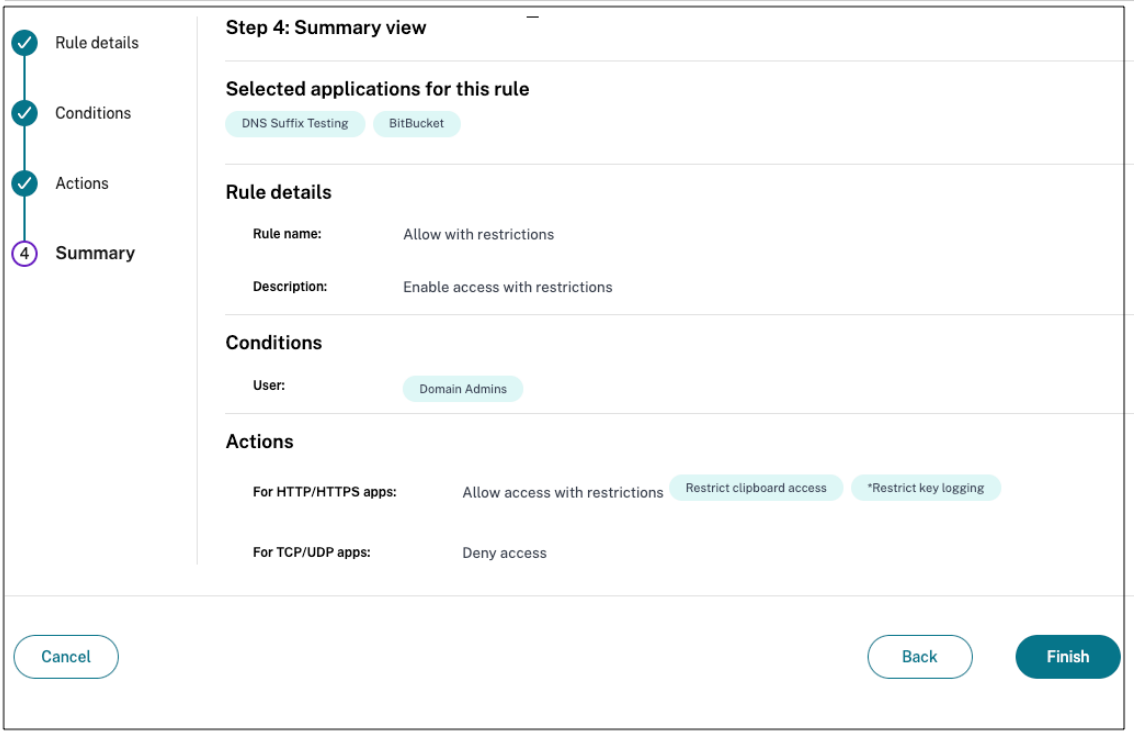
8. Click **Next**.
9. Select the actions that must be applied based on the condition evaluation.
   - For HTTP/HTTPS apps, you can select the following:
     - **Allow access**
     - **Allow access with restrictions**
     - **Deny access**

     > **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**

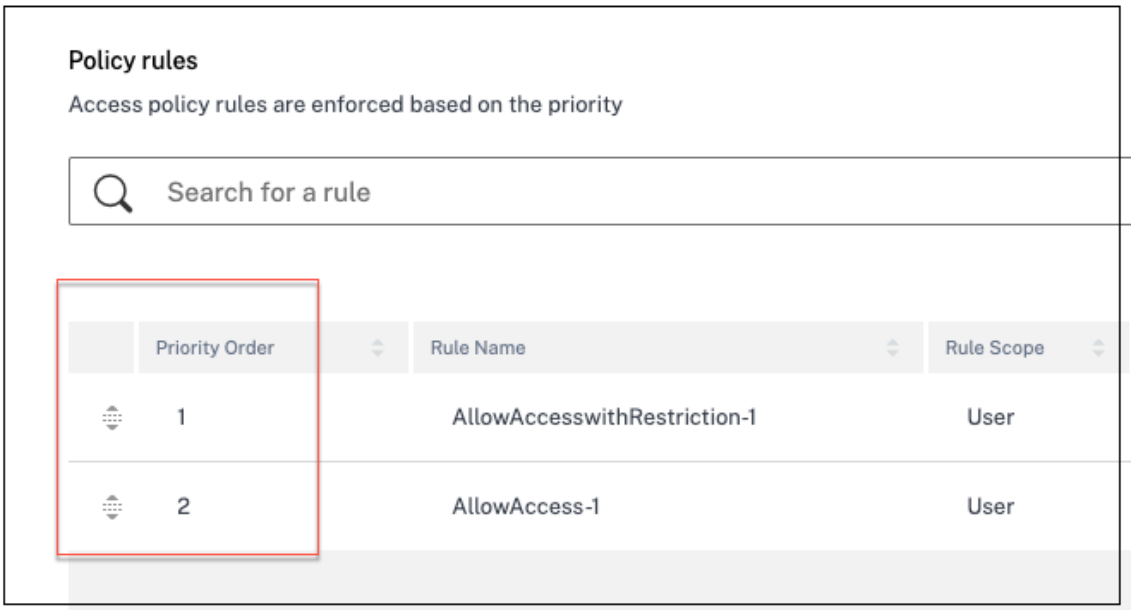


10. Click **Next**. The Summary page displays the policy details.
11. You can verify the details and click **Finish**.



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.



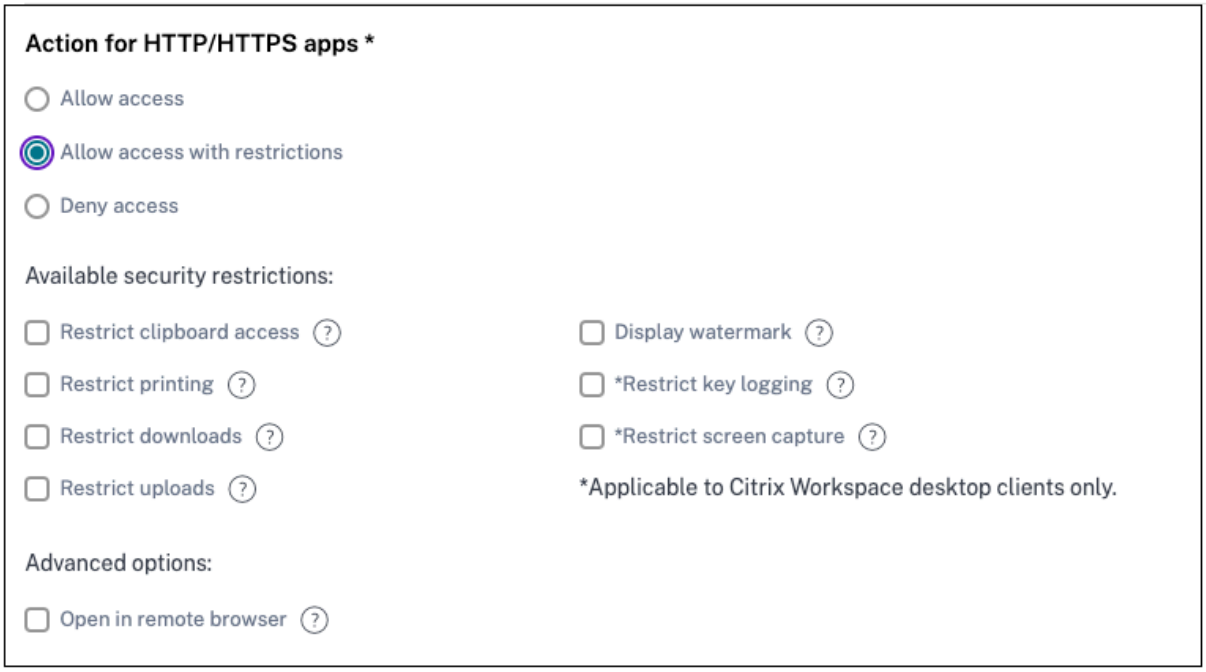
Evaluation of rules with priority order example:

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 application.



- **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.
- **Open in remote browser:** Opens the app in the Citrix Remote Browser.
  - If you select **Open in remote browser** and if the remote browser catalogs are missing for Secure Private Access, the following message appears:

    There is no Published Remote Isolation catalog available to host this application. Go to the Remote Browser Isolation console to publish the catalog.

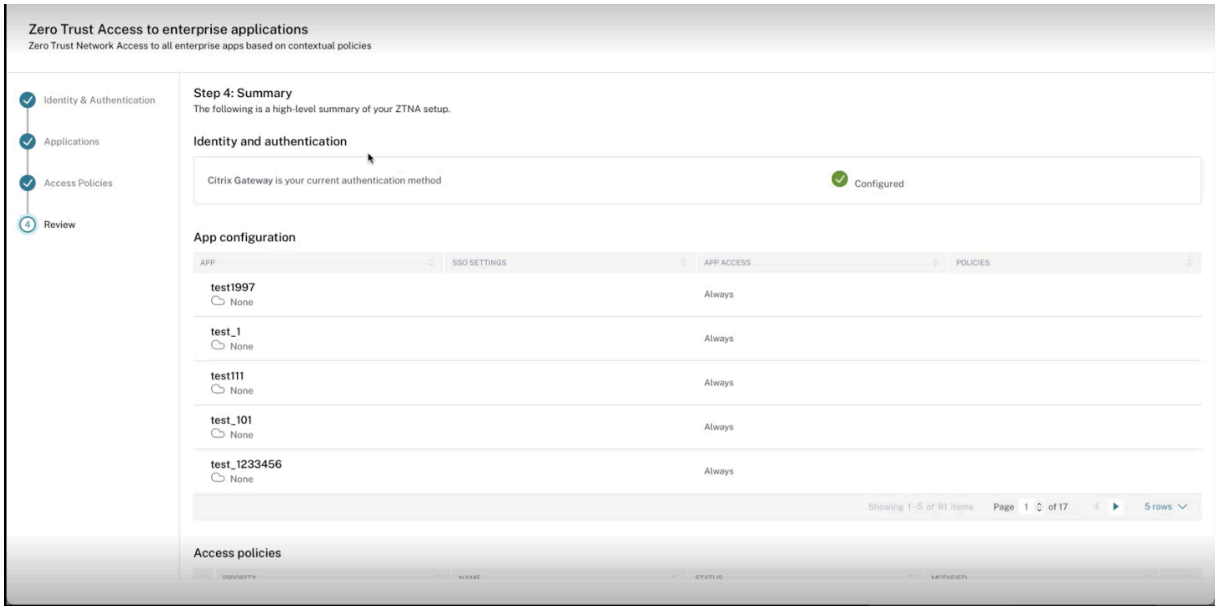
- Also, whey you try to launch a Web or SaaS app, the app launch fails if the RBI catalogs are missing and the following message appears:

  No catalogs have been created to handle this request. Please contact your administrator.

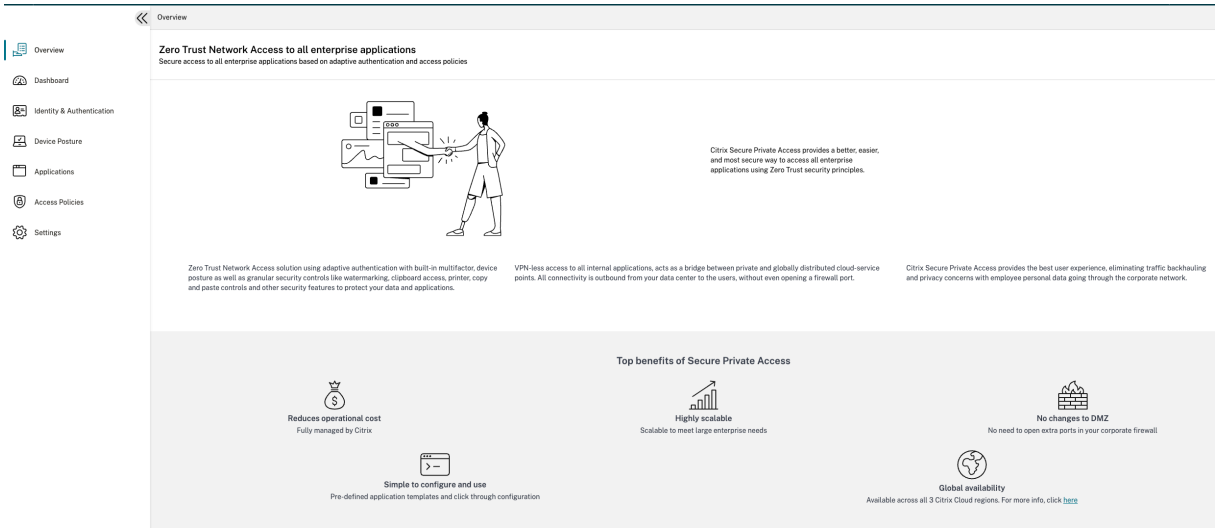
For more information on Citrix Remote Browser Isolation, see Remote Browser Isolation.

Step 4: Review summary of each configuration

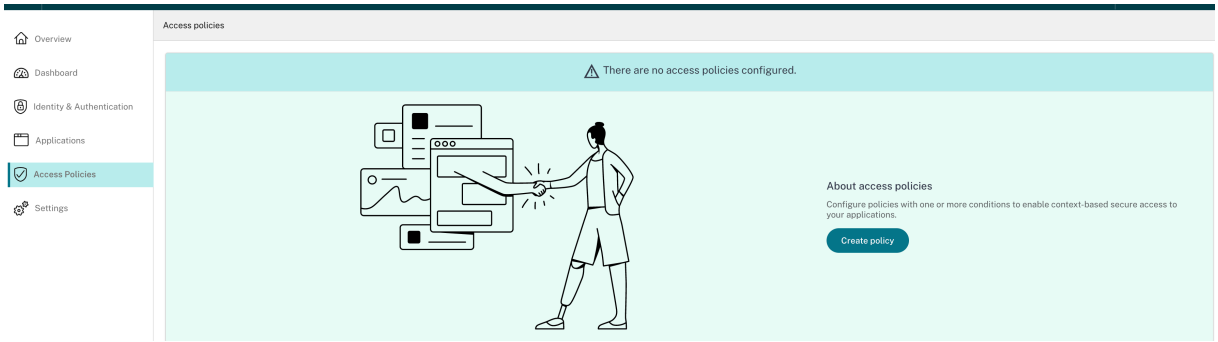
From the Review page, you can view the complete app configuration and then click **Close**.



The following figure displays the page after you have completed the 4-step configuration.



> **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. In this case, the following screen appears if you have deleted all the policies.



Policy modeling tool

June 10, 2024

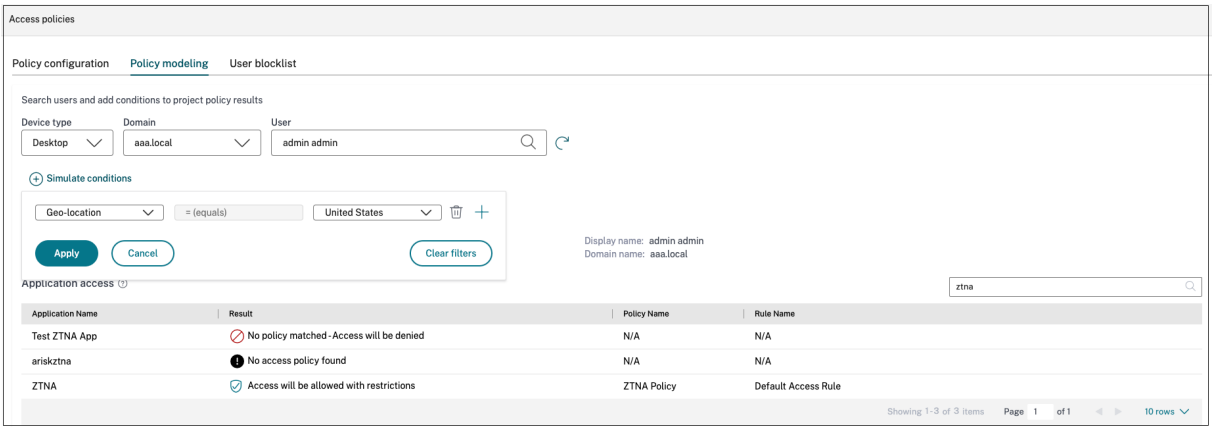
Admins can create multiple policies and assign these policies to multiple applications. As a result, it might become difficult for admins to understand the application access results for their end-users; that is if the end-user is allowed or denied access based on the application and access policy configurations. The policy modeling tool (**Access policies > Policy modeling**) helps resolve these issues by giving the administrators full visibility into the expected application access result (allowed/allowed with restriction/denied). Admins can check the access results for specific users and add user conditions such as device type, device posture, geo-location, network location, user risk score and workspace URL. The tool also displays the list of policies and rulenames associated with the applications.

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

1. In the Secure Private Access console, click **Access Policies** and then click the **Policy modeling** tab.
2. Add the following details:
   - **Device type**: Select the device type of the end user. (Desktop is selected, by default.)
   - **Domain**: Select the domain associated with the user.
   - **User**: Select the user name for which you want to analyze the applications and associated policies.
3. You can also simulate a set of conditions/constraints on the end user and their devices.

4. Click **Simulate conditions**.
5. Select the condition (Device posture, Geo-location, Network location, User risk score and Workspace URL) and then select the associated value.
6. Click the **+** sign to add additional conditions.
7. Click **Apply**.

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



Dashboard overview

June 10, 2024

The Secure Private Access service dashboard displays the diagnostics and usage data of the SaaS, Web, TCP, and UDP apps. The dashboard provides admins full visibility into their apps, users, connectors health status, and bandwidth usage in a single place for consumption. This data is fetched from Citrix Analytics. The data for the various entities can be viewed for the preset time or for a custom timeline. For some of the entities, you can drilldown to view further details.

The metrics are broadly classified into the following categories.

- **Logging and Troubleshooting**
  - Diagnostic logs: Logs related to authentication, application launch, app enumeration, and device posture checks.
- **Users**
  - Active users: Total number of unique users accessing the applications (SaaS, Web, and TCP) for the selected time interval.

  - Uploads: Total volume data uploaded through the Secure Private Access service for the selected time interval.
  - Downloads: Total volume of data downloaded through the Secure Private Access service for the selected time interval.

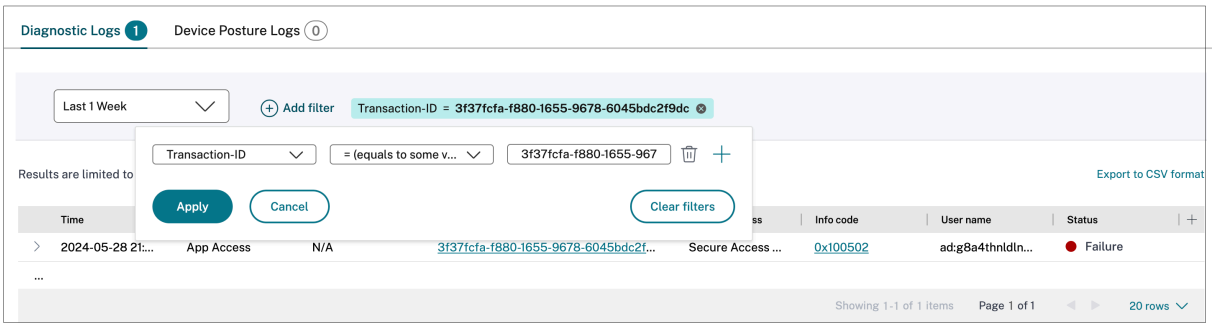
- **Applications:**
  - Applications: Total number of applications (independent of the time interval) configured currently.
  - Application launch count: Total number of applications (app sessions) launched by each user for the selected time interval.
  - Domains configured: Total number of domains configured for the selected time interval.
  - Applications discovered: Total number of unique, individual domains that have been accessed but are not associated with any apps

- **Access policies**
  - Access policies: Total number of access policies (independent of the time interval) configured currently.

Diagnostic logs

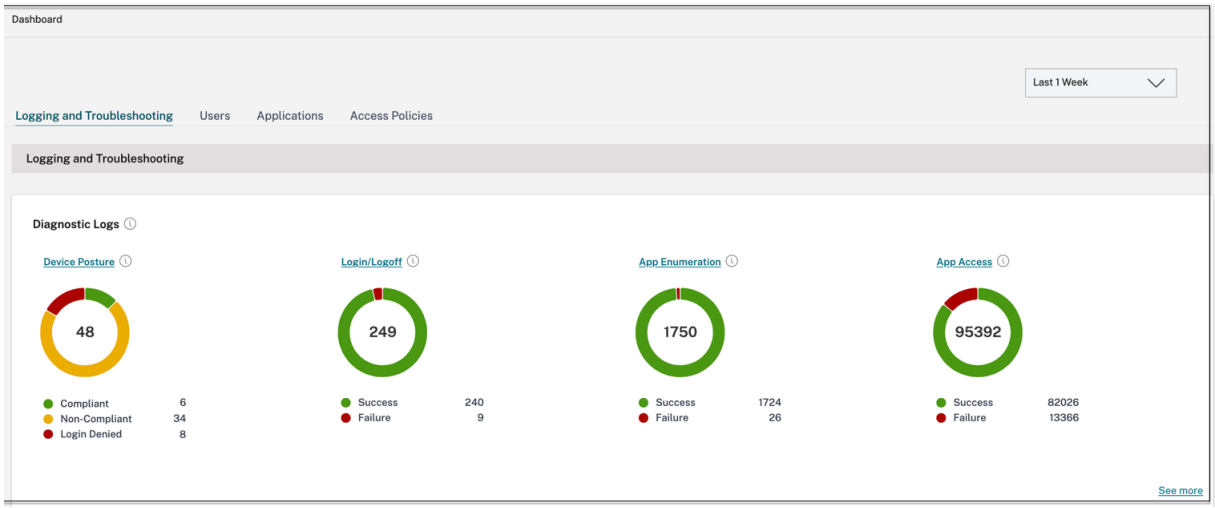
Use the **Diagnostics Logs** chart to view the logs related to authentication, application launch, app enumeration, and also logs related to device posture. You can click the **See more** link to view the details of the logs. The details are presented in a tabular format. You can view the logs for the pre-set time or for a custom timeline. You can add columns to the chart by clicking the + sign depending on what information you want to see in the dashboard. You can export the user logs into CSV format.

- You can use the **Add Filter** option to refine you search based on the various criteria such as app type, category, description, and so on. For example, in the search fields, you can select `Transaction ID`, `= (equals to some value)`, and enter `7456c0fb-a60d-4bb9-a2a2-edab8340bb15`in this sequence, to search for all logs related to this transaction ID. For details on search operators that can be used with the filter option, see Search operators.

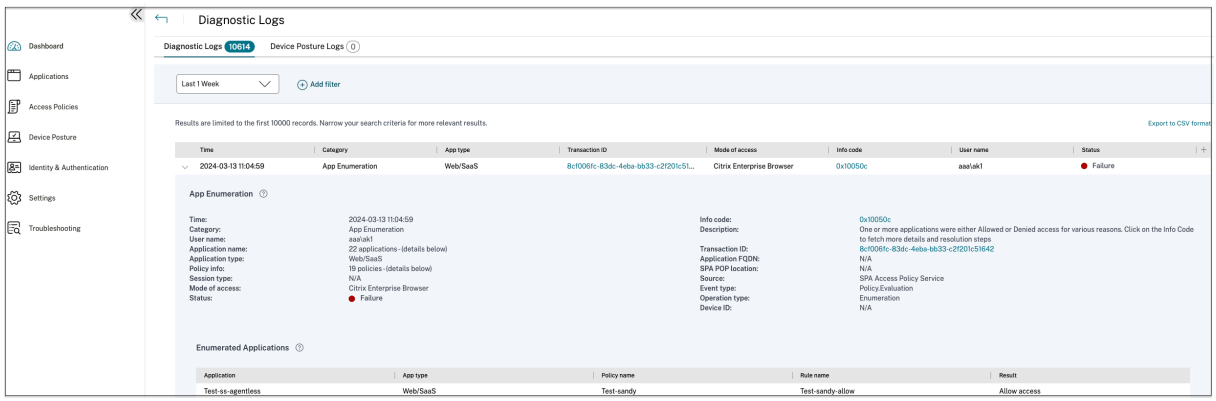


- **Device posture logs:** You can refine your search based on the policy results (**Compliant, Non-compliant, and login Denied**). For details on device posture, see Device Posture.

> **Note:**
>
> - Every failure event within the Secure Private Access diagnostic logs dashboard has an associated info code. For details, see Info code.
> - Transaction ID correlates all Secure Private Access logs for an access request. For details, see Transaction ID.



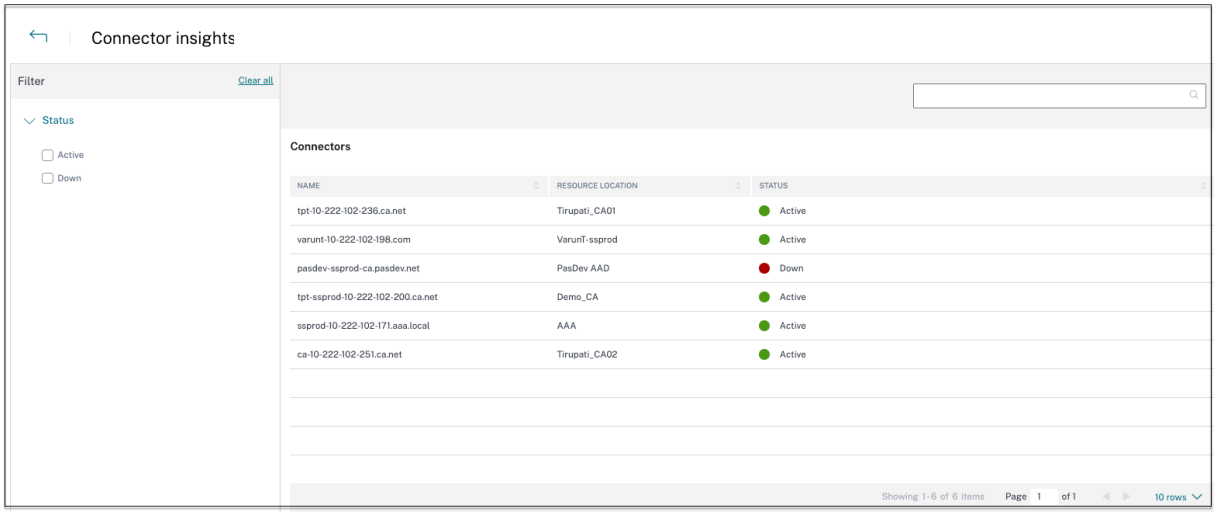
- You can click the expand icon (>) to view the complete details of the logs.
- The **Diagnostic Logs** page displays the embedded domains for each of the main URLs that are accessed. Admins can view the embedded domains by clicking the expand icon (>) from the main URL. Admins can use the embedded domains list to address issues related to app access or app rendering. For example, if a domain was missed in the application configuration, then the specific app cannot be accessed by the end user. In this case, the admin can view the list of embedded domains, identify the missing domain, and then update the app configuration with the missing domain.



> **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.

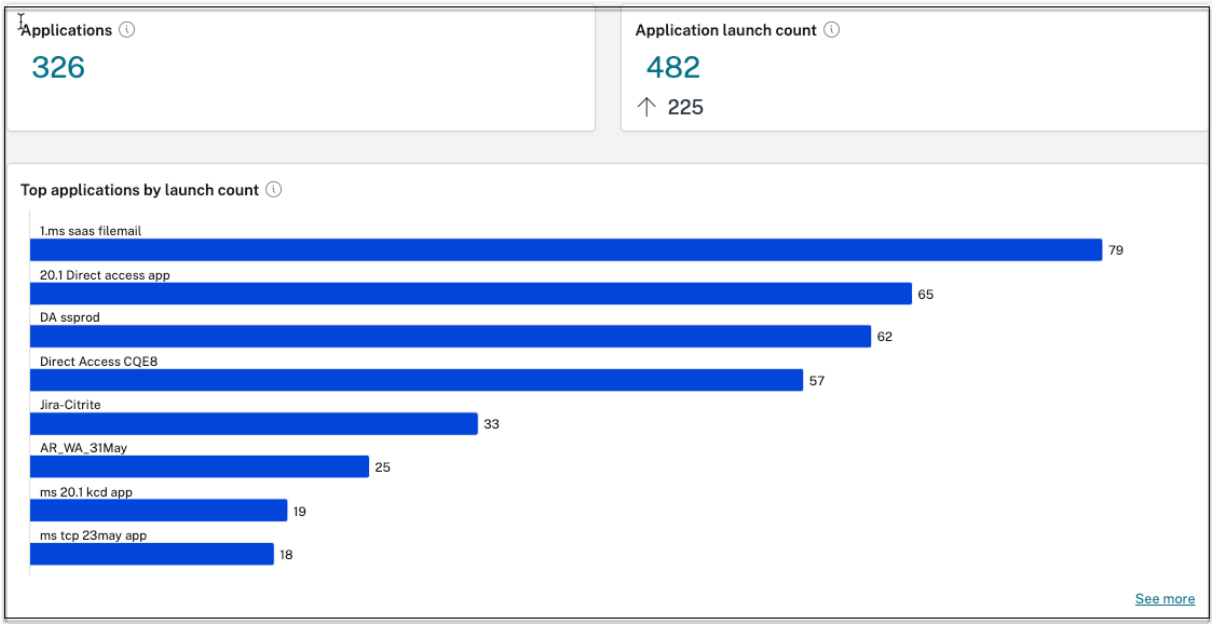
Connector status

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.



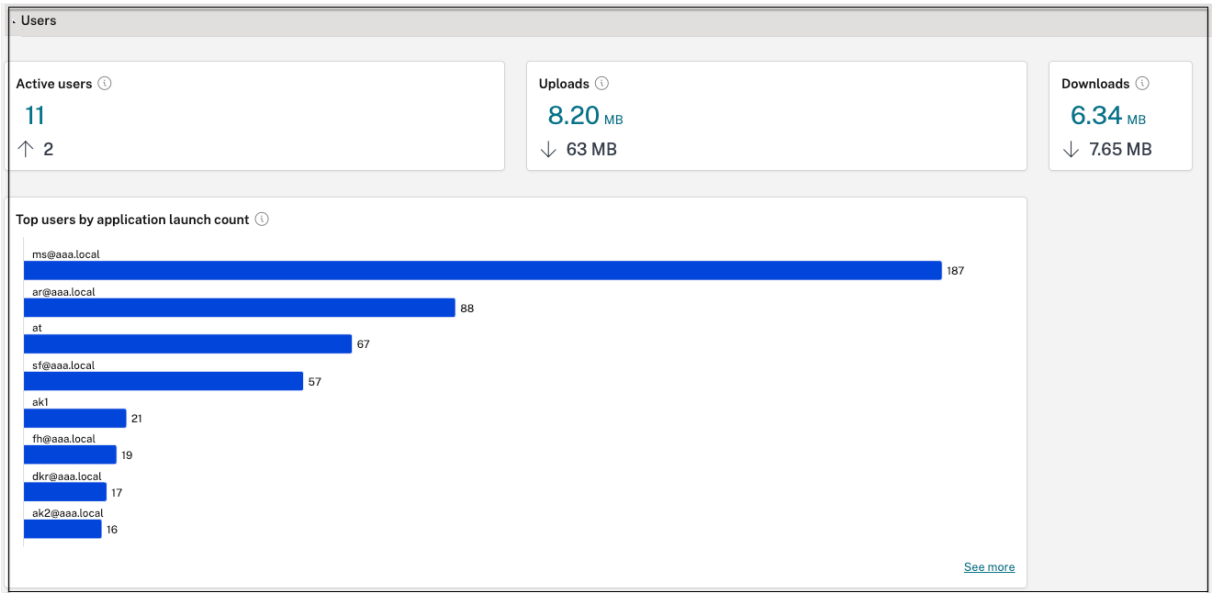
Top applications by launch count

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.

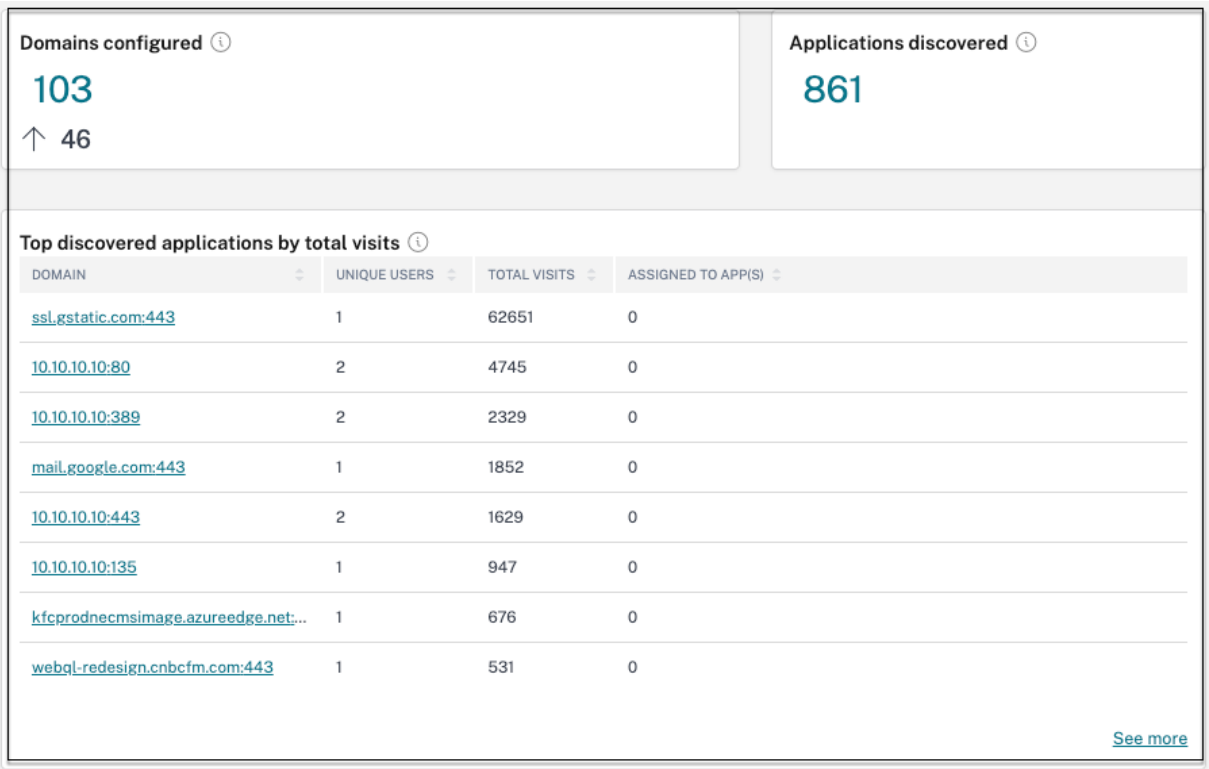


Top access policies by enforcement

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

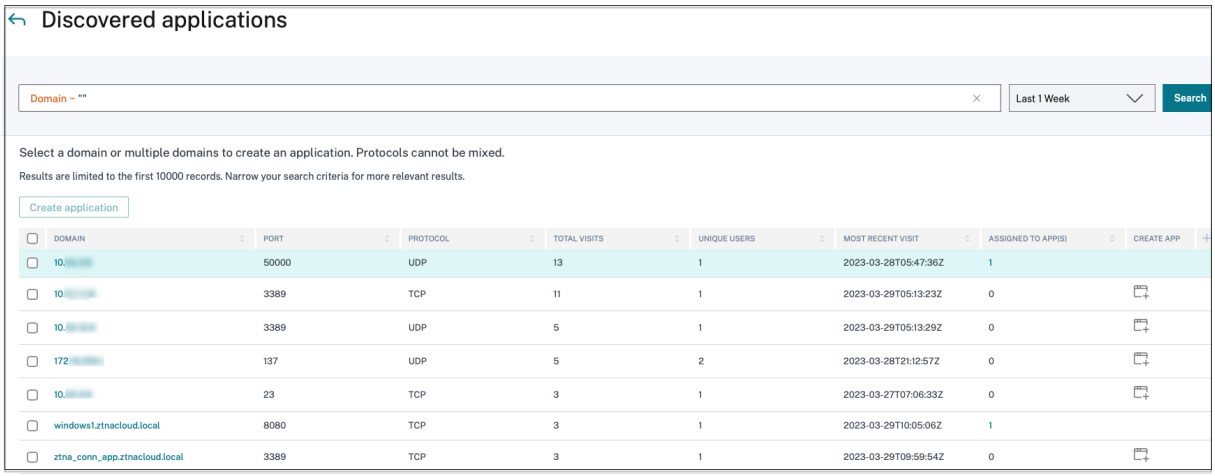
Use the **Top discovered applications by total visits chart** to view the list of unique, individual domains that have been accessed at some point but are not associated with any apps. These domains are listed based on the number of total visits to those domains. Admins can use this chart to see if any domain of particular interest is accessed by many users. In such cases, admins can create an app with that domain for easy accessibility.



DOMAIN	UNIQUE USERS	TOTAL VISITS	ASSIGNED TO APP(S)
ssl.gstatic.com:443	1	62651	0
10.10.10.10:80	2	4745	0
10.10.10.10:389	2	2329	0
mail.google.com:443	1	1852	0
10.10.10.10:443	2	1629	0
10.10.10.10:135	1	947	0
kfcprodnecmsimage.azureedge.net:...	1	676	0
webql-redesign.cnbcfm.com:443	1	531	0

In the chart, the **ASSIGNED TO APPs** column displays the total number of applications that have this domain configured as a part of their related URL or Destination URL values. Clicking the number displays the apps that are assigned to this domain.

You can click the **See more** link to view more details about all the domains.



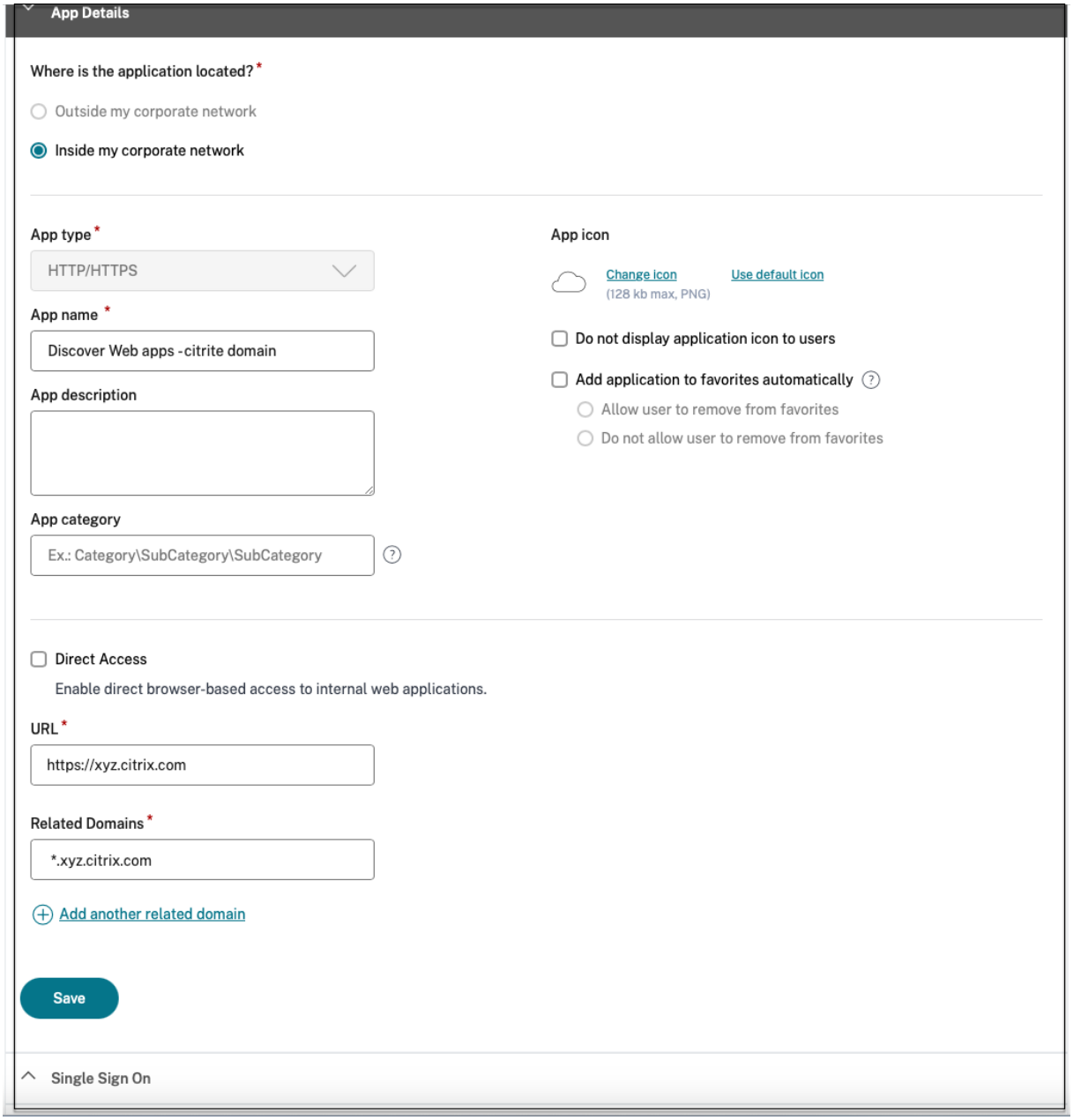
The **Discovered applications** page displays the details of the domains such as domain name, port, protocol, total visits, unique users, and the most recent visit date. All the columns in the chart are sortable. You can use the search bar to search based on domain.

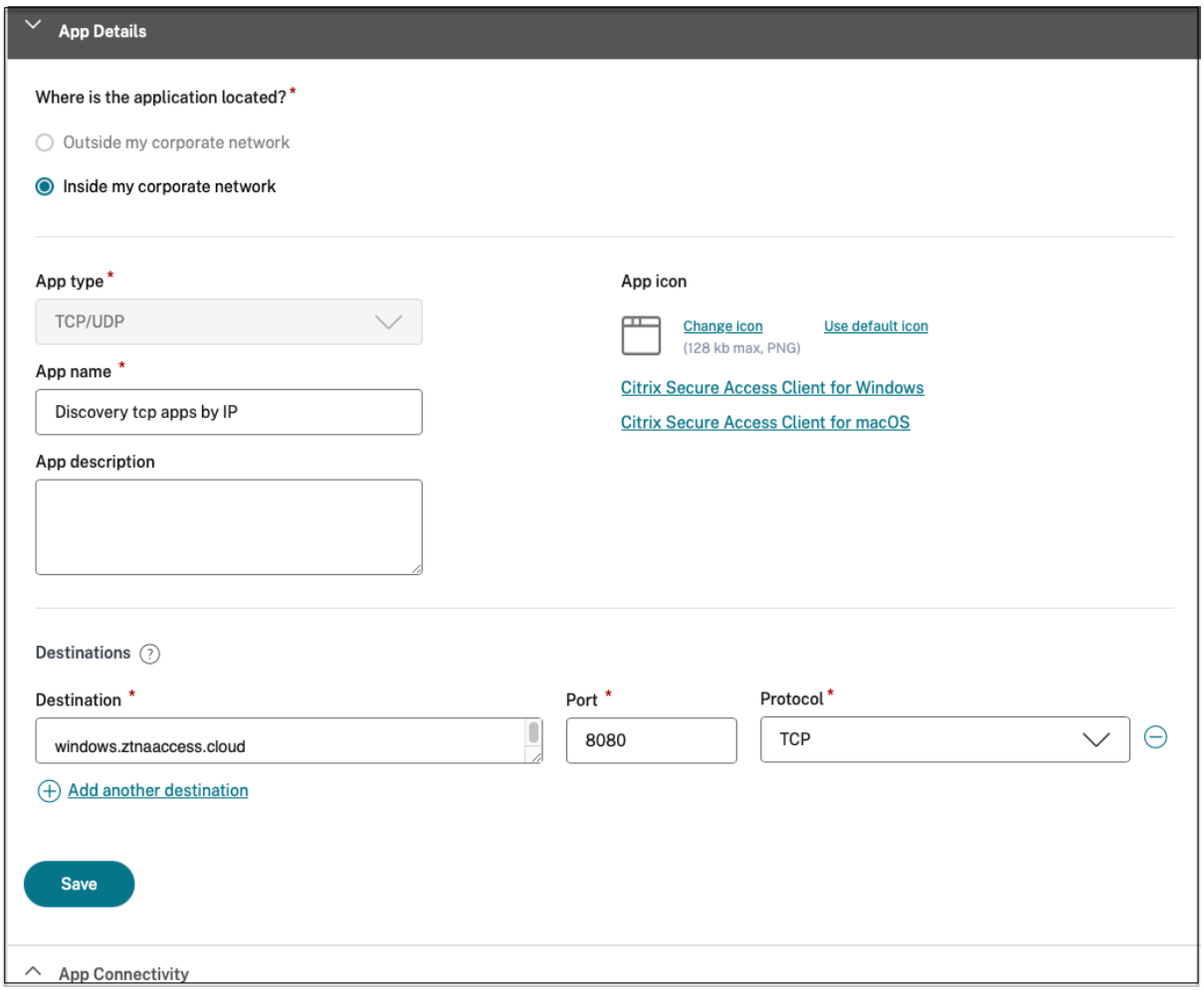
> **Note:**
>
> - The protocols are derived based on the standard ports used by customers.
> - The list of discovered domains is limited to 10000 records.

Creating an app from the chart

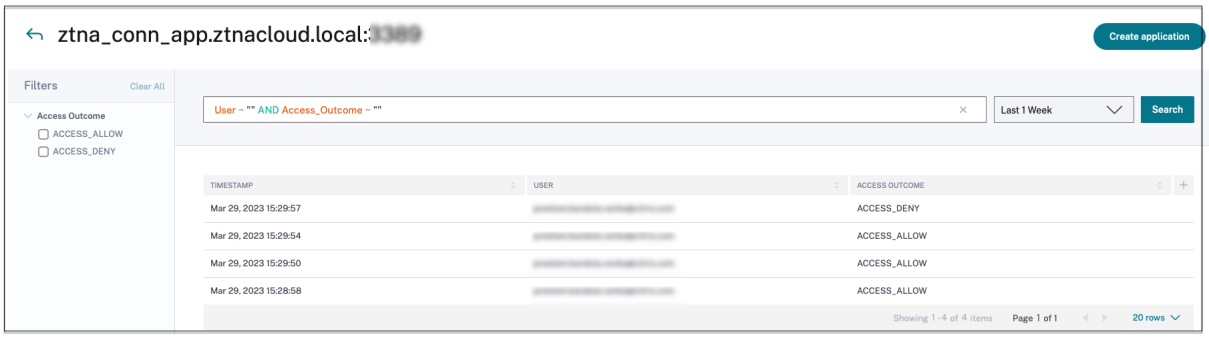
Click the **+** icon in line with the respective domain to create an app. The app configuration wizard pops up. The create app icon does not appear for the rows in which an app is already created with the same domain, port, and protocol combination, and is in complete state.

- The app type is auto populated based on the app's protocol that you have selected. However, you can change the type, if necessary.
- The values in the **URL, Related Domains, Destination, Port, Protocol** fields are all auto-populated. Complete the steps for adding an app. For details, see Admin-guided workflow for easy onboarding and set up.





You can also click the unique domain link to see more details and create an application for that domain. When you click a domain link, the user authentication logs for the domain are displayed. Click the **Create application** button. Complete the steps for adding an app.



Search operators

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

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

Application discovery

November 21, 2023

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. To enable the app discovery feature within the Citrix Secure Private Access service, admins have to configure the subnets or the wildcard domains or both within which applications and user access needs to be discovered and reported. Admins use the Application configuration workflow to define the broad subnets and wildcard domains, and complete the same application access policy workflow that is used for all application definition configurations.

Configure application discovery

Application discovery can be done by one of the following ways:

- Configure the system to monitor and report the exact IP address destinations and ports that are TCP/UDP based.

  Specify the subnet along with the TCP/UDP protocol and range of ports (enter * to include entire range). This enables discovering all TCP and UDP apps from the secure access agent.

  Example: 10.0.0.0/8: TCP : Port (*)

- Configure the system to monitor and report the host names or fully qualified domains (FQDNs) or both for the apps accessed using the TCP or UDP protocol.

Specify the wildcard domain belonging to the web apps that must be monitored and reported.

Example: `*.citrix.com : TCP : Port (*)`

- Configure the system to monitor and report the fully qualified domains (FQDNs) that might be accessed from the Citrix Enterprise Browser.

  Specify at least one FQDN for a web app that belongs within the domain or subdomain within which you want to discover internal web apps. Configure the related domain to include the wildcard domain within which that app belongs.

  Example:

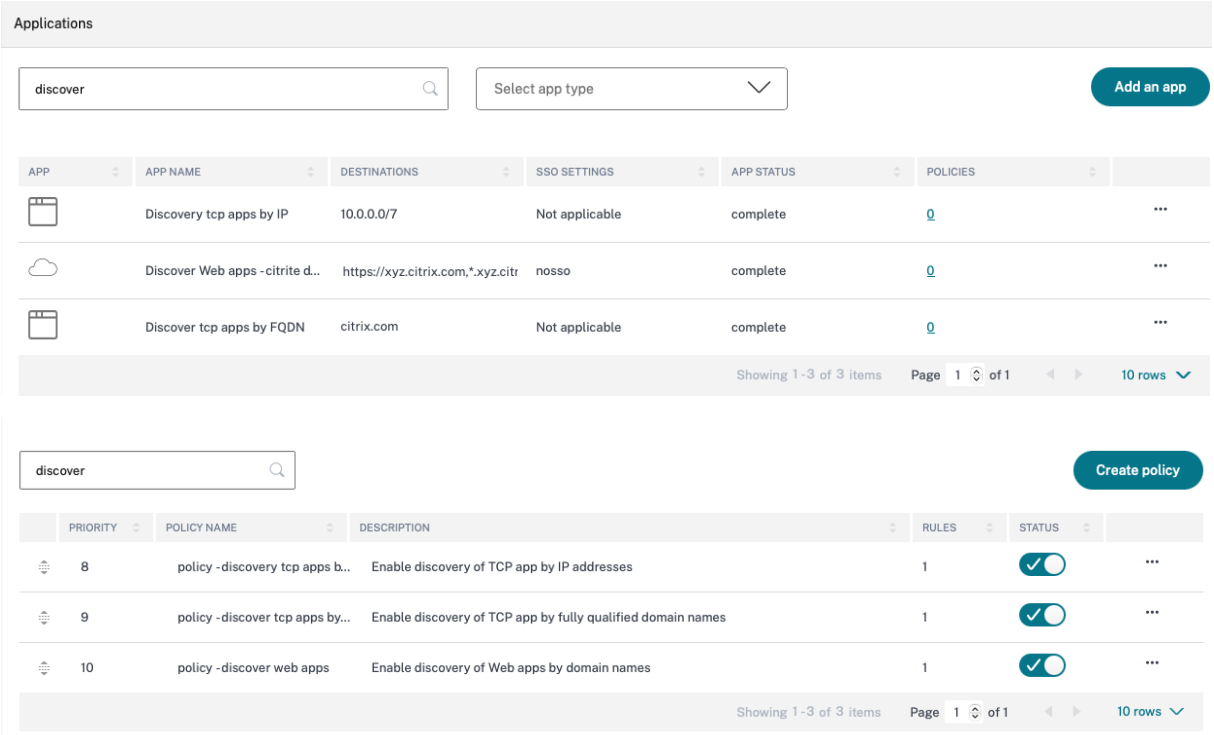
  Web app URL: `https://test.citrix.com/`

  Related domain: *.citrix.com

Important:

- In addition to creating the apps, you must also define users that are allowed access to apps with the configured domains and IP subnets. This is to prevent unauthorized or inadvertent access from other user groups that are outside the allowed user groups.

> - 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.



After creating the applications and corresponding access policies, users can continue to access applications from the Citrix Workspace app and access different domains. For accessing TCP/UDP apps, users need to 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 dashboards.

Apps configuration and management

November 21, 2023

Apps delivery using the Citrix Secure Private Access service provides you an easy, secure, robust, and scalable solution to manage the apps. 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 SaaS apps –Template based configuration of popular apps. These templates pre-fill much of the information required for configuring applications. Only the information specific to the customer must be still provided.

Support for Enterprise web apps

May 30, 2024

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.

SSO and remote access to web apps are available as part of the following service packages:

- Secure Private Access Standard
- Secure Private Access Advanced

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 Secure Workspace Access with Connector Appliance.

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 details
2. Set the preferred sign-on method
3. Define application routing

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 that you use the wizard. In the subsequent usages, you can directly navigate to the **Applications** page and then click **Add an app.**

3. Select the app that you want to add and 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.**
   - **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 that you enter here's 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 **Direct 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.

- Click **Add application to favorites automatically** 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.

6. Click **Next.**

> **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 configuration, see Best practices for Web and SaaS application configurations.

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.

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

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

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

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

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

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

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

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 **Next.**

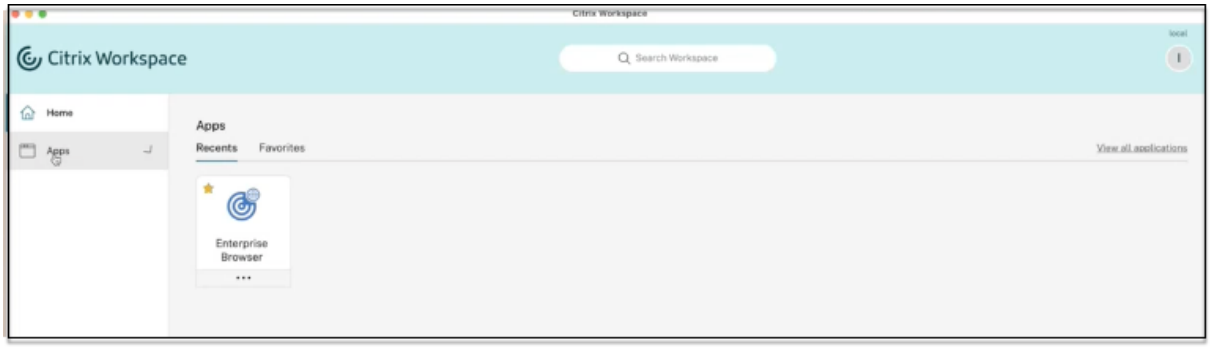
Define application routing

1. 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. For details, see Route tables to resolve conflicts if the related domains in both SaaS and web apps are the same.
2. 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.

Connector Appliance for Secure Private Access

April 27, 2024

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.

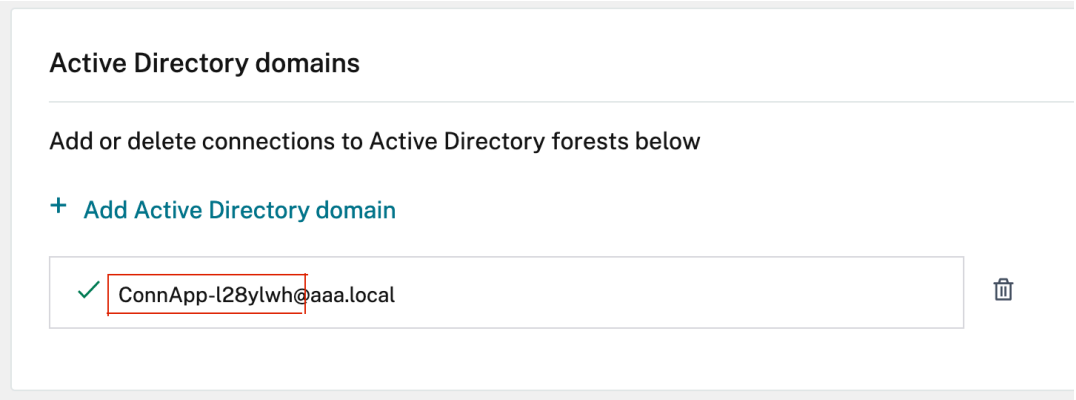
      Joining an Active Directory forest enables you to use Kerberos Constrained Delegation (KCD) when configuring Secure Private Access, but it does not enable identity requests or authentication to use the Connector Appliance.

      - 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.

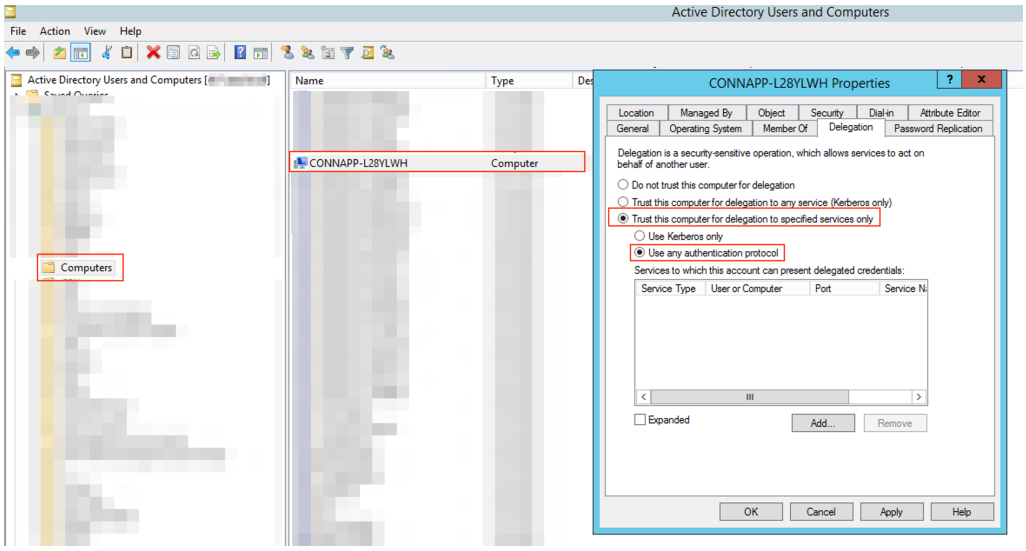
        If you don't have an **Active Directory domains** section in your administration page, contact Citrix to request enrollment in the preview.
      - Enter the domain name in the **Domain Name** field. Click **Add**.
      - The Connector Appliance checks the domain. If the check is successful, the **Join 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**.

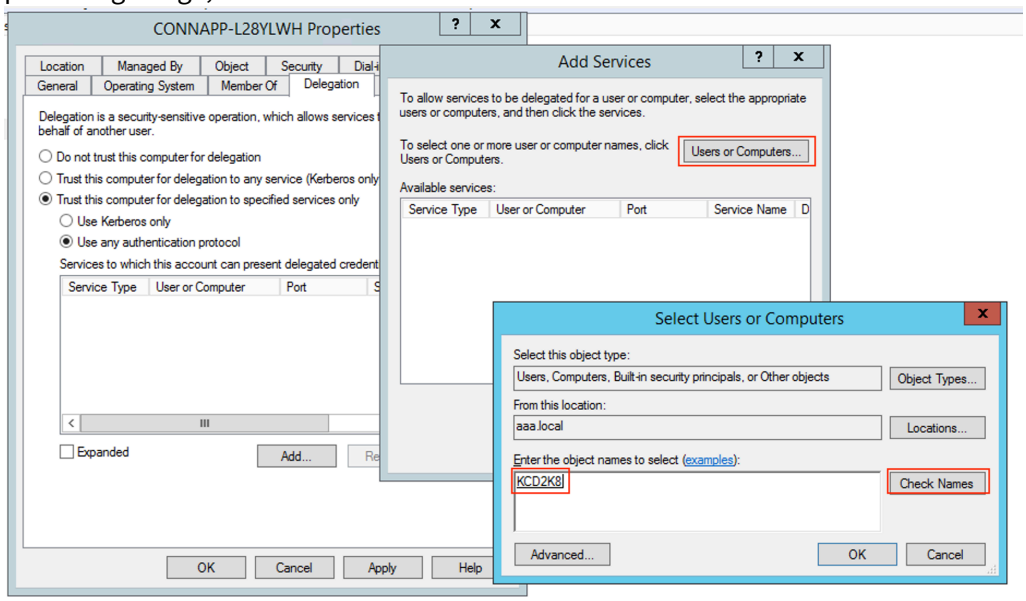
   b) Configure Kerberos Constraint Delegation for web server without a load balancer.



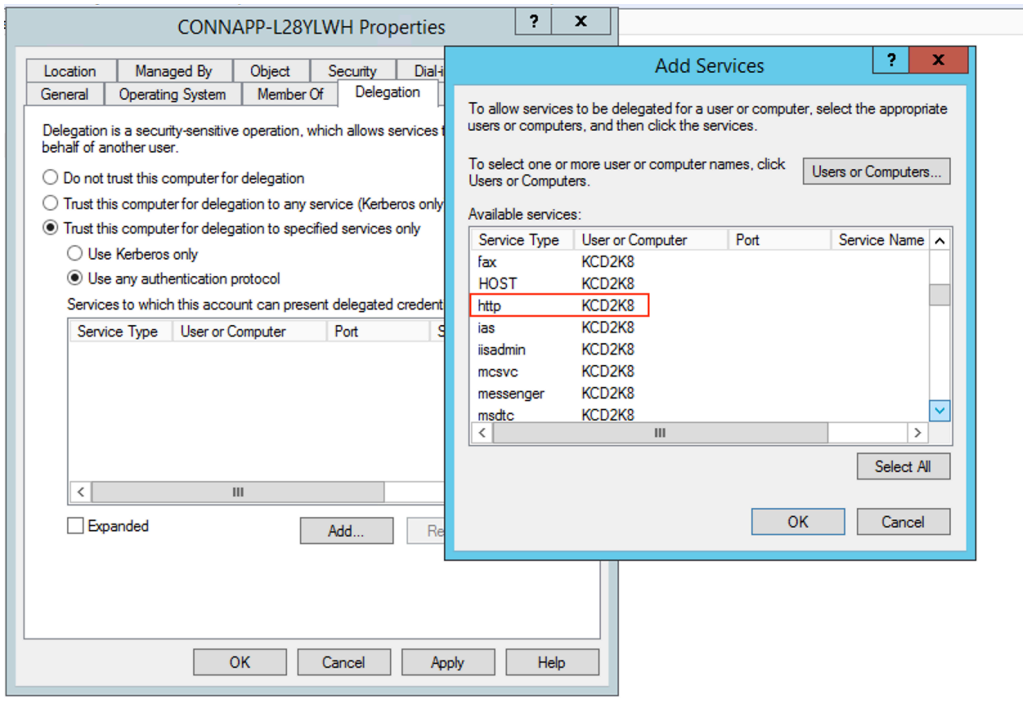
- Identify the connector appliance computer name. You can get this name either from the place where you hosted or simply from the connector UI.
- On your Active Directory controller, look for the connector appliance computer.
- Go to the properties of the Connector Appliance computer account, and navigate to the **Delegation** tab.
- Choose **Trust the computer for delegation to specified services only.** and then select **Use any authentication protocol.**



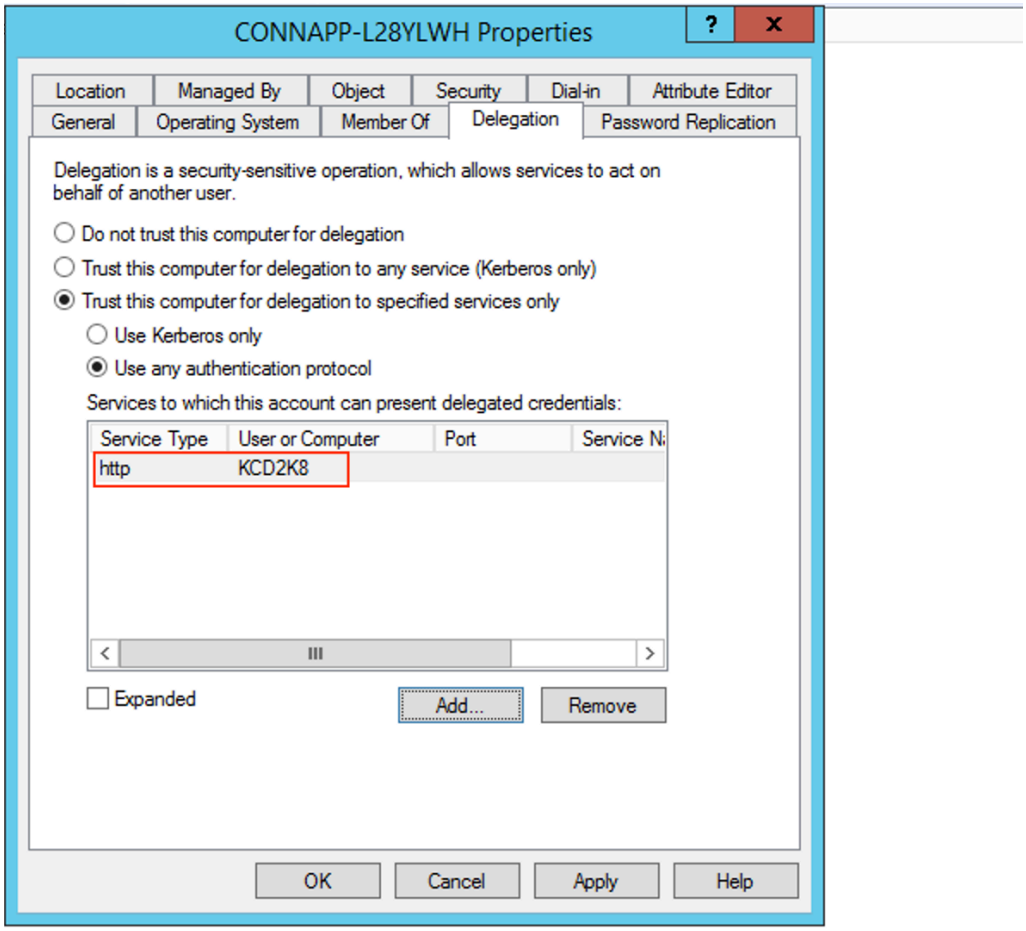
- Click **Add.**
- Click **Users or Computers.**
- Enter the target web server computer name, and then click **Check Names.** In the preceding image, **KCD2K8** is the web server.



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



- Click **OK**.
- Click **Apply,** and then click **OK**.

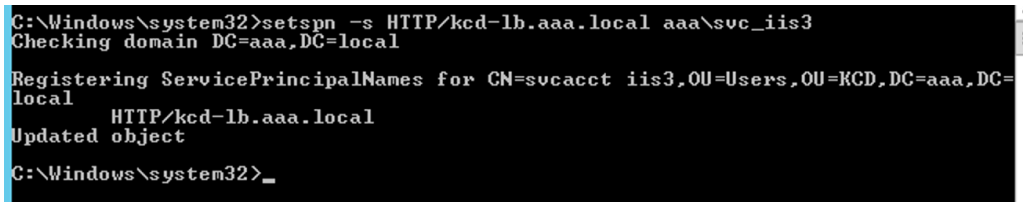


This completes the procedure for adding delegation for a web server.

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.

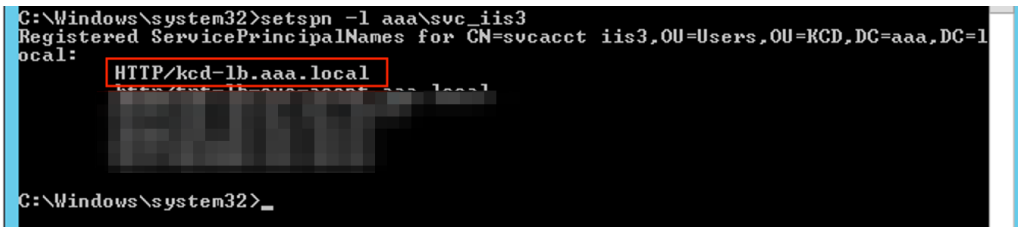
  `setspn -S HTTP/<web_server_fqdn> <service_account>`



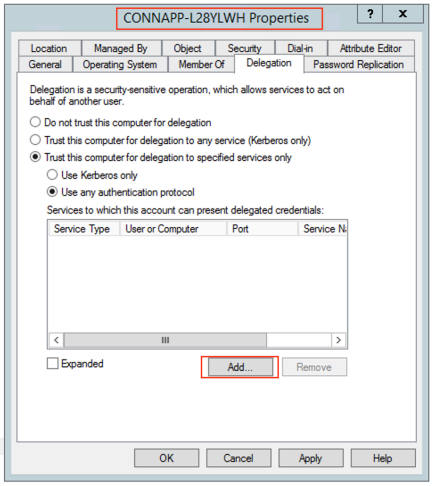
```
C:\Windows\system32>setspn -s HTTP/kcd-lb.aaa.local aaa\svc_iis3
Checking domain DC=aaa,DC=local

Registering ServicePrincipalNames for CN=svcacct iis3,OU=Users,OU=KCD,DC=aaa,DC=
local
        HTTP/kcd-lb.aaa.local
Updated object

C:\Windows\system32>_
```

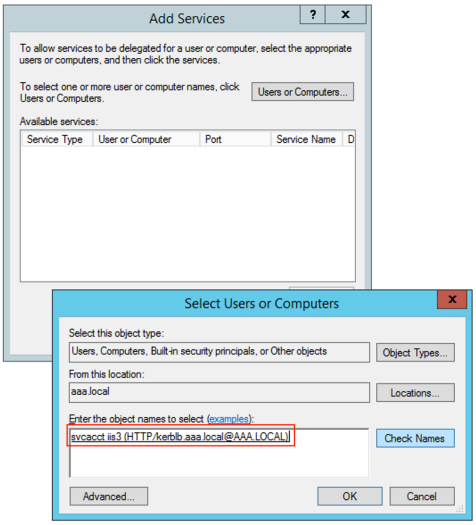
- Confirm the SPNs for the service account using the following command.

  `setspn -l <service_account>`

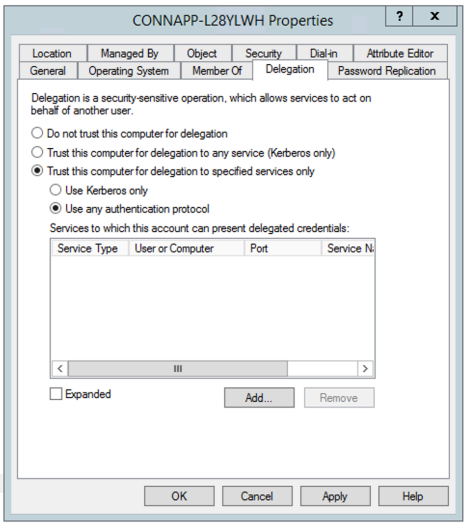


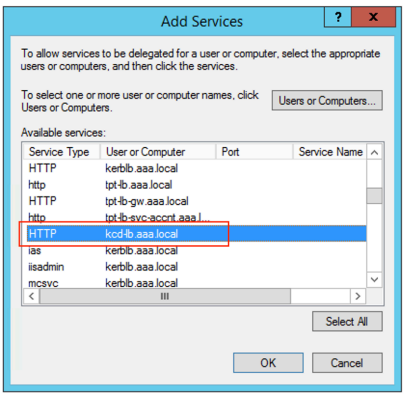
- Create a delegation for the connector appliance computer account.
  - Follow the steps to *Configure Kerberos Constraint Delegation for the webserver* without a load balancer to identify the CA machine and navigate to the Delegation UI.
  - In select **Users and Computers**, select service account (for example, aaa\svc_iis3).



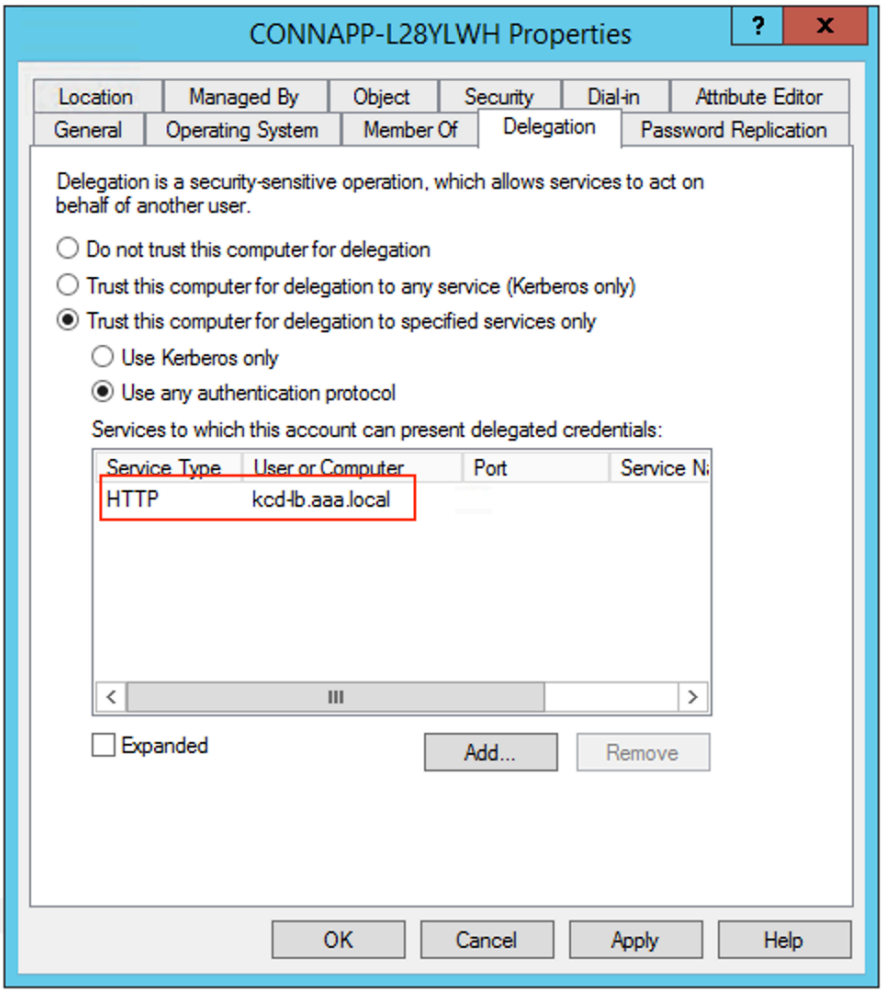


  - In the services, select the entry **ServiceType: HTTP** and User or Computer: web server (for example, `kcd-lb.aaa.local`)





- Click **OK**.
- Click **Apply,** and then click **OK**.



d) Configure Kerberos Constrained Delegation (KCD) for a group managed service account.

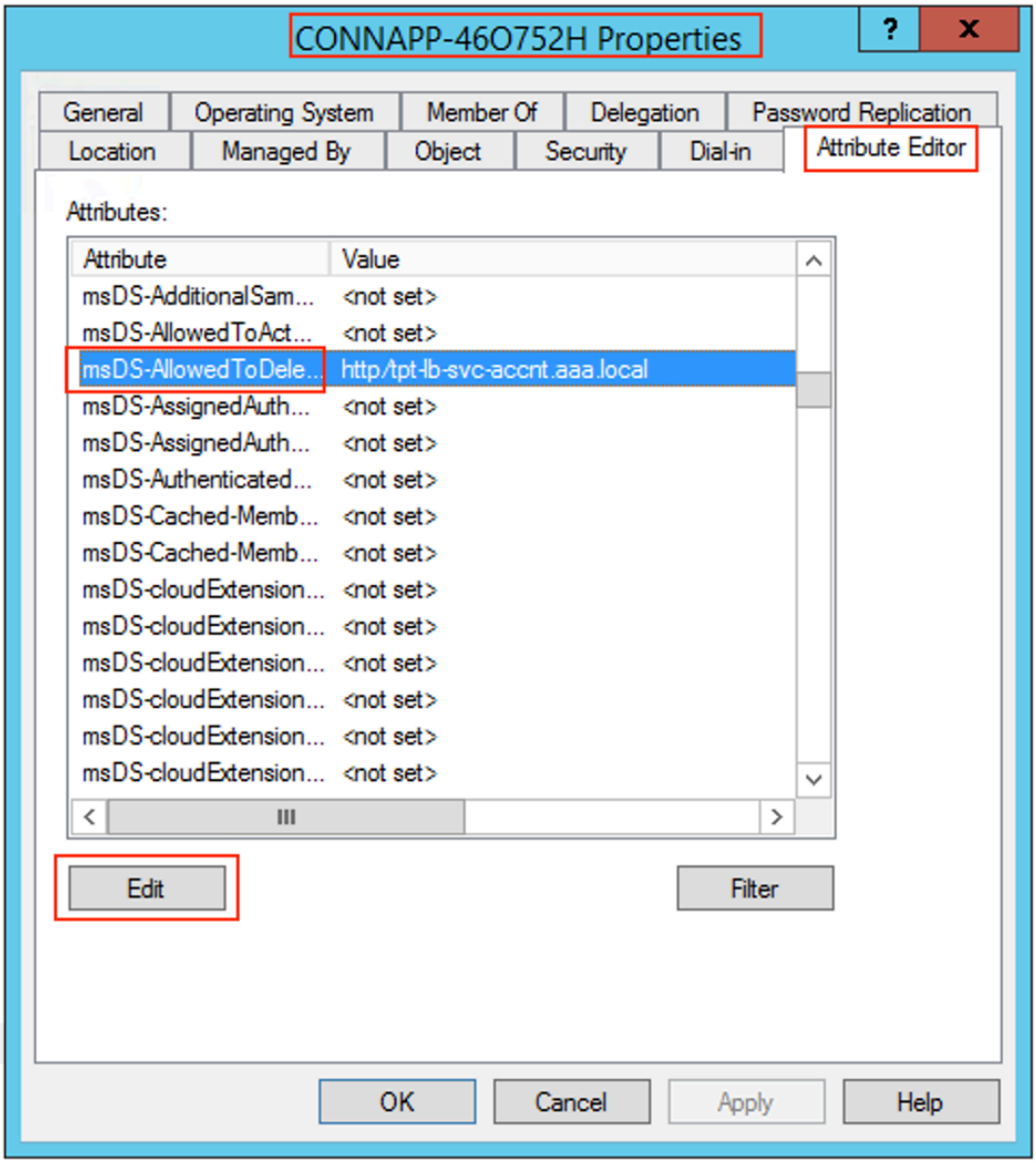
- Add SPN to the group managed service account if not already done.
  `setspn -S HTTP/<web_server_fqdn> <group_manged_service_account>`
- Confirm the SPN using following command.
  `setspn -l <group_manged_service_account>`

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

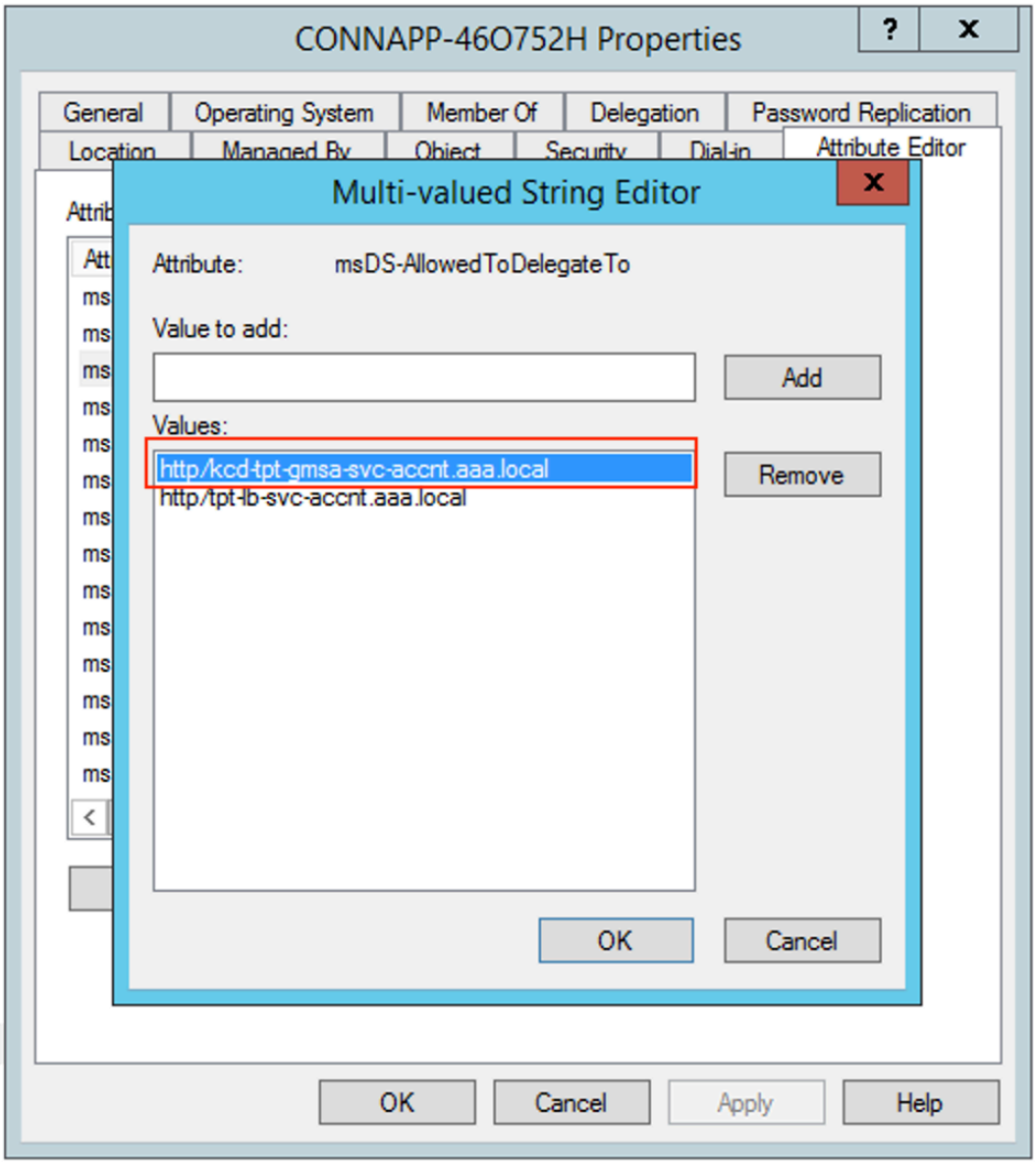
- In the Connector Appliance computer properties, navigate to the **Attribute Editor** tab,

and look for the `msDA-AllowedToDeleteTo` attribute.

- Edit the `msDA-AllowedToDeleteTo attribute`, and then add the SPN.



)



)

e) Migrate from Citrix Gateway Connector to Citrix Connector Appliance.

- As SPNs is already set to service account while configuring the gateway connector, you do not need to add any more SPNs for the service account if no new kerberos app is configured. You can view the list of all SPNs assigned for the service account by following command and assign them as delegated entries for the CA computer account.

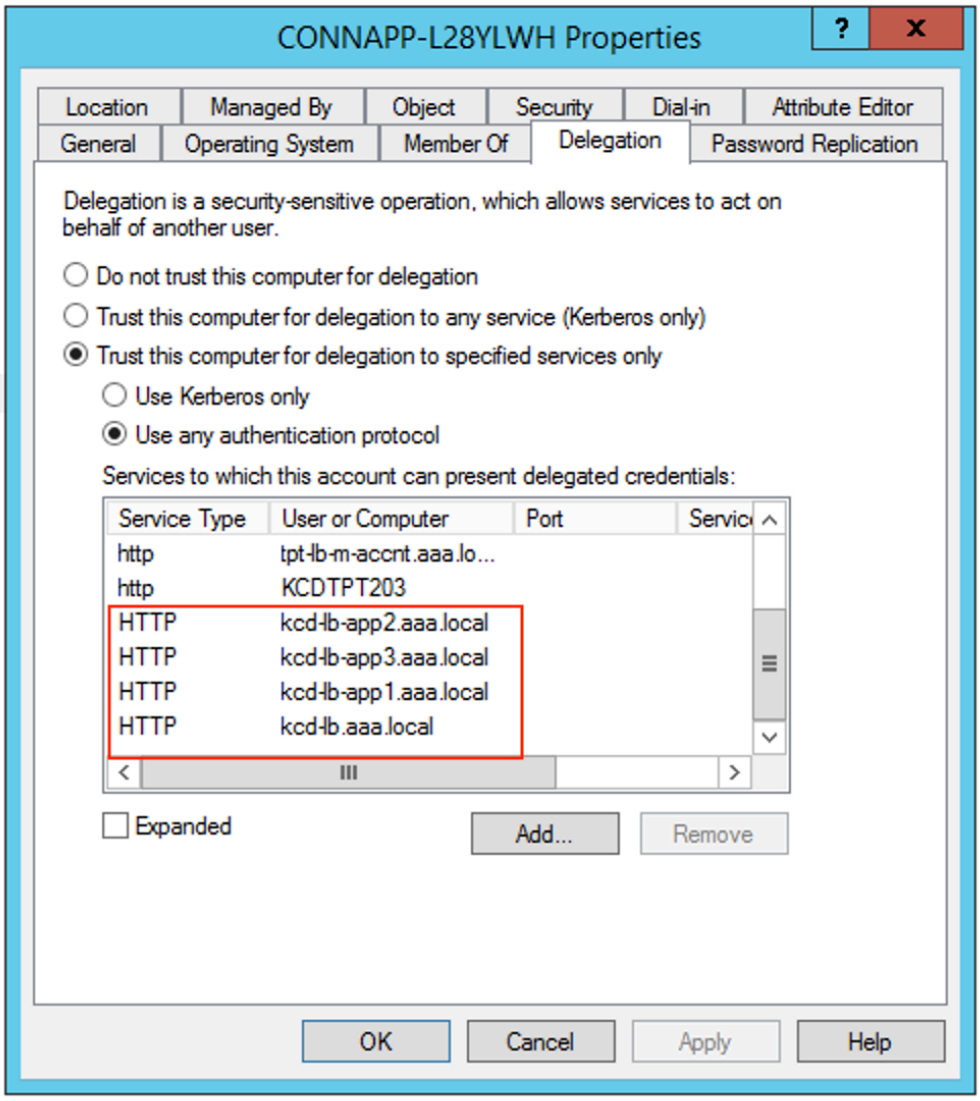
```
setspn -l <service_account>
```



```
C:\Windows\system32>setspn -l aaa\svc_iis3
Registered ServicePrincipalNames for CN=svcacct iis3,OU=Users,OU=KCD,DC=aaa,DC=l
ocal:
        HTTP/kcd-lb-app3.aaa.local
        HTTP/kcd-lb-app2.aaa.local
        HTTP/kcd-lb-app1.aaa.local
        HTTP/kcd-lb.aaa.local
        HTTP/kerblb.aaa.local
        host/kerblb.aaa.local

C:\Windows\system32>_
```

In this example, the SPNs (`kcd-lb.aaa.local`, `kcd-lb-app1.aaa.local`, `kcd-lb-app2.aaa.local`, `kcd-lb-app3.aaa.local`) are configured for KCD.

- Add the required SPNs to the connector appliance computer account as the delegated entry. For details, step *Create a delegation for the connector appliance computer account*.



In this example, the required SPN is added as delegated entires for the CA computer account.

Note: These SPN were added to the service account as delegated entries while configuring the gateway connector. As you are moving away from service account delegation, those entires can be removed from the service account **Delegation** tab.

f) Follow the Citrix Secure Private Access documentation to set up the Citrix Secure Private Access service. During the set up, Citrix Cloud recognizes the presence of your Connector Appliances and uses them to connect to your resource location.

- Get started with Citrix Secure Private Access
- Configure Citrix Secure Private Access
- Connector Appliance for Cloud Services
- Internet Connectivity Requirements.
- Support for Enterprise web apps

Validating your Kerberos configuration

If you use Kerberos for single sign-on, you can verify that the configuration on your Active Directory controller is correct from the **Connector Appliance administration page**. The **Kerberos validation** feature enables you to validate a Kerberos realm-only mode configuration or a Kerberos Constrained Delegation (KCD) configuration.

1. Go to the **Connector Appliance administration page**.
   a) From the Connector Appliance console in your hypervisor, copy the IP address to your browser address bar.
   b) Enter the password that you set when you registered your Connector Appliance.
2. From the Admin menu on the top right, select **Kerberos Validation**.
3. In the **Kerberos Validation** dialog, choose the **Kerberos Validation Mode**.
4. Specify or select the **Active Directory Domain**.
   - If you are validating a Kerberos realm-only mode configuration, you can specify any Active Directory domain.
   - If you are validating a Kerberos Constrained Delegation configuration, you must select from a list of domains in the joined forest.
5. Specify the **Service FQDN**. The default service name is assumed to be `http`. If you specify "computer.example.com", this is considered the same as `http/computer.example.com`.
6. Specify the **Username**.
7. If you are validating a Kerberos realm-only mode configuration, specify the **Password** for that user name.

8. Click **Test Kerberos**.

If the Kerberos configuration is correct, you see the message `Successfully validated Kerberos setup`. If the Kerberos configuration is not correct, you see an error message that provides information on the validation failure.

Migrate Gateway Connector to Connector Appliance

November 21, 2023

Citrix Gateway Connector is deprecated. Citrix recommends its customers using Citrix Gateway Connectors in their environment, to start deploying Connector Appliance for all Secure Private Access use cases that were previously supported by the Citrix Gateway Connector. This topic provides guidelines on migrating Gateway Connector to Connector Appliance.

High-level steps to migrate Gateway Connector to Connector Appliance

1. Install the Connector Appliances in addition to the Gateway Connectors in the same resource location.
2. Shut down the Gateway Connectors and test the existing Web apps for connectivity. Check if the Web app hosted on the same resource location is accessible.
3. Remove the Citrix Gateway Connector once testing is complete.

To install Connector Appliance

Use the following steps to install a Connector Appliance.

1. Sign in to Citrix Cloud.
2. From the menu in the top left of the screen, select **Resource Locations**.
3. Click the plus icon next to Connector Appliance for the resource location that you want to add a Connector Appliance.
4. Select the hypervisor and click **Download Image**.
5. Download and Install the Connector Appliance on your hypervisor.
6. Log in to the Web UI (IP address provided on the hypervisor's console) and set up a proxy if necessary.
7. Click the **Register** button and obtain the short code.

8. Paste the short code into the Citrix Cloud user interface used when downloading the Connector Appliance (step 5).

   The Connector Appliance is registered.

For detailed steps, see Connector Appliance for Cloud Services.

FAQs

- How do I download the Connector Appliance?

  Download the Connector Appliance.
- How do I install the Connector Appliance?

  Installing the Connector Appliance.
- How do I register the Connector Appliance?

  Registering the Connector Appliance.
- What are the connectivity requirements for the Connector Appliance?

  Connector Appliance Internet Connectivity Requirements.
- What are the system requirements for the Connector Appliance?

  Connector Appliance System Requirements.
- How is Connector Appliance updated?

  Connector Appliance Updates

Direct access to Enterprise web apps

May 30, 2024

Enterprise web applications like SharePoint, JIRA, Confluence, and others which are hosted by the customer either 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 access to the web apps by clicking links from their emails, collaboration tools, or browser bookmarks. Thus provisioning a true zero footprint solution to the customers.

How it works

- Add a new DNS record or modify an existing DNS record for the configured Enterprise web apps.
- IT administrator would add 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 direct 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 direct 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 that you use the wizard. In the subsequent usages, you can directly navigate to the **Applications** page and, then click **Add an app**.

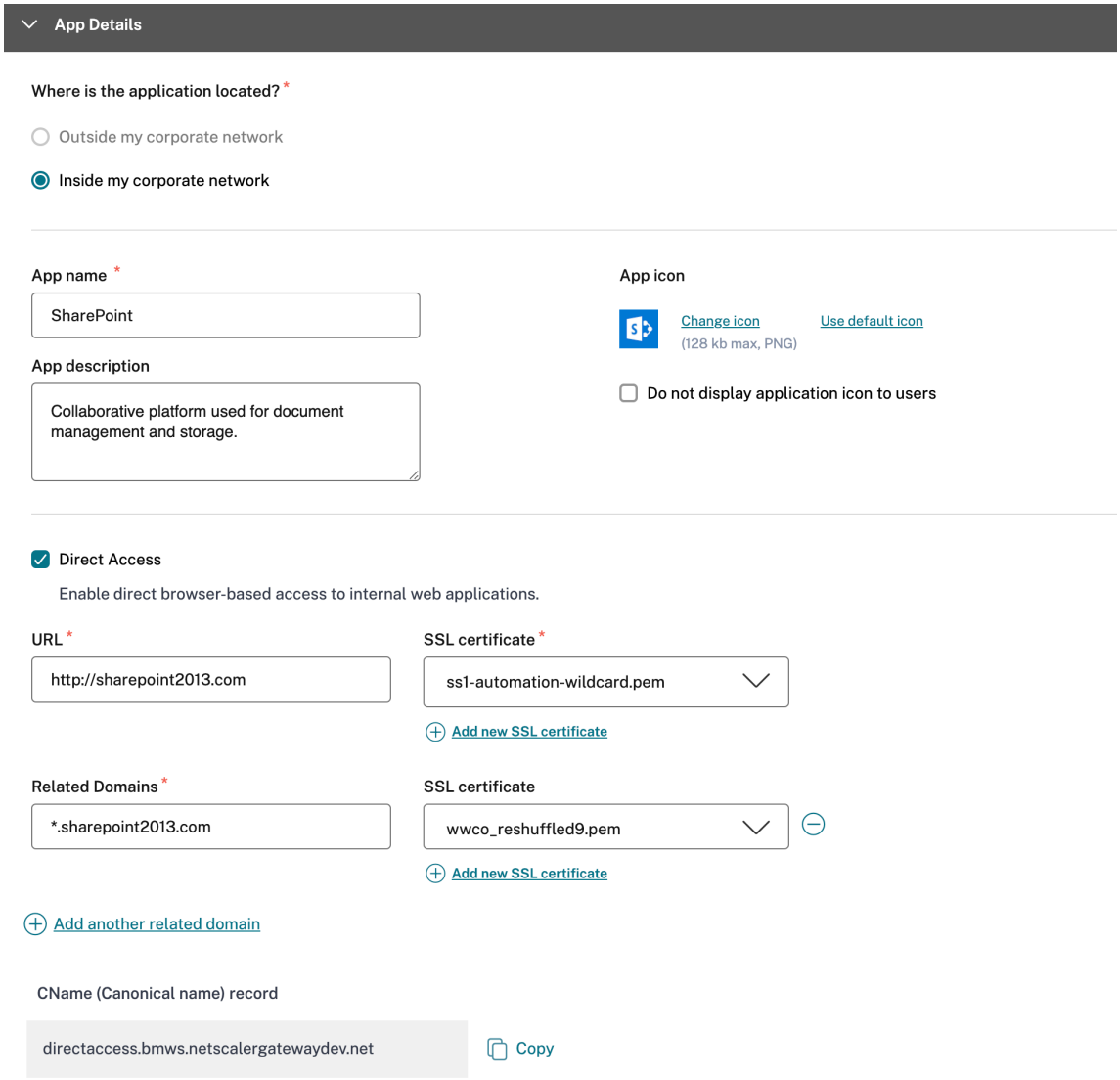
2. Set up identity and authentication. For details, see Admin guided workflow for easy onboarding and set up.

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** –Select the app type (HTTP or HTTPS).
   - **App name** –Name of the application.
   - **App description** - A brief description of the app. This description that you enter here's 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.

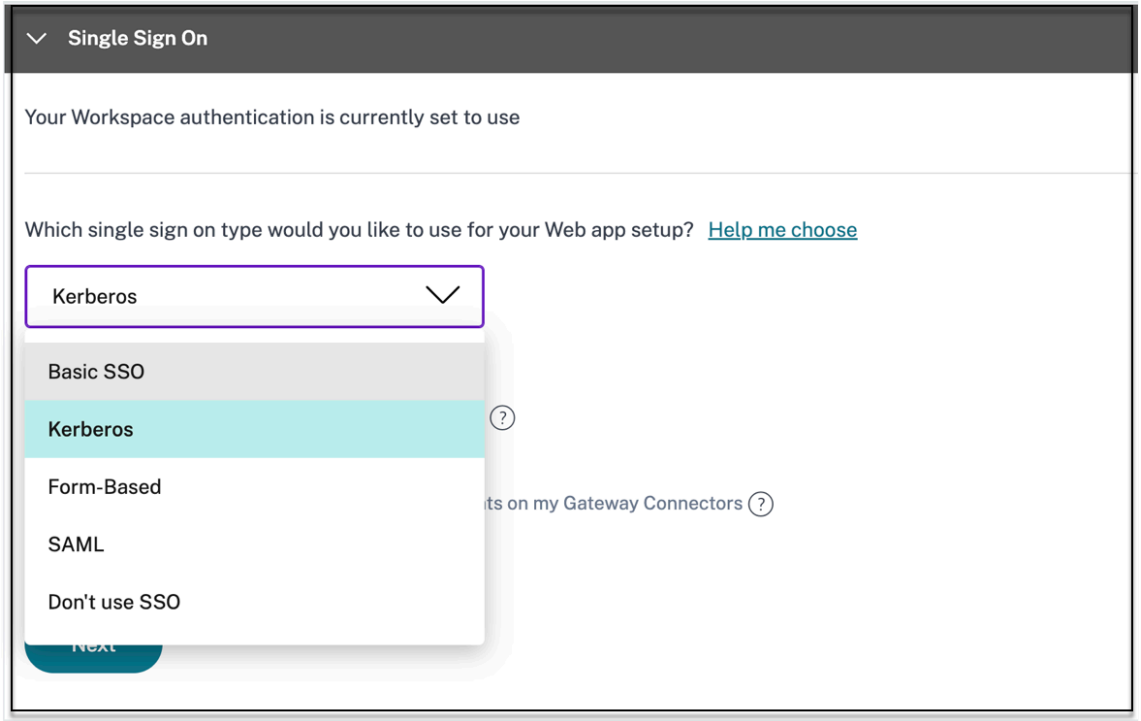
     If you do not want to display the app icon, select **Do not display application icon to users**.
7. Select **Direct Access** to enable users access the app directly from a client browser. Enter the following details.
   - **URL** –URL for the back-end application. The URL must be in HTTPS format and 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**.

     Points to note:

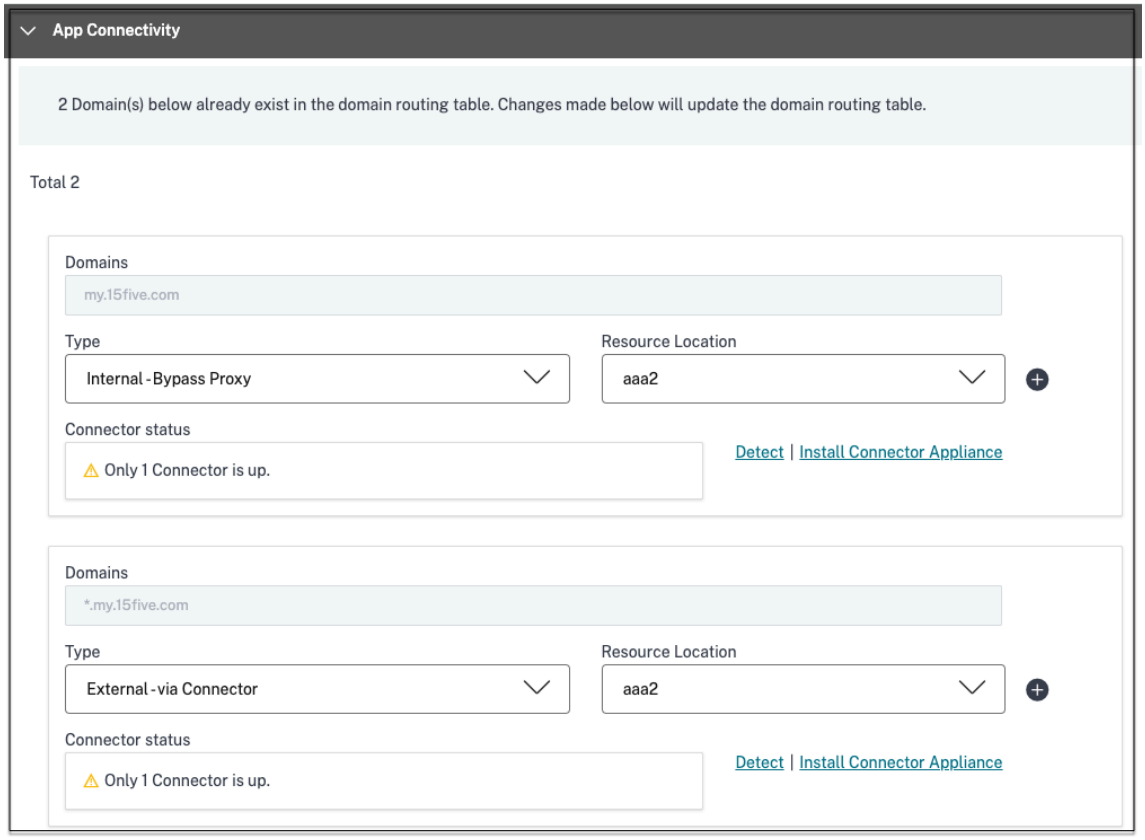
     - Only a public or a trusted CA certificate is supported. Self-signed certificates aren't supported.
     - A full chain of certificates must be uploaded.
   - **Related Domains** –The related domain is auto-populated based on the URL that you've provided. Related domain helps the service to identify 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.
   - **CName record** –Auto generated by Secure Private Access. This is the value that must be entered in the DNS to enable direct access to the application.



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



10. 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.



11. Click **Finish**. The app is added to the Applications page. You can or edit or delete an 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 configuration, see Best practices for Web and SaaS application configurations.

Support for Software as a Service apps

May 30, 2024

Software as a Service (SaaS) is a software distribution model to deliver 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.

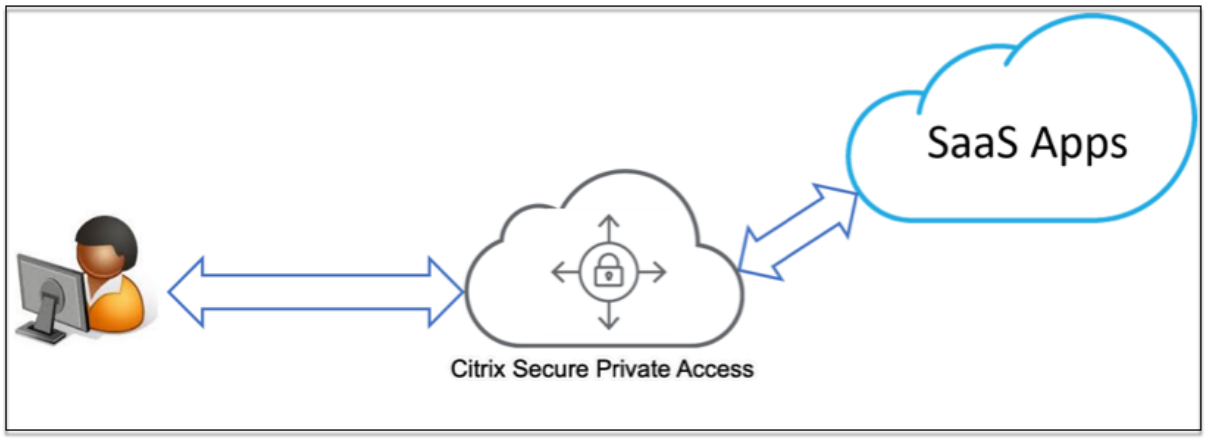
SaaS app delivery using the Secure Private Access service provides you an easy, secure, robust, and scalable solution to manage the apps. SaaS apps delivered on the cloud have the following benefits:

- **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 details
2. Set the preferred sign-on method
3. Define application routing

Configure application details

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

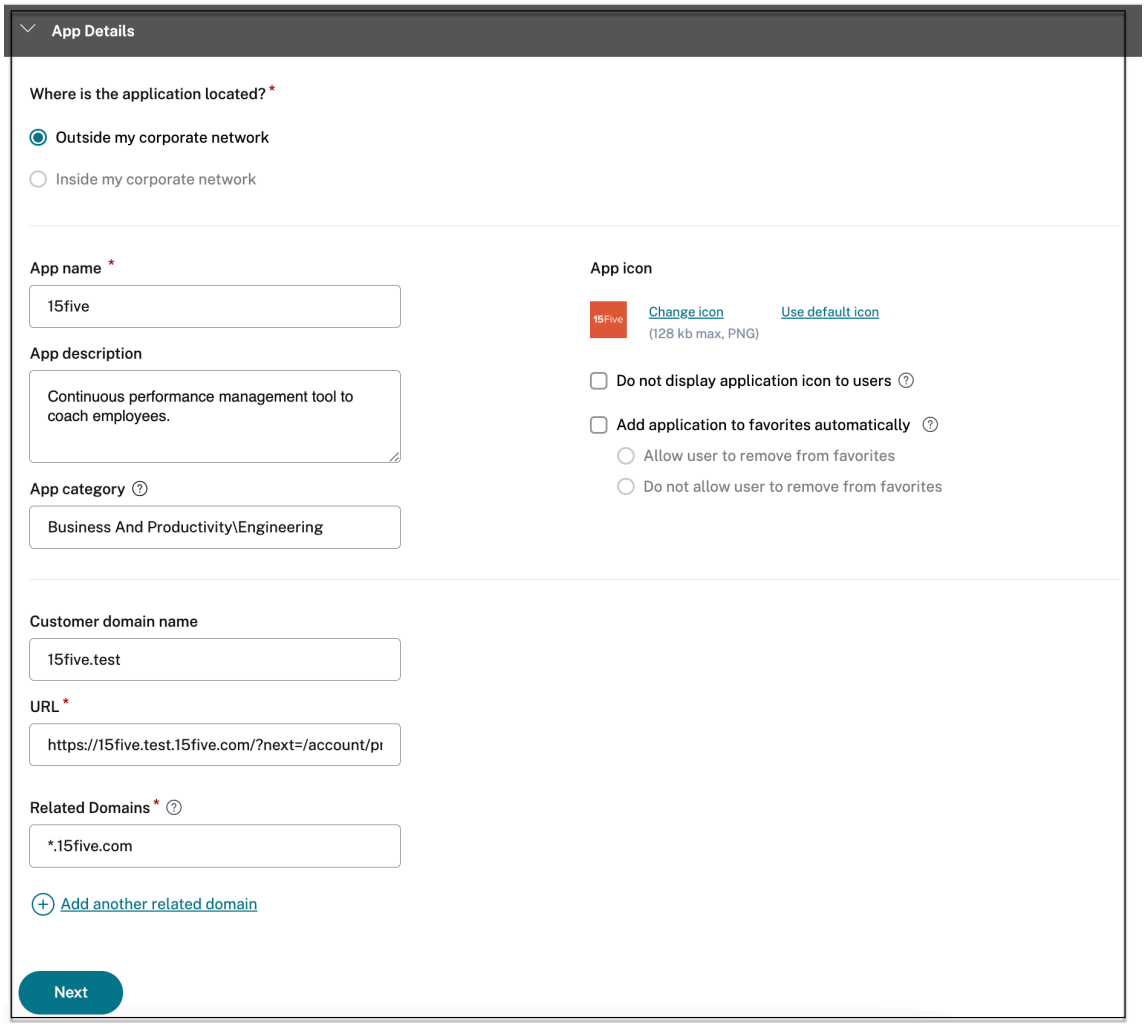
   > **Note:**
   >
   > - The **Continue** button appears only for the first time that you use the wizard. In the subsequent usages, you can directly navigate to the **Applications** page and then click **Add an app.**
   > - You can add a SaaS app manually by entering the app details or select an app 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 name** –Name of the application.
- **App description** - A brief description of the app. This description that you enter here's 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` 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.

- Click **Add application to favorites automatically** 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.

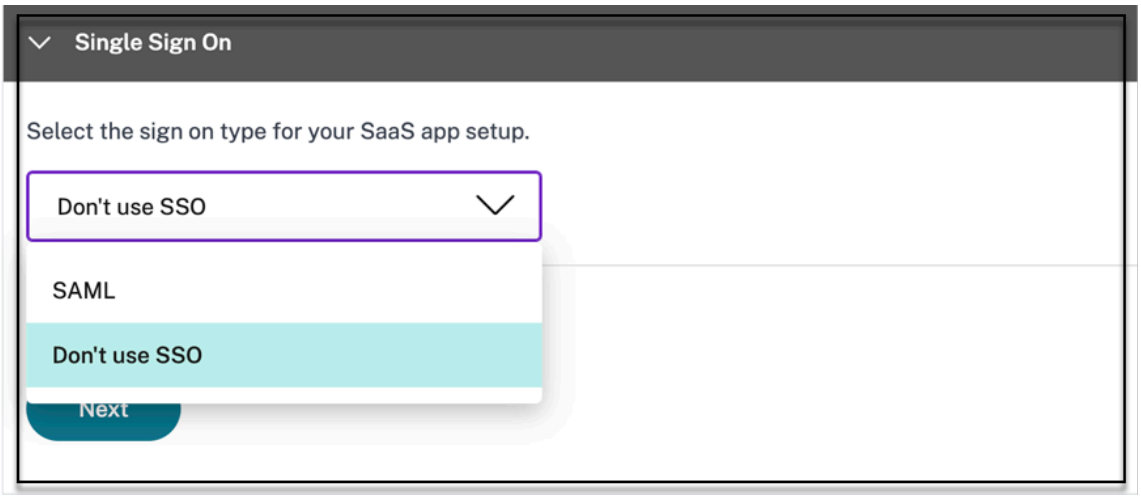
  If you remove the apps marked as favorites from the Secure Private Access service console, then these apps must be removed manually from the favorites list in Citrix Workspace. The apps aren't auto deleted from the Workspace app if removed from the Secure Private Access service console.

5. Click **Next.**

> **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 configuration, see Best practices for Web and SaaS application configurations.

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.



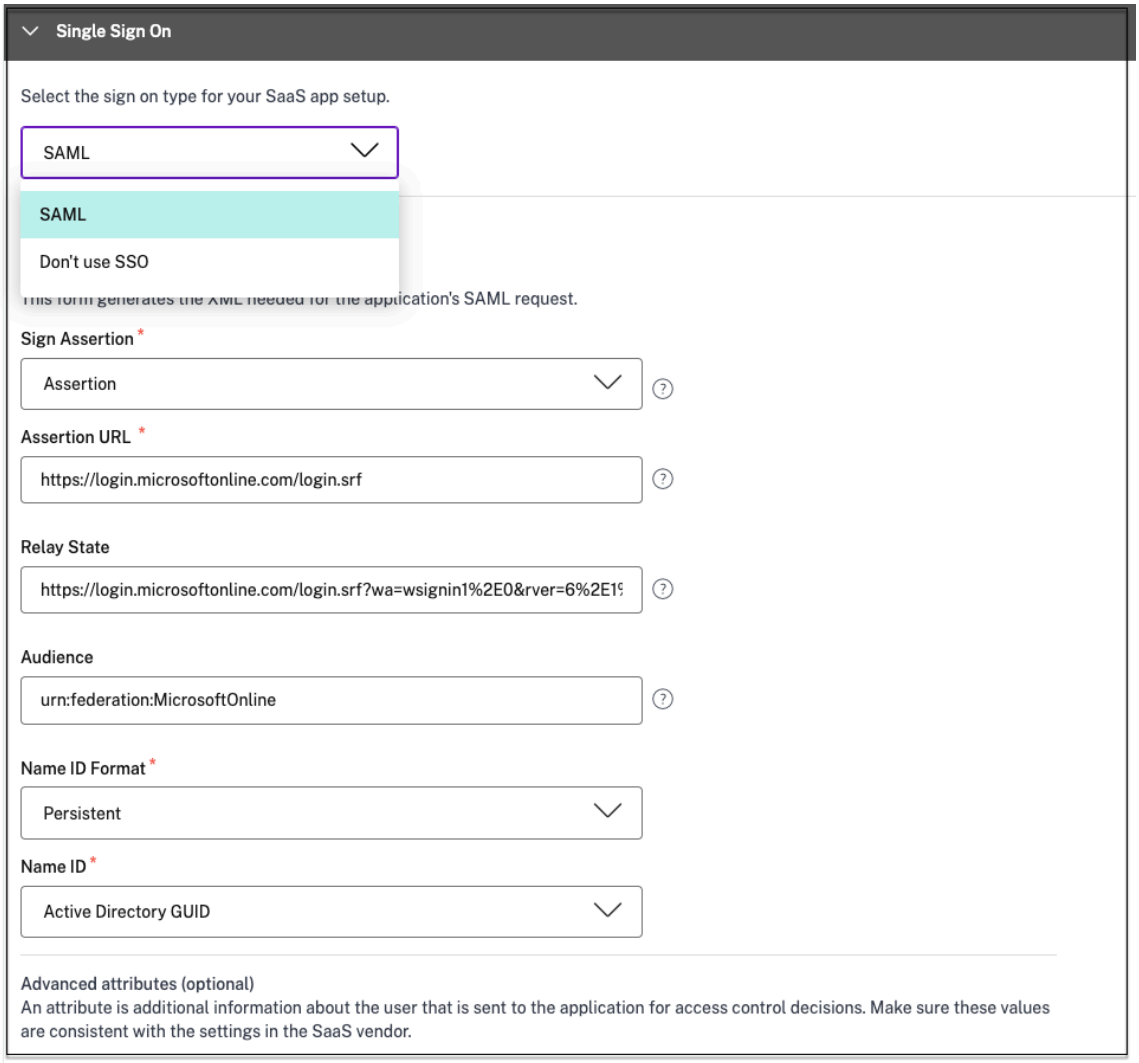
   - **Don't use SSO** –Use the **Don't use SSO** option when you do not need to authenticate a user on the back end server. When the **Don't use SSO** option is selected, the user is redirected to the URL configured under the **App details** section.
   - **SAML** - Choose **SAML** for SAML-based SSO into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



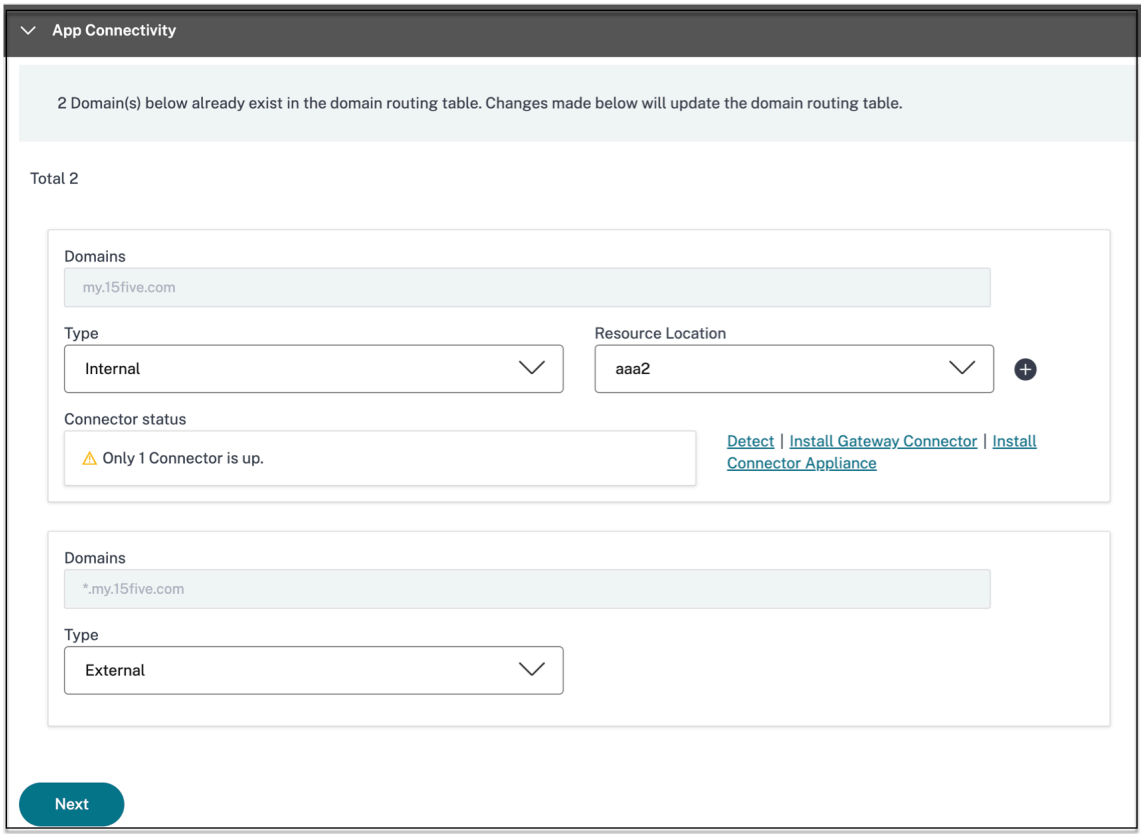
3. Download the metadata file by clicking the link under **SAML Metadata**. Use the downloaded metadata file to configure SSO on the SaaS apps server.

> **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 **Next.**

Define application routing

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

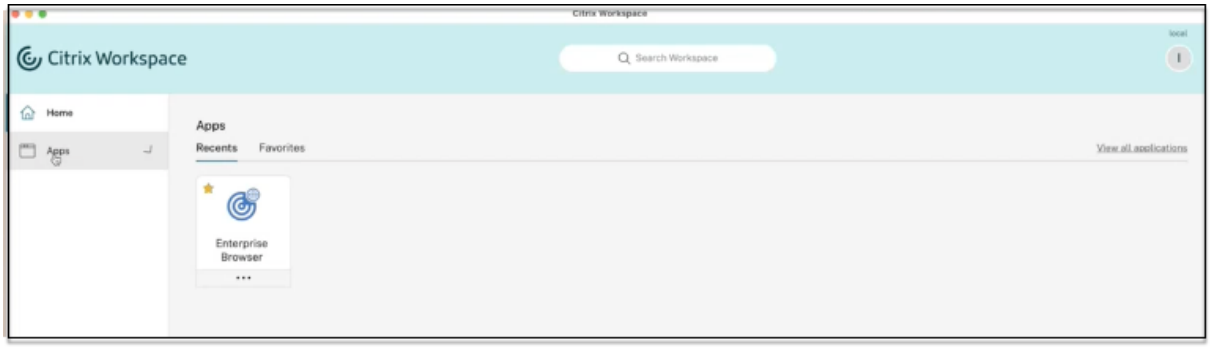


2. Click **Finish.**

   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.



References

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

Support for client-server apps

November 21, 2023

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.

With the additional support of 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.

Preview features

Support for DNS suffixes to resolve FQDNs to IP addresses.

How it works

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

- For Windows, the client version (22.3.1.5 and later) can be downloaded from https://www.citrix.com/downloads/citrix-gateway/plug-ins/citrix-secure-access-client-for-windows.html.
- For macOS, the client version (22.02.3 and later) can be downloaded from the App Store.

Admin Configuration –Citrix Secure Access client-based access to TCP/UDP apps

Prerequisites

Ensure that the following requirements are met to access TCP/UDP apps.

- Access to Citrix Secure Private Access in Citrix Cloud.
- Citrix Cloud Connector - Install a Citrix Cloud Connector for Active Directory domain configuration as captured in Cloud Connector Installation.
- Identity and access management - Complete the configuration. For details, see Identity and access management.
- 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.

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

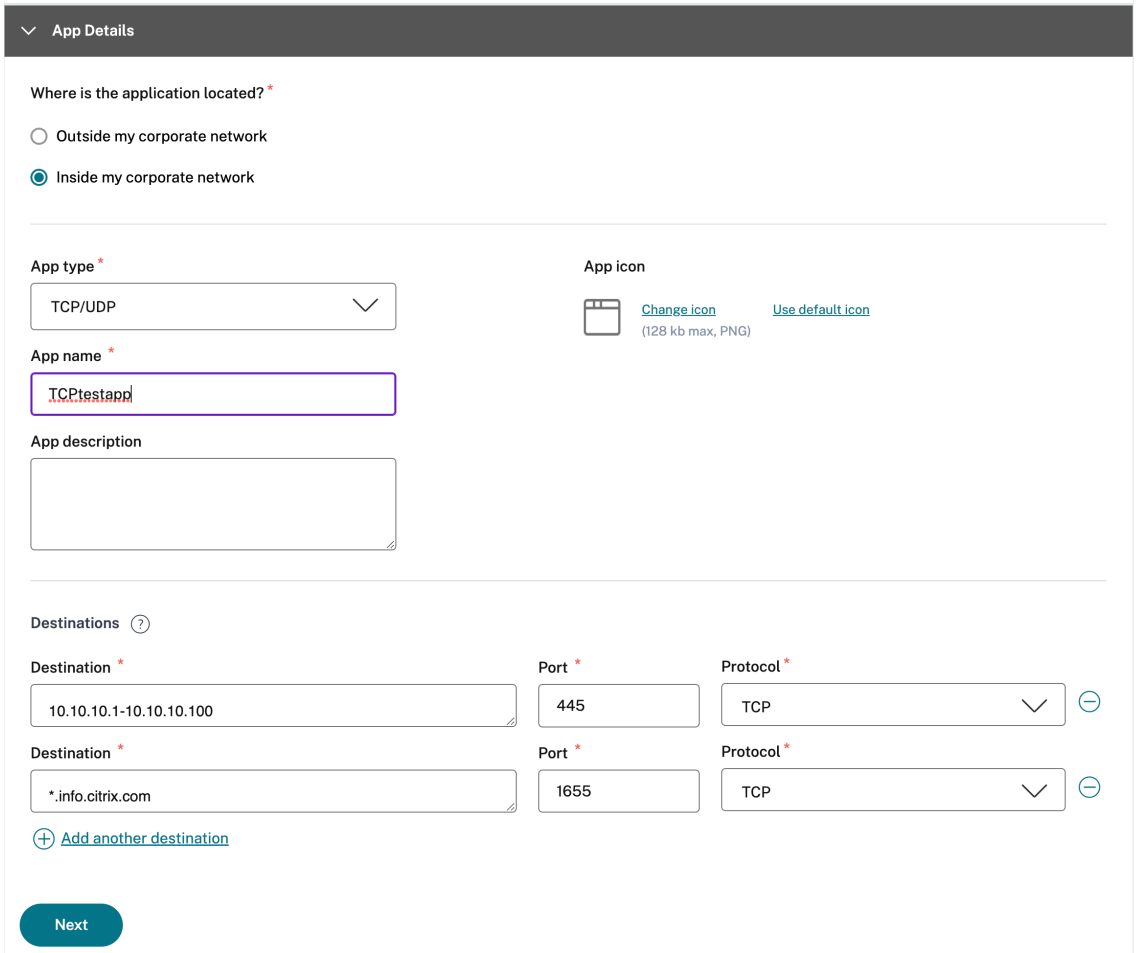
1. On the Citrix Secure Private Access tile, click **Manage**.
2. Click **Continue** and then click **Add an app**.

   > **Note:**
   >
   > The **Continue** button appears only for the first time that you use the wizard. In the subsequent usages, 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**.



- **App type** –Select TCP/UDP.
- **App name**–Name of the application.
- **App icon**–An app icon is displayed. This field is optional.
- **App description** –Description of the app you are adding. This field is optional.
- **Destinations** –IP Addresses or FQDNs of the back-end machines residing in the resource location. One or more destinations can be specified as follows.
  - **IP address v4**
  - **IP address Range** –Example: 10.68.90.10-10.68.90.99
  - **CIDR** –Example: 10.106.90.0/24

- **FQDN of the machines or Domain name** –Single or wildcard domain. Example: ex.destination.domain.com, *.domain.com

> **Important:**
>
> End users can access the apps using FQDN even if the admin has configured the apps using the IP address. This is possible because the Citrix Secure Access client can resolve an FQDN to the real IP address.
> The following table provides examples of various destinations and how to access the apps with these destinations:

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

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

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

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

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

- **Protocol** –TCP/UDP

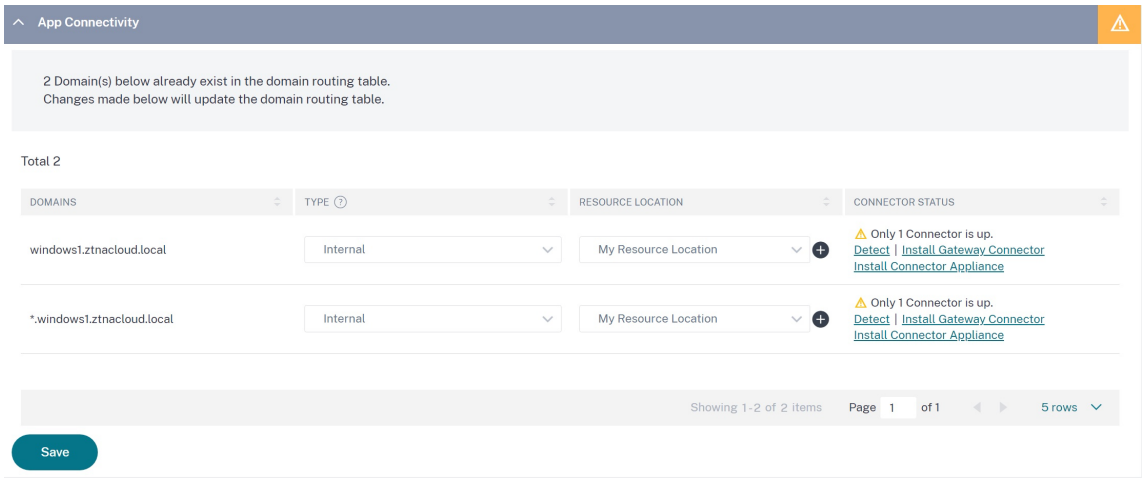
5. In the **App Connectivity** section, a mini version of the **Application Domains** table is available to make the routing decisions. For each destination, you can choose a different or same resource location. Destinations configured in the previous step are populated under the **DESTINATION** column. Destinations added here are also added to the main **Application Domains** table. The **Application Domains** table is the source of truth for making the routing decision to direct connection establishment and traffic to the correct resource location. For more information on the **Application Domains** table and possible IP conflict scenarios, see *Application Domains - IP address conflict resolution* section.
6. For the following fields, select an input from the drop-down menu and click **Next**.

> **Note:**
>
> Only the Internal route type is supported.

- **RESOURCE LOCATION** –From the drop-down menu, you must connect to a resource location with at least one Connector Appliance installed.

> **Note:**
>
> Connector Appliance installation is supported from the App Connectivity section. You

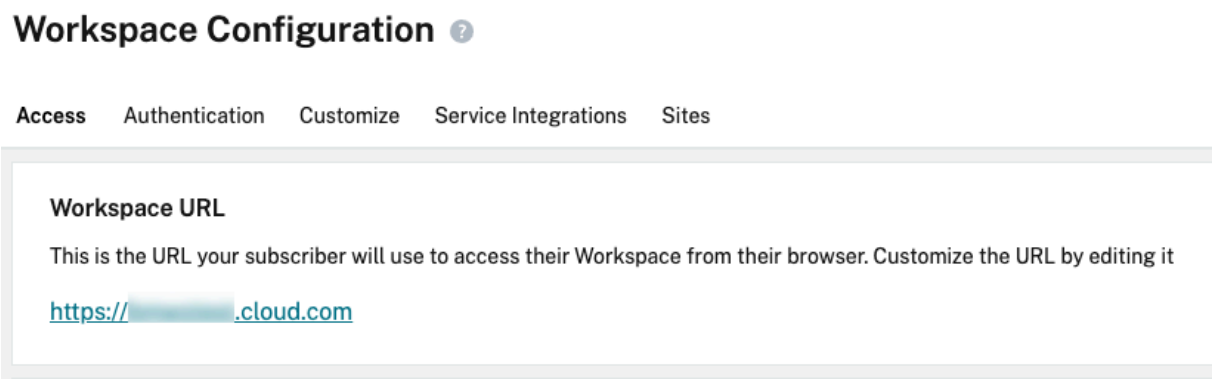
> can also install it under the Resource Locations section in the Citrix Cloud portal. For more information on creating a Resource Location, see Set up resource locations.



7. 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 Set up 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.



Admin Configuration –Citrix Secure Access client-based access to HTTP/HTTPS apps

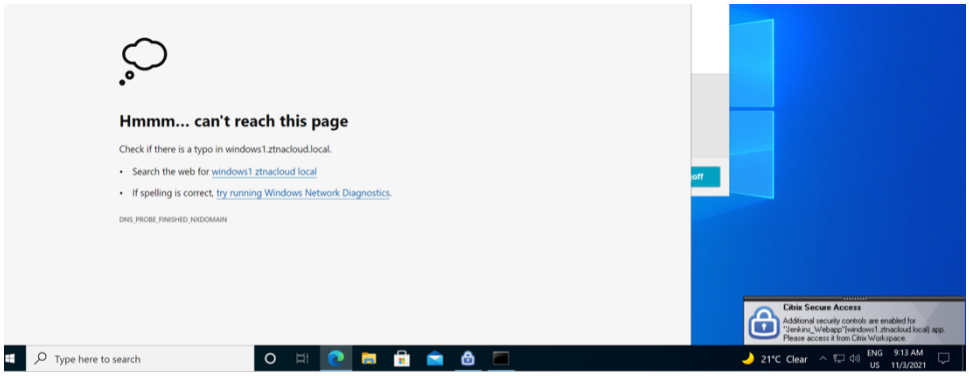
> **Note:**
>
> To access existing or new HTTP/HTTPS apps using the Citrix Secure Access client, you must install at least one (recommended two for high-availability) Connector Appliance in your resource location. The connector appliance can be installed on-premises, in the data center hypervisor, or in the public cloud. For details of Connector Appliance and its installation, see Connector Appliance for Cloud Services.

Prerequisites

- Access to Citrix Secure Private Access in Citrix Cloud.

Points to note

- Internal web apps enforced with enhanced security controls cannot be accessed through the Citrix Secure Access client.
- 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 Ana-

lytics 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 TCP/UDP applications.

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.

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.

DNS resolution

The connector appliance must have a DNS server configuration for DNS resolution.

Steps to install Citrix Secure Access client on a Windows machine

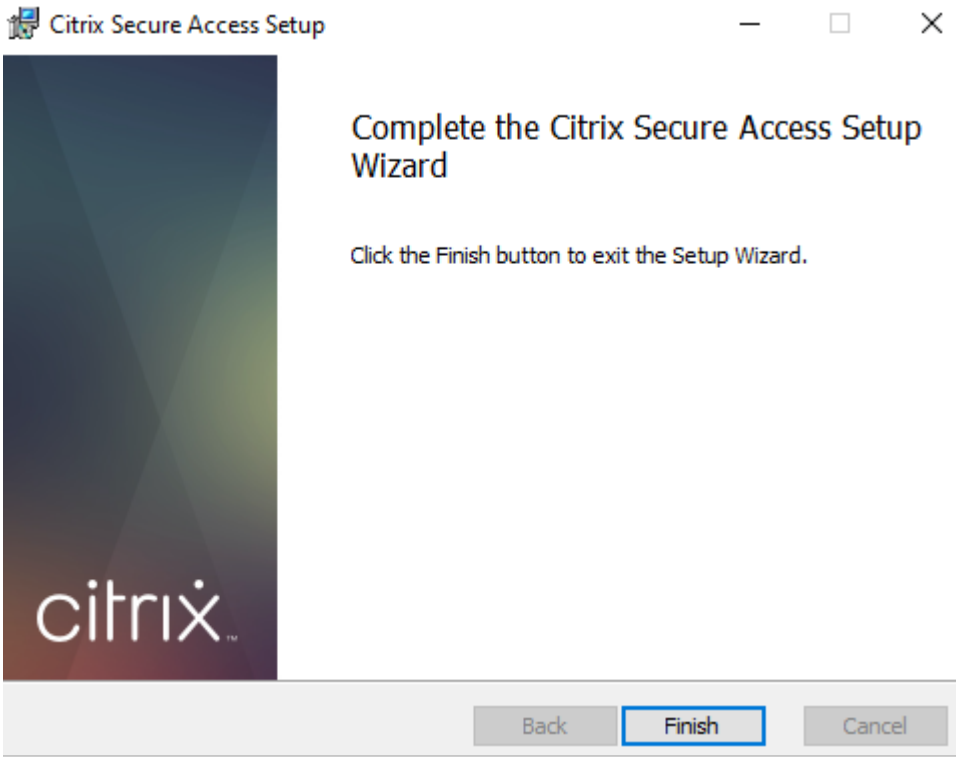
Supported OS versions:

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

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

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

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



> **Note:**
>
> Multi-user sessions in Windows is not supported.

Microsoft Edge Runtime installation steps

Microsoft Edge Runtime is now required for the authentication UI on the Secure Access client.
It is installed by default in the latest Windows 10 and Windows 11 machines. For machines on earlier versions, perform the following steps.

1. Go to the following link, https://go.microsoft.com/fwlink/p/?LinkId=2124703.
2. Download and install Microsoft Edge. If the user system doesn't have the Microsoft Edge runtime installed, the Citrix Secure Access client prompts you to install when you try to connect to the Workspace URL.

> **Note:**
>
> You can use an automated solution like SCCM software or a group policy to push the Citrix Secure Access client or Microsoft Edge Runtime to the client machines.

Steps to install Citrix Secure Access client on a macOS machine

Prerequisites:

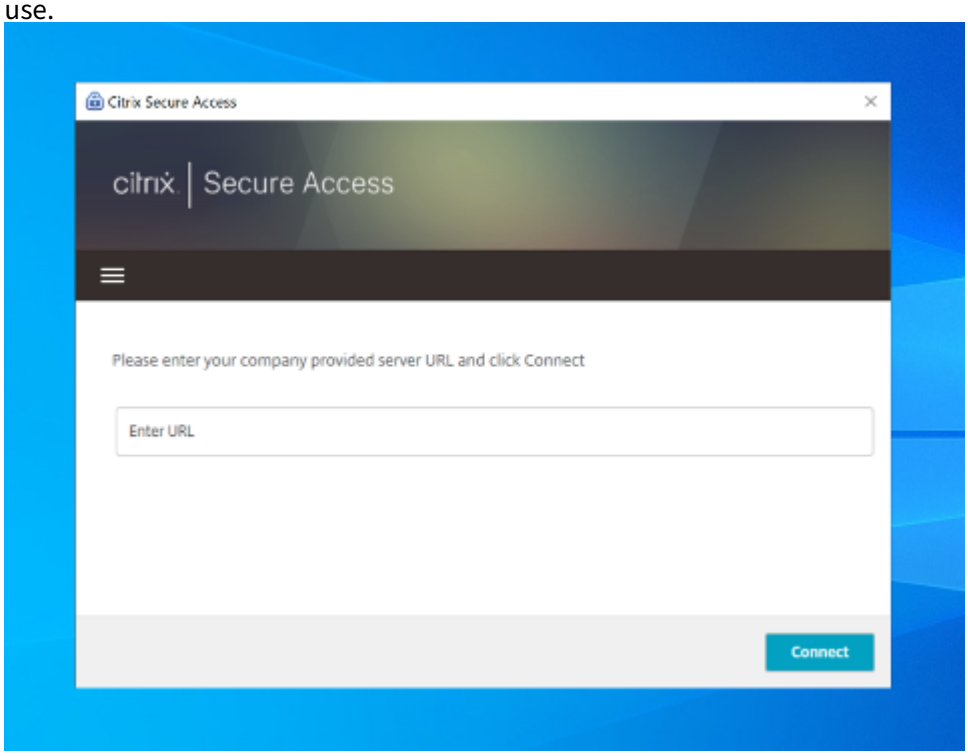
- Download the Citrix Secure Access client for macOS from the App Store. This app is available from macOS 10.15 (Catalina) and later.
- Preview builds are available in the TestFlight app only for macOS Monterey (12.x).
- If you are switching between the App Store app and the TestFlight preview app, you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

Supported OS versions:

- macOS: 12.x (Monterey). 11.x (Big Sur), and 10.15 (Catalina) are supported.
- Mobile devices: iOS and Android is not supported.

Launch a configured app - End-user flow

1. Launch the Citrix Secure Access client on the client device.
2. Enter the Workspace URL provided by the customer admin in the URL field in the Citrix Secure Access client and click **Connect**. It is a one-time activity and the URL is saved for subsequent use.



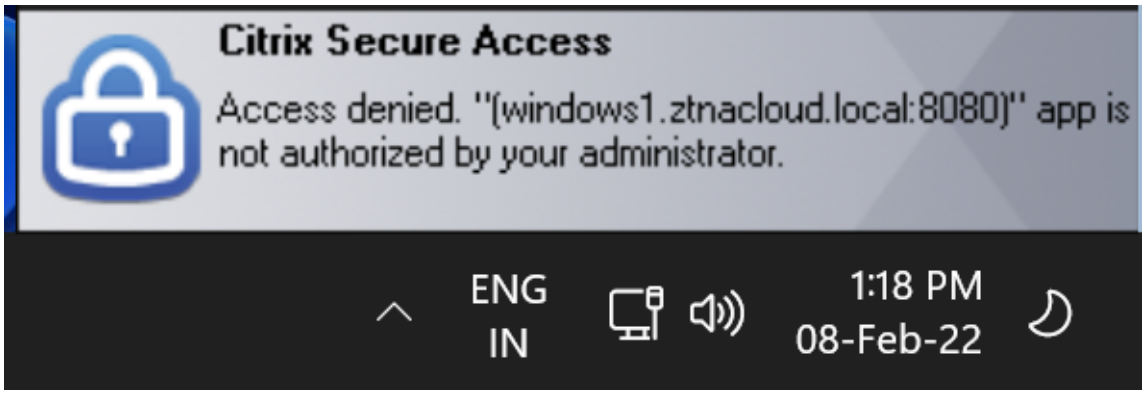
3. User is prompted for authentication based on the authentication method configured in Citrix Cloud.
   Upon successful authentication, the user can access the configured private apps.

User notification messages

A pop-up notification message appears in the following scenarios:

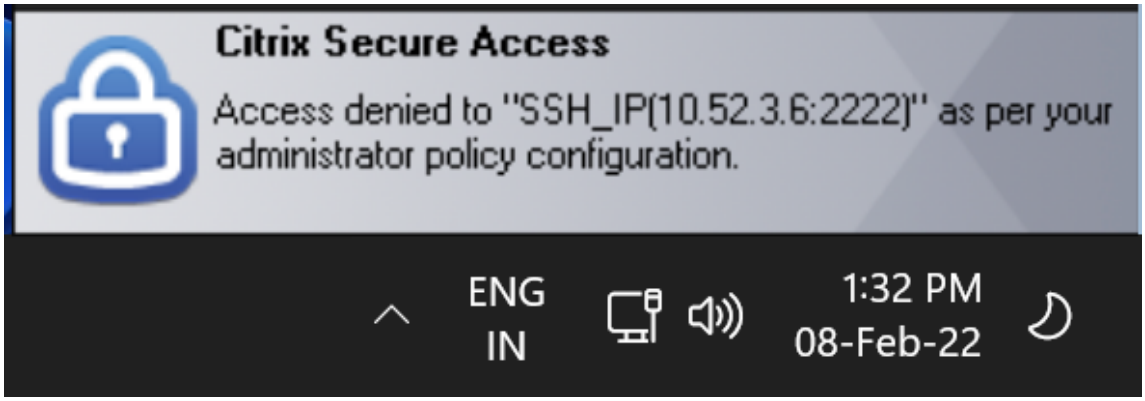
- The app is not authorized by the admin for the user.

  Cause: The application configured for the accessed destination IP address or FQDN is not subscribed for the logged in user.



- The access policy evaluation results in denial of access.

  Cause: Access to the destination IP address or FQDN is denied because the policy bound to the application is evaluated to “Deny Access”to the logged in user.



- The enhanced security control is enabled for the app.

  Cause: The enhanced security control is enabled to the application for the accessed destination. The application can be launched using the Citrix Workspace App.

Additional Information

Application Domains - IP address conflict resolution

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

Conflict Scenarios	Existing application domain entry	New entry from app addition	Behavior
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. Please change the existing routing IP Entry or configure a different destination
Complete Overlap	10.10.10.0/24 RL1	10.10.10.0-10.10.10.255 RL2	Error; `<Completely overlapping IP domain's value>` IP domain completely overlaps with existing entries. Please 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 exist in the domain routing table. Changes made updates 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.

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

Release notes references

- Citrix Secure Access for Windows release notes
- Citrix Secure Access for macOS release notes
- Citrix Secure Private Access release notes

Reserved CIDR addresses for the TCP and UDP servers

November 21, 2023

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.

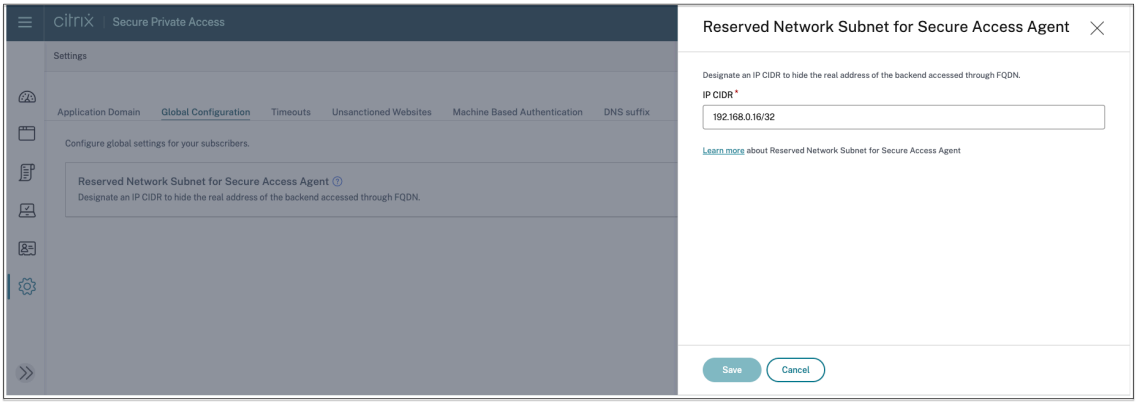
The following are the allowed reserved CIDR IP address ranges:

- 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

November 21, 2023

DNS suffix is a global configuration that is applied for all end users. The DNS suffix feature of the Citrix Secure Private Access service can be used for the following use cases:

- Enable the Citrix Secure Access client to resolve a non-fully qualified domain name (host name) to a fully qualified domain name (FQDN) by adding the DNS suffix domain for the back-end servers.
- Enable admins to configure applications using IP addresses (IP CIDR/IP range), so that the end users can access the applications using the corresponding FQDN under the DNS suffix domain.

For example, while resolving a non-fully qualified domain name “workday”, if the DNS suffix “citrix.net”is configured, the operating system appends the suffix “citrix.net”and resolves to “workday.citrix.net”.

If multiple DNS suffixes are configured, the DNS suffixes are resolved in a sequence. For example, assume that the following suffixes are added:

- `".citrix.net"`
- `".citrix.com"`
- `".xenserver.com"`

When an end user types “workday”, the operating system attempts to resolve the FQDNs in the following sequence. If it succeeds with one suffix, the remaining suffixes are skipped.

1. workday.citrix.net
2. workday.citrix.com
3. workday.xenserver.com

> **Important:**
>
> - DNS suffix configuration can only enable the client to resolve a non-fully qualified domain name by suffixing the domain configured using the DNS suffix feature. For an end user to access an FQDN under the DNS suffix domain, the admin must configure an application with an IP address, FQDN, or a wildcard domain. For details, see point 4 in Use case example.
> - If two different applications are configured, one with FQDN and another with IP address, both corresponding to the same back-end server), then the policy of the application with IP address takes higher precedence. For details, see point 5 in Use case example.

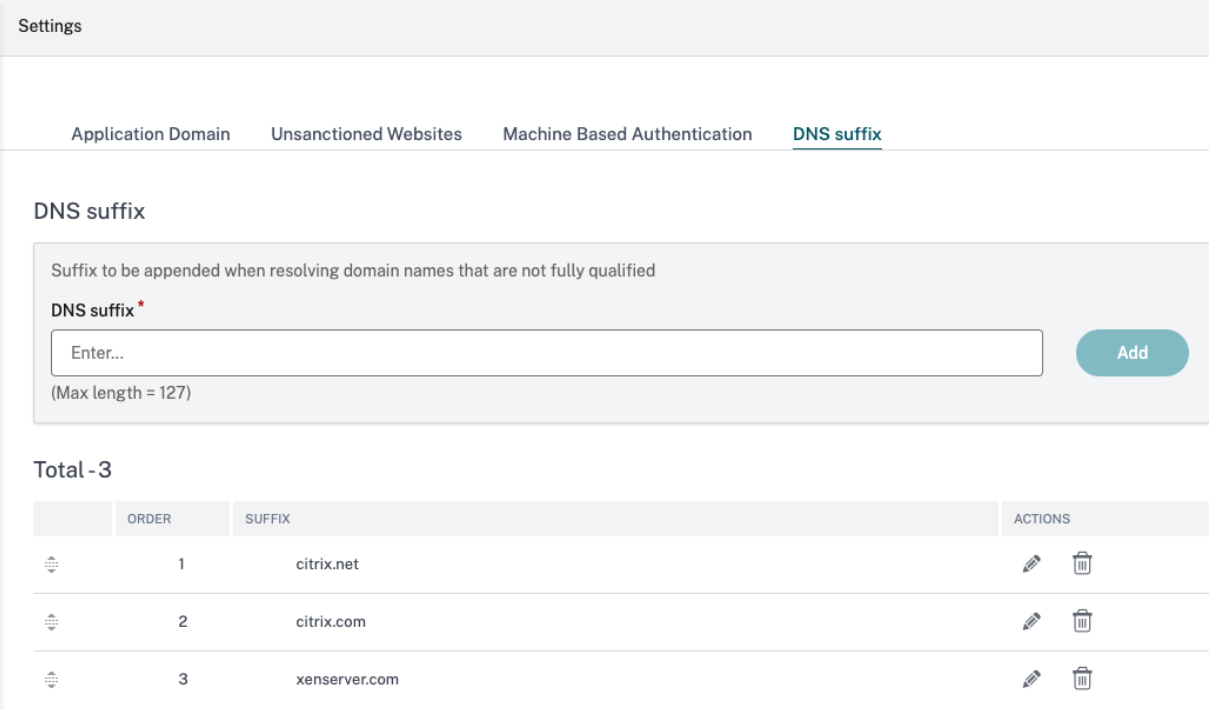
Prerequisites

> - Customers must be entitled to the Secure Private Access Advanced edition to use the DNS Suffix feature.
> - Contact the Citrix Product Management team to get the DNS suffix feature flags enabled.

How to add DNS suffixes

1. On the Secure Private Access tile, click **Manage**.
2. On the Secure Private Access landing page, click **Settings,** and then click **DNS suffix**.
3. In the **DNS Suffix** field, enter the suffix that must be appended when resolving a non-fully qualified name.
4. Click **Add**.

The suffixes are listed based on the order that they are added. Admins can delete or modify the suffixes.



Example use case

Consider the following:

- An admin has assigned the IP address 192.0.2.1 to a machine in the customer network.
- The FQDNs for the machine (with IP addresses 192.0.2.1) are under the domain “citrix.net”(example, workday.citrix.net).

	DNS suffix and app configuration	End-user experience
1	Admin configures the DNS suffix as “citrix.net”and creates an app with IP address 192.0.2.1 with an access policy set to “allow”for user1.	When user1 tries to connect to “workday”, the FQDN is suffixed with “citrix.net,” (workday.citrix.net) and the IP address is resolved to 192.0.2.1. Because 192.0.2.1 is allowed for user1 with an app configured, access is granted. **Note:** End user can access the Workday app with 192.0.2.1 or workday.citrix.net or “workday”. Without DNS Suffix configuration, access through “workday” and “workday.citrix.net” are denied.
2	Admin configures the DNS suffix as “citrix.net”, creates an app with FQDN (workday.citrix.net), and sets the access policy to “allow”for user1.	When user1 tries to connect to “workday”, “citrix.net”is suffixed to “workday” (workday.citrix.net). End user can access Workday because an application is configured with “workday.citrix.net” and the access policy is set to “allow”for user1.

		DNS suffix and app configuration	End-user experience
			Note: End user can access the Workday app with workday.citrix.net or “workday.” Access to 192.0.2.1 is denied as there is no app configured with this IP address.
	3	Admin configures the DNS suffix as “citrix.net”, creates an app with wildcard domain “*.citrix.net,” and sets the access policy to “allow”for user1.	When user1 tries to connect to “workday”, “citrix.net”is suffixed to “workday” (workday.citrix.net). End user can access Workday because an application is configured with “*.citrix.net”and the access policy is set to “allow”for user1. **Note:** End user can access Workday with workday.citrix.net or “workday”. Access to 192.0.2.1 is denied as there is no app configured with this IP address.

	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 (work-day.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.

Single sign-on to the Citrix Secure Access client via Citrix Workspace app

November 21, 2023

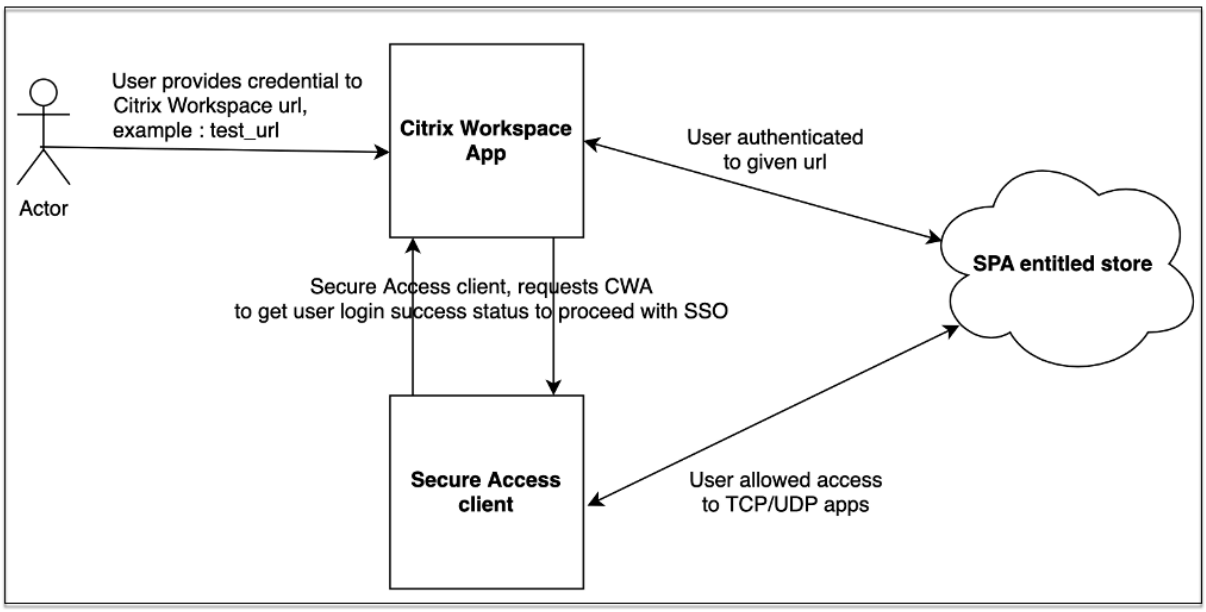
Citrix Secure Access client now supports single sign-on for the Workspace URL when already logged in via Citrix Workspace app. This SSO functionality enhances the user experience by avoiding multiple authentications.

Prerequisites

- Both the Citrix Workspace app and the Secure Access client must be installed on the device.
- Users must have logged into the Citrix Workspace app first for the automatic SSO to happen in the Citrix Secure Access client.

> **Note:**
>
> The single sign-on feature is only supported for the primary store that is configured in Citrix Workspace app. If the user logs into any other store other than the primary store, then SSO does not happen. The user has to manually log in to the Citrix Secure Access client.

The following figure displays the SSO flow between the Citrix Workspace app and the Citrix Secure Access client.



Feature requirements for Windows

- Citrix Workspace Application version - **Citrix Workspace 22.10.5.14(2210.5) or above**

- Citrix Secure Access version - **22.10.1.9 or later**
- Citrix Secure Access Windows Registry - **EnableCWASSO**

The SSO feature is disabled, by default. To enable this feature, add the following registry on the end-user machine.

- Registry Name - EnableCWASSO
- Registry Path - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\Secure Access Client
- Registry Type - REG_DWORD
- Registry Value - 1

> **Important:**
>
> Sometimes, the end user machines might need to reboot for successfully establishing single sign-on with Citrix Workspace app.

Terminate active user sessions and add users to the disabled user list

April 27, 2024

Admins can 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.

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. Blocked users cannot launch any new applications until they are removed from the disabled user list.

> **Note:**
>
> - Adding a user to the disabled user 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 is removed from the list, the existing Secure Private Acccess access policies for the user are reinstated.
> - Users are automatically removed from the disabled user list after 7 days.
> - 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 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 disabled user 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 to the disabled user list

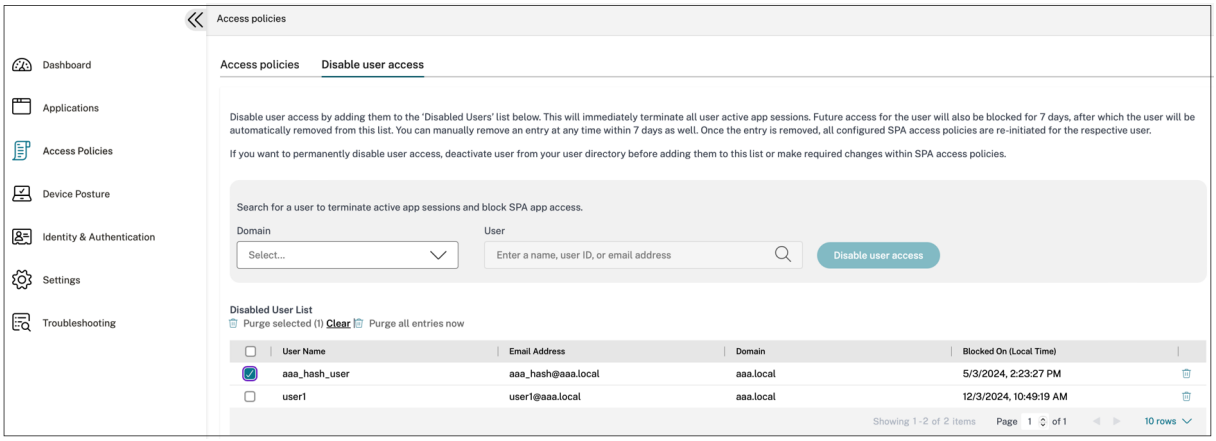
1. Navigate to **Secure Private Access > Access Policies** and then click the **Disable user access** tab.
2. In **Domain**, select the domain for which the access must be disabled.
3. In **User**, search for the user name that must be added to the disabled user list. All user names that match the search criteria are displayed. If the user is removed from the directory service, then that user name does not appear in the **User** list.
4. Click **Disable user access**.

   The user is added to the disabled user list. The following actions occur once the user is added to the disabled user list:

   - 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 disabled user list. Only access to published Secure Private Access applications is blocked.
   - All disabled users are automatically removed from the disabled user list after 7 days. After removal, Secure Private Access access policies take precedence and access is reinstated.

You can use the **Purge Selected** option to remove users from the disabled user list.

You can use the **Purge all entries now** option to remove all users from the disabled user list.



Recommendations:

- To revoke access for a user indefinitely, remove the user from your respective directory service, such as Active Directory, and then add them to the disabled user list. This terminates the user's active Secure Private Access session, blocks future app access, and once the user is logged out of Workspace, the user cannot log in again due to inactive directory credentials.
- The user is automatically removed from the disabled user list after 7 days, after which the existing Secure Private Access access policies are reinstated. If you want to extend blocking of access, then re-add the user to the list after 7 days.

Timeouts for user sessions

November 21, 2023

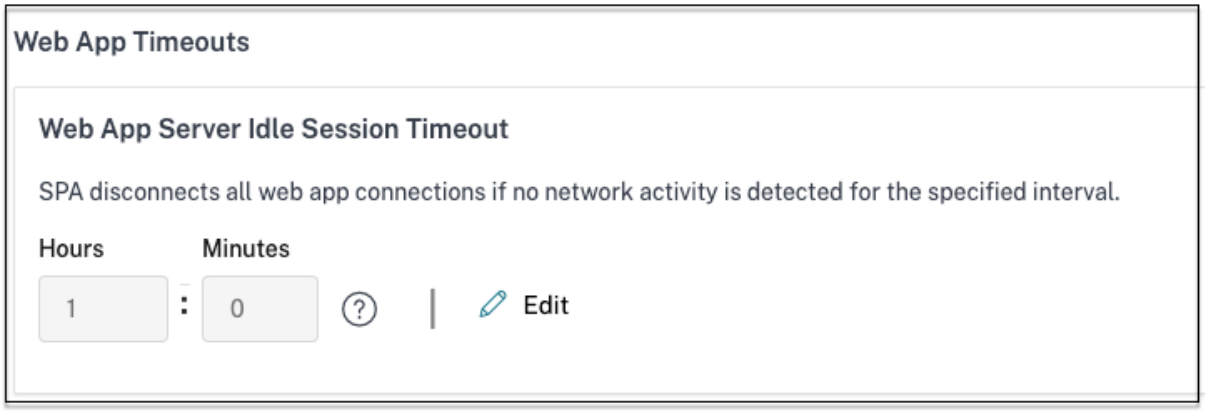
You can configure a timeout period for the Web apps and the Citrix Secure Access client to end user sessions if there is no network activity for the specified time period.
For the Citrix Secure Access client, you can also configure the Citrix Secure Access client to terminate a session if there is no user activity for that specified time period. Also, you can configure a forced disconnection on the Citrix Secure Access client regardless of the user and network activity, once the configured time period expires.

Timeout for the Web app servers

1. Navigate to **Settings > Timeouts**.
2. In **Web App Server Idle Session Timeout**, select the duration, in hours and minutes, for which the Web app session can be idle. The Secure Private Access service terminates the session after

this time expires if the session remains idle.

The minimum duration is 1 hour and the maximum duration can be 168 hours. Default value is 2 hours.

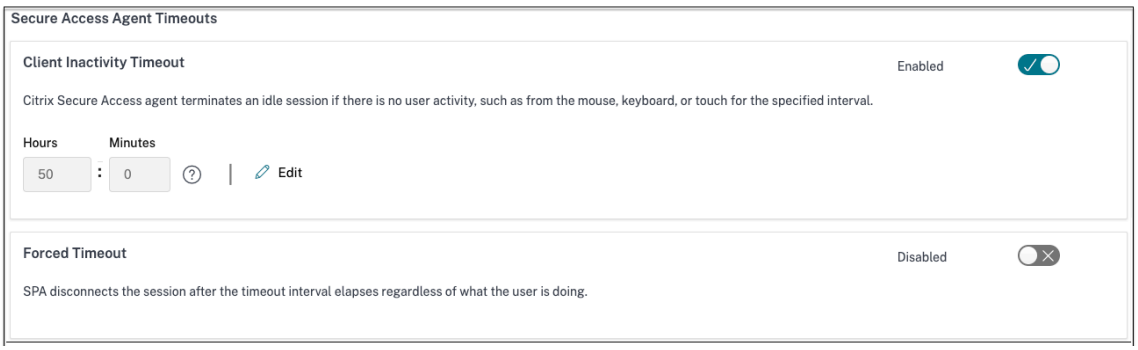


Timeouts for the Citrix Secure Access client

You can configure the following timeouts for the Citrix Secure Access client:

- Client inactivity
- Forced timeout

1. Navigate to **Settings > Timeouts**.



2. In **Secure Access Agent Timeout**, select the duration, in hours and minutes, for the timeout that you want to enforce.

   - **Client inactivity timeout**: The duration after which the Citrix Secure Access client terminates a session, if there is no user activity (mouse or keyboard) for the configured period. This option is disabled, by default. You must enable the option by using the toggle switch to enforce the configured timeout period. However, if you disable the toggle switch after the configuration is saved, the client does not initiate a timeout.

     The minimum duration is 5 minutes and the maximum duration can be 168 hours. Default value is 8 hours.

- **Forced timeout**: The duration after which the Citrix Secure Access client terminates a session irrespective of the user or network activity. This option is disabled, by default. You must enable the option by using the toggle switch to enforce the configured timeout period. However, if you disable the toggle switch after the configuration is saved, the client does not initiate a timeout.

  A notification message appears 15 minutes before the session termination.

  The minimum duration is 1 hour and the maximum duration can be 168 hours. Default value is 168 hours.

> **Note:**
>
> If you enable more than one of these settings, the first timeout interval to expire closes the user connection.

Migration of app security controls and access policies to the new access policy framework

November 21, 2023

Citrix has made changes to enabling application access in the product. Previously, applications needed to be subscribed to the users or user groups in the **Applications > App subscribers** section in the wizard to enable access. Going forward, at least one access policy is required to enable access to the applications. While creating the policies, the **Users or groups** condition is a mandatory condition to be met to grant access to the applications for the users. For details, see Create access policies.

Also, the **Enhanced Security** section in the application configuration is deprecated. You can now enforce granular security controls like clipboard restriction, download restriction, print restrictions in addition to advanced options like opening an app in the remote browser from Access Policies. With this change, customers can enforce adaptive security based on context like users, location, device, risk.

To migrate your apps' security controls and access policies to the new access policy framework and to avoid any downtime in the application access, Citrix has made the required changes. As a result, you might notice some changes in your policies list such as the following:

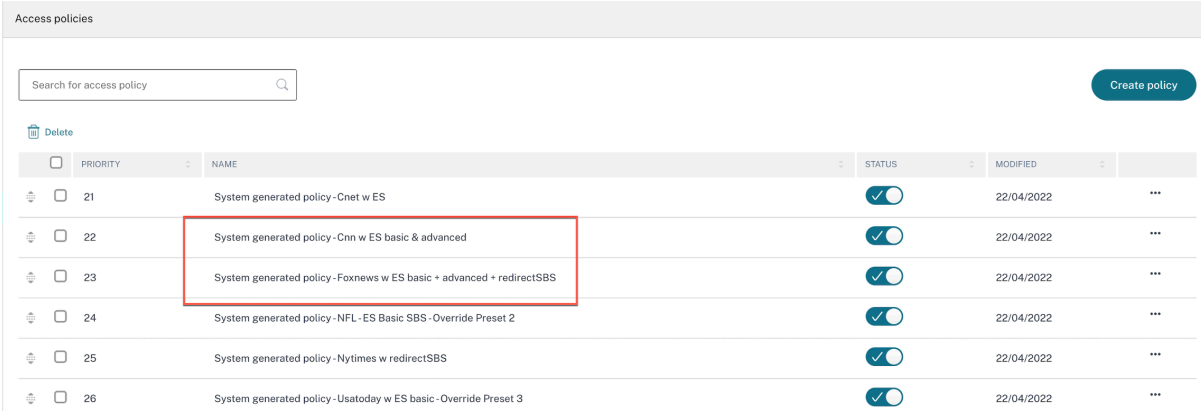
- New policies created
- A single policy split into multiple policies
- Policy names prefixed with `<System generated policy - App name>`

> **Note:**
>
> If the apps do not have users or groups added, then new policies are not created.

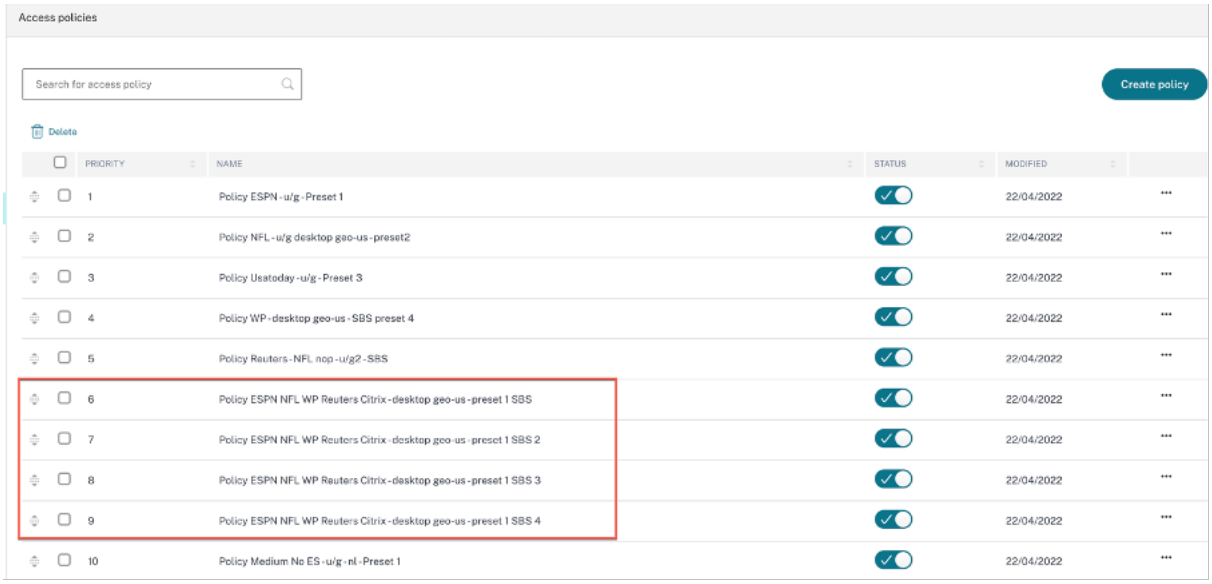
The following table summarizes the changes.

If you had configured an …	Then …
App without any enhanced security conditions	A new policy is created with users and groups as the mandatory condition. The users or groups is derived from the access policies. The action is set to **Allow Access**.
App with enhanced security conditions	A new policy is created with users and groups as the mandatory condition. The users or groups is derived from the access policies. The action is set is **Allow with restriction.** Based on the app level security condition configured earlier. The corresponding security restrictions are selected while creating the policy. The migrated policies are prefixed with `<System generated policy - App name>`.
Access policy with presets	If the policy already had a user group condition selected, then a new policy is created as-is and the corresponding security conditions are selected in the access policy based on the presets.
Access policy without user or group condition	As the users or groups is a mandatory condition to access the apps, a single policy that was configured for multiple apps is now split into multiple policies as each app might have different set of users or groups. The users or groups is derived from the access policies. For each policy, users or groups is set as a mandatory condition.

The following figure displays sample policy names prefixed with `<System generated policy - App name>`.



The following figure displays a sample of a single policy split into multiple policies.



Apps configuration using a template

November 21, 2023

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 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.

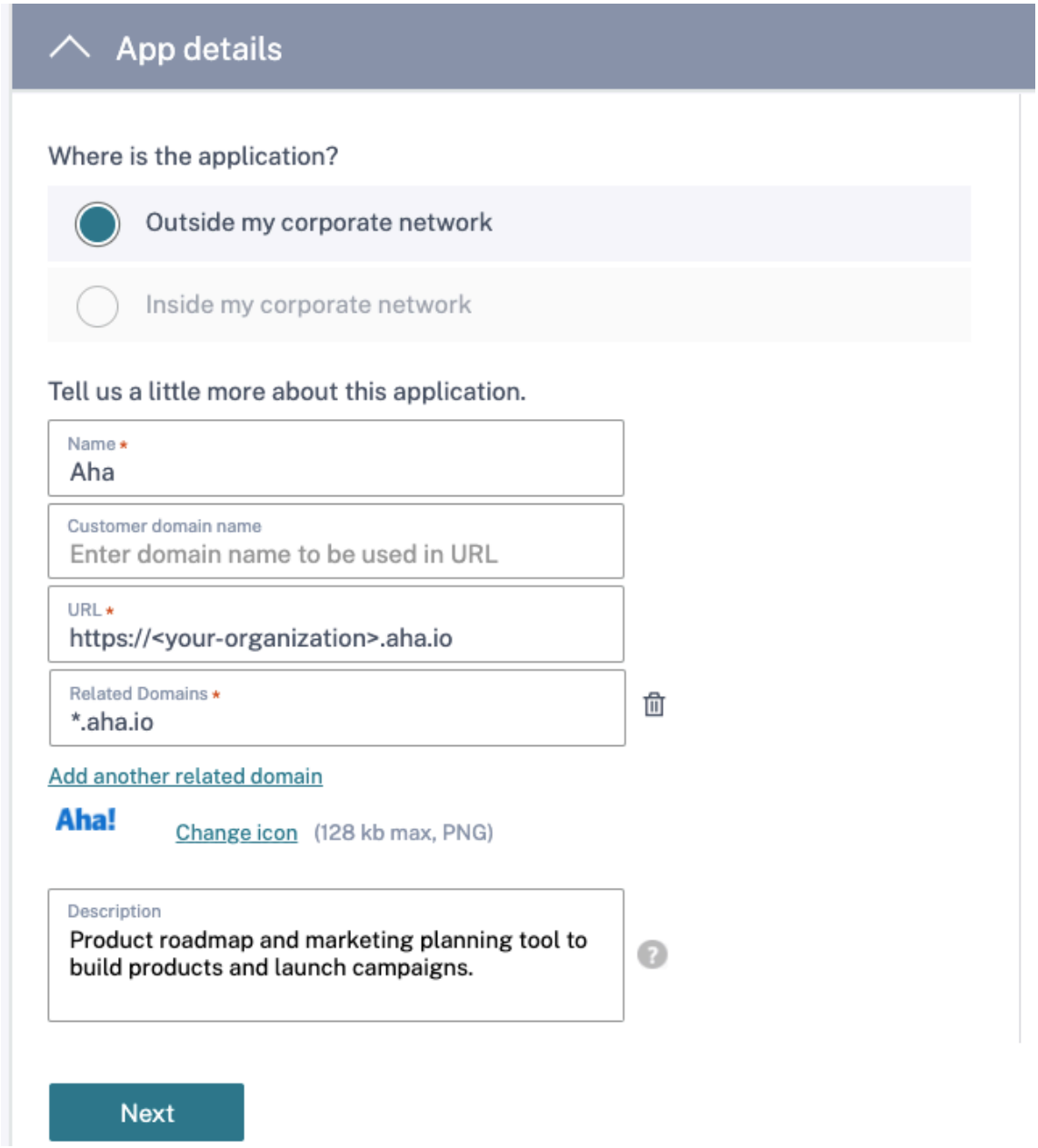
   Customer domain name and **Customer domain ID** - Customer domain name and ID are used to create an app URL and other subsequent URLs in the SAML SSO page.

   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.



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

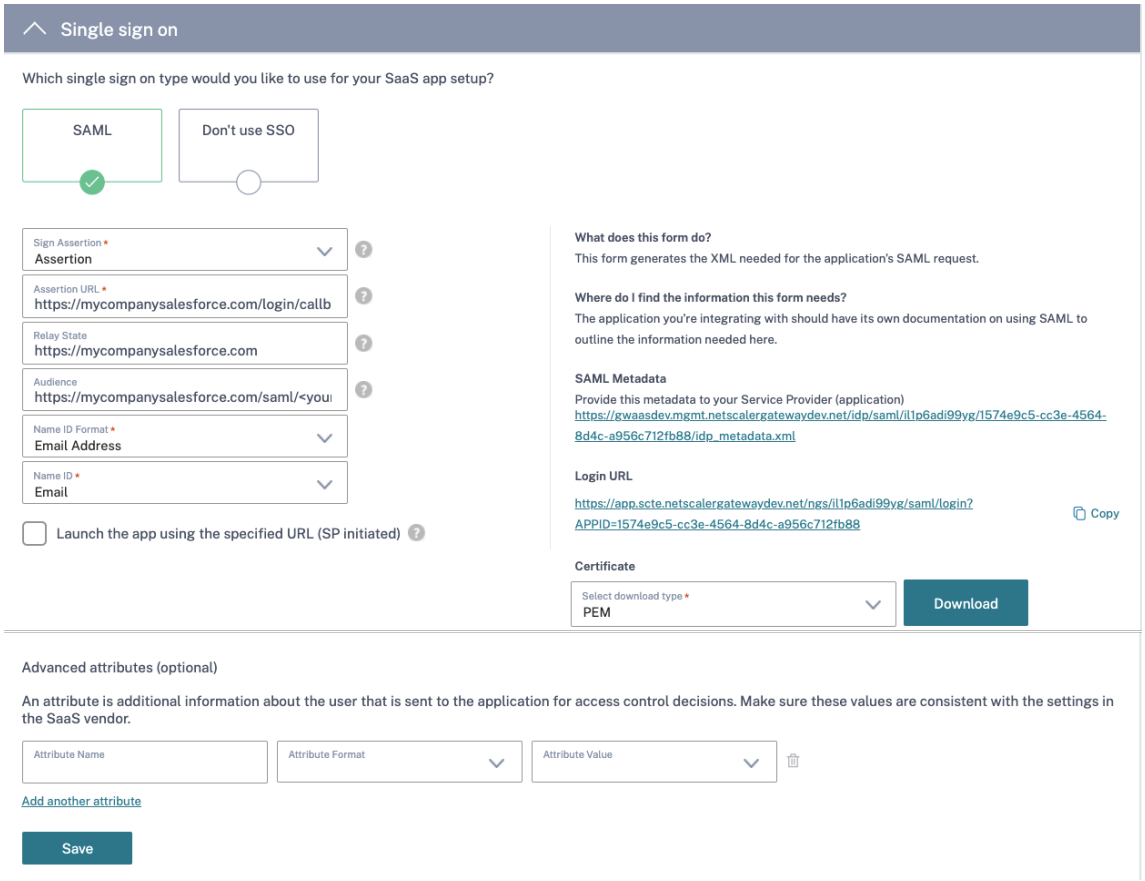
   Assertion URL –SaaS app SAML assertion URL provided by the application vendor. The SAML assertion is sent to this URL.

   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.



Note:

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

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

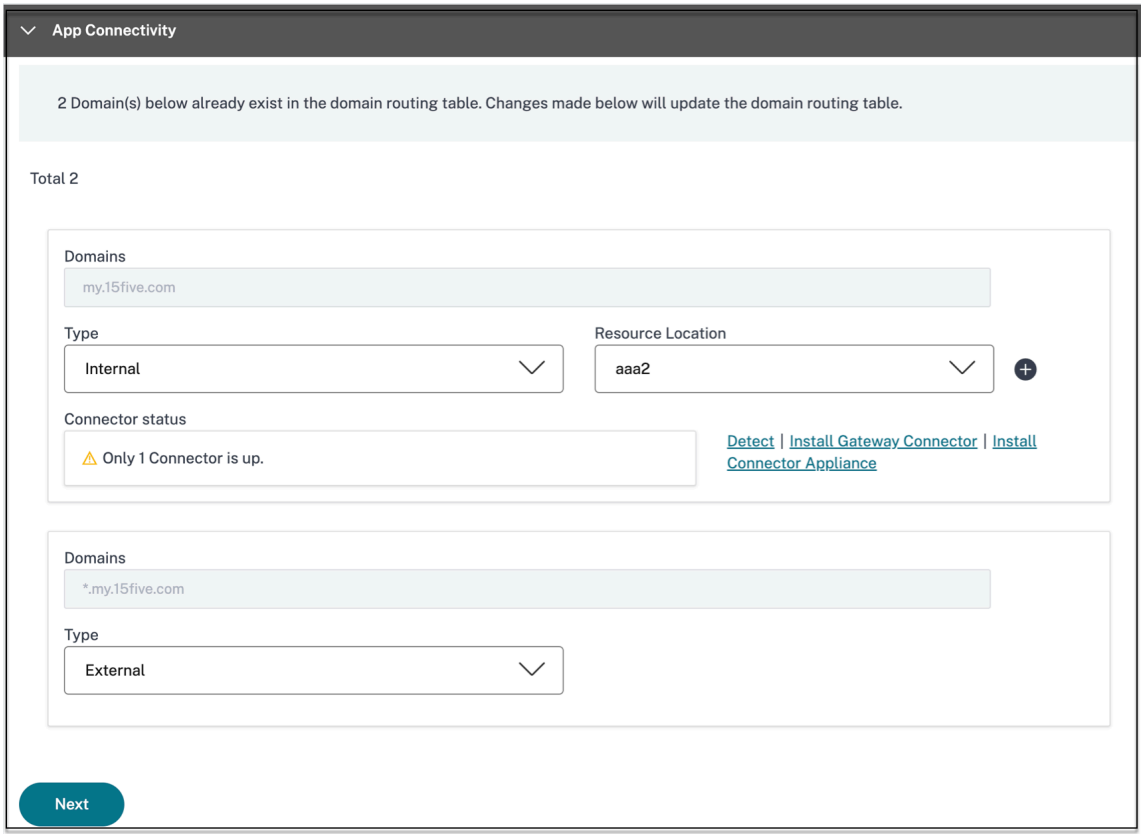
   Note:

   - 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.

6. Click **Next.**

7. 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 de-

tails, see Route tables to resolve conflicts if the related domains in both SaaS and web apps are the same.



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

November 21, 2023

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

- 15Five - Continuous performance management tool to coach employees.
- 10000 ft - Project management tool to plan for growth.
- 4me - Service management tool for collaboration between internal, external, and outsourced teams.
- Abacus - Real-time expense reporting software.
- Absorb - Learning management tool.
- Accompa - Requirements management tool to build products.
- Adobe Captivate Prime - Learning management system to deliver personalized learning experiences across devices.
- Aha - Product roadmap and marketing planning tool to build products and launch campaigns.
- AlertOps - Collaboration incidence response tool to manage IT incidents.
- Allocadia - Marketing performance management tool to manage an organization's marketing planning process.'
- Ana plan - Planning tool to help organizations with decision making by connecting data, people, and plans.
- &frankly - An engagement tool to drive change in the workplace.
- Anodot - An AI platform that monitors times series data, detects anomalies and forecasts business performance in real time.
- App Follow - Product management tool for accelerating global app growth and increasing customer loyalty.
- Assembla - Version control and source code management tool for software development.
- Automox - Patch management tool to track, control, and manage the patching process.
- Azendoo - Collaboration tool for teams to converse and collaborate.
- BambooHR - Human resources management tool to manage employee data.
- Bananatag - Tool to track and schedule emails, track files and create email templates
- Base CRM - Sales management tool to manage emails, phone calls, and notes.
- Beekeeper - Tool to integrate multiple operational systems and communication channels in one Secure Hub that is accessible from desktop and mobile devices.

- BitaBIZ - Absence and vacation planning and communication tool for leave and absence management.
- BlazeMeter - Testing suite.
- Blissbook - Policy management tool to create employee handbooks.
- BlueJeans - Video conferencing solution.
- Bold360 - Live chat tool for customer engagement.
- Bonusly - Employee recognition and reward management tool to recognize team contributions.
- Box - Content management and file sharing tool to manage, share, and access your content.
- Branch - A mobile linking platform powering deep links and mobile.
- Brandfolder - Digital asset management tool to store and share digital assets.
- Breezy HR - Recruiting software and applicant tracking system.
- Buddy Punch - Time management tool to monitor employee attendance.
- Bugsnag - Monitoring tool to manage application stability and report errors and diagnostic data.
- Buildkite - Infrastructure tool for continuous integration software development.
- Bullseye Locations - Store locator tool to locate a store or dealer on a device.
- CA Flowdock - Collaboration tool for teams to converse and collaborate.
- CakeHR - Human resources management tool for attendance and performance management.
- Cardboard - Collaborative product planning tool to track disorganized information.
- Citrix Cedexis - Traffic management tool for large websites to leverage multivendor sourcing of data centers, cloud providers, and content delivery networks.
- CipherCloud - Platform that provides an end-to-end data protection and advanced threat protection, and comprehensive compliance capabilities for an enterprise embracing cloud-based applications.
- Celoxis - Project management tool to create project plans, automate work and collaborate.
- CircleHD - Training, learning, and collaboration tool to share videos and slides within the organization.
- Circonus - Data analytics and monitoring tool to deliver alerts, graphs, dashboards, and machine-learning intelligence.
- Cisco Umbrella - Cloud security platform to provide the first line of defense against threats on the internet.
- Citrix RightSignature - A solution to get documents signed electronically.

- ClearSlide - Sales engagement tool to let users share content and sales material for customer interaction.
- Cloudability - Cloud cost management platform to improve visibility, optimization, governance across cloud environments.
- CloudAMQP - Message queue tool to pass messages between processes and other systems.
- CloudCheckr - Cost management, security, reporting, and analytics tool to help users optimize their AWS and Azure deployments.
- CloudMonix - Tool for cloud and on-premises resources monitoring and automation.
- CloudPassage - Visibility and continuous monitoring tool to reduce cyber risk and maintain compliance.
- CloudRanger - Tool to streamline your backups, disaster recovery, and server control for AWS Cloud.
- Clubhouse - Project management tool for software development.
- Coggle - Mind mapping web application to create hierarchically structured documents, like a branching tree.
- Comm100 - Customer service software and communication tool for customer service professionals.
- Confluence - Content collaboration tool to help teams collaborate and share knowledge.
- ConceptShare - Proofing tool to deliver content faster, quicker, and cheaper.
- Concur - Travel and expense management tool to manage expenses on the go.
- ConnectWise Control - Business management tool to provide remote support and access.
- Contactzilla - Contact management tool to access up to date contact information.
- ContractSafe - Contract management tool to track, store, and manage contracts.
- Contentful - Software for content to create, manage, and distribute content to any platform.
- Convo - Team communication and collaboration tool for internal conversations.
- Copper - CRM tool.
- Cronitor - Monitoring tool for cron jobs.
- Crowdin - Solution that provides seamless and continuous localization for developers.
- Dashlane - Password management tool that also manages digital wallets.
- Declaree - Travel and expense management tool for business travel.
- Dell Boomi - An integration tool to connect cloud and on-premises applications and data.

- Deskpro - Help desk tool to facilitate ticket management, customer self-help, and customer feedback.
- Deputy - Workforce management tool for scheduling and tracking employees'time, tasks, and communication.
- DigiCert - Certificate management and troubleshooting tool for SSL certificates for websites.
- Dmarcian - Email monitoring tool to filter spam, malware, and phishing.
- DocuSign - An online signature tool for different documents, such as insurance, medical, and real estate.
- DOME9 ARC - Security and compliance tool to manage public cloud environments.
- Dropbox - Cloud storage tool for secure file sharing and storage.
- Duo - Security tool to provide secure access to your applications.
- Dynatrace - Medical laboratory services.
- Easy Projects - Project Management tool.
- EdApp - Learning management tool for workspace learning.
- EduBrite - Learning management tool to create, deliver, and track training programs.
- Ekarda - Electronic card designing tool.
- Envoy - Visitor management tool to manage people and packages.
- Evernote - Application for note taking, organizing, task lists, and archiving.
- Expensify - Expense management tool for expense report management, receipt tracking, and business travel.
- ezeep - Print infrastructure management tool to print from any device, any location to any printer in the Cloud.
- EZOfficeInventory - Inventory management tool to track all your assets and equipment.
- EZRentOut - Equipment rental tool to track equipment quality and availability.
- Fastly - Edge cloud platform to serve and secure applications closer to the users.
- Favro - Planning and collaboration tool for organizational flow.
- Federated Directory - Cross-company contact directory tool to search through the corporate address books of different companies.
- Feeder
- Feedly - News aggregation tool to compile news feeds from different sources.

- FileCloud - Software solution that provides a robust and secure file hosting and sharing platform for organizations.
- Fivetran - Tool to help analysts replicate data into a cloud warehouse.
- Flatter Files - Digital flat file cabinet for drawings and documents to provide a secure and simple way for providing access to content.
- Float - Resource planning tool for project scheduling and managing the teams'utilization.
- Flock - Collaboration tool.
- Formstack - An online form builder and data collection tool.
- FOSSA - Automated open source license scanning and vulnerability management tools built natively into CI/CD.
- Freshdesk - Customer support tool to help support the needs of customers.
- Freshservice - IT help desk tool to simplify IT operations.
- FrontApp - Collaboration tool to manage all conversations in one place.
- Frontify - Platform to facilitate and streamline day-to-day branding, marketing, and development operations.
- Fulcrum - Mobile data collection platform that allows you to easily build mobile forms and collect data.
- Fusebill - Billing management and recurring billing software.
- G-Suite - Set of intelligent apps to connect the people in your company.
- GetGuru - Knowledge management software.
- GitBook - Tool to create and maintain your documentation.
- GitHub - A web-based hosting service for version control using Git for repositories hosted behind a corporate firewall.
- GitLab - A complete DevOps platform, delivered as a single application.
- GlassFrog - Software to Holacracy practice.
- GoodData - An embedded BI and analytics platform that provides fast, reliable, and easy to use analytics
- GotoMeeting - Online meeting software with HD Video Conferencing capabilities.
- HackerRank - Provides competitive programming challenges for consumers and businesses.
- HappyFox - Online help desk software and web based support ticket system.
- Helpjuice - Knowledge management solution to create and maintain knowledge bases.

- Help Scout - Customer service software and knowledge base tool for customer service professionals.
- Hello sign - E-signing interface to enable signing from anywhere, at any time, on any device.
- HelpDocs - knowledge base software to guide your users when they are stuck.
- Honeybadger - Application health monitoring tool.
- Harness - Tool for continuous delivery and integration for Java, .NET apps in AWS, GCP, Azure, and Bare Metal.
- HelpDocs - Tool to create an authoritative knowledge base to guide your users when they're stuck.
- Helpmonks - A collaborative email platform for team collaboration.
- Hoshinplan - Tool to visualize your strategic plans and track statuses in one canvas.
- Hosted Graphite - Tool to monitor your website, app, server, and container performance.
- Humanity - Online employee scheduling software to manage shifts, schedules, payroll, and time clocking.
- Igloo - Digital workplace and intranet solution provider to solve IT challenges across your organization.
- iLobby - Cloud-based visitor registration management solution.
- Illumio - Security system to prevent spread of breaches inside data center and cloud environments.
- Image Relay - Digital asset management and brand management software to securely organize and share digital files.
- Informatica - Tool for SaaS apps integration and a platform for developing and deploying custom integration services.
- Intelligent contract - Contract management software.
- iMeet Central - Project management software for marketers, creative agencies, and enterprise businesses.
- InteractGo - Tool to measure real-time and historical data on system performance.
- iQualify One - Learning and management tool to deliver authentic learning experiences.
- InsideView - Data and intelligence solutions to solve sales, marketing, and other business challenges.
- Insightly - A cloud-based customer relationship management (CRM) and project management tools for small and medium size businesses.

- ITGlue - A cloud-based IT documentation platform to help MSPs standardize documentation, create knowledge bases, manage passwords. and track devices.
- Jitbit - Help desk software and ticketing system to manage and track incoming support request emails and their associated tickets.

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

- Kanbanize - An online portfolio Kanban software for lean management.
- Klipfolio - An online dashboard platform for building powerful real-time business dashboards for your team or your clients.
- Jira - Tool to plan, track, and manage your issues and projects.
- Kanban Tool - Visual management software to improve your team performance and boost productivity.
- Keeper Security - Password manager and security software to protect your passwords and private information.
- Kentik - Tool to apply big data for network and performance monitoring, DDoS protection, and real-time ad-hoc network flow analytics.
- Kissflow - Workflow tool and business process workflow management software to automate your workflow process.
- KnowBe4 - Tool to provide security awareness training and simulated phishing.
- KnowledgeOwl - Knowledge base and authoring tool.
- Kudos - Retail, job, project, and fulfillment process systems.
- LaunchDarkly - Feature management platform to enable dev and ops teams to control the feature lifecycle.
- Lifesize - Video conferencing solution.
- Litmos - Learning management system for employee training, customer training, compliance training, and partner training.
- LiquidPlanner - Online project management software for your business.
- LeanKit - Lean-based, enterprise process and work management software to help enterprises visualize work, optimize processes, and deliver faster.
- LiveChat - Live chat and help desk software for businesses.
- LogDNA - Tool to collect, monitor, parse, and analyze logs from all sources in one centralized logging tool.

- Mango - Team collaboration software to consolidate and streamline siloed applications into one single platform.
- Manuscript - A writing tool to help you plan, edit, and share your work.
- Marketo - Automation software to help marketing teams master the art and science of digital marketing.
- Matomo - A Web analytics platform that evaluates the entire user-journey of everyone who visits the website.
- Meisterplan - Software that helps organizations create project portfolios.
- Mingle - Am agile project management and collaboration tool to provide a combined workplace for the entire team.
- MojoHelpdesk - Help desk software and ticketing system.
- Monday - Team management software to plan, track, and collaborate all your work in one tool.
- Mixpanel - System to track user interactions with web and mobile.
- MuleSoft - Integration software to connect SaaS and enterprise applications in the cloud and on-premises.
- MyWebTimesheets - Online time tracking system to track time spent on various projects/jobs/activities.
- New Edge - Secure application networking service for Hybrid IT.
- NextTravel - Corporate travel management software tool.
- N2F - Expense report management tool to manage your business and travel expenses.
- New Relic - Digital intelligence platform to measure and monitor the performance of applications and infrastructure.
- Nmbrs - Cloud HR and payroll software for businesses.
- Nuclino - Collaboration software to collaborate and share information in real-time.
- Office365 - Microsoft's cloud-based subscription service.
- OfficeSpace - 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 Apex recorder.
- Oracle ERP Cloud - Cloud-based software application suite to manage enterprise functions.
- Pacific Timesheet - Web-based timesheet tool for payroll, project hours, and expenses.
- PagerDuty - Digital operations management system.
- PandaDoc - A mobile app for iPhone users access to their documents, analytics, and dashboard directly on their mobile phones.
- Panopta - Infrastructure monitoring tool.
- Panorama9 - Cloud-based IT management platform for enterprise network monitoring.
- Papyrs - Editor to design your own intranet pages.
- ParkMyCloud - Single-purpose SaaS tool to connect to AWS, Azure Services, or GCP.
- Peakon - Tool to measure and improve employee engagement.
- People HR - HR software system for all key HR functions.
- Pingboard - Tool to build organization charts for organizing teams and workforce planning.
- Pigeonhole Live - Interactive Q&A platform.
- Pipedrive - Sales CRM and pipeline management software.
- PlanMyLeave - Leave management system for managing and tracking employee's leave of absence.
- PlayVox - Customer service quality monitoring tool.
- Podbean - Podcast service provider.
- Podio - A web-based tool to organize team communication, business processes, data, and content in project management workspaces.
- POPin - Crowd-solving platform and mobile app that operationalizes team engagement for problem-solving
- Postman - API development environment.
- Prescreen - Applicant tracking tool to publish job vacancies online and offline.
- ProductBoard - Product management tool.
- ProdPad - Product management software to develop product strategies.
- Proto.io - Application prototyping platform to create fully interactive, high-fidelity prototypes.
- Proxyclick - Cloud-based visitor management solution to manage visitors, build their brand image, and ensure the security.

- Pulumi - Cloud native development platform for containers, serverless, infrastructure, and Kubernetes.
- PurelyHR - Leave management tool for accessing employee leave data.
- Promapp - Business process management (BPM) tool.
- Prescreen - Cloud-based applicant tracking system to publish job vacancies online and offline.
- QAComplete - Software test management tool.
- Qualaroo - Feedback tool to gain insights from customers.
- Quality Built, LLC - Insurance, financial, and construction industry for providing reliable and innovative Third Party Quality Assurance Services.
- Qubole - Self-service platform for Big Data analytics built on Amazon.
- Questetra BPM Suite - Web-based business process platform for routine workflows.
- QuestionPro - Online survey software to create surveys and questionnaires.
- Quandora - Question and answer based knowledge management solution.
- Quip - Collaborative productivity software suite for mobile and the Web.
- Rackspace - Managed cloud computing services.
- ReadCube - Tool for web, desktop, and mobile reference management.
- RealtimeBoard - Whiteboard Collaboration tool for organizations to collaborate beyond formats, tools, locations, and time zones.
- Receptive - Tool to gather feedback from customers, teams, and the market at one place.
- Remedyforce - IT service management and help desk system.
- Retrace - An Application performance management tool that provides bug tracking, data aggregation, and automatic alerts.
- Robin - Workplace experience tools to schedule conference meeting rooms and desk bookings.
- Rollbar - Real-time error alerting and debugging tools for developers.
- Really Simple Systems - Cloud-based CRM software for small businesses to manage their sales and marketing.
- Reamaze - Customer support software to support, engage, and convert customers with chat, social, SMS, FAQ, and email on a single platform.
- Resource Guru - Resource management software to schedule people, equipment, and other resources.
- Retrace - Application performance management to integrate code profiling, error tracking, application logs, and metrics.

- Roadmunk - Product roadmap software and roadmap tool to create product roadmaps.
- Runscope - Tool to create, manage, and run functional API tests and monitors.
- Salesforce –CRM tool to manage customer contact information, integrate social media, and facilitate real-time customer collaboration.
- SalesLoft - Sales engagement platform for efficient and revenue-boosting sales
- Salsify - Product experience management (PXM) platform.
- Samanage - Tool for IT service management.
- Samepage - Collaboration software to manage online projects.
- Screencast-O-Matic –Tool to screencast and edit video.
- ScreenSteps –Tools to create visual documents centered on screen captures.
- SendSafely –Encryption platform for secure exchange of files and emails.
- Sentry - Open-source error tracking software.
- ServiceDesk Plus - Tool for IT service desk.
- ServiceNow - Cloud platform to create digital workflows.
- SharePoint –Collaborative platform used for document management and storage.
- Shufflrr - Presentation management tool to create, update, share, and broadcast presentations.
- Sigma Computing –An Analytics tool to explore, analyze, and visualize data.
- Signavio –A business process modeling tool.
- Skeddly - Tool to automate AWS resources.
- Skills Base - Talent management tool to track and document employee's performance and skills.
- Skyprep - Learning management system (LMS) to train customers and employees.
- Slack - Collaboration tool to communicate and share information.
- Slemma - Data analysis tool to create data reports from multiple data sets.
- Sli.do - Interaction tool for meetings, events, and conferences.
- SmartDraw - Diagram tool used to make flowcharts, organization charts, mind maps, project charts, and other business visuals.
- SmarterU - Learning management system (LMS) to train customers and employees.
- Smartsheet - Collaboration tool to assign tasks, track project process, manage calendars, and share documents.

- SparkPost - Email delivery service.
- Split - Bill splitting application.
- Spoke - Service desk tool to file service tickets.
- Spotinst - A SaaS optimization platform that helps companies purchase and manage cloud infrastructure capacity.
- SproutVideo - Platform to host business videos.
- Stackify - Troubleshooting tool that provides support with a suite of tools including Prefix and Retrace.
- StatusCast - Hosted page to keep your employees and customers aware about downtime and website maintenance.
- StatusDashboard - Communications platform for hosting status dashboards and broadcasting incident notifications to customers.
- Status Hero - Tool for tracking status updates and daily goals from your team.
- StatusHub - Platform to host the service state page.
- Statuspage - Tool to communicate status and incidents.
- SugarCRM - CRM tool for Salesforce automation, marketing campaigns, customer support, collaboration, Mobile CRM, Social CRM, and reporting.
- Sumo Logic - Data analytics software that focuses on security, operations, and BI use cases.
- Supermood - HR platform to gather employee's feedback in real-time.
- Syncplicity - Tool to share and synchronize files.
- Tableau - Tool to create interactive data visualization.
- TalentLMS - Learning management system (LMS) to facilitate online seminars, courses, and other training programs.
- Tallie –Tool to capture and upload receipts, generate expense reports, and customize expense details.
- Targetprocess - Agile project management software to Scrum, Kanban, SAFe, and so on.
- Teamphoria - Software to provide real-time employee engagement metrics, employee reviews, and recognition.
- TeamViewer - Proprietary software application for remote control, desktop sharing, online meetings, web conferencing, and file transfer between computers.
- Tenable.io - Tool that provides data to identify, investigate, and prioritize the remediation of vulnerabilities and misconfigurations in your IT environment.

- Testable - Tool to create behavioral experiments and surveys.
- TestingBot - Tool to provide various browser versions for live and automated testing.
- TestFairy - Mobile testing platform, to provide companies with video recordings, logs, and crash reports of mobile sessions.
- TextExpander - Communication tool to insert snippets of text from a repository of emails, and other content, as you type.
- TextMagic - Messaging service to connect with customers.
- ThousandEyes - Tool to monitor network infrastructure, troubleshoot application delivery, and map internet performance.
- Thycotic Secret server - Account management software tool to manage passwords.
- TimeLive –Tool to provide timesheets and track time.
- Tinfoil Security - Security solution software to check for vulnerabilities.
- Trisotech - Tool that allows customers to discover, model, analyze their digital enterprise.
- Trumba - Tool to publish online, interactive, calendars of events.
- TwentyThree - Video marketing platform to integrate and add videos to the marketing stack.
- Twilio - A developer platform for communications.
- Ubersmith - Business management software for usage-based billing, quoting, order management, infrastructure management, and help desk ticketing solutions.
- UniFi - Communication and collaboration software with voice, web collaboration, and video conferencing capabilities.
- UPTRENDS –Website monitoring solution to track website uptime and performance.
- UserEcho - Community forum tool that helps businesses manage customer feedback.
- UserVoice - Product feedback management software to enable businesses to make data-driven product decisions.
- VALIMAIL - Email authentication software to authenticate legitimate emails and block phishing attacks.
- Veracode - Source code analyzer and code scanner protect enterprises from cyber threats and application backdoors.
- Velpic - Learning management system (LMS) designed to streamline workplace training.
- VictorOps - Incident management software to provide DevOps observability, collaboration, and real-time alerting.
- VIDIZMO - Enterprise live and on-demand video streaming software.

- Visual Paradigm - Visual modeling and diagramming online platform for team collaboration.
- Vtiger - CRM tool that enables sales, support, and marketing teams to organize and collaborate.
- WaveMaker –Software for building and running custom apps.
- Weekdone - Tool to create managers'dashboard and team management service for companies.
- Wepow - Tool to connect recruiters, job candidates, and employers through 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.

Launch a configured app - end user workflow

November 21, 2023

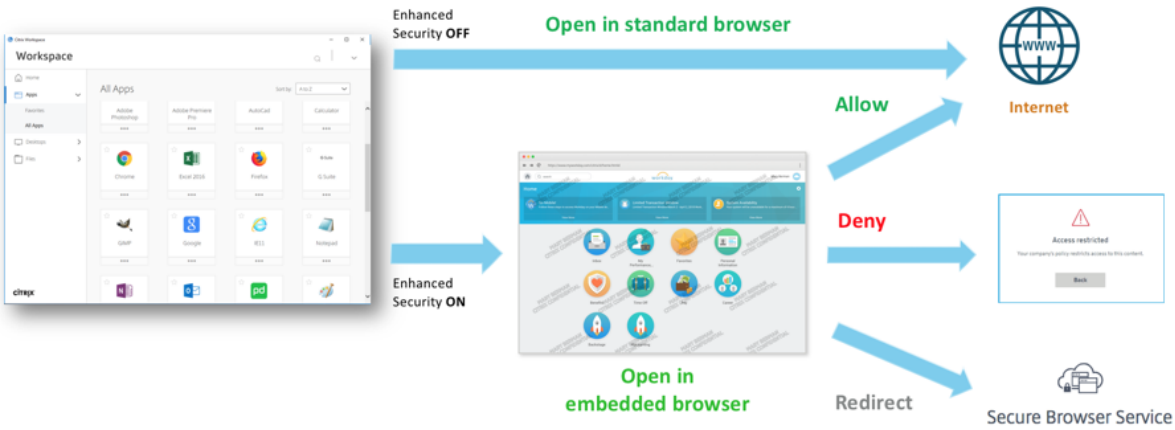
As an end user, you must do the following:

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

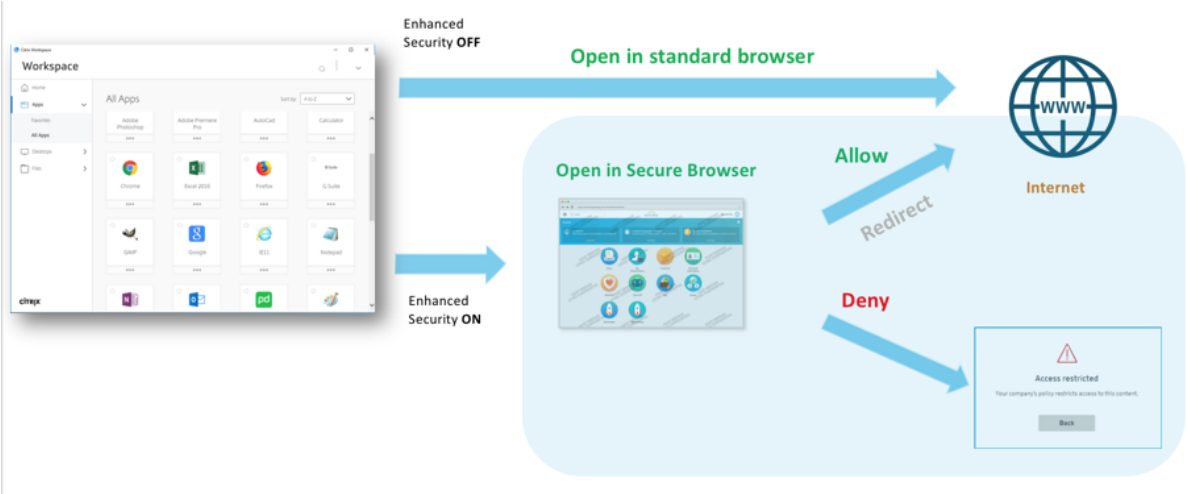
You can now use the SaaS app from within the Citrix Workspace app or from the Citrix Workspace web portal.

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.



Read-only access for admins to SaaS and Web apps

November 21, 2023

Organizations usually comprise multiple administrators and admins must be provided with different levels of access privileges. Security admin teams using the Secure Private Access service can provide granular controls, such as read-only access to admins. Administrators who do not add or modify an app can be provided with read-only access to view the app details. Secure Private Access service admins with read-only access cannot perform the following tasks.

- Add Enterprise Web or SaaS apps.
- Add new Connector Appliances in existing or new resource locations.

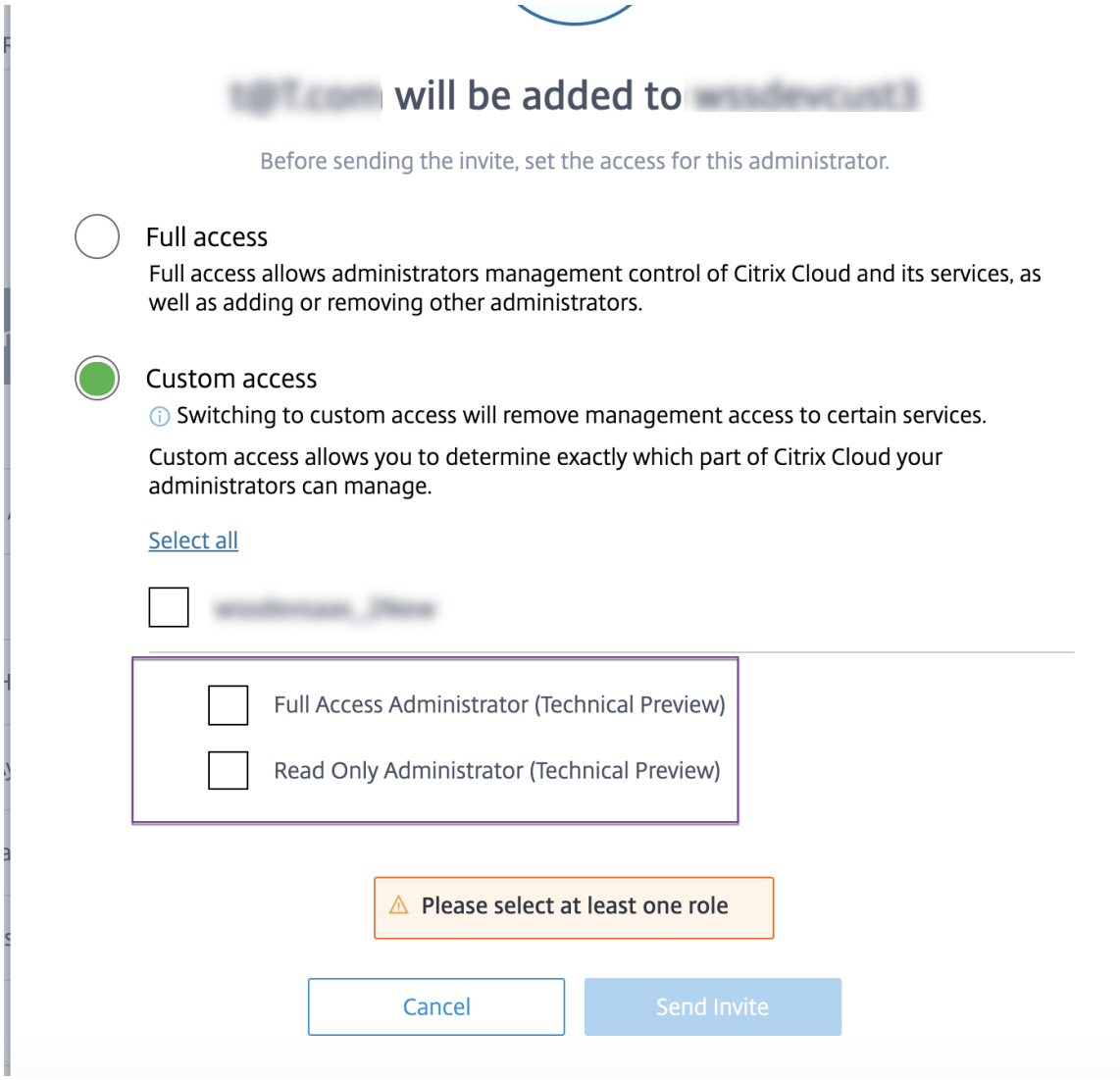
How to provide read only access to admins

After signing in to Citrix Cloud, select **Identity and Access Management** from the menu.
On the Identity and Access Management page, click **Administrators**. The console shows all the current administrators in the account.

Add an administrator with read only access

1. In **Add administrators**, 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).
2. If **Citrix Identity** is selected, enter the user's email address and then click **Invite**.

3. If Azure Active Directory is selected, type the name of the user you want to add and then click Invite.
4. Select **Custom access**. The following options appear:
   - **Select Full Access Administrator (Technical Preview)** –Provides full access.
   - **Read Only Administrator (Technical Preview)** –Provides read-only access.
5. Select **Read Only Administrator (Technical Preview)**.



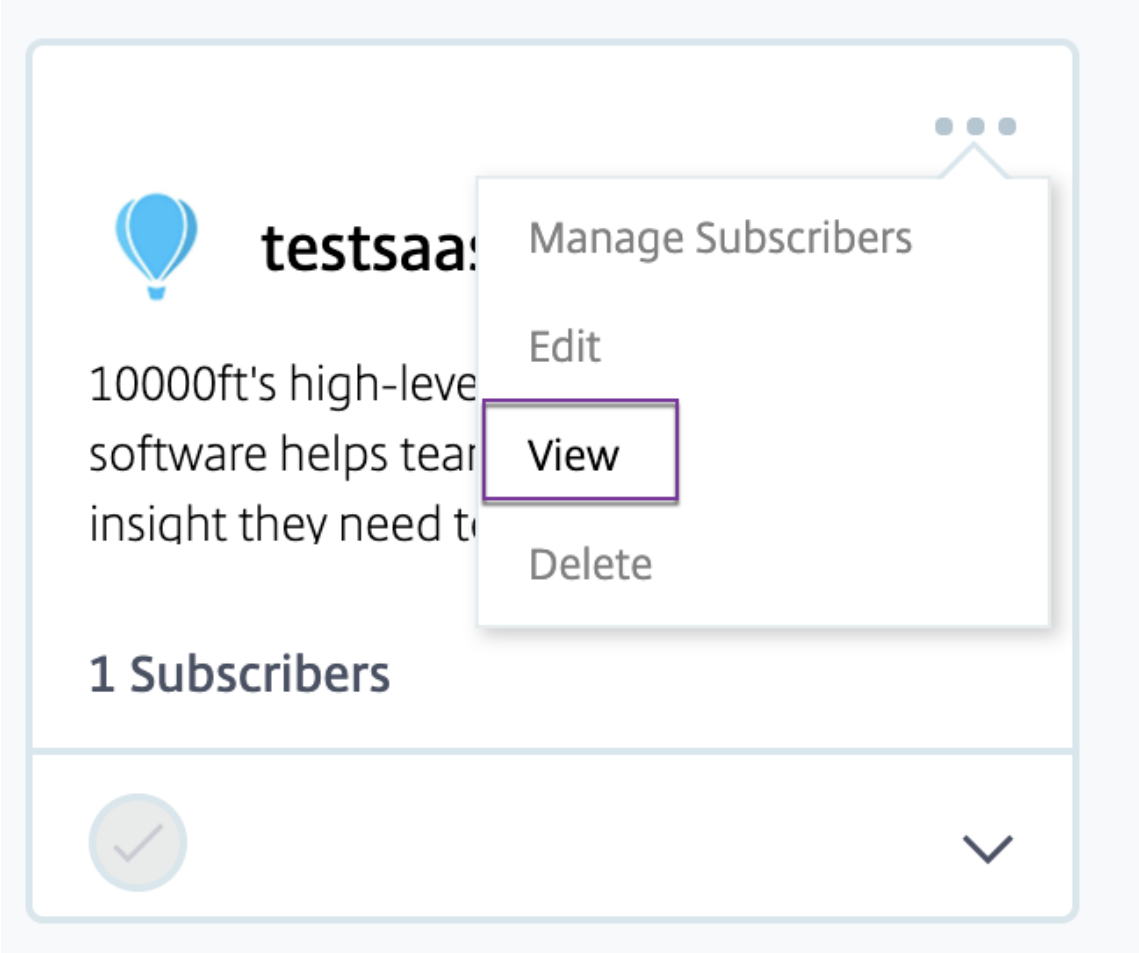
6. Click **Send Invite**.

> **Important:**
>
> - When you provide **Read Only Administrator** access to Citrix Gateway Service admins, you must also enable **Library** from the **General Management** list for those admins. Only then the **View** option for the apps is enabled for the admins.

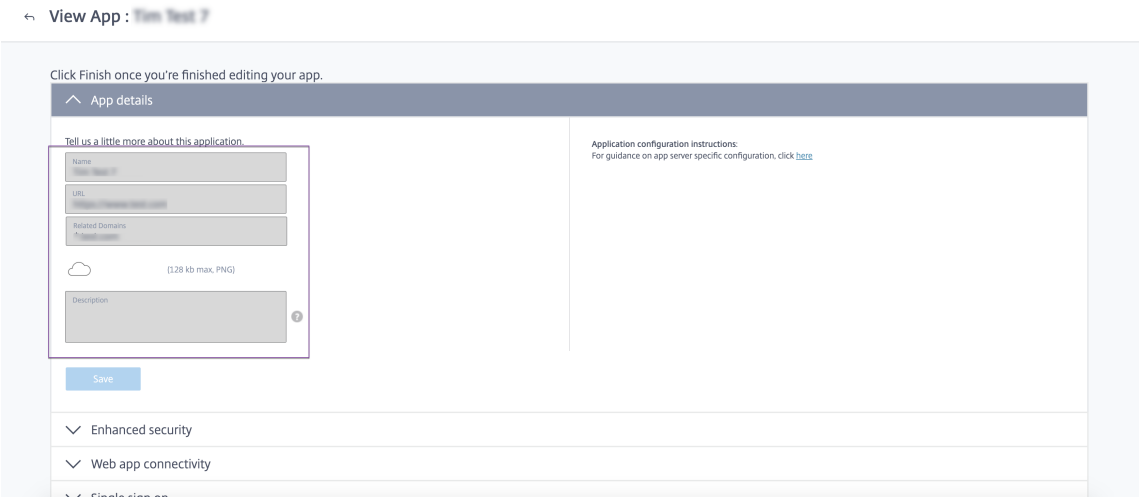
> - The **Add a Web/SaaS App** button is disabled for users with **Read Only Administrator** access.

To view the app details when admins have read only access

1. After signing in to Citrix Cloud, select **Library** from the menu.
2. Select the app that you want to view the details and click the **ellipsis**.
   Only the **View** option is enabled. All other options are disabled.



3. Click **View**.



Best practices for Web and SaaS application configurations

April 17, 2024

Application access for published and unpublished apps is dependent 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	`https://app.intranet.local`	*.cdn.com
Wiki	`https://wiki.intranet.local`	*.intranet.local

Policy name	Priority	User and associated apps
PolicyA	High	Eng-User5 (Intranet)
PolicyB	Low	HR-User4 (Wiki)

If `HR-User4` accesses `app.intranet.local`, then the following happens:

a) Secure Private Access searches all policies for an exact match for the domain being accessed, `app.intranet.local` in this case.
b) Secure Private Access finds `PolicyA`, and checks if the conditions match.
c) As the conditions do not match, Secure Private Access stops here and does not continue to check the wildcard matches, even though `PolicyB` would have matched (since `app.intranet.local` does match on the Wiki app's related domain of `*.intranet.local`) and given access.
d) Hence `HR-User4` is denied access to the Wiki app.

Example 2: Consider the following apps and policy configuration where same domain is used in multiple applications:

Application	Application URL	Related domain
App1	xyz.com	app.intranet.local
App2	app.intranet.local	-

Policy name	Priority	User and associated apps
PolicyA	High	Eng-User5 (App1)
PolicyB	Low	HR-User7 (App2)

When user `Eng-User5` accesses `app.intranet.local`, both App1 and App2 will be a match based on the exact FQDN match and hence `Eng-User5` user gets access through `PolicyA`.

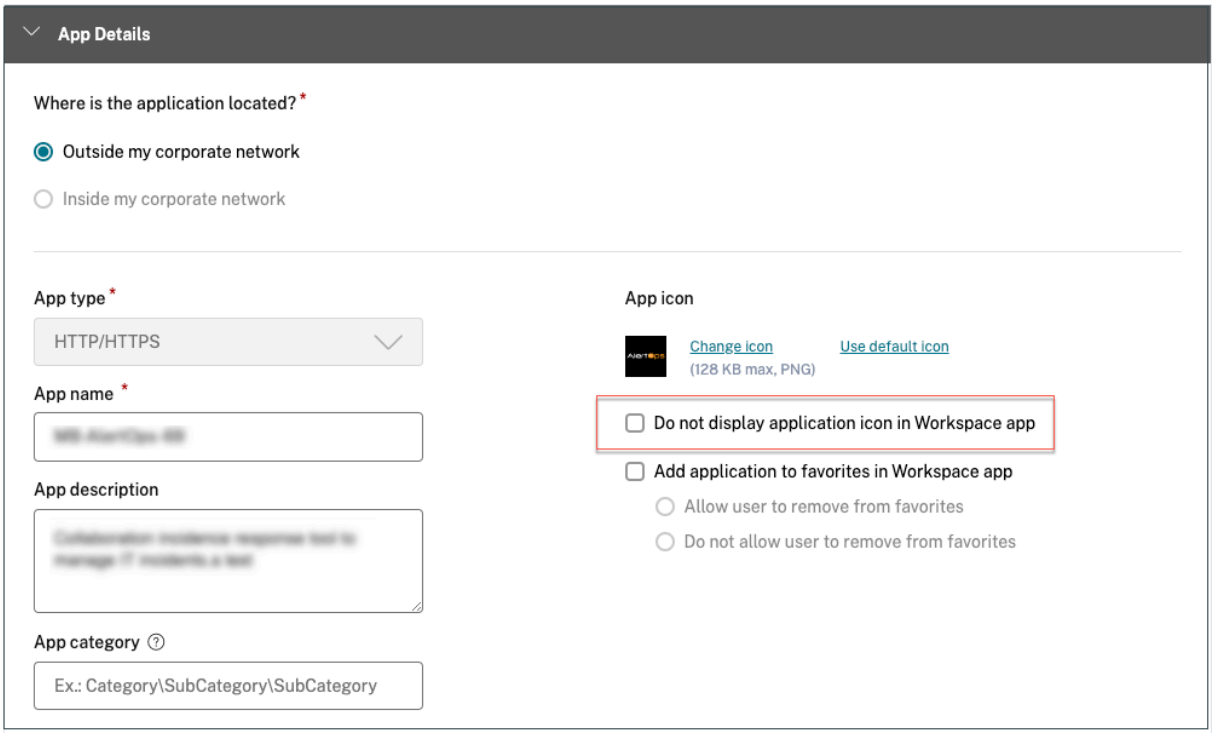
However, if App1 had `*.intranet.local` as a related domain instead, then the access for `Eng-User5` would have been denied since `app.intranet.local` would have exact-matched `PolicyB`, for which the user, `Eng-User5`, does not have access.

App configuration best practices

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 app configuration so that it does not enumerate on workspace. For information, see Configure application details.



> **Note:**
>
> This app configuration only enables access to the IDP authentication page. Further access to individual applications still depends on the individual app configurations and their respective access policies.

Example configuration:

1. Configure all common FQDNs into their own apps, grouping them together where applicable.

   For example, if you have a few apps that use Azure AD as an IdP and you need to configure `login.microsoftonline.com` and other related domains (`*.msauth.net`), then do the

following:

- Create a single common applciation 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 unique related domain to be configured within a single app.

Incorrect configuration examples:

- **Example: Duplicate related domains across multiple applications**

  Assume you have 2 apps where both need access to Okta (example.okta.com):

App	application URL domain	Related domain
App1	`https://code.example.net`	example.okta.com
App2	`https://info.example.net`	example.okta.com

Policy name	Priority	User and associated apps
Deny App1 to HR	High	User group HR for App1
Grant Everyone access to App1	Medium	Enable access to user group Everyone to App1
Grant Everyone access to App2	Low	Enable access to user group Everyone”to App2

Problem with the configuration: Although the intent was to give all users access to App2, the user group HR cannot access App2. The user group HR gets redirected to Okta but is stuck based on the first policy that denied access to App1 (which also has the same related domain `example.okta.com` as App2).

This scenario is very 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 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 should be set accordingly.
- Admins must evaluate if this shared related domain needs to 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.

Deep-link URLs

For deep-link URLs, the intranet application URL domain must be added as the related domain:

Example:

Intranet app has URL is configured with `https://example.okta.com/deep-link-app-1` as the main application URL domain and the related domain has the intranet application URL domain i.e `*.issues.example.net`.

In this case, separately create an IdP app with URL `https://example.okta.com` and then related domain as `*.example.okta.com`.

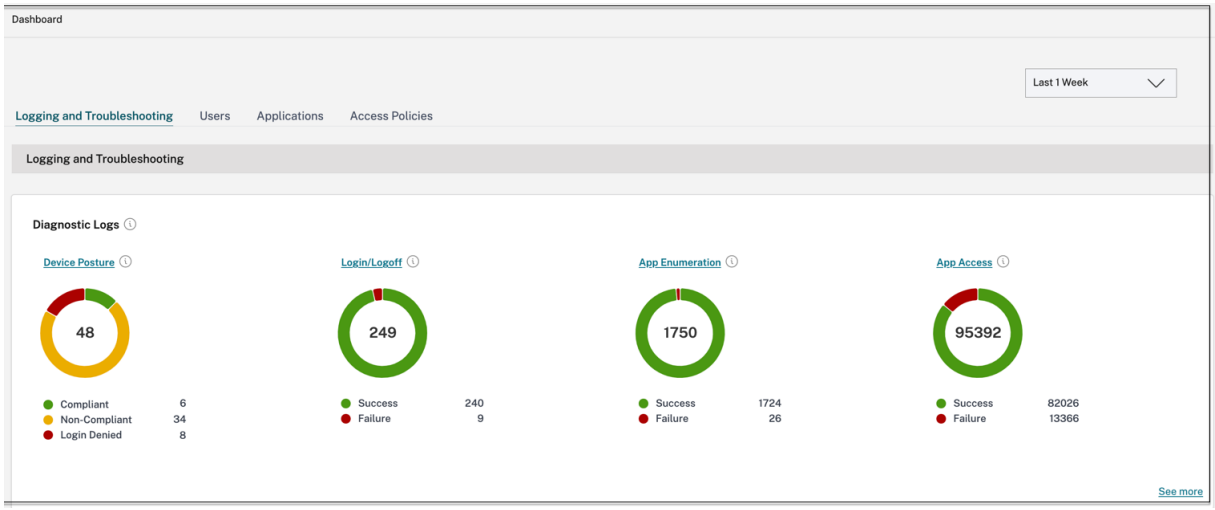
Diagnostic logs

June 10, 2024

The Secure Private Access service dashboard displays the diagnostics and usage data of the SaaS, Web, TCP, and UDP apps. Use the **Diagnostics Logs** chart to view the logs related to authentication, application launch, app enumeration, and also logs related to device posture. You can click the **See more** link to view the details of the logs. The details are presented in a tabular format. You can view the logs for the pre-set time or for a custom timeline. You can add columns to the chart by clicking the + sign depending on what information you want to see in the dashboard. You can export the user logs into CSV format.

- You can use the **Add Filter** option to refine you search based on the various criteria such as app type, category, description. For example, in the search field, you can click `Transaction ID`, `= (equals to some value)`, and enter `7456c0fb-a60d-4bb9-a2a2-edab8340bb15`, to search for all logs related to this transaction ID. For details on search operators that can be used with the filter option, see Search operators.
- **Device posture logs:** You can refine your search based on the policy results (**Compliant, Non-compliant, and login Denied**). For details on device posture, see Device Posture.

> **Note:**
>
> - Every failure event within the Secure Private Access diagnostic logs dashboard has an associated info code. For details, see Info code.
> - Transaction ID correlates all Secure Private Access logs for an access request. For details, see Transaction ID.



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.

Audit logs

January 29, 2024

Secure Private Access service related events are now 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 the System Logs. The admin events can be, but not limited to, the following:

- Configuring a Web or a SaaS app
- Subscribing an app
- Deleting an app
- Configuring an adaptive access policy

The following figure displays the Secure Private Access related events in the **System Log**. For details such as exporting events, retrieving events for a specific time period, forwarding log events, and data retention, see System Log.

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

April 27, 2024

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 the following security restrictions:

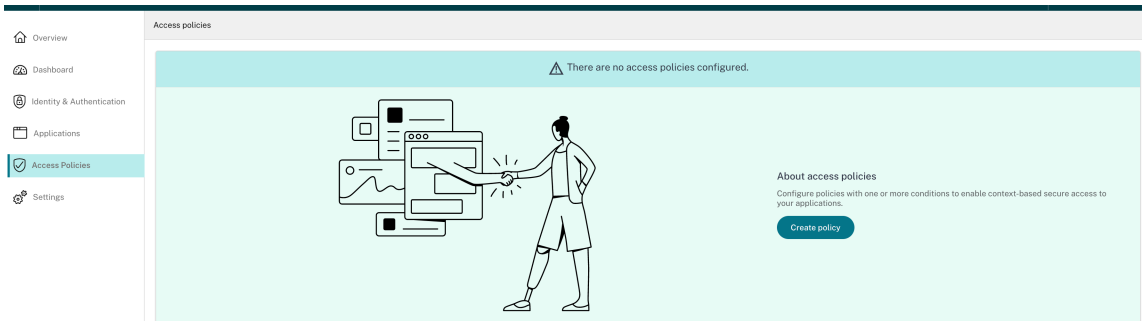
- Restrict clipboard access
- Restrict printing
- Restrict downloads
- Restrict uploads
- Display watermark
- Restrict key logging
- Restrict screen capture

For more information on these restrictions, see Available access restrictions options.

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

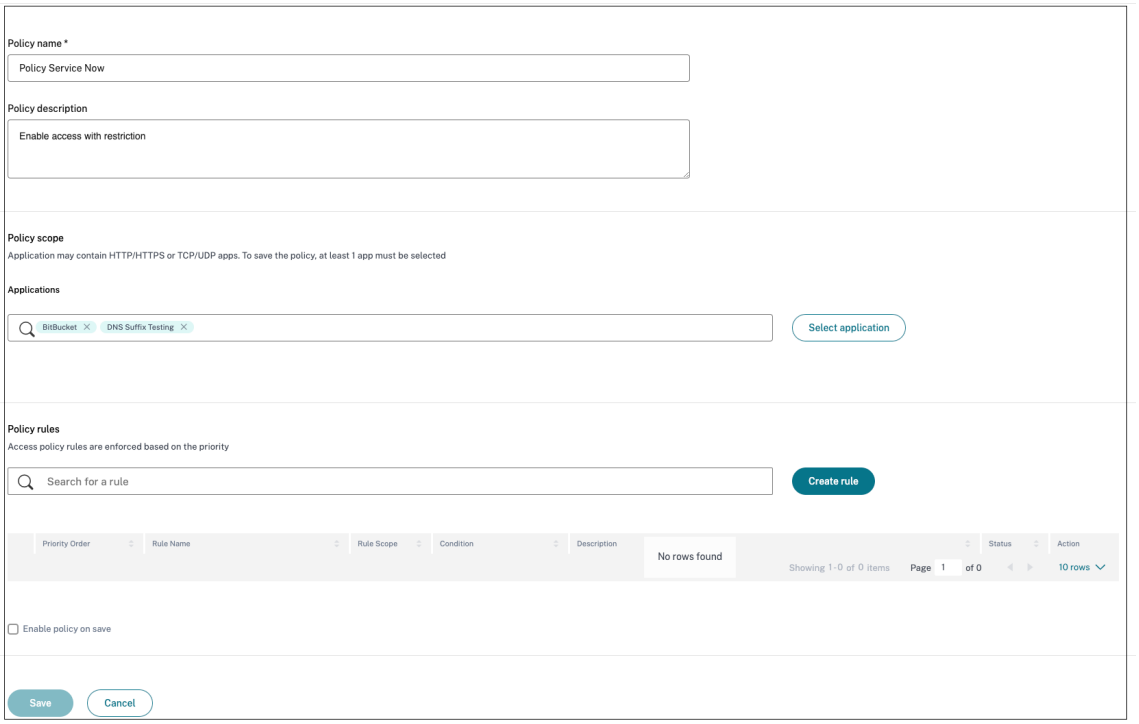
- Set up identity and authentication
- Configured applications

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

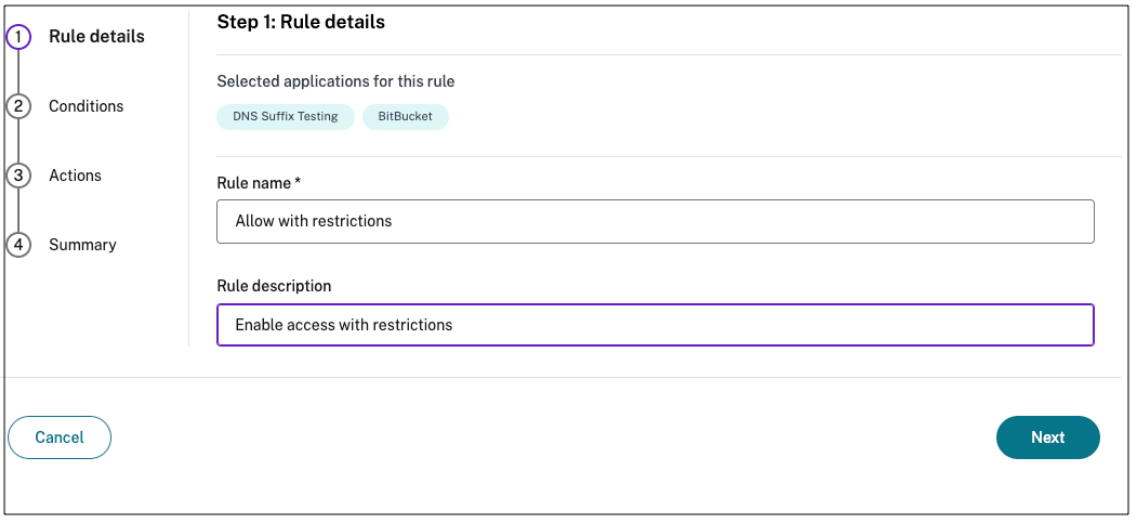


For the first-time users, the **Access Policies** landing page does not display any policies. Once you create a policy, you can see it listed here.

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.

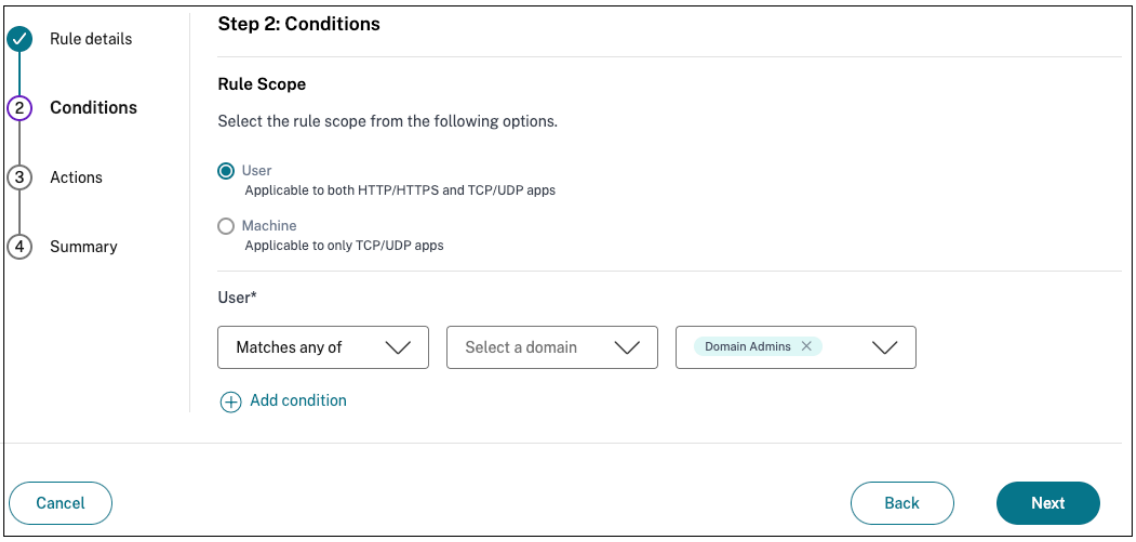


5. Enter the rule name and a brief description of the rule, and then click **Next**.



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



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.

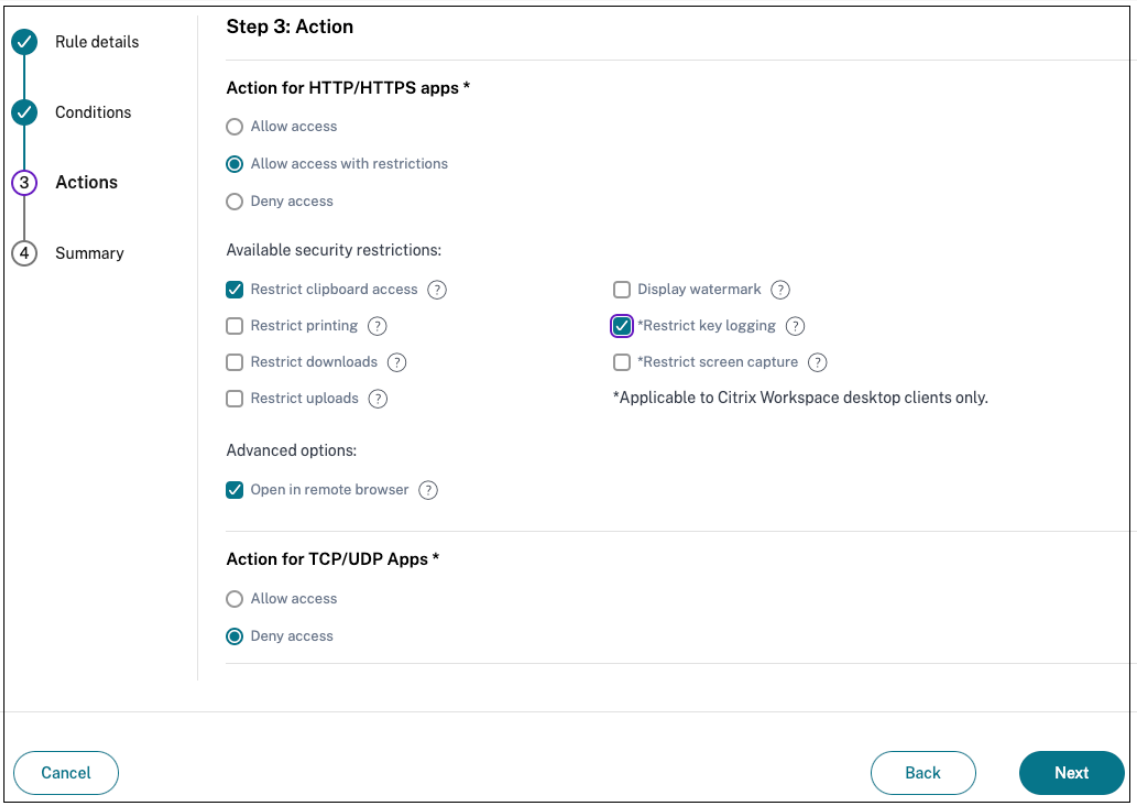
8. Click **Next**.

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

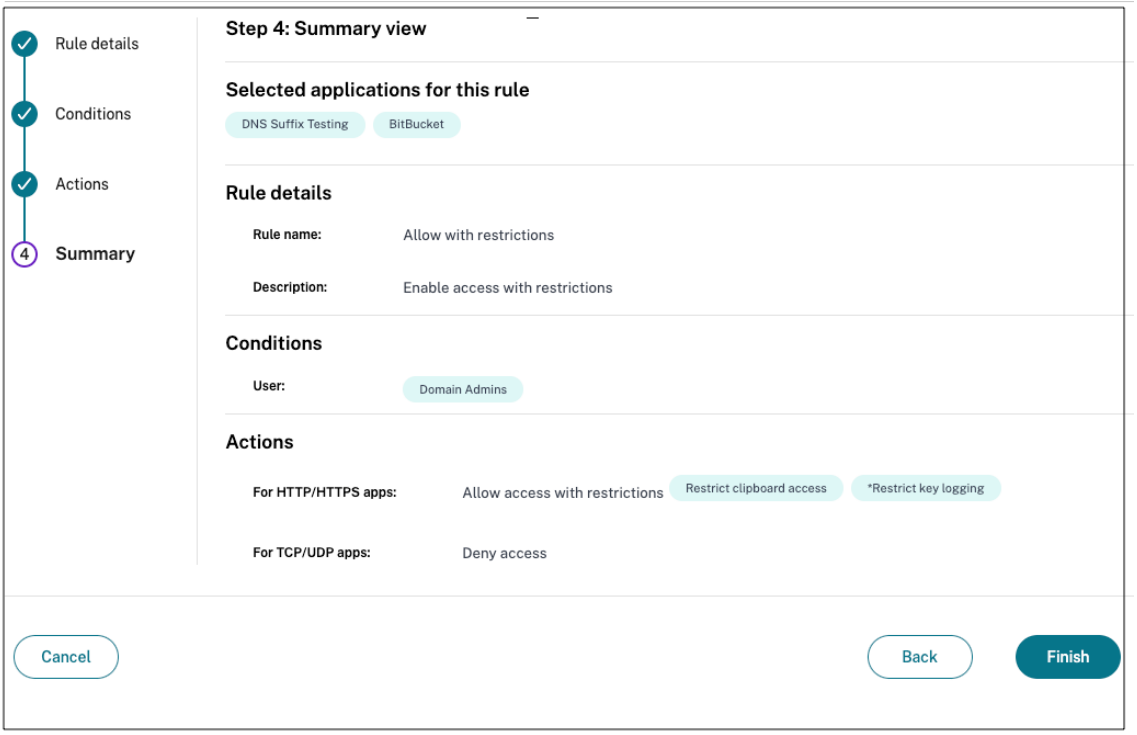
   - For HTTP/HTTPS apps, you can select the following:
     - **Allow access**
     - **Allow access with restrictions**
     - **Deny access**

> **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**

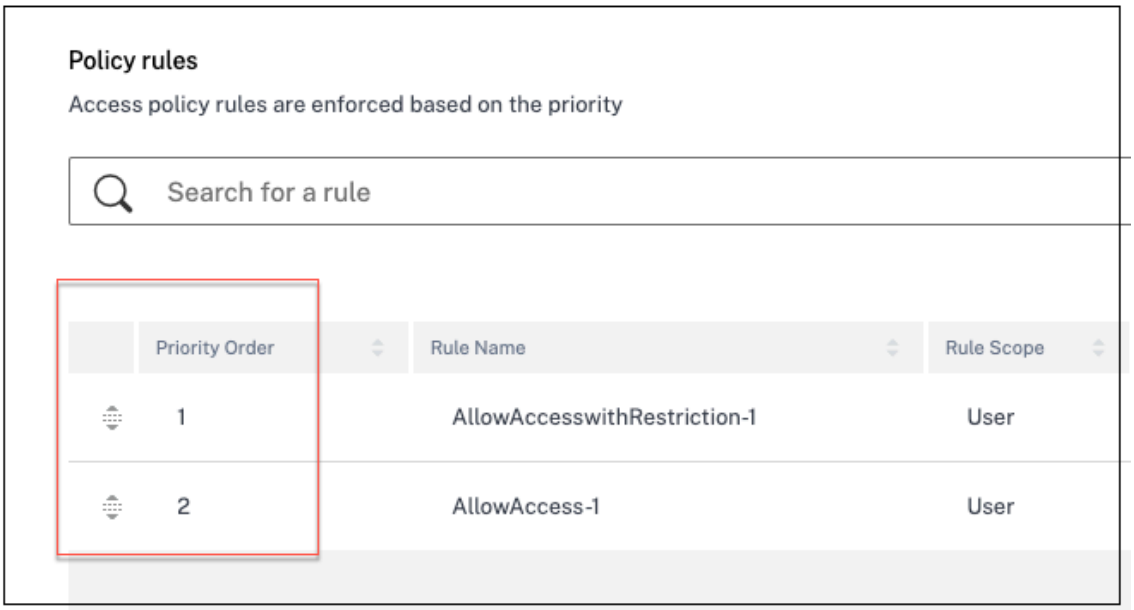


10. Click **Next**. The Summary page displays the policy details.
11. You can verify the details and click **Finish**.



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.



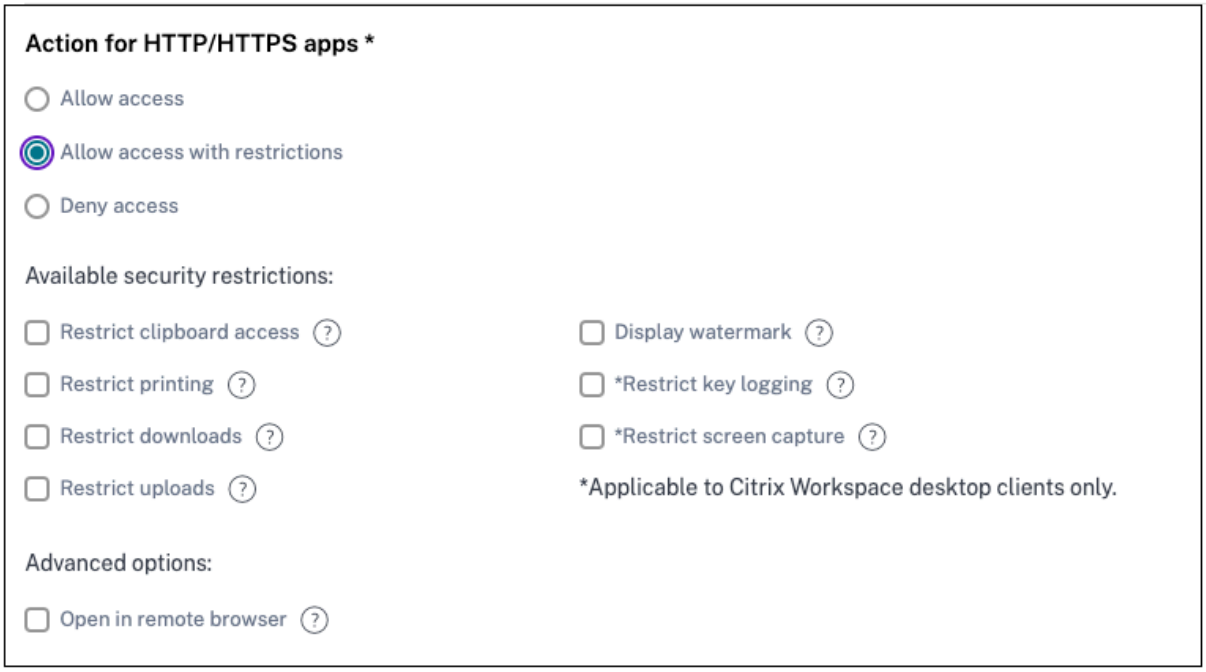
Evaluation of rules with priority order example:

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. The following security restrictions can be enabled for the application.



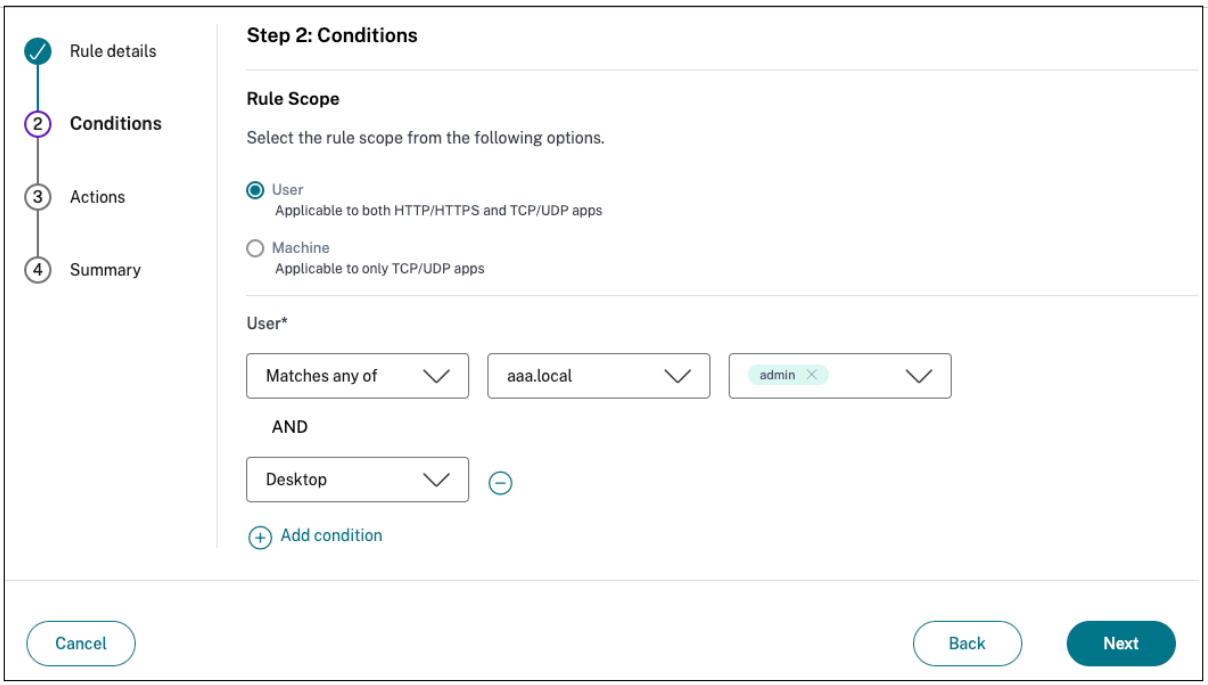
- **Restrict clipboard access:** Disables cut/copy/paste operations between the app and the system clipboard.
- **Restrict printing:** Disables the ability to print from within the Citrix Enterprise Browser.
- **Restrict downloads:** Disables the user's ability to download from within the app.
- **Restrict 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.

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.



Adaptive access based on the location

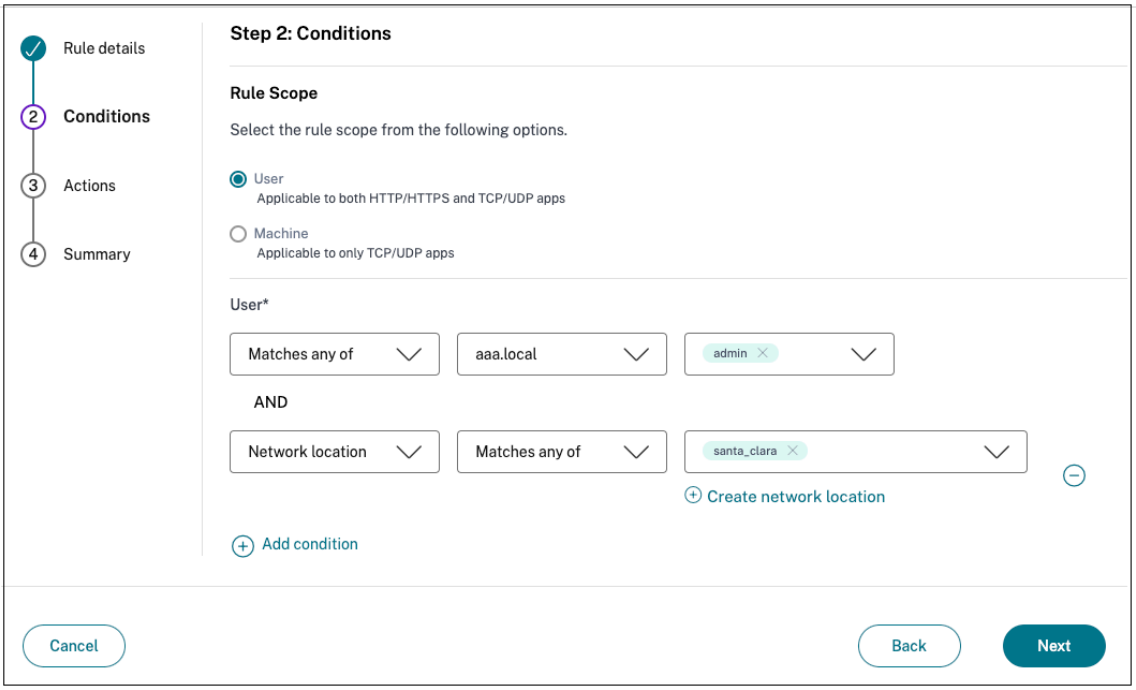
An admin can configure the adaptive access policy based on the location from where the user is accessing the application. The location can be the country from where the user is accessing the application or the user's network location. The network location is defined using an IP address range or subnet 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

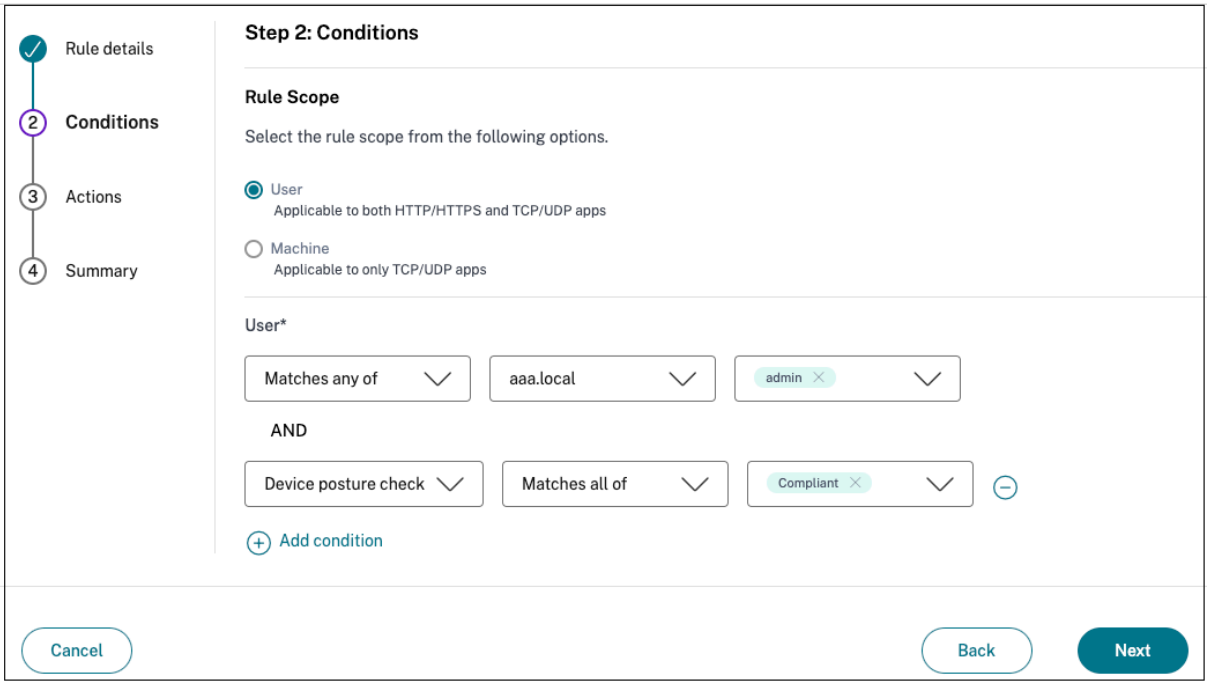
You can configure Secure Private Access service to enforce access control using device posture tags. After a device is allowed to log in after the device posture verification, the device can be classified as compliant or non-compliant. This information is available as tags to Citrix DaaS service and 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.



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

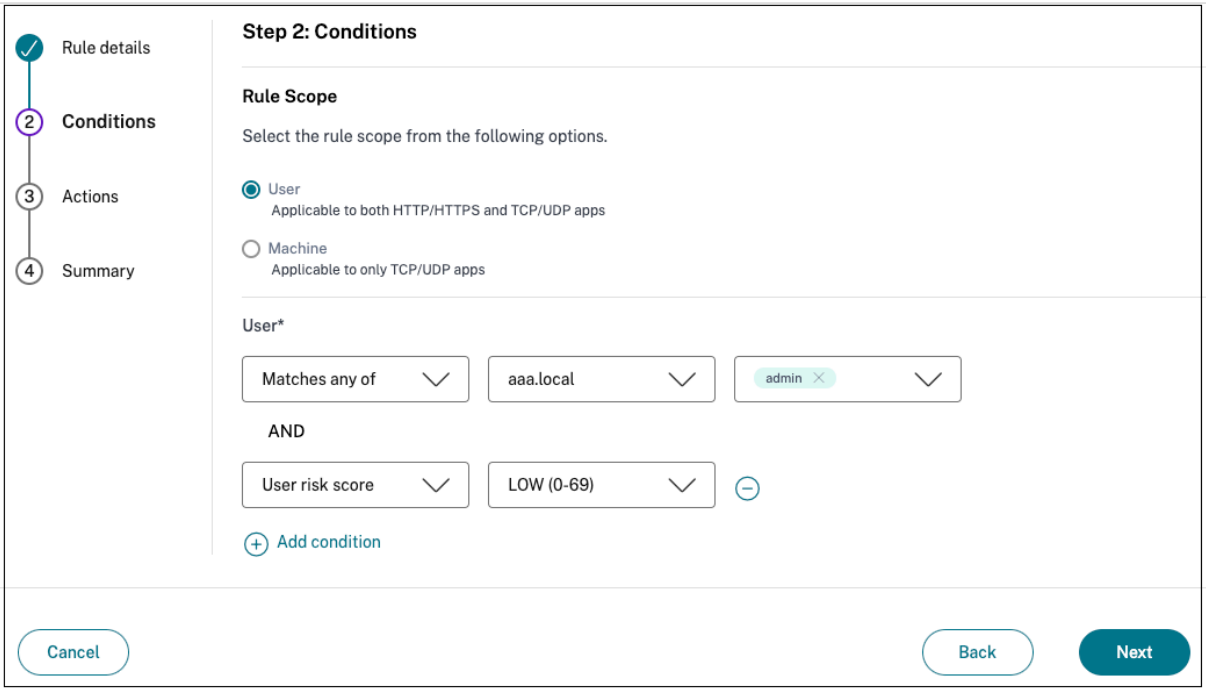
the normal. Each risk indicator can have one or more risk factors associated with it. These risk factors help you to determine the type of anomalies in the user events. The risk indicators and their associated risk factors determine the risk score of a user. The risk score is calculated periodically 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**



Route tables to resolve conflicts resulting from same related domains

November 21, 2023

The application domains feature of the Citrix Secure Private Access service enables customers to make routing decisions that allow related domains of applications to be routed externally or internally through Connector Appliances.

Consider that the customer has configured the same related domains within both a SaaS app and an internal web app.
For example, if Okta is the SAML IdP for both Salesforce (SaaS app) and Jira (internal web app), then the admin might configure `*.okta.com` as a related domain in both apps'configuration. This leads to a conflict and the end user experiences inconsistent behavior. In this scenario, the admin can define rules to route these applications either externally or internally through the Connector Appliances, as per the requirement.

Application Domains feature also enables admins to configure the Connector Appliances to bypass the customer's web proxy servers to reach the internal web servers. These bypass policies were previously configured manually by running the NSCLI commands on the Connector Appliance.

How the route table works

The admins can define the route type for the apps as External, Internal, or External via Connector Appliance depending on how they want to define the traffic flow.

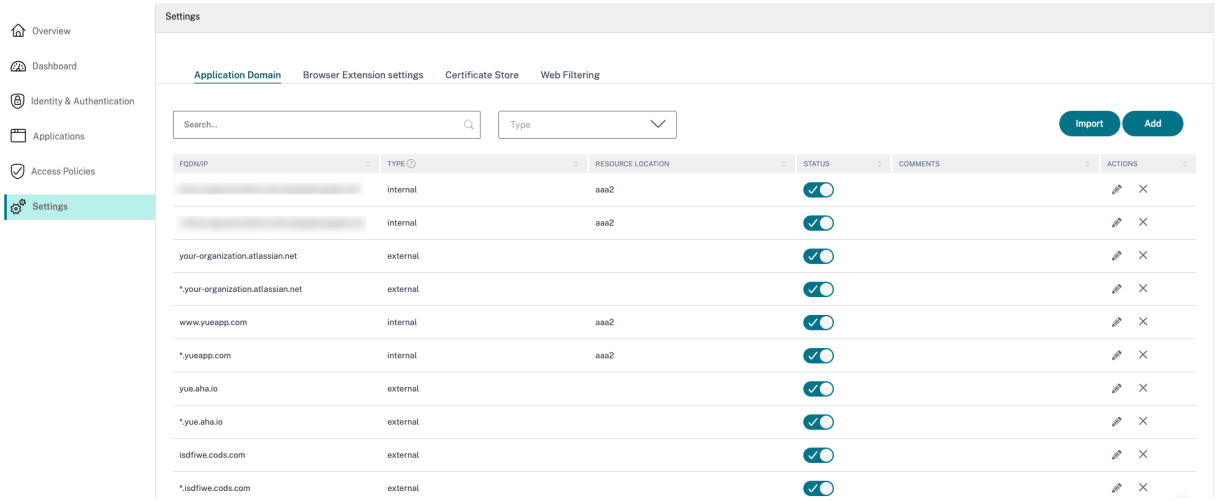
- **External** –The traffic flows directly to the internet.
- **Internal** –The traffic flows via the Connector Appliance.
  - For a web app, the traffic flows within the data center.
  - For a SaaS app, the traffic is routed outside the network through the Connector Appliance.
- **Internal –bypass proxy** - The domain traffic is routed through Citrix CloudConnector Appliances, bypassing the customer's web proxy configured on the Connector Appliance.
- **External via Connector** - The apps are external but the traffic must flow through the Connector Appliance to the outside network.

> **Note:**
>
> - Route entries do not impact the security policies that are configured on the apps.
> - If admins do not intend to use an entry in the route table or if the corresponding apps are not working as intended, admins can simply disable the entry instead of deleting it.
> - All Connector Appliances for a particular customer, irrespective of the app type, get the SSO settings. Previously, the SSO setting for a particular app was tied to a resource location.

Main route table

The main route table is accessible from the **Secure Private Access** tile.

1. Log on to Citrix Cloud account.
2. On the Secure Private Access tile, click **Manage**.
3. In the navigation pane, click **Settings.** The **Application Domains** page appears.



The main route table displays the following columns.

- **FQDN/IP:** FQDN or the IP address for which the type of traffic routing is desired to be configured.
- **Type**: App type. **Internal**, **External**, or **External via Connector** as selected when adding the app.

  > **Important:**
  >
  > If there are conflicts, then an alert icon is displayed for the respective row in the table. To resolve the conflict, admins must click the triangular icon and change the app type from the main table.

- **Resource location:** Resource location for routing of type **Internal**. If a resource location is not allocated, a triangular icon appears in the **Resource location** column for the respective app. When you hover on the icon, the following message is displayed.

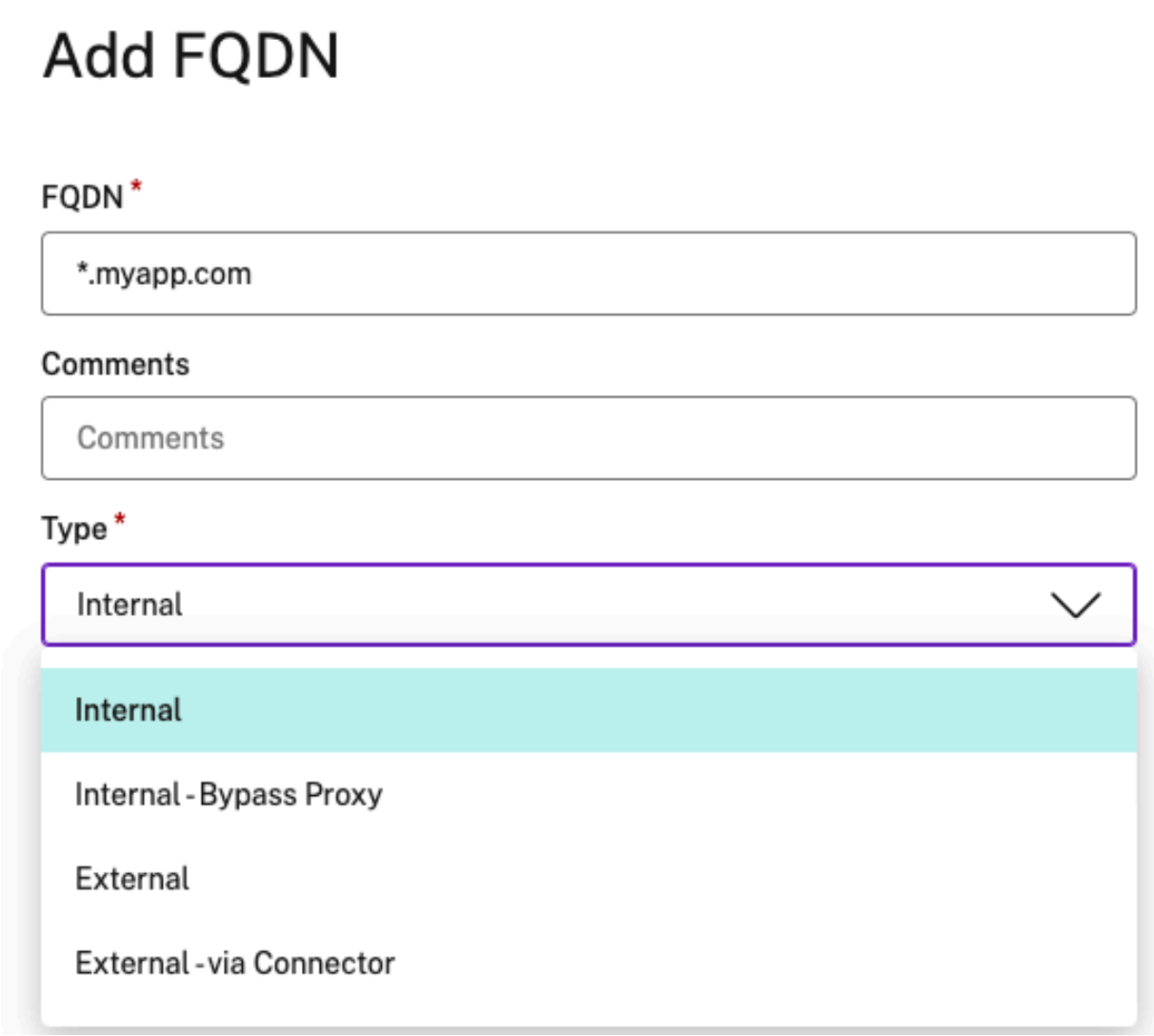
  Missing resource location. Ensure that a resource location is associated with this FQDN.

- **Status:** The toggle switch in the **Status** column can be used to disable the route for a route entry without deleting the app. When the toggle switch is turned OFF, the route entry does not take effect. Also, if FQDNs of exact match exist, admins can select the route to be enabled or disabled.
- **Comments:** Displays comments, if any.
- **Actions:** The edit icon is used to add a resource location or change the type of route entry. The delete icon is used to delete the route.

Add an FQDN to the Application Domains table

Admins can add an FQDN into the Application Domains table and choose the appropriate routing type for it.

1. Click **Add** in the Applications Domain page.
2. Enter the FQDN name and select the appropriate routing type for the FQDN.



Mini route table

A mini version of the Application Domains table is available to make the routing decisions during app configuration. The mini route table available in the **App Connectivity** section in the Citrix Secure Private Access service user interface.

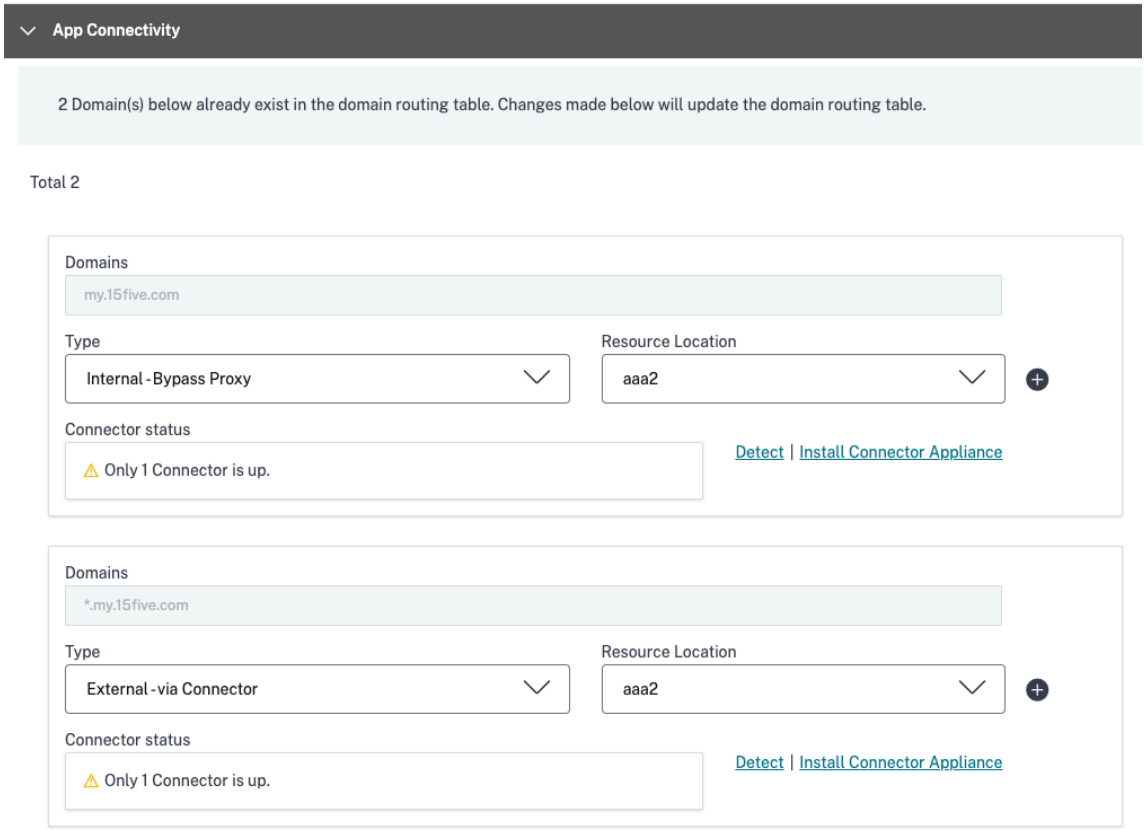
To add routes to the mini route table

The steps to add an app in the Citrix Secure Private Access service remain the same as described in the topics Support for software as service apps and Support for Enterprise web apps except for the following two changes:

1. Complete the following steps:

- Choose a template.
- Enter app details.
- Choose enhanced security details, as applicable.
- Select the single sign-on method, as applicable.

2. Click **App Connectivity**. - A mini version of the Application Domains table is available to make the routing decisions during app configuration.



- **Domains:** The Domains column displays one or more rows for a particular app. The first row displays the actual app URL that the admin has entered while adding the app details. The other rows are all related domains that are entered while adding the app details. If the app URL and the related domains are the same, they are displayed in one row.

One row displays the SAML assertion URL, if SAML SSO is selected.

- **Type:** Select one of the following options.
  - **External** –The traffic flows directly to the internet.
  - **Internal** –The traffic flows via the Connector Appliance and the app is treated as a web app.
    - 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** - Domain traffic is routed through Citrix Cloud Connector Appliances, bypassing the customer's web proxy configured on the Connector Appliance.
  - **External via Connector** –The apps are external but the traffic must flow via the Connector Appliance to the outside network.
- **Resource Location:** Autopopulated when you select the type Internal for an app. Change it if a different resource location is desired.
- **Connector Appliance Status:** Autopopulated, along with resource location, when you select the type Internal for an app.

Unsanctioned websites

March 28, 2024

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

For all other internet URLs or SaaS applications that do not have an app configured, admins can use the **Settings > Unsanctioned Websites** tab from the admin console to allow or deny access via Citrix Enterprise Browser. 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.
3. 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.

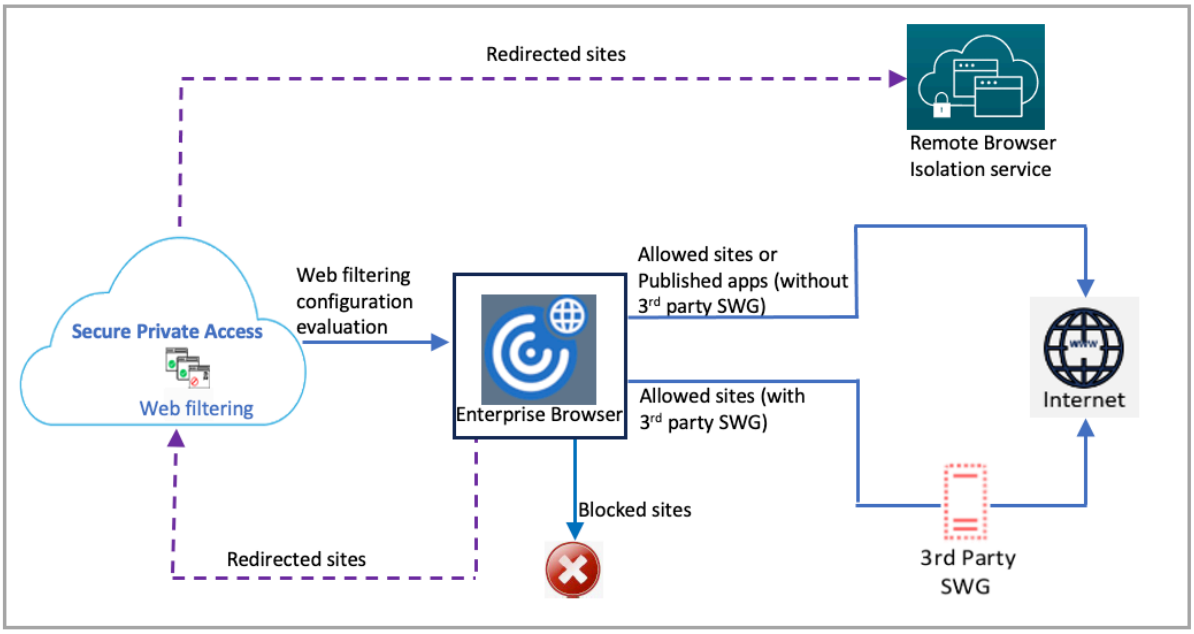
> **Note:**
>
> By default, settings are configured to ALLOW access to all internet URLs or SaaS apps via Citrix Enterprise Browser.

How unsanctioned websites work

1. URL analysis check is done to determine if the URL is a Citrix service URL.
2. The URL is then checked to determine if it is an Enterprise web or SaaS app URL.

3. The URL is then checked to determine if it is identified as a blocked URL, or if 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.

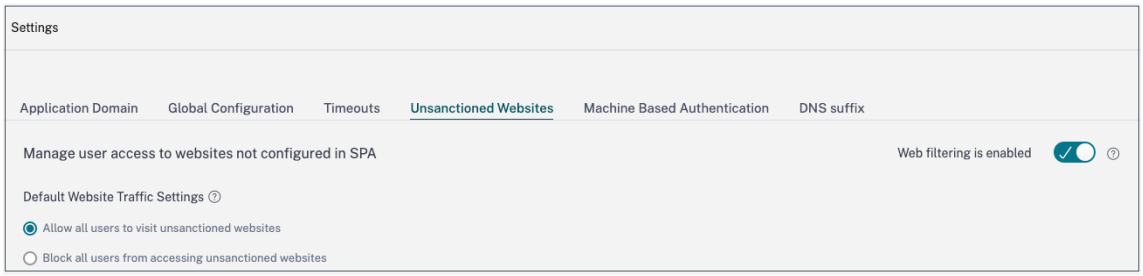


When a request arrives, the following checks are performed, and corresponding actions are taken:

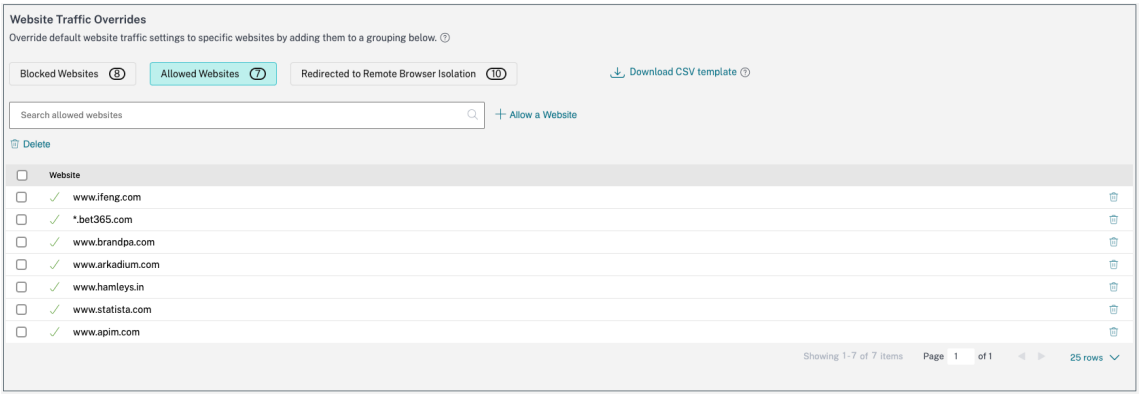
1. Does the request match the global allow list?
   a) If it matches, the user can access the requested website.
   b) If it does not match, website lists are checked.
2. Does the request match the configured website list?
   a) If it matches, the following sequence determines the action.
      i. Block
      ii. 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.

ADFS integration with Secure Private Access

November 21, 2023

Claim rules are necessary to control the flow of claims through the claims pipeline. Claim rules can also be used to customize the claims flow during the claim rule execution process. For more information about claims, see Microsoft documentation.

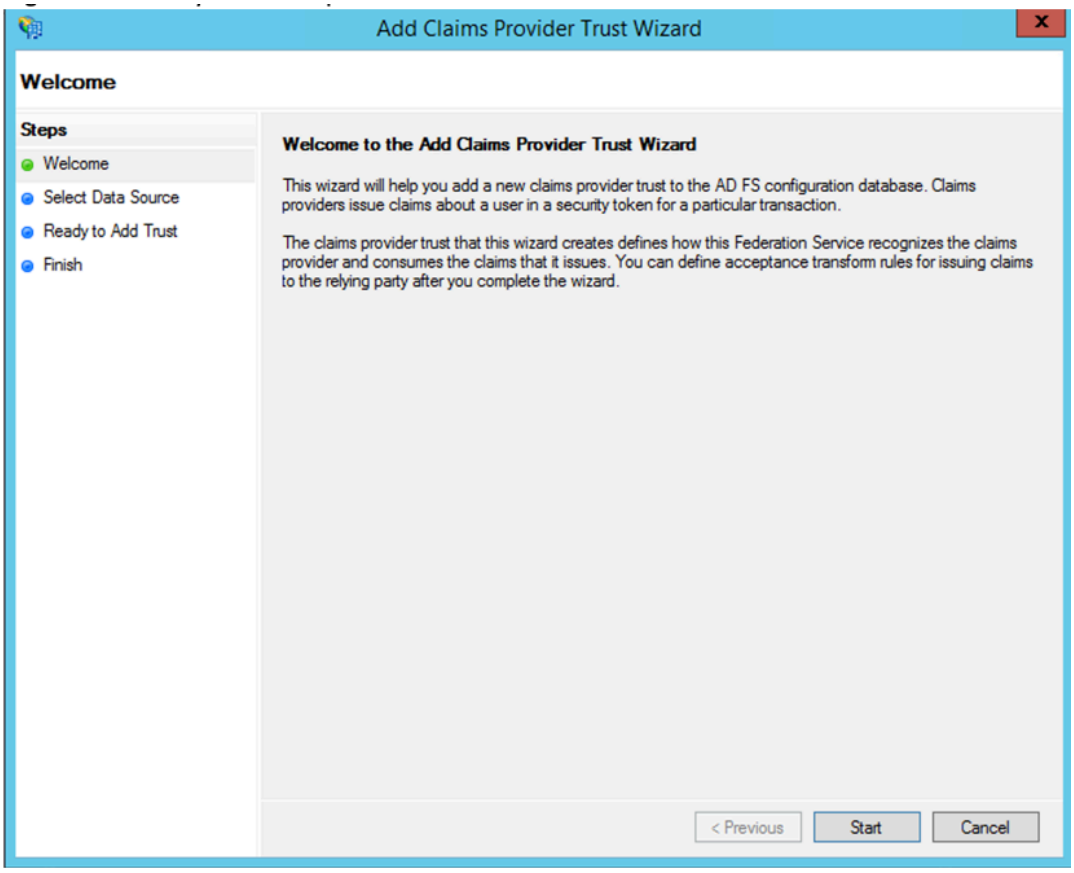
To set up ADFS to accept claims from Citrix Secure Private Access, you must perform the following steps:

1. Add claim provider trust in ADFS.
2. Complete the app configuration on Citrix Secure Private Access.

Add claim provider trust in ADFS

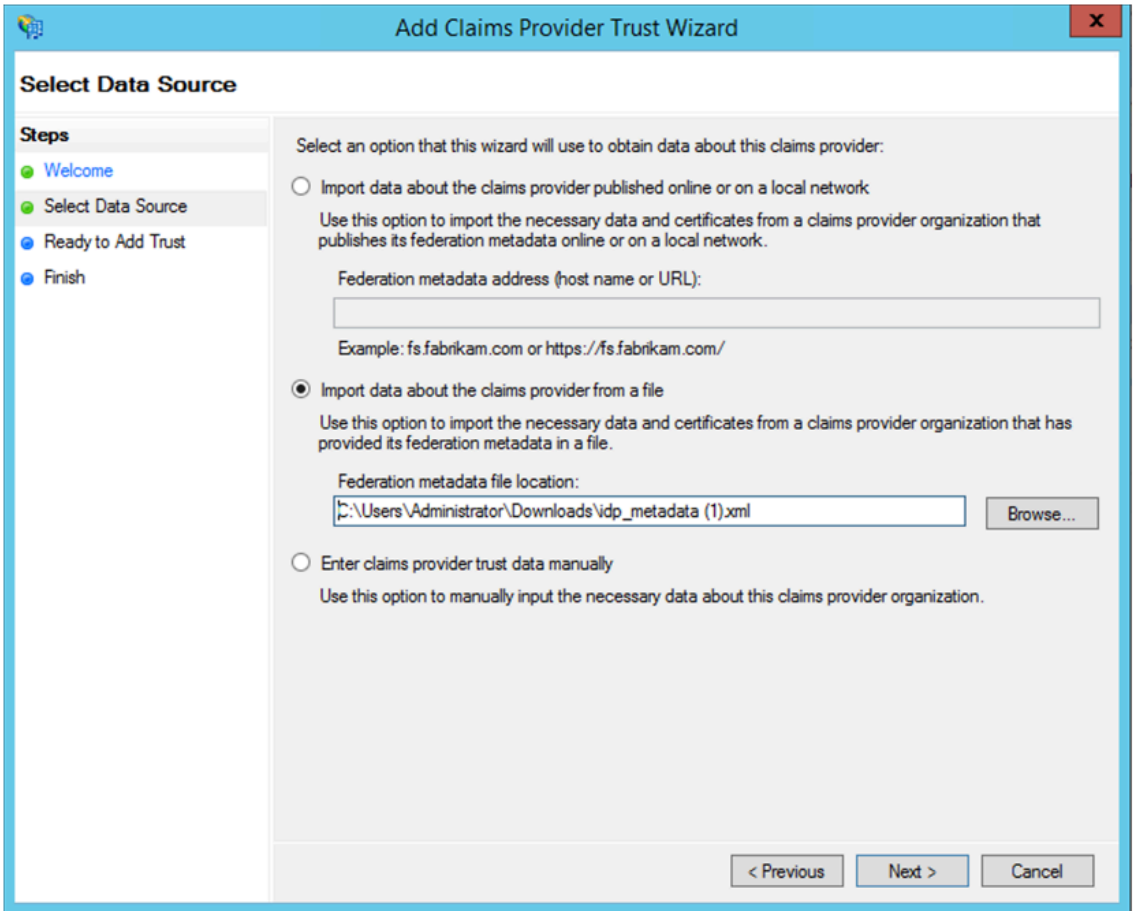
1. Open ADFS management console. Go to **ADFS > Trust relationship > Claim provider Trust**.

    a) Right-click and select **Add Claim Provider Trust**.

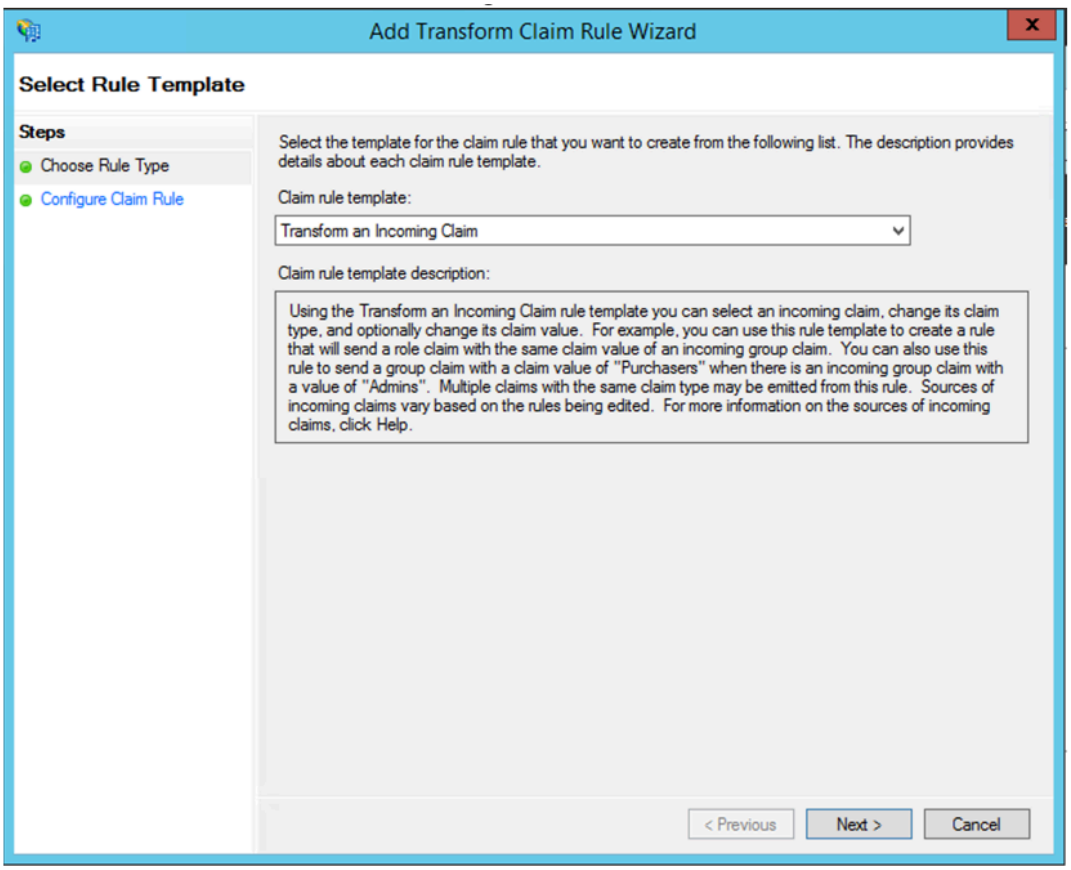


b) Add an app in Secure Private Access that is used to federate to ADFS. For details see, App configuration on Citrix Secure Private Access.

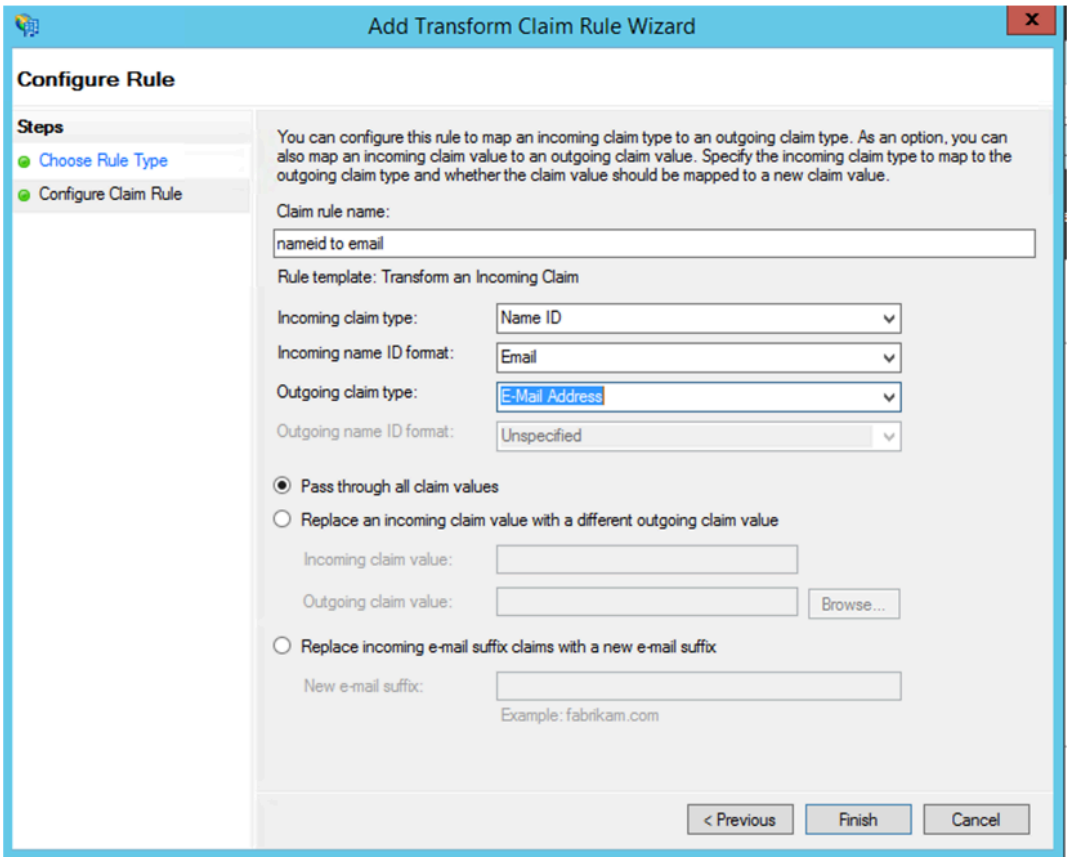
> **Note:**
>
> First add the app and from the app's SSO configuration section, you can download the SAML metadata file, and then import the metadata file into ADFS.



a) Complete the steps to finish adding claim provider trust. After you complete adding the claim provider trust, a window to edit the claim rule appears.
b) Add a claim rule with **Transform An Incoming Claim**.



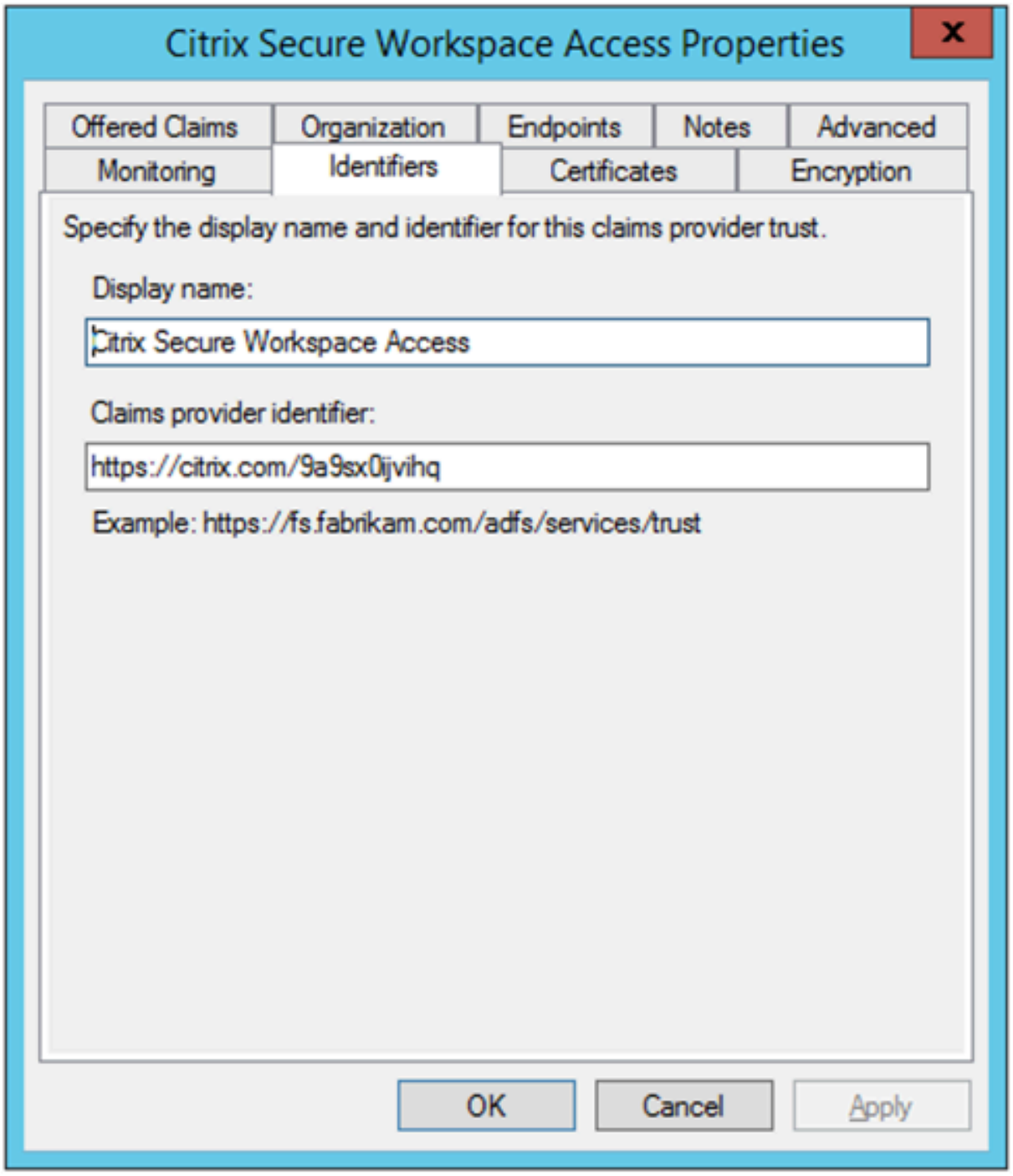
c) Complete the settings as shown in the following figure. If your ADFS accepts other claims, then use those claims and configure SSO in Secure Private Access also accordingly.



You have now configured the claim provider trust that confirms ADFS now trusts Citrix Secure Private Access for SAML.

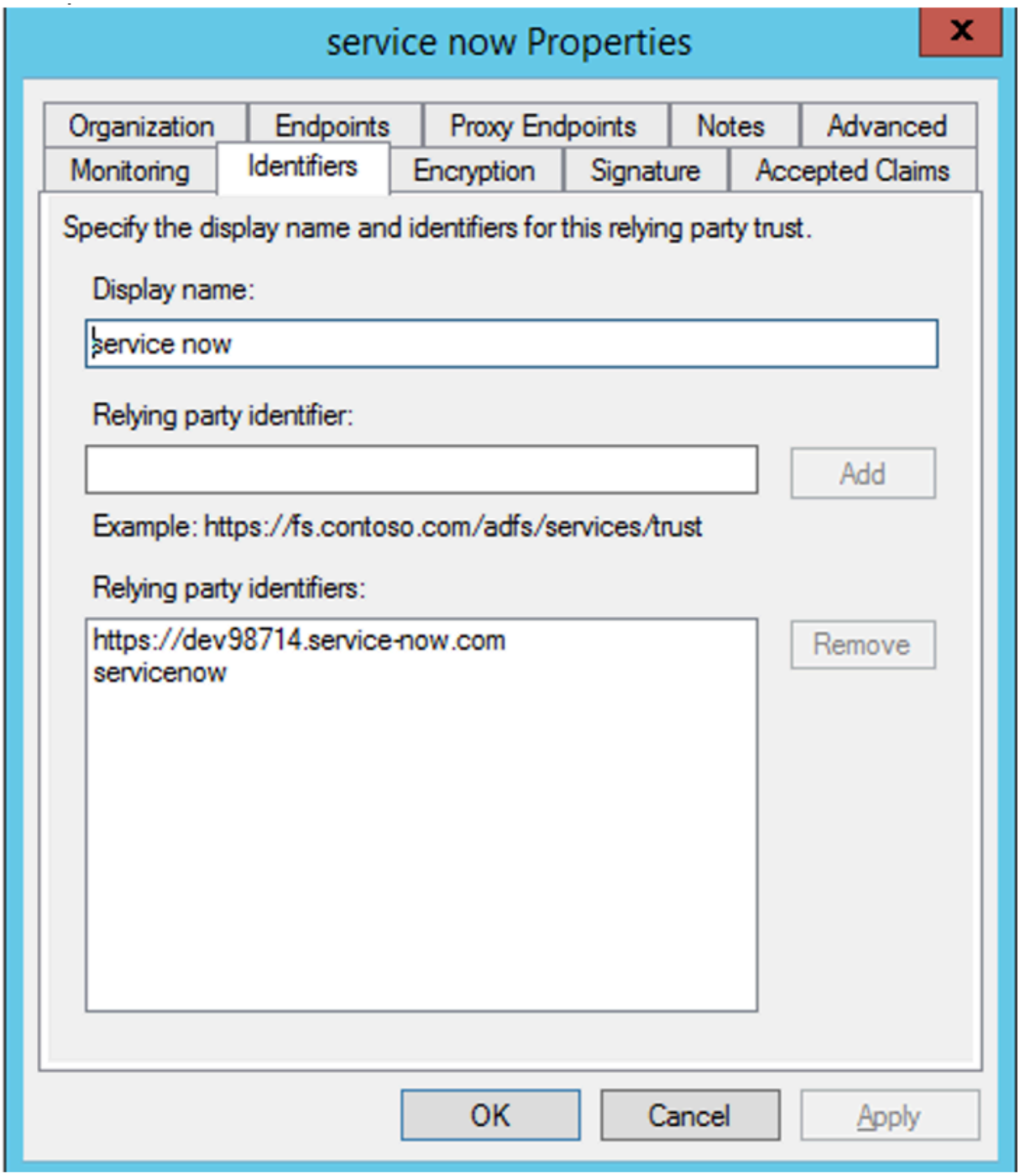
Claim Provider trust ID

Make a note of the claim provider trust id that you added. You need this ID while configuring the app in Citrix Secure Private Access.



Relaying Party Identifier

If your SaaS app is already authenticated using ADFS, then you must already have the Relaying party trust added for that app. You need this ID while configuring the app in Citrix Secure Private Access.



Enable relay state in IdP initiated flow

RelayState is a parameter of the SAML protocol that is used to identify the specific resource the users access after they are signed in and directed to the relying party's federation server. If RelayState is not enabled in ADFS, users see an error after they authenticate to the resource providers that requires it.

For ADFS 2.0, you must install update KB2681584 (Update Rollup 2) or KB2790338 (Update Rollup 3) to provide RelayState support. ADFS 3.0 has RelayState support built in. In both cases RelayState still needs to be enabled.

To enable the RelayState parameter on your ADFS servers

1. Open the file.
   - For ADFS 2.0, enter the following file in Notepad: %systemroot%\inetpub\adfs\ls\web.config
   - For ADFS 3.0, enter the following file in Notepad: %systemroot%\ADFS\Microsoft.IdentityServer.Service
2. In the microsoft.identityServer.web section, add a line for useRelyStateForIdpInitiatedSignOn as follows, and save the change:
   ```
   <microsoft.identityServer.web> ... <useRelayStateForIdpInitiatedSignOn
    enabled="true"/> ...</microsoft.identityServer.web>
   ```
   - For ADFS 2.0, run `IISReset` to restart IIS.
3. For both platforms, restart the Active Directory Federation Services `(adfssrv)service.`
   Note: If you have windows 2016 or Windows 10 then use the following PowerShell command to enable it.
   ```
   Set-AdfsProperties -EnableRelayStateForIdpInitiatedSignOn $true
   ```

Link to commands - https://docs.microsoft.com/en-us/powershell/module/adfs/set-adfsproperties?view=win10-ps

App configuration on Citrix Secure Private Access

You can either configure the IdP initiated flow or the SP initiated flow. The steps to configure IdP or SP initiated flow in Citrix Secure Private Access are the same except that for SP initiated flow, you must select the **Launch the app using the specified URL (SP initiated)** check box in the UI.

IdP initiated flow

1. While setting up the IdP initiated flow, configure the following.
   - **App URL** –Use the following format for the app URL.
     ```
     https://<adfs fqdn>/adfs/ls/idpinitiatedsignon.aspx?LoginToRP
     =<rp id>&RedirectToIdentityProvider=<idp id>
     ```
   - **ADFS FQDN** –FQDN of your ADFS setup.
   - **RP ID** –RP ID is the ID that you can get from your relaying party trust. It is the same as the Relaying Party Identifier. If it is a URL, then URL encoding happens.

- **IDP ID** –IdP ID is the same as the claim provider trust ID. If it is a URL, then URL encoding happens.

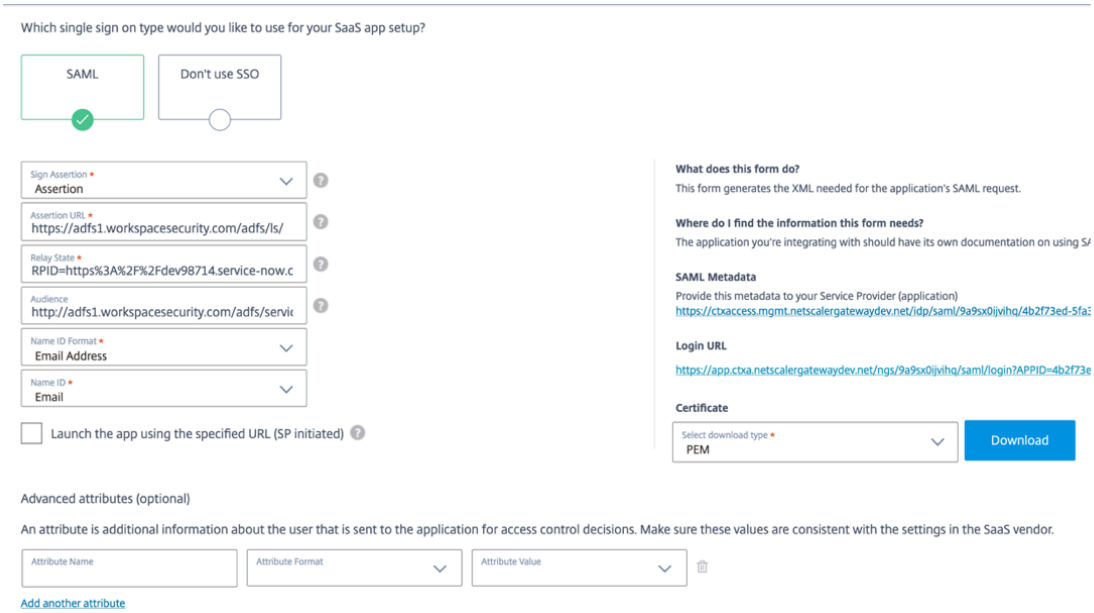
  Example: https://adfs1.workspacesecurity.com/adfs/ls/idpinitiatedsignon.aspx?LoginToRP=https%3A%2F%2Fdev98714.service-now.com&RedirectToIdentityProvider=https%3A%2F%2Fcitrix.com%2F9a9sx0ijvihq

2. SAML SSO configuration.

   The following are the default values of the ADFS server. If any of the values are changed, get the correct values from the metadata of the ADFS server. Federation metadata of the ADFS server can be downloaded from its federation metadata endpoint, whose endpoint can be known from **ADFS > Service > Endpoints.**

   - **Assertion URL** –`https://<adfs fqdn>/adfs/ls/`
   - **Relay State** –Relay state is important for the IdP initiated flow. Follow this link to construct it properly - `https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/jj127245(v=ws.10)`

     Example: RPID=https%3A%2F%2Fdev98714.service-now.com&RelayState=https%3A%2F%2Fdev987
     now.com%2F
   - **Audience** –`http://<adfsfqdn>/adfs/services/trust`
   - For the other SAML SSO configuration settings, see to the following image. For more details, see https://docs.citrix.com/en-us/citrix-secure-private-access/service/support-saas-apps.html



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.

Troubleshoot Secure Private Access issues

April 23, 2024

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?

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 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	App launch failed because app FQDN length exceeded
0x180022	App launch failed as Authentication Service is down	App launch failed as authentication service is down
0x180001, 0x18001A, 0x18001B, 0x18008A 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	App access is denied
0x1800EF	Problem connecting to Connector Appliance	Problem connecting to Connector Appliance
0x18009D	DNS lookup/Connection failed	Secure Browser Service - DNS lookup/connection errors
0x1800A0, 0x1800A2, 0x1800A3, 0x1800A5 0x1800A6, 0x1800A7	Web app launch failed as unable to connect to back end web app	Web app launch failed as unable to connect to back-end web app
0x1800BC, 0x1800BF	User is not entitled to access the Web/SaaS app	User is not entitled to access the Web/SaaS app
0x1800BD	User is not entitled to access the Web/SaaS app for DirectAccess	User is not entitled to access the Web/SaaS app for DirectAccess
0x1800D0	Citrix Secure Access agent Session launch has failed while fetching the application configuration	Citrix Secure Access agent Session launch has failed while fetching the application configuration
0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA	Citrix Secure Access agent Session launch has failed while fetching the application configuration, Citrix Secure Access agent App launch has failed during policy evaluation, Citrix Secure Access agent App launch has failed	Malformed client requests

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

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

Info code	Description	Resolution
0x1300000B	The client closed the connection	Client closed the connection with Secure Private Access service
0x1300000C	The FQDN resolution over ZTNA failed	Unable to resolve FQDN by the DNS server
0x001800D3	Applications configuration download failure while login	Failed to fetch configured application destinations list
0x001800D9, 0x001800DA	TCP/UDP app launch has failed during parsing policy evaluation response, TCP/UDP app launch has failed with invalid result during policy evaluation	Application configuration issue
0x001800DB	TCP/UDP app launch has failed with invalid resource location configuration	Issue with resource location
0x13000006, 0x001800DC, 0x001800DD	TCP app launch has failed due to unsupported Enhanced Security policy configured for the app, TCP app launch has failed due to unsupported Secure Browser Service redirection configured for TCP App	Enhanced security policy is bound to the HTTP application
0x001800DE	TCP/UDP app launch has failed as there is no application configuration found for the destination	Unable to locate the application
0x001800EA	TCP app launch has failed due to destination FQDN is too long	Host name length exceeds 256 characters
0x001800ED	TCP app launch has failed because of invalid destination IP	Invalid IP address
0x001800EF	TCP app launch has failed during connection establishment to private TCP server	Unable to establish end-to-end connection

Info code	Description	Resolution
0x001800F5	UDP app launch failed because of IPV6 address	IPv6 received in the app request
0x001800F9	UDP Traffic failed to deliver as client connection is lost	UDP traffic failed to deliver
0x001800FF	UDP Data traffic delivery failed	UDP data traffic delivery failed
0x10000401	Citrix rendezvous server dial failed	Application launch failed because of network connectivity issues
0x10000402, 0x1000040C	Unable to register the Connector Appliance, UDP network connection initialization failure	Connector appliance failed to register to Secure Private Access service
0x10000403, 0x10000404, 0x10000407, 0x1000040A 0x1000040B, 0x1000040F, 0x10000410	Connection error, Control packet transmission failure, Error on reading Gateway service, Control packet parsing failure, Error on writing	Connectivity issue with Connector Appliance
0x10000405, 0x10000408, 0x10000409, 0x1000040D 0x1000040E, 0x10000412	Back-end Unreachable, UDP packet transmission failure, UDP packet receiving failure, Error on writing back-end, back-end closed the connection	Connectivity issues with Connector Appliance and back-end private TCP/UDP servers
0x10000406	DNS resolution failed	Connector appliance fails to resolve DNS for FQDNs
0x10000411	Gateway service closed the connection	Private server connection terminated
0x10000413	Error in determining connection teardown reason	Failed to connect or send data to the private service IP or FQDN
0x100508	User context does not match the access rule conditions	No matching policy condition
0x100509	Access policy not associated with the application	No access policy associated with the application
0x10050C	Policy evaluation results of multiple applications that the user might be entitled to	App enumeration information

Info code	Description	Resolution
0x00180101	TCP/UDP app launch failed as routing entry is missing in application domain table	TCP/UDP app launch failed as routing entry is missing in application domain table
0x00180102	TCP/UDP app launch failed as connectors are not healthy	TCP/UDP app launch failed as connectors are not healthy
0x00180103	UDP/DNS request failed, as Connector is unreachable	UDP/DNS request failed, as Connector is unreachable
0x20580001	Failed to load the page as NGS Cookie is expired	Failed to load the page as NGS Cookie is expired
0x20580002	Access policy fetch failed because of network failure	Access policy fetch failed because of network failure
0x20580003	Access policy fetch failed while parsing the JSON web token	Access policy fetch failed while parsing the JSON web token
0x20580004	Network failure to fetch Access Policy details	Network failure to fetch Access Policy details
0x20580005	Policy fetch failed while fetching public certificate	Policy fetch failed while fetching public certificate
0x20580007	Policy fetch failed while validating signature of JWT	Policy fetch failed while validating signature of JWT
0x20580008	Policy fetch failed while validating the public certificate	Policy fetch failed while validating the public certificate
0x2058000A	Failed to determine store environment to form a policy URL	Failed to determine store environment to form a policy URL
0x2058000B	Failed to get response of access policy fetch request	Failed to get response of access policy fetch request
0x2058000C	Access policy fetch failed due to an expired secondary DS auth token	Access Policy fetch failed due to an expired secondary DS auth token
0x10200002	Connector appliance is not registered	Connector appliance is not registered
0x10200003	Unable to connect to connector appliance	Unable to connect to connector appliance

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

Resolution steps

The following sections provide resolution steps for most of the info codes. For the codes that do not have the resolution steps captured, contact Citrix Support.

One or more apps not listed in the user dashboard

Info code: 0x180055, 0x1800DF, 0x1800E3

Due to the contextual policy settings, apps might not be seen for some users or devices. Parameters like trust factors (device posture or risk score) can affect the accessibility of the applications.

1. Copy the transaction ID from the `reasons` column for error code `0x18005C` in the Diagnostic Logs csv file.
2. Modify the `prod` column filter in the csv file to show events from the component called `SWA.PSE` or `SWA.PSE.EVENTS`. This filter shows logs related to policy evaluation only.
3. Search for the evaluated policy payload in the `reason` column. This payload shows the evaluated policy for the user's context for all apps that the user is subscribed to.
4. If the policy evaluation indicates as app denied for the user, the possible reasons can be:
   - Incorrect matching conditions in policy - check App policy configuration in Citrix Cloud
   - Incorrect matching rules in policy - check App policy configuration in Citrix Cloud
   - Incorrect matching default rule in policy - this is a fall-through case. Adjust the conditions accordingly.

User is not entitled to access the Web/SaaS app

Info code: 0x1800BC, 0x1800BF

The user might have clicked the app link for which the user might not have a subscription.

Ensure that the user has a subscription to the applications.

1. Go to the application in the management portal.
2. Edit the app and go to the **Subscription** tab.
3. Ensure that the targeted user has an entry in the subscription list.

Slow back-end app performance

Info code:0x18000F

There are cases where the customer network is flaky due to the connectors in a resource location that can be down or the back-end server itself might not be responding.

1. Ensure that the connector appliance is positioned geographically close to the back-end server to rule out network latencies.
2. Check if the back-end server's firewall is not blocking the connector appliance.

3. Check if the client is connecting to the nearest cloud POP.

   For example, `nslookup nssvc.dnsdiag.net` on the client, the canonical name in the answer indicates the geo-specific server such as `aws-us-w.g.nssvc.net`.

App launch failed because App FQDN length exceeded

Info code: 0x180006, 0x1800B7

App FQDNs must not exceed 512 characters in length. Check the application FQDN in the app configuration page. Ensure that the length does not exceed 512 bytes in size.

1. Go to the **Applications** tab on the management console.
2. Look for the application whose FQDN exceeds 512 characters.
3. Edit the application and fix the app FQDN length.

App details length exceeded

Info code: 0x18000E

Check the policies if they are blocking the app access.

1. Go to **Access Policies**.
2. Look for the policies where the app has entitlement.
3. Review the policy rules and conditions for the end user.

App access is denied

Info code: 0x180001, 0x18001A, 0x18001B, 0x18008A, 0x1800A9, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3, 0x180048

This is related to contextual policies, where policies are denying the app for a given user.

Check the policies if they are blocking the app access

1. Go to **Access Policies**.
2. Look for the policies where the app has entitlement.
3. Review the policy rules and conditions for the end user.

Applications not enumerated

Applications can be missing from the enumerated list because of policy denials or if the Secure Private Access integration is not enabled.

- If access must be enabled for some of the apps but you see zero apps, try enabling the Secure Private Access integration.
  - Sign into Citrix Cloud.
  - Select **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 `WebAppUnSupportedAut` 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 `FailedToConstructForL` 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.

Unable to locate the application

Info code: 0x001800DE

You might be unable to locate the application for the accessed destination for the user. This might occur if the destination to resource location mapping missing in the Application Domain table.

- Ensure that the TCP/UDP or HTTP application is configured for the accessed destination.
- Ensure that the user has a subscription to the application for the accessed destination.

1. Go to the application in the management portal.
2. Edit the app and go to the **Subscription** tab.
3. Ensure that the targeted user has an entry in the subscription list.
4. Ensure that the **Application Domain** table has the destination and the appropriate resource location.

Failed to fetch configured application destinations list

Info code: 0x001800D3

- Ensure that at least one TCP/UDP/HTTP app is configured. For details, see Add and manage applications.

- Ensure that the Application Domain table (**Secure Private Access > Settings > Application Domain**) page is not empty or not all entries are disabled. The destinations configured in the TCP/UDP/HTTP application are automatically added to this table. It is recommended not to delete or the disable the active TCP/UDP/HTTP application's destinations or URLs in the Application Domain table.

Application configuration issue

The application configuration contains a special character or some policy configuration issue.

Info code: 0x001800D9, 0x001800DA

Ensure the following:

- The app configuration does not contain unsupported characters.
- The destination IP address or IP address range or the IP CIDR are valid.
- The application destination is enabled in the Application Domain table (**Secure Private Access > Settings > Application Domain**).
- The policies are configured and bound to the respective application.
- The access policies 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 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.

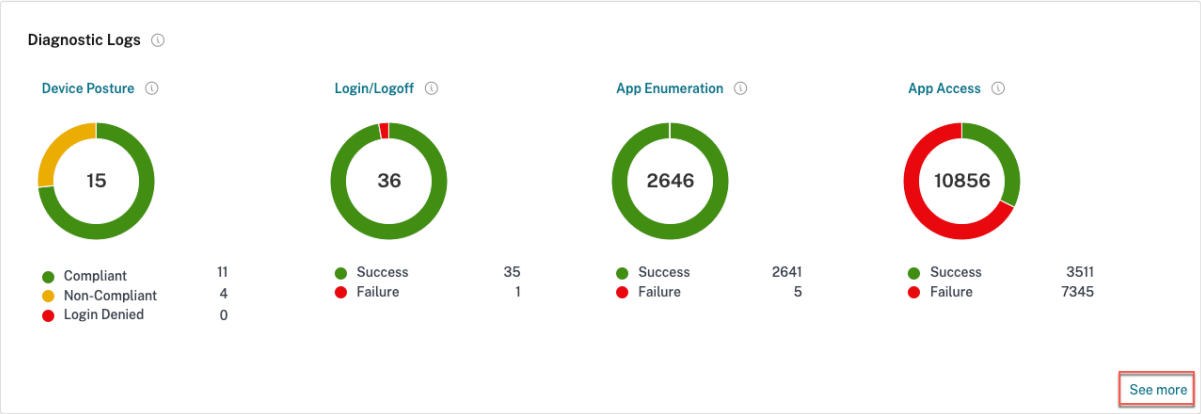
Answers to FAQs

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.

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.



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** - 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** - 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

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?

Transaction ID correlates all Secure Private Access logs for an access request. One app access request can have multiple logs generated, starting from authentication, then app enumeration 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.

What are all the Secure Private Access PoP locations?

The following is the list of Secure Private Access 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

PoP name	Zone	Region
az-in-s	Azure southindia	Chennai
az-asia-hk	Azure eastasia	Hong Kong

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