Citrix Secure Private Access
Contents

What’s new 3
Fixed issues 11
Known issues 15
Feature deprecations 17
Admin-guided workflow for easy onboarding and set up 17
Dashboard overview 25
Apps configuration and management 30
Support for Enterprise web apps 31
Connector Appliance for Secure Private Access 35
Citrix Gateway Connector 40
Citrix Gateway Connector dashboard 60
Migrate Gateway Connector to Connector Appliance 62
Direct access to Enterprise web apps 63
Support for client-server apps 69
Support for Software as a Service apps 83
Migration of app security controls and access policies to the new access policy framework 90
Apps configuration using a template 92
SaaS app server specific configuration 97
Launch a configured app - end user workflow 111
Read-only access for admins to SaaS and Web apps 112
Diagnostic logs for Enterprise Web and SaaS apps access 116
Adaptive Authentication service 119
Smart Access using Adaptive Authentication 150

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Data Governance 156
Adaptive access and security controls for Enterprise Web, TCP, and SaaS applications 159
Route tables to resolve conflicts if the related domains in both SaaS and web apps are the same 172
Web filtering 176
Configure website filtering 177
Available categories list for Citrix Secure Private Access 181
Citrix Cloud Gateway Connector availability in Azure Marketplace 187
Citrix Cloud Gateway Connector availability in Azure 193
Deploy a Citrix Gateway Connector instance on AWS - Preview 200
ADFS integration with Secure Private Access 206
Troubleshoot apps related issues 215
Data Governance 235
What’s new

July 19, 2022

V15.3 (July 15, 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]

V14.5 (June 01, 2022)

• **Adaptive Authentication service**

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

  [CGS-6510]

V14.2 (April 04, 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 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]

---

**V13.4 (February 16, 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]

**V12.1 (October 11, 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.

V11.4 (July 30, 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]

V10.5 (June 09, 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]

V10.4 (May 22, 2021)

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

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

V10.2 (May 01, 2021)

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

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

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

V9.6 (March 15, 2021)

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

- Improved web apps performance
  
  The web apps performance when the web applications are accessed from the system browser using clientless VPN has been improved.
Enabling Citrix Gateway Connector to use TLS1.2 Grade A or above cipher suites

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

[NGSWS-16068]

V8.4 (November 11, 2020)

Renaming of Citrix Access Control service

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

[NGSWS-14934]

V8.2 (October 15, 2020)

Enhanced security option to launch SaaS and Enterprise Web apps within Secure Browser service

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

[ACS-123]

V7.6 (October 8, 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]

V7.5 (September 24, 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]

V7.1 (July 7, 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]

V6.6 (June 19, 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]

V6.3 (May 8, 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 files 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 secure browser service redirects.** Automatic geo routing is now enabled for secure browser 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.
Fixed issues

May 24, 2022

**V12.1 (October 11, 2021)**

- If the NameID configured in the SAML SSO settings of an application is not available in the user’s token, then the string “Anonymous” is used in the SAML assertion. As a result, the SAML SSO in SP initiated flow fails.

  [NGSWS-16761]

**V11.4 (July 30, 2021)**

- Sometimes, the message “Error modifying application...” might appear when you click the Finish button after adding a Web or a SaaS app.

  [NSHELP-28336]

**V10.2 (May 01, 2021)**

- Access to Enterprise web apps fail if the plus (+) character is used to replace whitespace in query parameters.

  [NSHELP-26792]

- Existing and new Enterprise Web apps cannot be assigned to the resource location if the resource location name is modified. With this fix, you can rename the resource locations of the existing and new Enterprise Web apps from the Citrix Gateway Service if you have modified from the resource location name from the Citrix Cloud home page.

  [NGSWS-16641]

**V9.6 (March 15, 2021)**

- Adding an Enterprise web app or a SaaS app with numbers in the FQDN fails. For example, https://sample-site.2k3.net fails.

  [NGSWS-16847]
Sometimes, if **Enhanced Security** is enabled for an application, the watermark on an application displays the name as “Anonymous” instead of the user’s display name.

[NGSWS-16371]

If a SaaS app or an Enterprise web app name contains a period “.” in the name, the name gets truncated after the period “.” on saving the configuration.

[NGSWS-16758]

**V9.3 (January 20, 2021)**

- When adding an enterprise Web app, the App Connectivity page does not open.
  
  [NGSWS-16332]

- An error message appears when you change the authentication type from **Don’t use SSO** to **SAML**. This error message appears when you try to edit an app after you click the **Finish** button.

  [NGSWS-16315]

- The **SAML single sign-on** option is grayed out for some SaaS applications that are created without using the template.

  [NGSWS-16162]

- When adding an Enterprise Web app, an alert symbol appears even after the gateway connector detection is complete.

  [NGSWS-15562]

**V2019.06.01**

- Edits made in the Access Control page are not propagated to the database because the failed jobs were retried incorrectly. [NGSWS-7733]

**V2019.05.01**

- If a customer’s data center has an authentication-enabled proxy server configured for Gateway Connector, the connector fails to register itself with Citrix Cloud. [NGSWS-7231]

- When adding an Enterprise Web app, if the FQDN contains an underscore ( _ ) in the domain name, an error is displayed. [NGSWS-7033]

- If the SSO type for a SaaS app is changed from Don’t use SSO to SAML, the configuration change fails. [NGSWS-7466]
V2019.04.02

- In rare cases, web filtering UI configuration changes do not take effect to the tenant traffic. [NGSWS-7147]
- Memory leaks on ICA service nodes, resulting in a high memory usage. [NGSWS-7014]
- Application fails to launch because the Citrix Gateway service node does not send the X-NGS-Session-Id header as part of the policy document retrieval request to the CVMs. [NGSWS-6963]
- Authentication and app enumeration on the Citrix Gateway service fail if the token size for authentication exceeds 64 KB. [NGSWS-5932]

V2019.04.01

- Web app launch fails for a customer when the value of the CustomerId is in the camel case. [NGSWS-6705]
- Connection to a Secure Mail server is not possible with FQDN. If the customer configuration has FQDN configured for the mail server, then the connection fails. [NGSWS-6566]
- App launch fails after the Gateway Service session times out. The end user must relogin to access the apps. [NGSWS-6917]
- When renaming a SaaS app, the name changes in the GUI but does not change in the Workspace app. Similarly, when changing or adding an icon of certain SaaS apps and Web apps, the icon updates in the GUI but is not propagated to the Workspace app. [NGSWS-6915]
- If Enhanced Security is enabled on a Web app (hosted inside the corporate network) and if that app is launched from a native browser, then the app launch is redirected to the secure browser service because the native browser cannot enforce enhanced security policies. [NGSWS-6804]
- An app fails to launch if the app FQDN is in the camel case. [NGSWS-6587]
- Deleted applications still show up in the cloud library. [NGSWS-6525]
- When there is an outbound proxy configured for Gateway Connector and if the proxy has authentication enabled, Gateway Connector cannot perform authentication with the proxy server.
In race conditions, app configuration does not get propagated intermittently.  
App launch fails intermittently with a “Failed to fetch Policy Document.” error.
Deleted apps still show up in the Workspace app.
Gateway Service supports form response sizes up to 32k for Web applications with form based SSO which is not sufficient for certain applications. With this fix, Gateway ServiceNow supports form response sizes of up to 64k for Web Applications with form based SSO type.

Sometimes, the Gateway Connector crashes when multiple threads access the same resource.
Sometimes, delete operation using an administrator credential for a Web or SaaS application that does not have subscribed users or groups fails.
Configurations for the Citrix Gateway Connector are lost upon editing Form based SSO parameters.

Add another app option does not work when you access the option navigating as follows, Edit app > Overview > Add another app.
A newly added connector takes too long to show up in the UI.
Outbound connections from a connector fail when the connector uses the external FQDN value for the connection via an outbound proxy.
Sometimes, app enumeration fails for a customer when the value of the CC-Customer-Id field has letters in lower case and in upper case.
• Upon launching an application in a Secure Browser session, the display message incorrectly shows “Connecting to [application id]” instead of “Connecting to “[application name].”
[NGSWS-6061]

• Athena tokens which exceed 64k bytes in size upon decompressing is not supported.
[NGSWS-5932]

**Known issues**

May 24, 2022

**V13.4 (February 16, 2022)**

• Enhanced security controls are not enforced for applications opened in a Secure Browser (remote browser) when the apps are launched from a native browser.

  Workaround: Add additional related domains with wildcard domains which satisfy the app URL. For example, if the app FQDN is finapp.acme.com, adding *.acme.com to the related domains enforces the settings as expected.

• HTTP / Web App URL configured with IP address is not supported.

• During ZTNA login, Webview intermittently takes a longer time to load.

**V11.4 (July 30, 2021)**

• The disabled setting of an entry in the application routing table is not enforced during the application launch.
[NGSWS-18296]

• The error page title is not globalized to display the text in the local language.
[NGSWS-19119]

• If the NameID configured in the SAML SSO settings of an application is not available in the user’s token, then the string “Anonymous” is used in the SAML assertion. As a result, the SAML SSO in SP initiated flow fails.
[NGSWS-16761]
V10.5 (June 09, 2021)

- If the NameID configured in the SAML SSO settings of an application is not available in the user’s token, then the string “Anonymous” is used in the SAML assertion. As a result, the SAML SSO in SP initiated flow fails.

[NGSWS-16761]

V3.5 (August 19, 2019)

- Launching an Enterprise Web app for an NTLM authentication enabled resource from Citrix Workspace fails if both of the following conditions are met:
  - Customer’s data center has a proxy server and that proxy server is configured on the Gateway Connector
  - Web App is configured with no SSO (Don’t use SSO)

Workaround:
  - Publish the Web app as a Basic SSO app or
  - Do not have a proxy server configured on Gateway Connector

[NGSWS-8266]

- If there are SSL intercepting devices in the on-premises data center where the Citrix Gateway Connector must be deployed, the connector registration does not succeed if SSL interception is enabled for the following FQDNs.
  - *.nssvc.net
  - *.netscalermgmt.net
  - *.citrixworkspacesapi.net
  - *.citrixnetworkapi.net
  - *.citrix.com
  - *.servicebus.windows.net
  - *.adm.cloud.com

The SSL interception must be disabled for these FQDNs for successful connector registration.

[NGSWS-8923]

- Download logs option is available in Gateway Connector from version 401.251. If you are on an earlier version of the connector and you upgrade the connector to version 401.251, you cannot download the logs even though the Download Logs link is available.

[NGSWS-8438]
Feature deprecations

June 23, 2022

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.

<table>
<thead>
<tr>
<th>Item</th>
<th>Deprecation announced in</th>
<th>Deprecation date</th>
<th>Alternative</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restrict navigation security control</td>
<td>April 2022</td>
<td>15 June 2022</td>
<td>NA</td>
</tr>
<tr>
<td>Citrix Gateway Connector</td>
<td>May 2022</td>
<td>30 September 2022</td>
<td>Connector Appliance. To migrate your Gateway Connector to Connector Appliance, see Migrate Gateway Connector to Connector Appliance.</td>
</tr>
</tbody>
</table>

Admin-guided workflow for easy onboarding and set up

August 9, 2022

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 authen-
tication is a Citrix Cloud service that enables advanced authentication for customers and users log-
ing 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 Pre-
  view)** 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
Citrix Secure Private Access

- Configure direct access to Web apps
- Configure Citrix Gateway Connector
- Citrix Gateway Connector dashboard

• 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 - Preview

• 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: Create access policies

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

1. For users of these applications - This field lists all the applications that an admin has configured in the Secure Private Access service. Admins can select the applications to which this adaptive access policy must be applied.

2. If the following condition is met - Select the condition for which this adaptive access policy must be evaluated. Select the subsequent options based on the selected condition.

  Important:

  The Users or groups condition is a mandatory condition to be met to enable access the applications. Apps subscription alone does not provide your customers access to the applications.
3. Click **Add Condition** to add more conditions.

   An AND operation is performed between the conditions, and then the adaptive access policy is evaluated.

4. **Then do the following** - If the set condition matches, admins can select the action to be performed for the users accessing the application.

   - **Allow access** - Allow access without any preset conditions. **Note:** This option is applicable for browser-based applications only.
   - **Deny access** – When selected, access to the apps is denied. All other options are grayed out.
   - **Allow access with restrictions** - Select one of the preset security policy combinations. These security policy combinations are predefined in the system. Admins cannot modify or add other combinations.

   When you choose **Allow access with restrictions**, you can select the security controls as per your requirement. The following security restrictions can be enabled for the application.

   - **Restrict clipboard access**: Disables cut/copy/paste operations between the app and system clipboard
   - **Restrict printing**: Disables ability to print from within the Citrix Workspace app browser
   - **Restrict navigation**: Disables the next/back app browser buttons
   - **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 Office365 and the user edit an Office365 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.

**Note:**

For TCP applications, both **Allow access** and **Deny access** options are available.

Then do the following:

- Allow access with restrictions

Available security restrictions:

- [ ] Restrict clipboard access
- [ ] Restrict printing
- [ ] Restrict navigation
- [ ] Restrict downloads
- [ ] Restrict uploads
- [ ] Display watermark
- [ ] *Restrict key logging
- [ ] *Restrict screen capture

*Applicable to Citrix Workspace desktop clients only.

5. **In Policy name**, enter the name of the policy.
6. Slide the toggle switch **ON** to enable the policy. The policy is disabled by default.

   **Note**: You can also enable the policy from the Access Policies page by enabling the toggle switch from the **Status** column.

   Click **Create Policy**.

**Note:**

If the admin has configured per-app level enhanced security controls, these are overwritten by the access policies.

**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.
Dashboard overview

August 9, 2022

The dashboard provides admins full visibility into their top apps, top users, connectors health status, bandwidth usage, and so 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 each entity, you can also drill down to view further details.

- **Active users**: Provides details about the active users using the applications (SaaS and Web).
- **Applications**: Provides details about the applications (SaaS and Web) launched over the selected period.
- **Application sessions**: Provides details about the total applications launched versus usage and number of sessions versus users.
- **Uploads**: Displays the upload volume of each app.
- **Downloads**: Displays the download volume of each app.
- **Domains configured**: Summarizes the details of the domains, URLs, and apps accessed by the users.
- **Access policies**: Displays the total number of access policies configured.
- **Diagnostics**: Provides details about the logs related to authentication, application launch, and app enumeration.
- **Connector insights**: Provides insights into the connector statuses.
Diagnostics

Use the Diagnostics chart to view the logs related to authentication, application launch, and app enumeration. 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 or remove columns as per your requirement by clicking the + sign. You can export the user logs into CSV format.

You can use the filters (Event type, Operation type, Result) in the User logs page to narrow down to the logs as per your need. You can also use the Search option in the User logs page to filter the logs based on the categories that you have added to the report, as per your requirement.

For example, you can enter the string Result = “Success”. This search result lists all the logs for which the authentication was successful.

Also, to search for the logs of type app enumeration, you can enter the string Operation-Type = “App
**Enumeration**

To view the list of available categories, click the + sign. You can add or remove categories as required.

**Note:**

By default, the **User logs** page displays the current week's data and only the recent 1000 records. Use the custom date search and filters to refine your search results further.
**Connector status**

Use the **Connector status** chart to view the status of the connectors and the resource locations where the connectors are deployed. Click the **See more** link to view the details. In the **Connector insights** page, you can use the filters **Active** or **Inactive** to filter the connectors based on their status.

![Connector insights](image)

**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 following operators to further refine your search.

- `=`: To search for the policies that exactly match the search criteria.
- `!~`: To search for the policies that do not contain the specified criteria.
- `~`: To search for policies that match the search criteria partially.
- `!~`: To search for policies that do not contain some of the specified criteria.

For example, you can search for policy names “Workday” by using the string `Policy-Name = Workday`. To search for policies that do not contain the term “workday”, use the string `Policy-Name ~ Workday`. 
Apps configuration and management

March 31, 2022

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.
After you have added an Enterprise Web app or a SaaS app, you can assign users or groups to the app. Also, you can edit or delete a published app, and add more subscribers to the published app.

**Support for Enterprise web apps**

July 16, 2022

Web apps 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:

- Gateway Service Standard
- Workspace Standard, Workspace Premium, or Workspace Premium Plus

**System requirements**

You need any one of the connector types for the Enterprise web apps.

**Connector Appliance** - You can 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.

**Important:**

- Citrix Gateway Connector is planned to be deprecated in the upcoming release. Citrix recommends that you migrate to Connector Appliance that is a single Zero Trust Network Access connector. For details on Connector Appliance, see Connector Appliance for Cloud Services.
- To migrate your Gateway Connector to Connector Appliance, see Migrate Gateway Connector to Connector Appliance.
- For TCP apps, Connector Appliance must be used.

**Citrix Gateway Connector** – A virtual appliance that facilitates the remote access to the Enterprise web apps. Citrix Gateway Connector is a virtual appliance. The virtual machine specification must at least have:

- Number of vCPUs must be exactly 2.
Citrix Secure Private Access

- 4 GB RAM minimum.
- 1 Network Adapter (virtual NIC). You can add an extra virtual NIC upon requirement.

Install the Gateway Connector before configuring Enterprise web apps for a cleaner approach.

For more information about Citrix Gateway Connector, see [Citrix Gateway Connector](#).

**Note:**
If there are SSL intercepting devices in the on-premises data center where the Citrix Gateway Connector must be deployed, the connector registration does not succeed if SSL interception is enabled for these FQDNs. The SSL interception must be disabled for these FQDNs for successful connector registration.

For more information on Citrix Gateway Connector, see [Citrix Cloud Gateway Connector](#).

**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 Gateway connector 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.

**To configure an Enterprise web app**

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 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**.

• 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 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.

6. Click **Next**.

7. 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 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** – 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.

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

9. 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.

10. Click **Next.**

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

12. Click **Next.**
13. In the **App Subscribers** section, assign users or groups to the app.

   - In **Choose a domain**, select the domain applicable to the app, and then in **Choose a group or user**, select the group or user to whom you are subscribing this app. You can differentiate between a user and a group based on the appearance of the alphabets U or G that against the name.

   - Click **Save**. The subscriber details are loaded automatically.

You can unsubscribe a subscribed user or a group by clicking the delete icon next to **Status**.

**Important:**

Access to the apps is enabled only after the admin adds an access policy in addition to the app subscription.

14. Click **Finish**.

After you click **Finish**, the app is added to the Applications page. You can delete, manage subscribers, or edit 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.

- **Manage Subscribers**
- **Edit Application**
- **Delete**

## Connector Appliance for Secure Private Access

June 8, 2022

To configure Secure Private Access with Connector Appliance, complete the following steps:

1. Install 2 or more Connector Appliances in your Resource Location.

   For more information about setting up your Connector Appliances, see **Connector Appliance for Cloud Services**.

2. If you need 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) On your Active Directory controller, perform the following.

  - Use the following command to add a service principal name (SPN) for the webserver that must use KCD.

    ```bash
    1. `setspn -A http://<webserver fqdn> <domain\Kerberos user>`
    2. <!--NeedCopy--> 
    ```

    - Confirm the SPNs for the Kerberos user using the following command.

    ```bash
    1. `setspn -l <Kerberos user>`
    2. <!--NeedCopy--> 
    ```

    In the following example, an SPN is added for a webserver that the KCD account must access.

    ```bash
    C:\Windows\system32\setspn -A http://iis1.xmtest.net kcdadmin
    Checking domain DC=xmtest,DC=net
    Registering ServicePrincipalNames for CN=kcdadmin test,CN=Users,DC=xmtest,DC=net
    http://iis1.xmtest.net
    updated object
    C:\Windows\system32\setspn -l kcdadmin
    Registered ServicePrincipalNames for CN=kcdadmin test,CN=Users,DC=xmtest,DC=net: http://iis1.xmtest.net
    ```

    Notice that the **Delegation** tab appears after you run the `setspn` command.
• Select **Trust this user for delegation to specified services only** and **Use any authentication protocol**.

• Add the web server for which you need Kerberos SSO, and select the **Service Type** as **http**.
c) Follow the Citrix Secure Private Access documentation to set up the Citrix Secure Private Access service. During setup, Citrix Cloud recognizes the presence of your Connector Appliances and uses them to connect your resource location.

Note:
Use the machine account name instead of creating a new user account.
For more information, see the following webpages:

- Get started with Citrix Secure Private Access
- Configure Citrix Secure Private Access

Where this article refers to information about the Cloud Connector (prerequisite #4), instead see the Connector Appliance documentation:

- 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 about how the validation failed.

© 1999–2022 Citrix Systems, Inc. All rights reserved.
Citrix Gateway Connector

May 12, 2022

Citrix Gateway Connector is a Citrix component which serves as a channel of communication between Cloud services (Secure Private Access service, ADM, and so on) and on-premises components such as Web servers. It is a virtual appliance compatible with Citrix Hypervisor, VMware ESXi, and Microsoft Hyper-V with a small form factor. Citrix Gateway Connector facilitates the remote access to the Enterprise web apps.

**Important:**
- Citrix Gateway Connector is planned to be deprecated in the upcoming release. Citrix recommends that you migrate to Connector Appliance that is a single Zero Trust Network Access connector. For details on Connector Appliance, see [Connector Appliance for Cloud Services](#).
- To migrate your Gateway Connector to Connector Appliance, see [Migrate Gateway Connector to Connector Appliance](#).
- For TCP apps, Connector Appliance must be used.

**How it works**

Citrix Gateway Connector authenticates and encrypts all communication between Citrix Cloud and your resource locations. The communication between the Citrix Gateway Connector and Citrix Cloud is outbound. All connections are established from the Citrix Gateway Connector 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

**Note:**

If there are SSL intercepting devices in the on-premises data center where the Citrix Gateway Connector must be deployed, the connector registration does not succeed if SSL interception is enabled for these FQDNs. The SSL interception must be disabled for these FQDNs for successful...
Capabilities of Citrix Gateway Connector

The following are some of the capabilities of Citrix Gateway Connector.

- Acts as a reverse proxy – Citrix Gateway Connector acts as a reverse proxy to Enterprise Web apps. The required web application ports must be opened from the Gateway Connector to the apps.
- Enables single sign-on: The Citrix Gateway Connector provides the following single sign-on capabilities with the Secure Private Access service.
  - Basic SSO
  - Kerberos
  - Form-based
  - SAML
  - No SSO
- Enables application of optional security policies through Secure Private Access – The Citrix Gateway Connector provides enhanced security capabilities through the Citrix Secure Private Access service. For example,
  - Restrict clipboard access
  - Restrict printing
  - Restrict navigation
  - Restrict downloads
  - Display watermark
  - App protection policies
  - Enforce policy on mobile device

For details, see Support for Enterprise web apps and Support for Software as a Service apps.

System requirements

Citrix Gateway Connector is a virtual appliance. The minimum system requirements for the Citrix Gateway Connector are as follows:

- Number of vCPUs must be exactly 2.
- 4 GB RAM minimum.

Important:
The new minimum system requirement for RAM has changed. If you have an existing Citrix Gateway Connector, upgrade the system memory of your virtual machines to match the new requirement of 4 GB RAM.
Citrix Secure Private Access

For details, see Upgrade the system memory of Citrix Gateway Connector virtual machines.

- 1 Network Adapter (virtual NIC). You can add an extra virtual NIC upon requirement.
- Firewall:
  - UDP port 53 to DNS server
  - TCP and UDP port 389 to Active Directory Domain Controllers (optional *)
  - TCP port 636 to Active Directory Domain Controllers (optional *)
  - TCP port 3268 to Active Directory Domain Controllers (optional *)
  - TCP port 3269 to Active Directory Domain Controllers (optional *)
  - 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
  - TCP ports (**) to Web servers accessed using Citrix Gateway Connector
  - Open port 8443 inbound for web-based management
    * - Required to perform domain-based single sign-on to Web applications
    ** - Ports determined by the customers’ environment – ports 80 and 443 are typical

**Recommended:** Network with DHCP enabled to simplify the initial configuration.

Ways to install Citrix Gateway Connector

Citrix Gateway Connector can be installed in one of the following ways.

- From the Citrix Cloud user interface
- While adding an Enterprise Web app

In both cases, you must create a new virtual machine as described in the following section.

Create a new virtual machine

1. Sign in to Citrix Cloud.
2. From the menu in the top left of the screen, select Resource Locations.
• If you have no existing resource locations, click **Download** on the Resource Locations page. When prompted, save the cwcconnector.exe file. For details, see **Cloud Connector Installation**.

• If you have a resource location but no Cloud Connectors installed in it, click the Cloud Connectors bar and then click **Download**. When prompted, save the cwcconnector.exe file.

3. Click **Gateway Connectors**.

4. Select the hypervisor and click **Download Image**. Import the locally downloaded image to your hypervisor and create a new virtual machine (Citrix Gateway Connector).

5. Click **Get Activation Code**.

6. The activation code is generated as follows.

7. Once the installation is complete, Click **Detect**.

**Install the Citrix Gateway Connector by using the Citrix Cloud user interface**

The following are the steps to set up a resource location and install Citrix Gateway Connector using the Citrix Cloud user interface:

1. On top left of the **Citrix Cloud** screen, click the hamburger icon and select **Resource Locations**. Click the plus icon next to **Resource Locations**.

2. Provide a name for the resource location and click **Save**.

3. Double-click the plus icon next to Citrix Gateway Connectors under the newly created resource location.

4. Complete the steps as described in **Create a new virtual machine**.
Install Citrix Gateway Connector while adding an Enterprise Web app

While adding an Enterprise Web app using the Secure Private Access service user interface, you can set up a new resource location and download connectors. For details on adding an Enterprise Web app, see Support for Enterprise web apps.

To set up a resource location and download connectors, perform the following steps:

1. In the Web app connectivity section, select the Create New radio button. Provide a name for the resource location and click Save.

2. Click Install Citrix Gateway Connector.

3. Complete the steps as described in Create a new virtual machine.

Access the Citrix Gateway Connector user interface by using the URL

You can access the Citrix Gateway Connector user interface by using the URL that is displayed in one of the messages on the newly installed Citrix Gateway Connector VM. You can also log on to the Citrix Gateway Connector CLI as an administrator and run the show 1p command for viewing the IP address assigned to the Citrix Gateway Connector through DHCP. Then you can open https://<IP address>:8443 on your browser to access the Citrix Gateway Connector admin user interface.

Important:
For Azure, Citrix recommends that customers access the Citrix Gateway Connector user interface from inside the Azure Virtual network.

Log on and set up the Citrix Gateway Connector

After the Citrix Gateway Connector installation is complete, look for the following message on the newly installed VM (Citrix Gateway Connector).
Type the mentioned URL in a browser to access the Citrix Gateway Connector user interface. You can also log on to the Citrix Gateway Connector CLI as an administrator and run the `show ip` command. The command displays the IP address assigned to the Citrix Gateway Connector through DHCP. Then open `<https://IP address:8443>` on your browser to access the Citrix Gateway Connector admin user interface.

1. The user name and password for the following screen is `administrator` for the first time user.

2. Change the password by providing a password of your choice in the Set administrator password section and click Continue.

3. Enter the following configuration details in the System settings section and click Continue.
   
   • Connector IP Address – IP address of Gateway Connector.
   • Subnet Mask – Subnet mask of the Gateway Connector IP address.
   • Default Gateway – IP address of the default gateway.
   • DNS Server – IP address of the DNS server. Starting from Citrix Gateway Connector release 13.0, there is a change in the DNS server configuration. For details, see the section Changes to the DNS server settings.
   • Proxy IP – Your internal proxy server IP address.
   • Proxy Port – Port of the proxy server.
Changes to the DNS server settings:

Starting from Citrix Gateway Connector 13.0.400.xxx, the DNS configuration for both UDP and TCP protocol on the connector appliance is updated automatically when it is set in the System Settings section. However if you upgrade your connector from earlier versions, you have to manually delete the DNS setting and read it again. To do so, perform the following.

a) Navigate to the Citrix Gateway Connector dashboard > Edit Settings.

b) Click the delete icon next to the first DNS Server field and click Continue.

c) Navigate to the Edit Settings page, read the same DNS server, and click Continue.

d) Repeat the steps for the second DNS server.
Note:

- You do not have to perform these steps for new instances of the 13.0 Citrix Gateway Connector.
- You need not perform the earlier mentioned steps immediately after the upgrade. There is no loss of functionality if this is not done. These steps must be performed for enterprise customers who require DNS over TCP Functionality to make Enterprise Web apps to function correctly.

4. In the Single sign on section, check Enable Kerberos Single Sign On for capabilities beyond the basic authentication.

Active directory domain is the global domain and is set as the realm of the KCD account. If you want to override the global realm of the user, then you can use the following command in the connector. SSH to your gateway connector using the same credentials that you use to log on to the connector configuration page. Type the following command:

```
1  set kcdaccount ngs_kcdaccount -userRealm <value>
2  <!--NeedCopy--> 
```

Example:
In this example, realm aaa.local is the global domain and bbb.local is the overridden user realm.

```
1  ssh kcdaccount
2  KCD Account : ngs_kcdaccount
3  Keytab : 
4  Realm : AAA.LOCAL
5  User Realm : BBB.LOCAL
6  DelegatedUser : 
7  User Certificate : 
8  CA Certificate : 
9  Done
10  <!--NeedCopy--> 
```

You can validate the Kerberos details by two ways, realm-only mode and full Kerberos constrained delegation (KCD).

Important:
For using KCD on a Citrix Gateway Connector, you must first set up KCD in your data center before configuring KCD on a Citrix Gateway Connector. For details, see Prerequisites to set up KCD in your data center before configuring KCD on Citrix Gateway Connector.
Citrix Secure Private Access

You can use the Test option for debugging purposes. For example, if the Kerberos details are not correctly set and if an app is added, SSO to the app fails.

a) For realm-only mode, select Enable Kerberos Single Sign On, enter the following details, and then click Test Kerberos.

- **Active Directory Domain** – Active Directory domain for the users to be granted access.
- **Service FQDN** - FQDN of the service (the service FQDN that the user must access through configuring Web apps).
- **Username** – User name of the logged on user.
- **Password** – Password of the logged on user.

Test Kerberos Configuration

b) For full Kerberos constrained delegation, select Kerberos Constrained Delegation, enter the following details, and then click Test Kerberos.

- **Active Directory Domain** – Active Directory domain for the users to be granted access.
- **Service Account Username** – Service account user name used for delegation. For details, see Prerequisites to set up KCD in your data center before configuring KCD on Citrix Gateway Connector.
- **Service Account Password** – Password for the service account user name used for delegation.
- **Service FQDN** - FQDN of the service (the service FQDN that the user must access through configuring Web apps).
- **Username** - User name of the logged on user.
In both cases, based on whether the validation is successful or not, the respective messages appear. The following figure displays a sample validation error message.

5. Enter the activation code to register the connector with Citrix Cloud. Click **Save** and **Finish**.

6. Click **Connectivity Test**. (This step is optional)
The **Connectivity Test** option enables you to confirm that there are no errors in the Gateway Connector configuration and the Gateway Connector is able to connect to the URLs. This step is optional. You can skip this step and proceed with activating the Gateway Connector.

- When you click **Connectivity Test**, a set of URLs is run in the back end to ensure that the connector is able to connect to those URLs. If all the URLs are successfully run, the connectivity test success message appears. The following FQDNs are run when you click Connectivity Test.
  
  - agent.netscalermgmt.net
  - agent.netscalermgmt.net
  - trust.citrixnetworkapi.net
  - download.citrixnetworkapi.net
  - web-reg.c.nssvc.net
  - agent.adm.cloud.com
  - anse.agent.adm.cloud.com
  - railay.agent.adm.cloud.com
  - agent.netscalermgmt.net
  - evergreen.citrixnetworkapi.net
  - agenthub.citrixworkspacesapi.net
  - callhome.citrix.com

- If any of these URLs do not respond, an error message appears and the corresponding URL is displayed. The error messages are classified under three categories.

  - DNS error
  - Server error
  - SSL exception

The following images display sample error messages.
7. Finally enter the activation code to register the connector with Citrix Cloud and click **Save and Finish**.

For details on how to get the activation code, see [Create a new virtual machine](#).
Prerequisites to set up KCD in your data center before configuring KCD on Citrix Gateway Connector

1. Create a user account in the active directory that must be used for delegation.
2. Use the following command to add a service principal name (SPN) for the webserver that must use KCD.

```
setspn -A http://<webserver fqdn> <domain\Kerberos user>
```

3. Confirm the SPNs for the Kerberos user using the following command.

```
setspn -l <Kerberos user>
```

In the following example, an SPN is added for a webserver that the KCD account must access.
Notice that the **Delegation** tab appears after you run the `setspn` command.
4. Select Trust this user for delegation to specified services only and Use any authentication protocol.

5. Add the web server for which you need Kerberos SSO, and select the Service Type as http.
Note:
You can now use this user account when configuring KCD on a Citrix Gateway Connector. This user account must be added as the service account user name.
Troubleshoot Citrix Gateway Connector registration issues

You can use the Trace feature and the Download Logs feature to troubleshoot Citrix Gateway Connector registration issues.

Trace feature

While registering Citrix Gateway Connector, you might come across issues because of which the registration might not be successful. To troubleshoot these issues, you can use the Trace Info link that appears the first time you register the connector. You can download the trace files and share it with the administrators for troubleshooting. Trace files are in an encrypted format. The Trace Info link is also available in the Gateway Connector dashboard even after the registration. You can also capture and download trace files from the dashboard for debugging issues.

How to download trace files

1. Click Trace Info.

2. In the Trace dialog box, select the duration that you want to run the trace and then click Start. The Trace dialog box displays the progress.
3. You can stop the trace that is in progress before it is complete. You can then download the trace files by clicking the **Download** button. You can also start a new trace from the dialog box.

![Trace dialog box]

**Note:** For debugging registration failures, first start a trace with a given pre-set interval, enter the activation code, and submit for registration.

- If the registration fails, you can click the **Trace info** link to bring up the **Trace** dialog again, stop the trace, and then download the trace files.
- If the registration succeeds, then the Dashboard console comes up and the trace stops automatically in the background.

**Important:**

- Closing the **Trace** window before the trace is complete does not stop the trace. The trace keeps running in the background until it is completed.
- If you refresh or close the browser when the trace is in progress, you must manually stop the trace by clicking the **Trace Info** link to prevent the trace from running indefinitely. In this scenario, the **Trace Info** link displays only the **Stop** button and does not display the **Download** button. Therefore, you cannot download the captured trace. To capture the trace again, click **Start new trace**.

**Download logs**

Download logs option is available in Gateway Connector from version 401.251. If you are on an earlier version of the connector and you upgrade the connector to version 401.251, you still cannot download the logs even though the Download Logs link is available.

**How to download logs**

1. Click **Download Logs**.

   The **Download Logs** link is available even during the first-time use to help setup the connector.
A log file is generated. Generation of the log file takes some time. Once the log file if generated, a message with the link to the download file appears.

2. Click **Download**. A .tgz file is downloaded.

All files in the download folder are in an encrypted format. Contact the Citrix Cloud support team for help.

**Delete a Citrix Gateway Connector**

Perform the following to delete a Citrix Gateway Connector.

1. Sign in to Citrix Cloud.
2. Select **Resource Locations** from the menu in the top left of the screen.
3. In the Resource Locations page, click **Gateway Connectors** for a specific resource location.
4. Select the Gateway Connector that you want to delete and click the ellipsis menu.
5. Select **Remove Connector**.

A confirmation dialog box appears.

6. Click **OK**.

**Note**: It might take a couple of minutes for the gateway Connector to be removed from the Resource Locations page. Also, it might take sometime for the Gateway Connector to unregister from the gateway controller.

**Upgrade the system memory of Citrix Gateway Connector virtual machines**

Gateway connector RAM size is 2 GB, by default. Therefore, it is recommended that you increase the RAM size to 4 GB for optimal performance. This recommendation is applicable for new or existing connector installations.

If you have two connectors per resource location for high availability, perform the following to upgrade the connector virtual machines.

1. From the hypervisor, shut down one of the connector virtual machines.
2. Edit the hardware configuration or settings of the virtual machine depending on the type of hypervisor.
3. Navigate to Memory tab.
4. If the RAM size is 2,048 MB, increase it to 4,096 MB and save the configuration.
5. Power up the virtual machine.
6. Repeat these steps on the second connector virtual machine as well.
Important:
Ensure that you upgrade one connector at a time to avoid any outages.

Continuous availability of the Citrix Gateway Connector

As long as you ensure continuous availability of the Citrix Gateway Connector in each resource location, you can manage the machines where they are installed one at a time to avoid outage periods.

For continuous availability, install multiple Citrix Gateway Connectors in each of your resource locations. Citrix recommends at least two (2) Citrix Gateway Connectors in each resource location. If one Citrix Gateway Connector is unavailable for any time, the other Citrix Gateway Connectors can maintain the connection.

As long as there is one Citrix Gateway Connector available, there is no loss in communication with Citrix Cloud.

Citrix Gateway Connectors can be restricted to upgrade during a specified maintenance window every 24 hour, controlled per Resource Location.

Load management

Manage load by installing multiple Citrix Gateway Connectors in each resource location. Since each Citrix Gateway Connector is stateless, the load can be distributed across all available Citrix Gateway Connectors. There is no need to configure this load balancing function. It is automated.

Citrix Gateway Connector dashboard

May 12, 2022

The Citrix Gateway Connector dashboard provides key metrics such as CPU usage (packet and management), in-use memory, and TCP connection details.

Important:

- Citrix Gateway Connector is planned to be deprecated in the upcoming release. Citrix recommends that you migrate to Connector Appliance that is a single Zero Trust Network Access connector. For details on Connector Appliance, see Connector Appliance for Cloud Services.
- To migrate your Gateway Connector to Connector Appliance, see Migrate Gateway Connector to Connector Appliance.
- For TCP apps, Connector Appliance must be used.
You can perform the following from the Gateway Connector dashboard.

**Restart the connector**

Click **Restart** to restart the connector from the user interface. You can either do a warm reboot or a complete restart of the Gateway Connector.

**Re-register the connector with Citrix Cloud**

Click **Retry activation code** if you want to install the already registered connector in a different resource location. Enter the activation code that was provided when you downloaded the Gateway Connector.

**Download support logs**

Click **Download Logs** to download the support logs from the Gateway Connector. The **Download Logs** link is available even during the first-time use to help setup the connector.

1. Click **Download Logs**.

   A log file is generated. Generation of the log file takes some time. Once the log file if generated, a message with the link to the download file appears.

2. Click **Download**. A .tgz file is downloaded.
All files in the download folder are in an encrypted format. Reach out to the Citrix Cloud support team for help.

**Important:** Download logs option is available in Gateway Connector from version 401.251. If you are on an earlier version of the connector and you upgrade the connector to version 401.251, you still cannot download the logs even though the Download Logs link is available.

### Download trace files

You can use the Trace Info link to download the traces files. For details, see Download trace files for troubleshooting Citrix Gateway Connector registration issues.

### Migrate Gateway Connector to Connector Appliance

May 17, 2022

Citrix Gateway Connector is planned to be deprecated in the upcoming release. Therefore, 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

July 15, 2022

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 Gateway Connectors or 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 Gateway Connectors or 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 is displayed to your users in the workspace.
   
   - **App icon** – Click **Change icon** to change the app icon. The icon file size must be 128x128 pixels. If you do not change the icon, the default icon is displayed.

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

7. Select **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 are not supported.
   
   - Full chain of certificate must be uploaded.

   - **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. 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.
Where is the application located? *

- Outside my corporate network
- Inside my corporate network

App name *
SharePoint

App icon
Change icon
Use default icon

App description
Collaborative platform used for document management and storage.

Do not display application icon to users

Direct Access
Enable direct browser-based access to internal web applications.

URL *
http://sharepoint2013.com

SSL certificate *
ssl-automation-wildcard.pem

Add new SSL certificate

Related Domains *
*.sharepoint2013.com

SSL certificate
wwco_reshuffled9.pem

Add new SSL certificate

Add another related domain

CName (Canonical name) record

directaccess.bmws.netscalergatewaydev.net

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 Gateway connector or a 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. In the **App Subscribers** section, assign users or groups to the app.

- In **Choose a domain**, select the domain applicable to the app, and then in **Choose a group or user**, select the group or user to whom you are subscribing this app. You can differentiate between a user and a group based on the appearance of the alphabets **U** or **G** that
Click **Save**. The subscriber details are loaded automatically.

You can unsubscribe a subscribed user or a group by clicking the delete icon next to **Status**.

12. Click **Finish**. The app is added to the Applications page. You can delete, manage subscribers, or edit 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.

- **Manage Subscribers**
- **Edit Application**
- **Delete**

With this configuration in place, the end users can access the configured web app directly using their client browser.

**Support for client-server apps**

June 28, 2022

With Citrix Secure Private Access, you can now access all private apps including TCP/HTTPS apps either using a native browser or a native client application via the Citrix Secure Access agent 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.

**How it works**

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

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

**Not included in this release**

- Access to UDP apps is not supported.
Admin Configuration – ZTNA agent-based access to TCP apps

Prerequisites

- 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.

Note:
You must use a Connector Appliance for TCP apps.

Steps to configure TCP 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 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:**
If the admin has configured the IP based destinations, end users are expected to
access the app with the IP address only. Similarly, if the application is configured with an FQDN, the users are expected to access the application through the FQDN only. You cannot access an app through the FQDN if the app is configured based on IP address.

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

<table>
<thead>
<tr>
<th>Destination input</th>
<th>How to access the app</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.10.1-10.10.10.100</td>
<td>End user is expected to access the app only through IP addresses in this range.</td>
</tr>
<tr>
<td>10.10.0/24</td>
<td>End user is expected to access the app only through IP addresses configured in the IP CIDR.</td>
</tr>
<tr>
<td>10.10.10.101</td>
<td>End user is expected to access the app only through 10.10.10.101</td>
</tr>
<tr>
<td>*.info.citrix.com</td>
<td>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</td>
</tr>
<tr>
<td>info.citrix.com</td>
<td>End user is expected to access info.citrix.com only and no subdomains. For example, sub1.info.citrix.com is not accessible.</td>
</tr>
</tbody>
</table>

- **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.

<table>
<thead>
<tr>
<th>Port input</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>*</td>
<td>By default, the port field is set to “*” (any port). The port numbers from 1 to 65535 are supported for the destination.</td>
</tr>
<tr>
<td>Port input</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>1300–2400</td>
<td>The port numbers from 1300 to 2400 are supported for the destination.</td>
</tr>
<tr>
<td>38389</td>
<td>Only the port number 38389 is supported for the destination.</td>
</tr>
<tr>
<td>22,345,5678</td>
<td>The ports 22, 345, 5678 are supported for the destination.</td>
</tr>
<tr>
<td>1300–2400, 42000–43000, 22,443</td>
<td>The port number range from 1300 to 2400, 42000–43000, and ports 22 and 443 are supported for the destination.</td>
</tr>
</tbody>
</table>

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

- **Protocol** – TCP

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 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. In the **App Subscribers** section, assign users or groups to the app.

   - In **Choose a domain**, select the domain applicable to the app, and then in **Choose a group or user**, select the group or user to whom you are subscribing this app. You can differentiate between a user and a group based on the appearance of the alphabets **U** or **G** that against the name.

   - Click **Save**. The subscriber details are loaded automatically.

You can unsubscribe a subscribed user or a group by clicking the delete icon next to **Status**.

8. Click **Finish**. The app is added to the Applications page. You can delete, manage subscribers, or edit 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.

   - **Manage Subscribers**
   - **Edit Application**
Citrix Secure Private Access

- **Delete**

- To configure the authentication methods required for your users, see [Set up identity and authentication](#).

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

**Workspace Configuration**

<table>
<thead>
<tr>
<th>Access</th>
<th>Authentication</th>
<th>Customize</th>
<th>Service Integrations</th>
<th>Sites</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Workspace URL**

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

https://bmwtest.cloud.com

**Admin Configuration – ZTNA agent-based access to HTTP(S) apps**

**Note:**

To access existing or new HTTP/HTTPS apps using the Citrix Secure Access agent, in addition to a Gateway connector you must also install at least one (recommended two for high-availability) Connector Appliance in your resource location. The connector 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**


**Points to note**

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

- 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 and HTTP(S) apps**

Adaptive access provides the ability for admins to govern access to business-critical apps based on multiple contextual factors like device posture check, user geo-location, user role, and the Citrix Analytics service provided risk score.

**Note:**
- You can deny access to TCP 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 app destinations configured for the ZTNA application.

**To create an adaptive access policy**

Admins can use the admin-guided workflow wizard to configure Zero Trust Network Access to SaaS apps, internal web apps, and TCP 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 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 agent. 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 holds good while accessing the app via the Secure Access agent.
- 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 agent on a Windows machine

Supported OS versions:


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

2. Click Install to install the agent on your Windows machine. If you have an existing Citrix Gateway agent, the same gets upgraded.
3. Click **Finish** to complete the installation.

![Citrix Secure Access Setup](image)

**Note:**

Multi-user session in Windows is not supported.

**Microsoft Edge Runtime installation steps**

Microsoft Edge Runtime is now required for the authentication UI on the Secure Access agent. 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](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 agent 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 Citrix Secure Access agent or Microsoft Edge Runtime to the client machines.

**Steps to install Citrix Secure Access agent on a macOS machine**

**Prerequisites:**
• Download the Citrix Secure Access app 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.

**Note:**

Mobile devices - iOS and Android are not supported.

**Launch a configured app - End-user flow**

1. Launch the Citrix Secure Access agent on the client device.
2. Enter the Workspace URL provided by the customer admin in the URL field in the Citrix Secure Access agent 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 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.

<table>
<thead>
<tr>
<th>Conflict Scenarios</th>
<th>Existing application domain entry</th>
<th>New entry from app addition</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subset Overlap</td>
<td>10.10.0.0-10.10.255 RL1</td>
<td>10.10.10.50-10.10.60 RL1</td>
<td>Allow; Warning info - Subset overlap of IP domain with existing entries</td>
</tr>
<tr>
<td>Subset Overlap</td>
<td>10.10.0.0-10.10.255 RL1</td>
<td>10.10.10.50-10.10.60 RL2</td>
<td>Allow; Warning info - Subset overlap of IP domain with existing entries</td>
</tr>
<tr>
<td>Partial Overlap</td>
<td>10.10.10.0-10.10.100 RL1</td>
<td>10.10.10.50-10.10.200 RL1</td>
<td>Allow; Warning info - Partial overlap of IP domain with existing entries</td>
</tr>
</tbody>
</table>
## Conflict Scenarios

<table>
<thead>
<tr>
<th>Conflict Scenarios</th>
<th>Existing application domain entry</th>
<th>New entry from app addition</th>
<th>Behavior</th>
</tr>
</thead>
<tbody>
<tr>
<td>Partial Overlap</td>
<td>10.10.10.0-10.10.10.100 RL1</td>
<td>10.10.10.50-10.10.10.200 RL2</td>
<td>Allow; Warning info - Partial overlap of IP domain with existing entries</td>
</tr>
<tr>
<td>Complete Overlap</td>
<td>10.10.10.0/24 RL1</td>
<td>10.10.10.0-10.10.10.255 RL1</td>
<td>Error; &lt;Completely overlapping IP domain's value&gt; IP domain completely overlaps with existing entries. Please change the existing routing IP Entry or configure a different destination</td>
</tr>
<tr>
<td>Complete Overlap</td>
<td>10.10.10.0/24 RL1</td>
<td>10.10.10.0-10.10.10.255 RL2</td>
<td>Error; &lt;Completely overlapping IP domain's value&gt; IP domain completely overlaps with existing entries. Please change the existing routing IP Entry or configure a different destination</td>
</tr>
<tr>
<td>Exact Match</td>
<td>20.20.20.0/29 RL1</td>
<td>20.20.20.0/29 RL1</td>
<td>Allow; Domains already exist in the domain routing table. Changes made updates the domain routing table</td>
</tr>
</tbody>
</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\SecureAccessClient

- Login script path: SecureAccessLogInScript type REG_SZ
- Logout script path: SecureAccessLogOutScript type REG_SZ

**Release notes references**

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

**Support for Software as a Service apps**

June 28, 2022

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 apps 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 Secure Private Access service UI (citrix.cloud.com). The admin then adds subscribers (users) for the apps.
2. Admin provides the service URL to the users to access Citrix Workspace.
3. Users subscribed for an app can see the app upon logon to Citrix Workspace.
4. To launch the app, a user clicks the enumerated SaaS app icon.
5. SaaS app trusts the SAML assertion provided by the Secure Private Access service and the app is launched.

**Note:**
Configured SaaS apps are aggregated along with virtual apps and other resources in Citrix Workspace for a unified user experience.

**Configure and publish SaaS apps**

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 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 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 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 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.

5. Click **Next**.

6. 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 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** – 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 service provider initiated flow.

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

![Single Sign On](image)

Select the sign on type for your SaaS app setup.

**SAML**

*Sign Assertion*

- **Assertion URL**

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

*Relay State*

https://login.microsoftonline.com/login.srf?wa=wsignint%2E0&ver=7%2E1

*Audience*

urn:federation:MicrosoftOnline

*Name ID Format*

- **Persistent**

*Name ID*

Active Directory GUID

Advanced attributes (optional)

An attribute is additional information about the user that is sent to the application for access control decisions. Make sure these values are consistent with the settings in the SaaS vendor.
8. 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.

9. Click **Next**.

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

11. Click **Next**.

12. In the **App Subscribers** section, assign users or groups to the app.
• In **Choose a domain**, select the domain applicable to the app, and then in **Choose a group or user**, select the group or user to whom you are subscribing this app. You can differentiate between a user and a group based on the appearance of the alphabets **U** or **G** that against the name.

• Click **Save**. The subscriber details are loaded automatically.

**Important:**
Access to the apps is enabled only after the admin adds an access policy in addition to the app subscription.

You can unsubscribe a subscribed user or a group by clicking the delete icon next to **Status**.

13. Click **Finish**.

After you click **Finish**, the app is added to the Applications page. You can delete, manage subscribers, or edit 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.

• **Manage Subscribers**
• **Edit Application**
• **Delete**

**References**

For a complete end-to-end configuration of an app, see [Admin guided workflow for easy onboarding and set up](#).
Migration of app security controls and access policies to the new access policy framework

July 16, 2022

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 “App subscriber” section of the application configuration wizard to enable access. Going forward, at least one access policy is required to enable access to the applications. App subscription alone will not enable access to the applications.

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 did not have user subscription, then new policies are not created.

The following table summarizes the changes.

<table>
<thead>
<tr>
<th>If you had configured an …</th>
<th>Then …</th>
</tr>
</thead>
<tbody>
<tr>
<td>App without any enhanced security conditions</td>
<td>A new policy is created with users and groups as the mandatory condition. The users or groups is derived from the user subscription. The action is set to Allow Access.</td>
</tr>
<tr>
<td>If you had configured an…</td>
<td>Then …</td>
</tr>
<tr>
<td>--------------------------</td>
<td>--------</td>
</tr>
</tbody>
</table>
| 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 user subscription. 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 subscriptions. The users or groups is derived from the user subscription. 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.

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

**Apps configuration using a template**

June 28, 2022

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.
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.

   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.

Single sign on

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

- SAML
- Don't use SSO

Advanced attributes (optional)

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

- Attribute Name
- Attribute Format
- Attribute Value

Add another attribute

Save

Note:

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

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

8. Click Next.

9. In the App Subscribers section, assign users or groups to the app.

   - In Choose a domain, select the domain applicable to the app, and then in Choose a group
or user, select the group or user to whom you are subscribing this app. You can differentiate between a user and a group based on the appearance of the alphabets U or G that against the name.

- Click Save. The subscriber details are loaded automatically.

You can unsubscribe a subscribed user or a group by clicking the delete icon next to Status.

Important:
Access to the apps is enabled only after the admin adds an access policy in addition to the app subscription.

10. Click **Finish**.

After you click **Finish**, the app is added to the Applications page. You can delete, manage subscribers, or edit 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.

- Manage Subscribers
- Edit Application
- Delete

### SaaS app server specific configuration

March 31, 2022

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 incident 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 time 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.

• **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.

• **HelloSign** - 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.
• **Oomniza** - 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.
- **Runscape** - 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.
• **Skedally** - 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.
• **ZIIVER** - 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**

March 31, 2022

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

March 31, 2022

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 Gateway connectors 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**.
Diagnostic logs for Enterprise Web and SaaS apps access

April 1, 2022

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.

Citrix Secure Private Access customers can now access this script and run the script in their environment to view the diagnostic logs. Customers can then use the logs to troubleshoot or debug SaaS/web apps access failures reported by their end users.

Points to note:

- Presently, there is no user interface to troubleshoot or debug the Enterprise Web/SaaS apps access failure logs. User Interface support is planned for future releases.
- The PowerShell script can be downloaded from [https://citrix.sharefile.com/d-s3096b922f9dd41c38d906c94b818ef26](https://citrix.sharefile.com/d-s3096b922f9dd41c38d906c94b818ef26).
- To run the PowerShell script, you must enter a client ID and Secret in the script.

**Following are the steps to create a client ID and Secret using Citrix Cloud user interface.**

1. From the Citrix Cloud menu, select **Identity and Access Management**.
2. On the **Identity and Access Management** tile, select **API Access** tab.
   
   ![Identity and Access Management](image)

   
   - **Authentication**
   - **Administrators**
   - **API Access**
   - **Domains**
   - **Recovery**

   - **Secure Clients**
   - **Product Registrations**

3. Provide a name for **Secure Client** and click **Create Client**.
4. Click **Download** on the following screen to download your ID and Secret.

To run the PowerShell script and save the diagnostic logs, open a PowerShell tool in your machine and type the following commands:

```powershell
1. Set-ExecutionPolicy RemoteSigned
2. <!--NeedCopy-->
**Note:** You must set the **PowerShell Execution Policy** to **RemoteSigned** or **Unrestricted** to allow local PowerShell scripts to be run.

For more information about the PowerShell Execution Policy, see the [Microsoft PowerShell article about Execution Policies](#).

**To download the diagnostic logs:**

1. Import-Module `<location of the locally downloaded PowerShell script>`
3. Enter the client secret.

The diagnostic logs get saved in the file specified under the **outFile** parameter in the previous command.

**Parameter description:**

- **ClientId** – Client ID created and downloaded from Citrix Cloud UI
- **ClientSecret** - Client secret created and downloaded from Citrix Cloud UI
- **Customer** - ID to be taken from the Citrix Cloud UI -> Identity and Access Management -> API Access
- **OutFile** - Location where you want to save your output log file

**Example command:**

```
1 Get-CitrixSecurePrivateAccessLogs -clientId "cd720b41-21f2-3232-9cc8-34c90kcm73f2" -customer "j5d24a513k3r" -timeRange "2022-01-25T00:00:00.000Z,2022-01-30T00:00:00.000Z" -outFile "C:\diagnosticLogs.csv"
2 <!--NeedCopy-->
```
Adaptive Authentication service

July 11, 2022

Citrix Cloud customers can use Citrix Workspace to provide Adaptive Authentication to Citrix DaaS. 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 that provides all the advanced authentication capabilities such as the following:

**Multifactor authentication:**
Multifactor authentication enhances the security of an application by requiring users to provide multiple proofs of identity to gain access. Customers can configure various combinations of factors in the multifactor authentication mechanism based on the business requirement. For details, see [Sample authentication configurations](#).

**Device posture scans:**
Users can be authenticated based on the device posture. Device posture scan, also known as endpoint analysis scan, checks if the device is compliant. For example, if the device is running the latest OS version, service packs, and registry keys are set. Security compliance involves scans to check if an antivirus is installed or the firewall is turned on and so on. The device posture can also check if the device is managed or unmanaged, corporate owned, or BYOL.

**Conditional authentication:**
Based on the user’s parameters, such as network location, device posture, user group, time of the day, conditional authentication can be enabled. You can use one of these parameters or a combination of these parameters for doing conditional authentication.

Example of a device posture-based authentication: You can do a device posture scan to check if the device is a corporate managed or BYOD. If the device is a corporate managed device, you can challenge the user with the simple AD (username and password). If the device is a BYOD, you can challenge the user with the AD plus RADIUS authentication.

If you plan to selectively enumerate virtual apps and desktops based on network location, then user management has to be performed for those delivery groups using Citrix Studio policies instead of workspace. When creating a delivery group, in the users setting, either choose **Restrict use of this Delivery Group to the following users** or **Allow any authenticated users to use this Delivery Group**.
This enables the **Access Policy** tab under Delivery Group to configure adaptive access.

**Contextual access to Citrix DaaS:**
Adaptive Authentication enables contextual access to Citrix DaaS. Adaptive Authentication surfaces all the policy information about the user to Citrix DaaS. Admins can use this information in their policy configurations to control the users actions that can be performed on Citrix DaaS. User action, for example, can be enabling or disabling clipboard access, and client drive mapping printer redirection.

Contextual access to Secure Internet Access and other Citrix Cloud services through Adaptive Authentication is planned in the upcoming releases.

**Logon page customization:**
Adaptive Authentication helps the user to highly customize the Citrix Cloud logon page.

**Adaptive Authentication capabilities**
The following are the capabilities supported in Citrix Workspace with Adaptive Authentication.

- LDAP (Active Directory)
- Directory Support for AD, Azure AD, Okta
- RADIUS support (Duo, Symantec)
- AD + token built-in MFA
- SAML 2.0
- OAuth, OIDC support
- Client Certificate authentication
- Device posture assessment (Endpoint analysis)
- Integration with third-party authentication providers
- Push notification through the app
- reCAPTCHA
- Conditional/policy driven authentication
- Authentication policies for SmartAccess (Contextual access)
- Logon page customization
- Self service password reset

**Prerequisites**
- Reserve an FQDN for your Adaptive Authentication instance. For example, `aauth.xyz.com`, assuming `xyz.com` is your company domain. This FQDN is referred as the Adaptive Authentication service FQDN in this document and is used when provisioning the instance. Map the FQDN with the IdP virtual server public IP address. This IP address is obtained after provisioning in the **Upload Certificate** step.
• Procure a certificate for auth.xyz.com. Certificates must contain the SAN attribute. Else the certificates are not accepted.

• Adaptive Authentication UI does not support uploading of certificate bundles. To link an intermediate certificate, see Configure intermediate certificates.

• Choose your connectivity type for the on premises AD/RADIUS connectivity. The following two options are available. If you do not want data center reachability, use the connector connectivity type.
  - Citrix Cloud Connector - For details, see Citrix Cloud Connector.
  - Azure VNet peering - For details, see Set up connectivity to on-premises authentication servers using Azure VNet peering.

• Configure network time protocol (NTP) server to avoid time skews. For details, see How to synchronize system clock with servers on the network.

Points to note

• Citrix recommends not to run clear config for any Adaptive Authentication instance or modify any configuration with the prefix AA (example, AAuthAutoConfig) including certificates. This disrupts Adaptive Authentication management and user access is impacted. The only way to recover is through reprovisioning.

• Do not add SNIP or any additional routes on the Adaptive Authentication instance.

• User authentication fails if the customer ID is not in all lowercase. You can convert your ID to all lowercase and set it on the ADC instance by using the command `set cloud parameter -customerID <all_lowercase_customerid>`.

• The nFactor configuration that is required for the Citrix Workspace or the Citrix Secure Private Access service is the only configuration customers are supposed to create directly on the instances. Currently there are no checks or warnings in the Citrix ADC that prevents admins from making these changes.

• Do not upgrade the Adaptive Authentication instances to random RTM builds. All upgrades are managed by Citrix Cloud.

• Only Windows based cloud connector is supported. Connector appliance is not supported in this release.

• If you are an existing Citrix Cloud customer and have already configured Azure AD (or other authentication methods), to switch to Adaptive Authentication (for example, device posture check), you must configure Adaptive Authentication as your authentication method and configure the authentication policies in the Adaptive Authentication instance. For details, see Connect Citrix Cloud to Azure AD.

• For RADIUS server deployment, add all connector private IP addresses as the RADIUS clients in the RADIUS server.
- Do not add your LDAP or RADIUS servers as a service or a server.
- In the current release, the external ADM agent is not allowed and therefore Citrix Analytics (CAS) is not supported.
- Citrix Application Delivery Management service collects the backup for your Adaptive Authentication instance. To extract the backup from ADM, onboard the ADM service. For details, see Config backup and restore. Citrix does not take the backups explicitly from the Adaptive Authentication service. Customers must take the backup of their configurations from the Application Delivery Management service if necessary.

How to configure the Adaptive Authentication service

Access the Adaptive Authentication user interface

You can access the Adaptive Authentication user interface by one of the following methods.

- Login using your credentials and select a customer.

After you are successfully authenticated, you are redirected to the Adaptive Authentication user interface.

OR

- Navigate to Citrix Cloud > Identity and Access Management.
- In the Authentication tab, in Adaptive Authentication, click the ellipsis menu and select Manage.

The Adaptive Authentication user interface appears.

The following figure illustrates the steps involved in configuring Adaptive Authentication.

© 1999‒2022 Citrix Systems, Inc. All rights reserved.
Citrix Secure Private Access

Step 1: Provision Adaptive Authentication

Perform the following steps:


2. Select the preferred connection for Adaptive Authentication.

   - **Citrix Cloud Connector**: For this connection type, you must set up a connector in your on-premises network. Citrix recommends that you deploy at least two Citrix Cloud Connectors in your environment to set up connection to the Citrix Gateway hosted on Azure. You must allow your Citrix Cloud Connector to access the domain/URL you have reserved for the Adaptive Authentication instance. For example, allow `https://aauth.xyz.com/*`.

     For details on Citrix Cloud Connector, see [Citrix Cloud Connector](#).

   - **Azure VNet peering** - You must set up the connectivity between the servers using Azure’s VNet peering.
     - Ensure that you have an Azure subscription account to set up the connectivity.
     - The customer VNet that is being peered must already have an Azure VPN gateway provisioned. For details, see [https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal](https://docs.microsoft.com/en-us/azure/vpn-gateway/tutorial-site-to-site-portal).

To add a Citrix Cloud Connector as your preferred connection:

Perform the following steps.
• Select the **Citrix Cloud Connector** option, and then select the end user agreement check box.
• Click **Provision**. Provisioning might take up to 30 minutes to set up.

**Note:**
For connector connectivity type, make sure that your Adaptive Authentication FQDN is reachable from the connector virtual machine after provisioning.

**To set up Azure VNet peering:**
If you select **Azure VNet peering** as your connection, you must add a subnet CIDR block that must be used to provision the Adaptive Authentication instance. You must also ensure that the CIDR block does not overlap with your organization’s other network ranges.

For details, see [Setup connectivity to on-premises authentication servers using Azure VNet peering](#).

3. Set up credentials to access the instances that you have enabled for Adaptive Authentication. You need the management console access for creating policies for authentication, conditional access, and so on.
   a) In the **Console access** screen, enter the username and password.
   b) Click **Next**.

**Note:** Users created from the **Console access** screen are provided with “SuperUser” privileges that have the shell access.

---

**Provision Adaptive Authentication**

<table>
<thead>
<tr>
<th>Provision Adaptive Authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Overview</strong></td>
</tr>
<tr>
<td><strong>Provision</strong></td>
</tr>
<tr>
<td><strong>Console access</strong></td>
</tr>
<tr>
<td><strong>Uploaded Certificate</strong></td>
</tr>
<tr>
<td><strong>Allowed IP addresses</strong></td>
</tr>
</tbody>
</table>

**Console access**

Enter the credentials you need to use for accessing the management console of Adaptive Authentication. You can use the management console to create policies for authentication, conditional access, and device posture.

- **User name**: citrixadmin
- **Password**: ***
- **Confirm password**: ***

**Provisioning was successful**
4. Add the Adaptive Authentication service FQDN and upload the certificate-key pair.
   You must enter the Adaptive Authentication service FQDN of your choice for the publicly accessible authentication server.
   
   a) In the **Upload Certificate** screen, enter the FQDN that you have reserved for Adaptive Authentication.
   b) Select the certificate type.
   c) Upload the certificate and the key.

**Note:**

- Install your intermediate certificate on the Adaptive Authentication instance and link it with the server certificate.
  
  a) Log into the Adaptive Authentication instance.
  b) Navigate to **Traffic Management > SSL**. For details, see **Configure intermediate certificates**.

- Only public certificates are accepted. Certificates signed by private or unknown CAs are not accepted.
- Certificate configuration must be done using the Adaptive Authentication UI only. Do not change it directly on the instance as this might result in inconsistencies.

---

5. Upload the certificate and the key.

The Adaptive Authentication instance now is connected to the Identity and Access Management
service. The **Adaptive Authentication** method status is displayed as **Connected**.

6. Set up an IP addresses through which the Adaptive Authentication management console can be accessed.

   a) In the **Allowed IP addresses** screen, for each instance, enter a public IP address as the management IP address. To restrict the access to the management IP address, you can add multiple IP addresses that are allowed to access the management console.

   b) To add multiple IP addresses, you must click **Add**, enter the IP address, and then click **Done**. This must be done for every IP address. If you do not click the **Done** button, the IP addresses are not added to the database but are only added in the user interface.
Step 2: Configure Adaptive Authentication policies

After the provisioning, you can access the Adaptive Authentication management IP address directly. However, accessing the instance using the IP address is not trusted and many browsers block the access with warnings. Citrix recommends that you access the Adaptive Authentication management console with FQDN to avoid any security barriers. You must reserve the FQDN for the Adaptive Authentication management console and map it with the primary and secondary management IP address.

For example, if your AA instance IP is 20.1.1.1 and Secondary: 20.2.2.2, then;

- primary.domain.com can be mapped to 20.1.1.1
- secondary.domain.com can be mapped to 20.2.2.2

After accessing the Adaptive Authentication instance, you can then configure the authentication flow use cases as per your requirement. For various use cases, see Sample authentication configurations.

To access the Adaptive authentication management console using the FQDN, see Configure SSL for ADC Admin UI access.
### Important:

- In a high availability setup, as part of the synchronization process, the certificates are also synchronized. So ensure that you use the wildcard certificate.
- If you need unique certificate for each node, upload the certificate files and keys in any folder that doesn’t get synchronized (for example, create a separate folder (nosync_cert) in the nsconfig/SSL directory) and then upload the certificate uniquely on each node.
- To enable single sign-on to applications, ensure that you enable the **Send Password** option in the OAuth IdP profile.

### Step 3: Enable Adaptive Authentication for Workspace

After provisioning is complete, you can enable authentication for Workspace by clicking **Enable** in the Enable Adaptive Authentication for Workspace section.
Note:
With this step, the Adaptive Authentication configuration is completed.

Migrate your authentication method to Adaptive Authentication

Customers already using Adaptive Authentication with authentication method as Citrix Gateway must migrate Adaptive Authentication and then remove the OAuth configuration from the Adaptive Authentication instance.

1. Switch to a different authentication method other than Citrix Gateway.
2. In Citrix Cloud > Identity and Access Management, click the ellipsis button corresponding to Citrix Gateway and then click Disconnect.
3. Select I understand the impact on the subscriber experience, and then click Confirm.

When you click Confirm, the workspace login to end users is impacted and adaptive authentication is not used for authentication until adaptive authentication is enabled again.

4. In the Adaptive Authentication instance management console, remove the OAuth related configuration.

By using the CLI:

```
1 unbind authentication vs <authvsName> -policy <oauthIdpPolName>
2 rm authentication oauthIdpPolicy <oauthIdpPolName>
3 rm authentication oauthIdpProfile <oauthIdpProfName>
```

By using the GUI:


b) Unbind the OAuth policy.

c) Navigate to Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > OAuth IDP.

d) Delete the OAuth policy and profile.


In the Authentication tab, in Adaptive Authentication, click the ellipsis menu and select Manage.

OR access https://adaptive-authentication.cloud.com

6. Click See Details.

7. In the Upload Certificate screen, do the following:
Add the Adaptive Authentication FQDN.
Remove the certificates and key files and upload it again.

Provision Adaptive Authentication

- **Overview**
- **Provision**
- **Console access**
- **Upload Certificate**
- **Allowed IP addresses**

Add FQDN and certificate key pair
Enter the FQDN for the adaptive authentication IDP access and upload an SSL certificate and private key to secure the end user requests. You can obtain a certificate that the key strength of the certificate keys is 2048 bits or higher and that the keys are signed with secure signature algorithms.

FQDN: ec.aaaath.xyz.com

**Important:**
If you edit an FQDN or the certificate-key pair directly without migrating to **Adaptive Authentication**, connection to Identity and Access Management fails and the following errors are displayed. You must migrate to the Adaptive Authentication method to fix these errors.

- ADC command failed with an error. A policy is already bound to the specified priority.
- ADC command failed with an error. Cannot unbind a policy that is not bound.

8. Click **Save Changes**.

At this point, Identity and Access Management displays **Adaptive Authentication** as **Connected** and the Adaptive Authentication instance has the OAuth profile auto configured.

You can validate this from the GUI.

- Access your Adaptive Authentication instance and log in with your credentials.
- Navigate to **Security > AAA - Application Traffic > Virtual Servers**. You must see that the OAuth IdP profile created.
- Navigate to **Citrix Cloud > Identity and Access Management**. Adaptive authentication is in the **Connected** status.

   ![Enable Adaptive Authentication for Workspace](image)

   **Enable Adaptive Authentication for Workspace**
   Select Adaptive Authentication as your preferred authentication method for subscribers signing in to Citrix Workspace.
   Complete this step before proceeding to the next step
   **Enable**

   This step enables the authentication method as Adaptive Authentication in your workspace configuration.

10. Click the workspace link on step 3 after clicking **Enable**. You must see that the authentication method is changed to Adaptive Authentication.

   **Note:**
   New users must follow the same steps excluding the step to remove the OAuth related configuration.

### Edit an FQDN

You cannot edit an FQDN if **Adaptive Authentication** is selected as the authentication method in the Workspace configuration. You must switch to a different authentication method to edit the FQDN. However, you can edit the certificate if necessary.

**Important:**
- Before modifying the FQDN, ensure that the new FQDN is mapped to the IdP virtual server public IP address.
- Existing users who are connected to Citrix Gateway using OAuth policies must migrate your authentication method to **Adaptive Authentication**. For details, see [Migrate your authentication method to Adaptive Authentication](#).

To edit an FQDN, perform the following:

1. Switch to a different authentication method from **Adaptive Authentication**.
2. Select **I understand the impact on the subscriber experience**, and then click **Confirm**.

   When you click **Confirm**, the workspace login to end users is impacted and Adaptive Authentication is not used for authentication until Adaptive Authentication is enabled again. Therefore, it is recommended that you modify the FQDN during a maintenance window.

3. In the **Upload Certificate** screen, modify the FQDN.
4. Click **Save Changes**.

   **Important:**
   If you edit an FQDN, you must also upload the certificate again.

5. Enable the Adaptive Authentication method again by clicking **Enable** (step 3) in the Adaptive Authentication home page.

6. Click **Refresh**.

**Advanced configuration options**

By using the Adaptive Authentication GUI, you can also set up the following.

- Schedule upgrade of your Adaptive Authentication instances
- Deprovision your Adaptive Authentication instances
- Enable secure access to the gateway
Schedule upgrade of your Adaptive Authentication instances

For the current site or deployment, you can select the maintenance window for upgrade.

**Important:**

Do not upgrade the Adaptive Authentication instances to random RTM builds. All upgrades are managed by Citrix Cloud.

1. On the Adaptive Authentication UI, in the Provision Adaptive Authentication instances section, click the ellipsis button.
2. Click Schedule upgrades.
3. Select the day and time for the upgrade.
Deprovisioning your Adaptive Authentication instances

Customers can deprovision the Adaptive Authentication instances in the following cases and as per the suggestion from Citrix support.

- The Adaptive Authentication instances are not accessible (especially after a scheduled upgrade), though this scenario might not occur.
- If the customer has to switch from VNet peering mode to connector mode or conversely.
- If the customer selected a wrong subnet at the time of provisioning VNet peering mode (the subnet conflicts with other subnets in their data center or Azure VNet).

Note:
Deprovisioning also deletes the config backup of the instances. Therefore you must download the backup files and save it before you deprovision your Adaptive Authentication instances.

Perform the following to deprovision an Adaptive Authentication instance:

1. On the **Adaptive Authentication** UI, in the **Provision Adaptive Authentication instances** section, click the ellipsis button.

2. Click **Deprovision**.

   **Note:**
   Before deprovisioning, you must disconnect **Citrix Gateway** from the Workspace Configuration.

3. Enter the customer ID to deprovision the Adaptive Authentication instances.
Enable secure access to the gateway

1. On the Adaptive Authentication UI, in the Provision Adaptive Authentication instances section, click the ellipsis button.

2. Click Secure access to the gateway.

3. In Keys should expire in, select an expiration duration for the new SSH key.

4. Click Generate and Download keys.
Copy or download the SSH private key for later use as it is not displayed after the page is closed. This key can be used to log in to the Adaptive Authentication instances with the user name authadmin.

You can click **Generate and Download keys** to create a new key pair if the earlier key pair expires. However, only one key pair can be active.

5. Click **Done**.

**Important:**

- If you are using PuTTY on Windows to connect to Adaptive Authentication instances, you must convert the downloaded private key to PEM. For details, see [https://www.puttygen.com/convert-pem-to-ppk](https://www.puttygen.com/convert-pem-to-ppk).

- It is recommended to use the following command to connect to the Adaptive Authentication instances via the terminal from the MAC or PowerShell/Command prompt from Windows (version 10).

  ```bash
  ssh -i <path-to-private-key> authadmin@<ip address of ADC>
  ```

- If you want the AD users to access the Adaptive Authentication GUI, you must add them as new administrators to the LDAP group. For details, see [https://support.citrix.com/article/CTX123782](https://support.citrix.com/article/CTX123782).

  For all other configurations, Citrix recommends that you use the Adaptive Authentication GUI and not the CLI commands.

---

**Set up connectivity to on-premises authentication servers using Azure VNet peering**

You must set up this configuration only if you have selected the connectivity type as Azure VNet peering.

**Note:** If you are using third-party IDPs like Okta, Azure AD, Ping, this step is not required.

1. On the Connect Adaptive Authentication UI, click **Provision**, and then click **Azure VNet Peering**.
The **Citrix Managed Service Principal** field contains the application ID of an Azure Service Principal created by Citrix for your customer. This service principal is required to allow Citrix to add a VNet peering to a VNet in your subscription and tenant.

To allow this service principal to log in to the customer tenant, the admin at the customer site (global admin of the tenant) must run the following PowerShell commands to add the SPN to the tenant. CloudShell can also be used.

```powershell
Connect-AzureAD
New-AzureADServicePrincipal -AppId $App_ID
```

Where `$App_ID` is an SPN Application ID shared by Citrix.

**Note:**

- The earlier-mentioned command outputs a service principal name that must be used for the role assignments.
- To allow this service principal to add an Azure VNet peering, the admin at the customer site (not limited to global admin) must add a “Network Contributor” role to the VNet that must be linked to the Citrix Managed VNet.
- SPN is a unique identifier that is used to associate the Citrix virtual network in Azure. Associating the SPN with VNet enables Citrix virtual network to connect to the customers’ on-premises network through Azure’s VNet.

2. Create a VNet peering.

   - Enter the tenant ID for which the earlier steps were run and click **Fetch**.
This populates the customer-managed VNet resource ID with the candidate VNets for which the network contributor role is added for the SPN. If you do not see your VNet, make sure that the earlier steps are run correctly or repeat the steps.

Note:
For details on how to find your tenant ID, see https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-to-find-tenant.

3. Select **Use Azure VPN Gateway** to connect your on-premises networks to Azure.

4. In **Customer managed VNet Resource ID**, select the VNet identified for peering, and click **Add**. The VNet is added to the table with the status initially as **InProgress**. Once the peering is completed successfully, the Status changes to **Done**.

5. Click **Done**.

6. Continue with the configuration, see **Step 1: Provision Adaptive Authentication**.

**Important:**
- For traffic to flow between the Citrix managed VNet and the on-premises network, firewall and routing rules might be changed on the on-premises to direct the traffic to the Citrix Managed VNet.
- You can add only one VNet peer at a time. Multiple VNet peerings are not allowed currently. You can delete a VNet peering or create one as required.

![Adaptive Authentication is now connected](image)

Complete these tasks to prepare and deploy Adaptive Authentication.

1. **Provision Adaptive Authentication instances**
   - Provision Adaptive Authentication instances and optionally configure a connection with your on-premises network.
   - Complete this step before proceeding to the next step.
   - See Details.

2. **Configure authentication policies**
   - Create and apply policies for authentication, conditional access, device posture, and more using the management console.
   - Complete this step before proceeding to the next step.
   - Access the Adaptive Authentication management console by visiting 20.106.227.13 (Primary). You can also add DNS entries for 20.106.227.13 (Primary) and 20.127.206.21 (Secondary) and access the management console using FQDNs.
   - Since primary instance may change, Click here to refresh the instance IPs.

3. **Enable Adaptive Authentication for Workspace**
   - Select Adaptive Authentication as your preferred authentication method for subscribers signing in to Citrix Workspace.
   - Complete this step before proceeding to the next step.
   - Enable.

4. **Connect an identity provider to access its user directory**
   - Make sure the identity provider of the directory you wish to access for user lookup and resource assignment is connected.
   - Take me to identity and access management.
Other related configurations

Change the authadmin password

You can use the following steps to change the password for the authadmin user, both on the instances and in the ADM device profile.

1. Navigate to System > User Administration > Users, and create the user. For details, see Configure user accounts.
2. Save the configuration.
3. In the Citrix Application Delivery Management service, perform the following:
   • Navigate to Networks > Instances > Citrix ADC.
   • Click Profiles and select the profile prefixed with gateway-hosted.
   • Select Change Password and set the password used in step 2.
   • Click Back.
   • Go to Citrix ADC > Select Action > Rediscover.

For more information, see How to change the Citrix ADC MPX and VPX root password.

Custom workspace URL or vanity URL

For the custom workspace URL or vanity URL, configure a new OAuthIDP profile with the same client ID, secret, and audience as your current one but with a redirect URL of https://your.company.com/core/login-cip. In this example, your.company.com is the custom workspace URL corresponding to your domain. For example, nssvctesting.net is the domain and custom workspace URL is ws1.nssvctesting.net.

Create a new OAuthIDP policy and bind it to the authentication and authorization virtual server.

Note:

Both OAuthIDP policies can co-exist and a user can access Workspace using the default Workspace URL or the custom workspace URL or both.

Config backup and restore

Application Delivery Management service performs backup management for the Adaptive Authentication instances. For details, see Back up and restore Citrix ADC instances.

1. On the Application Delivery Management tile, click Manage.
2. Navigate to Infrastructure > Instances and access the backups.

Note:
If you do not see the service onboarded, onboard the Application Delivery Management service. For details, see Getting started.

Troubleshooting

The issues are categorized based on the different stages in the configuration:

- Provisioning – Issues while provisioning the Adaptive Authentication instance
- Instance accessibility issue: Instance is provisioned but the admin cannot access it
- AD/Radius connectivity and authentication issue: Authentication policy is set up for the on-premises but it is not working
- Authentication issues
- EPA/device posture-related issues
- Smart tag-related issues
- Log collection

You can troubleshoot the issues using the Adaptive Authentication CLI as well. To connect to the CLI, do the following:

- Download SSH client like putty/securecrt on your machine.
- Access the Adaptive Authentication instance using the management IP (primary) address.
- Login with your credentials.

For details, see Access a Citrix ADC appliance.

Provisioning issues

- **Unable to access the Adaptive Authentication UI**
  Check if the entitlement is enabled for your customer ID/tenant.

- **Stuck in the provisioning page for more than 45 min**
  Collect the screenshot of the error, if any, and then contact Citrix Support for assistance.

- **VNet peer is down**
  - Check if there are alerts in the Azure Portal corresponding to this peering and take the recommended actions.
  - Delete the peering, add it again from the Adaptive Authentication UI.

- **Deprovisioning is not complete**
  Contact Citrix Support for assistance.
Instance accessibility issue

- **Management IP address is not accessible for the instance**
  - Check if the client’s public IP address used for access is among the allowed source IP addresses.
  - Validate if there is any proxy changing the client source IP address.

- **Unable to log in to the instance**
  Make sure that the admin access is working fine with the credentials you entered during provisioning.

- **End users do not have complete rights**
  Make sure while adding the user, you have bound the suitable command policy for access. For more information, see [User, user groups, and command policies](#).

AD or RADIUS connectivity issue

**Issue with Azure Vnet peering connectivity type:**

- Check if the customer managed Azure VNet is reachable from the Adaptive Authentication instances.
- Check if connectivity/reachability from customer managed Azure VNet to AD is working.
- Ensure that appropriate routes are added to direct traffic from on-premises to Azure VNets.

Windows based Connector:

- All logs are available in the directory `/var/log/ns.log` and each log is prefixed with `[NS_AAUTH_TUNNEL]`.
- ConnectionID from logs can be used to correlate different transactions.
- Ensure that the private IP address of the connector virtual machine is added as one of the RADIUS clients in the RADIUS server because that IP address is the source IP address for the connector.

  For every authentication request, the tunnel is established between the Adaptive Authentication Instance (NS - AAAD process) and the authentication server. Once the tunnel is established successfully, authentication occurs.

  Make sure that the connector virtual machine can resolve the Adaptive Authentication FQDN.

- Connector is installed however the on-premises connectivity fails.

  Validate if NSAUTH-TUNNEL is getting established.

  ```
  Cat ns.log | grep -I "tunnel"
  ```

  If the following sample log is not printed in the ns.log file for the authentication request, then there might be an issue while establishing a tunnel or some issue from the connector side.
**LDAP:**

```
[NS_AAUTH_TUNNEL] Entering bitpump for
Connection1 => Src : 192.168.0.7:28098, Dst : 10.106.103.60:636
Connection2 => Src : 10.106.103.70:2271, Dst : 10.106.103.80:443
```

**RADIUS:**

```
[NS_AAUTH_UDP_TUNNEL] MUX channel established"
```

Check the log details and take actions appropriately.

<table>
<thead>
<tr>
<th>Log details</th>
<th>Corrective action</th>
</tr>
</thead>
<tbody>
<tr>
<td>No logs with prefix [NS_AAUTH_TUNNEL] are included in the log file</td>
<td>Run the <code>show cloudtunnel vserver</code> command. This command must list both (TCP and UDP) cloud tunnel virtual server with the state “UP.”</td>
</tr>
<tr>
<td>[NS_AAUTH_TUNNEL] Waiting for outbound from connector</td>
<td>Check if the connector machine is able to reach to the Adaptive Authentication FQDN OR check the connector side firewall for outbound connections to the Adaptive Authentication FQDN</td>
</tr>
<tr>
<td>[NS_AAUTH_TUNNEL] Received connect command from connector and client connection lookup succeeded”</td>
<td></td>
</tr>
<tr>
<td>[NS_AAUTH_TUNNEL] Server is down or couldn't create connection to ip 0.0.0.0 and [NS_AAUTH_TUNNEL] Connect response code 401 is not 200 OK, bailing out</td>
<td>Reach out to Citrix Support.</td>
</tr>
</tbody>
</table>

**No response from connector:**

- Make sure that Adaptive Authentication FQDN is reachable from the connector virtual machine.
- Make sure that you have an intermediate certificate bound and linked to the server certificate on the Adaptive Authentication instance.

**Incorrect LDAP/RADIUS settings:**

If your AD/RADIUS server IP address is a public IP address, you must add the subnet or the IP addressing the expressions in the Citrix ADC appliance. Do not edit the existing ranges.
To add a subnet or IP address by using the CLI:

```
set policy expression aauth_allow_rfc1918_subnets "(CLIENT.IP.DST.BETWEEN(10.0.0.0,10.255.255.255)) || CLIENT.IP.DST.BETWEEN(172.16.0.0,172.31.255.255)) || CLIENT.IP.DST.BETWEEN(192.168.0.0,192.168.255.255)) || CLIENT.IP.DST.BETWEEN(13.14.0.0,13.14.255.255)) || CLIENT.IP.DST.EQ(1.2.5.4))"
```

To add a subnet or IP address by using the GUI:

Navigate to Appexpert > Expressions.
Add expression `aauth_allow_rfc1918_subnets`

If the tunnel is established but still authentication fails, use the following steps to troubleshoot the issue.

**LDAP:**

- Validate the Bind DN details.
- Use test connectivity to confirm the error.
- Validate the errors using `aaad debug`.
- Log in to the Adaptive Authentication instance by using the CLI.

```
1 shell
2 cd /tmp
3 cat aaad.debug
4 <!−−NeedCopy-->
```

**Common LDAP errors:**

- Server time out – No response from the connector for the LDAP query.
- Other LDAP errors, see [https://support.citrix.com/article/CTX138663](https://support.citrix.com/article/CTX138663).

**Radius:**

- Connector IP address must be added as the RADIUS client source IP address in the RADIUS server configuration.

**Authentication issues**

- Post assertion errors for OAuth
- Make sure that all the claims are provided by AD. You need 7 claims for this to be successful.
- Validate the logs in the `var/log ns.log` files to locate the error for OAuth failures.
- Validate the OAuth profile parameters.

**Azure AD authentication stuck at post assertion**
Add AD authentication as the next factor with authentication set to off. This is to get all the required claims for successful authentication.

**EPA related issues**

- **Plug-in is already present but the user is getting a prompt to download the plug-in.**
  Possible causes: Version mismatch or corrupt files
  - Run developer tools and validate if the plug-in list file contains the same version as that of the Citrix ADC and your client machine.
  - Make sure that the client version on the Citrix ADC is the same as on the client machine.
  
  Update the client on the Citrix ADC.
  
  On the Adaptive Authentication instance, navigate to **Citrix Gateway > Global Settings > Update client libraries.**
  
  The EPA plug-in libraries page on Citrix Downloads provides you the detailed information.
  
  - At times, the request can be cached on Citrix ADC even if the version is updated.
    
    `show cache object` displays the cached plug-in details. You can delete it by using the command;
    
    `flush cache object -locator 0x00000023345600000007`
    
    For details on EPA log collection, see [https://support.citrix.com/article/CTX209148](https://support.citrix.com/article/CTX209148).

- **Is there a way to revert the EPA settings (Always, Yes, No) after the user has selected an option.**
  
  Currently, EPA settings revert is done manually.
  
  - On the client machine, navigate to `C:\Users<user_name>\AppData\Local\Citrix\AGEE`
  
  - Open the `config.js` file and set `trustAlways` to null - ”trustAlways”:null

**Smart access tag issues**

- **After configuring the smart access, applications are not available**
  
  Make sure that the tags are defined on both the Adaptive Authentication instance and the Citrix VDA delivery groups.
Check that the tags are added on the Workspace delivery group in all capitals.

You can collect the ns.log and reach out to Citrix Support if this does not work.

**General log collection for Adaptive authentication instance**

- Technical support bundle: For details, see [How to collect the technical support bundle from SDX and VPX appliances for insight analysis](#).
- Trace files. For details, see [How to record a packet trace on Citrix ADC](#).

Contact Citrix Support for guidance.

**Sample authentication configurations**

Customers can configure an authentication policy of their choice and bind it to the authentication virtual server. Authentication profile bindings are not required for the authentication virtual server. Only the authentication policies can be configured. The following are some of the use cases.

**Important:**

Authentication configuration must be done on the primary nodes only.

**Multifactor authentication with conditional authentication**

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

**Third-party integration with multifactor authentication**

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

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

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

**Shared security responsibilities**

**Actions needed from customers**

Following are some of the actions from the customers as part of security best practices.

- Credentials for accessing the Adaptive Authentication UI: Customer is responsible for creating and maintaining the credentials for accessing the Adaptive Authentication UI. If the customer is working with Citrix Support to resolve an issue, the customer might need to share these credentials with support personnel.

- Change the authadmin password: As part of provisioning, Citrix creates an initial user called authadmin and the corresponding device profile in the Citrix Application Delivery Management service and Adaptive Authentication instances. Customers must change the password of this user in the primary node and in the device profile of ADM.

  Log on to your Citrix Gateway, change the user name and password. For details, see Change authadmin password.

- Remote CLI access security: Citrix provides remote CLI access for customers. However, customers are responsible for maintaining the security of the instance during runtime.

- SSL private keys: As the Citrix ADC is under customer control, Citrix does not have any access to the file system. Customers must ensure that they safeguard the certificates and keys that they are hosting on the Citrix ADC instance.

- Data backup: Back up the configuration, certificates, keys, portal customizations, and any other file system modifications.
Citrix Secure Private Access

- Disk images of the ADC instances: Maintain and manage the Citrix ADC disk space and disk cleanup. Customer is responsible for running these tasks safely and securely.

- Upgrade: Schedule upgrade of the Adaptive Authentication instances. For details, see Schedule upgrade of your Adaptive Authentication instances.

Actions needed from both the customer and Citrix

- Disaster recovery: In supported Azure regions, the Citrix ADC high availability instances are provisioned in separate availability zones to safeguard against data loss. In the event of Azure data loss, Citrix recovers as many resources in the Citrix-managed Azure subscription as possible.

In the event of the loss of an entire Azure region, the customer is responsible for rebuilding their customer-managed virtual network in a new region and creating a new VNet peering.

- Secure access via the public management IP address:

Secure the access to the management interfaces by assigned public IP addresses and allow outbound connectivity to the Internet.

Limitations

- Authentication through load balancing virtual server is not supported.

- Certificate bundle upload is not supported.

- RADIUS authentication is impacted for a few minutes if the connector serving the RADIUS request goes down. User must reauthenticate in this case.

- Currently, the Adaptive Authentication instance can send the on premises traffic request to any connector in any resource location. Data center connectivity might fail if data centers are disjoint. If needed, all of the on premises connectivity traffic can be sent to one resource location using the following command:

```
set cloudtunnel parameter -resourceLocation <RL>
```

To revert to default settings, use the following command:

```
set cloudtunnel parameter -resourceLocation 00000000-0000-0000-0000-000000000000
```

- DNS tunneling is not supported. Static records must be added on the Citrix ADC appliance for the FQDNs used in authentication policies/profiles (LDAP/RADIUS) for authentication servers in the customer’s on premises data center.
For details on adding DNS static records, see Create address records for a domain name.

- Test Network connectivity in the LDAP profile might show an incorrect result as “Server is reachable” even if the connectivity to the LDAP server is not established. Error messages such
as “port is not open”, or “server is not LDAP” might be displayed to indicate the failure. Citrix recommends collecting the traces in this scenario and troubleshooting further.

- For EPA scans to work on macOS, you must bind the default ECC curves to the authentication and authorization virtual server by selecting the ECC Curve option as ALL.

**Service quality**

Adaptive Authentication is a high availability (active-standby) service.

**Smart Access using Adaptive Authentication**

June 8, 2022

Citrix Cloud customers can provide Smart Access (adaptive access) to Citrix DaaS using Adaptive authentication as an IdP to Citrix Workspace.

Smart Access feature allows the Adaptive Authentication service to surface all the policy information about the user to Citrix Workspace or Citrix DaaS. The Adaptive Authentication service can provide device posture (EPA), network location (inside or outside the corporate network, geo-location), user attribute like user groups, time of day or a combination of these parameters as part of the policy information. The Citrix DaaS administrator can then use this policy information to configure contextual access to Citrix DaaS. Citrix DaaS can either be enumerated or not based on earlier parameters (access policy). Some user actions can also be controlled like clipboard access, printer redirection, client drive, or USB mapping.

Example use cases:

1. Administrator can configure the group of apps to be displayed or accessed only from specific network locations like the corporate network.
2. Administrator can configure the group of apps to be displayed or accessed only from corporate managed devices. For example, EPA scans can check whether the device is a corporate managed or BYOD. Based on the EPA scan result, the relevant apps can be enumerated for the user.

**Prerequisites**

- Adaptive Authentication as an IdP must be configured for Citrix Workspace. For details, see Adaptive Authentication service.
• Adaptive authentication service with Citrix DaaS is up and running.

Understanding the flow of events for Smart Access

1. User logs in to Citrix Workspace.
2. User gets redirected to the Adaptive authentication service configured as an IdP.
3. Adaptive authentication service performs an EPA check along with other checks.
4. Adaptive authentication service configured as an IdP does the authentication.
5. Adaptive Authentication service pushes the tags to the Citrix Graph service. User is redirected to the Citrix Workspace landing page.
6. Citrix Workspace fetches the policy information for this user session, matches the filter, and evaluates the apps or desktops that must be enumerated.
7. Configure the access policy on Citrix DaaS to restrict the ICA access for users.

Configuration scenario - App enumeration based on device posture scans

Step 1 - Configure Smart Access policies on the Citrix Adaptive Authentication instance:

In the following sample configuration, a different set of applications is enumerated based on domain-joined or non-domain joined logon.


2. On the Profiles tab, click Add to create a profile named Domainjoined-SmartAccessProfile with the tag as DomainJoined. Similarly create another policy named, NonDomainJoined-SmartAccessProfile with the tag as NonDomainJoined.

4. On the Configure Authentication Smart Access Policy page, Click **Add** to create a policy named **Domainjoined-SmartAccessPol.**

5. On the Configure Authentication Smart Access Policy page, under **Action**, select the previously created **DomainJoined-SmartAccessProfile** and click **Add.**

6. In Expression, type **AAA.USER.GROUPS.CONTAINS("DomainJoinedGroup")** and click **OK.**

7. Similarly create another policy named, **NonDomainJoined-SmartAccessPol** (under Action, select previously created **NonDomainJoined-SmartAccessProfile**).
8. Bind the smart access policy to the Authentication and authorization virtual server.

Step 2 - Citrix DaaS configuration:

1. Click Manage on the Citrix DaaS tile.
2. Navigate to Delivery groups and click Edit Delivery Group.
3. Right-click the delivery group and select Edit to configure when the apps of that delivery group must be enumerated and allowed to launch.
4. Click Access Policy and add the required tags. Farm must be always set to Workspace and the filter must have any of the tags that you created, based on the earlier configuration.
5. Repeat the previous steps to add more tags. When multiple tags are used, if at least one of the tags is present, the Delivery Group is available to the customer.
Note:

- Ensure that the tags are in upper case.
- If an administrator removes the configuration of a specific tag on the Adaptive Authentication service, then the tag must be removed from the Web Studio and the Delivery groups as well. Administrator must not reuse the deleted tag names. Admins must always use new tag names.

Upon successful configuration, the Domain-Joined logon enumerates the following apps.

Upon successful configuration, the Non-Domain-Joined logon enumerates the following apps.
Step 3 - Add an access policy for the smart access tags:

1. Under Manage, navigate to Policies, and create a policy.
2. Select the appropriate ICA policy control.
3. In Assign Policy To, select “access control.”

1. Assign the smart access tag (in upper case) in access condition.

Troubleshooting

- What if no tags are pushed:
  - Check if at least one policy is evaluated to true. For details see [https://support.citrix.com/article/CTX138840](https://support.citrix.com/article/CTX138840).
  - Check Citrix ADC connectivity to cas.citrix.com.

Additional changes for high availability setup:

Sometime there might be a delayed file synchronization in a high availability setup. As a result, the keys created when Citrix ADM registration happened is not read on time.

We are looking for the following three files on the secondary.

/var/mastools/conf/agent.conf
/var/mastools/trust/.ssh/private.pem
/var/mastools/trust/.ssh/public.pem
To address the file-sync issue, perform the following steps to rerun the ‘set cloud’ command on the secondary.

```bash
1 > shell cat /var/mastools/conf/agent.conf
2 <?xml version="1.0" encoding="UTF-8" standalone="no"?>
3 <mps_agent>
4 <uuid>temp_str</uuid>
5 <url>fuji.agent.adm.cloud.com</url>
6 <customerid>customer_id</customerid>
7 <instanceid>instance_id</instanceid>
8 <servicename>MAS</servicename>
9 <download_service_url>download.citrixnetworkapistaging.net</download_service_url>
10 <abdp_url>fuji.agent.adm.cloud.com</abdp_url>
11 <msg_router_url>fuji.agent.adm.cloud.com</msg_router_url>
12 </mps_agent> Done
13 > set cloud param -CustomerID customer_id -InstanceID instance_id -Deployment Production
14 <!--NeedCopy-->"
```

**Data Governance**

June 1, 2022

This topic provides information regarding the collection, storage, and retention of logs by the Citrix Adaptive Authentication service and the Adaptive Authentication instances. Any capitalized terms not defined in Definitions carry the meaning specified in the Citrix End User Services Agreement.

- Adaptive Authentication services: Citrix Cloud service that administrators can log in to deploy and manage Adaptive Authentication instances.
- Adaptive Authentication instances: Citrix ADC virtual machines deployed by the Adaptive Authentication service to allow administrators to manage user authentication.

**Data residency**

**Adaptive Authentication services**

The Citrix Adaptive Authentication service customer content data resides in the Azure Cloud Services East region. They are replicated to the following Azure regions for availability and redundancy:

- US West
The following are the different destinations for the service configuration and runtime logs.

- Splunk service for system monitoring and debugging logs, in the US and EU (European Union) locations only.
- Citrix Application Delivery Management service for the aggregated user access logs. For details, see Citrix ADM Data Governance.
- Citrix Cloud System Logs service for admin audit logs. For details, see Citrix Cloud Services Customer Content and Log Handling and Geographical Considerations.

**Adaptive Authentication instances**

Citrix Application Delivery Management service for backing up all configurations, instance specific artifacts. For details, see Citrix ADM Data Governance.

**Data collection**

Citrix Adaptive Authentication service allows the customer administrators to configure the service through the Adaptive Authentication UI and the companion Connector Appliances through the console. The following customer content is collected:

- Adaptive Authentication service
  - FQDN (fully qualified domain name) and IP address of the IdP (identity provider) endpoint.
  - IP addresses/ranges, ports, and protocols
  - Certificates used to access the IdP authentication virtual server
  - Public IP address of the management endpoint
  - For Azure VNet peering, service principal with network contributor role. For details, see Set up connectivity to on-premises authentication servers using Azure VNet peering.

- User identifiers for app entitlements
- Citrix Cloud Connector related details. For details, see Citrix Cloud Connector.
  - IP addresses or FQDNs
  - Users, devices, and resource location identifiers
  - Internal proxy configuration

For runtime logs collected by the service components, the key information consists of the following:

- Client IP address and port
- Destination FQDN/address and port
- Client User-Agent
- Application URL path
- Application access time and duration
- Request byte count
Citrix Secure Private Access

- Response byte count
- HTTP transaction ID
- Deployment mode (Connector or Azure VNet peering)
- Azure resources
  - Resource group names
  - VNets (IP addresses, CIDRs)
  - Subnets (IP addresses, CIDRs)
  - Virtual machine names

**Data transmission**

Citrix Adaptive Authentication service sends logs to the destinations (Splunk) protected by the transport layer security.

**Data control**

Citrix Adaptive Authentication service does not currently provide options for the customers to turn off sending logs or prevent customer content from being replicated globally.

**Data retention**

Based on the Citrix Cloud data retention policy, the customer configuration data is purged from the service 90 days (about 3 months) after subscription has expired.

The log destinations maintain their service-specific data retention policy.

- For the events stored in Citrix Application Delivery Management. See Citrix ADM Data Governance.
- The Splunk logs are archived and eventually removed after 90 days (about 3 months).
- The Adaptive Authentication instances are deallocated 30 days (about four and a half weeks) after the subscription has expired.

**Data export**

There are different data export options for several types of logs.

- The admin audit logs are accessible from the Citrix Cloud System Log console.
- The Splunk logs are not for customers to consume. These events can also be exported from Splunk as a CSV file.
Definitions

- Customer content means any data uploaded to a customer account for storage or data in a customer environment to which Citrix is provided access to perform the services.
- Log means a record of events related to the services, including records that measure performance, stability, usage, security, and support.
- Services mean that the Citrix Cloud services outlined earlier for the purposes of facilitating the customer use cases.

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

June 1, 2022

In today’s ever changing situations, application security is vital for any businesses. 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, TCP, or SaaS 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 an embedded browser or a Secure Browser service – The embedded browser enforces some security controls. These controls are enforced by the client. When the embedded 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 embedded browser.

Create an adaptive access policy

1. On the Secure Private Access service tile, click Manage.
3. Click Create Policy.

Note:

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

1. For these applications - This field lists all the applications that an admin has configured in the Secure Private Access service. Admins can select the applications to which this adaptive policy must be applied.

2. If the following condition is met - Select the context for which this adaptive access policy must be evaluated.

   Important:
   The Users or groups condition is a mandatory condition to be met to enable access the
3. Click **Add Condition** to add extra conditions, based on your requirement. An AND operation is performed on the conditions, and then the adaptive access policy is evaluated.

4. **Then do the following** - If the set condition matches, admins can select the action to be performed for the users accessing the application.
   - **Allow access** - Allow access without any preset conditions. **Note:** This option is applicable for browser-based applications only.
   - **Deny access** – When selected, access to the apps is denied. All other options are grayed out.
• **Allow access with restrictions** - Select one of the preset security policy combinations. These security policy combinations are predefined in the system. Admins cannot modify or add other combinations.

When you choose *Allow access with restrictions*, you can select the security controls as per your requirement. The following security restrictions can be enabled for the application:

- **Restrict clipboard access**: Disables cut/copy/paste operations between the app and system clipboard
- **Restrict printing**: Disables ability to print from within the Citrix Workspace app browser
- **Restrict navigation**: Disables the next/back app browser buttons
- **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 Office365 and the user edit an Office365 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.

**Note:**

For TCP applications, both *Allow access* and *Deny access* options are available.

5. **In Policy name**, enter the name of the policy.
6. Turn the toggle switch ON to enable the policy.

7. Click **Create Policy**.

**Adaptive access based on users or groups**

To configure an adaptive access policy based on users or groups, use the Create an adaptive access policy procedure with the following changes.

- In **If the following condition is met**, select **Users or groups**.

- If you have configured multiple users or groups, then select one of the following as per your requirement.
  - **Matches any of** – The users or groups match any of the users or groups configured in the database.
  - **Does not match any** – The users or groups do not match with the users or groups configured in the database.

- Complete the policy configuration.
**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 procedure with the following changes.

- **In If the following condition is met**, 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 procedure with the following changes.

- **In If the following condition is met**, 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**.

**Create network location**

Network locations correspond to the public IP address ranges of the networks that your users connect from, such as your office or branch locations. Citrix Cloud uses public IP addresses to determine whether your users are launching virtual apps and desktops internally or externally to the company network.

Fill in the required fields below to create a new network location.

**Location name** *

Enter a friendly name for this location

**Public IP address range** *

x.x.x.x/x

**Location tags** *

Use commas to separate multiple tags

Choose a network connectivity type:

- External
- Internal

- Save
- Cancel

- 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

The Citrix Secure Private Access service provides adaptive access based on a device posture by using an on-premises Citrix Gateway or a Citrix hosted Citrix Gateway (adaptive authentication) as an IdP to Citrix Workspace. The Enterprise Web, TCP, or SaaS apps can either be enumerated or hidden from the end user based on the EPA check results and the configured smart access policy.

**Note:** Adaptive authentication is a Citrix Cloud service that enables advanced authentication for users logging in to Citrix Workspace. Adaptive authentication gives a gateway instance running in cloud and you can configure the authentication mechanism for this instance, as required.
Citrix Secure Private Access

Prerequisites

- Citrix Gateway as an IdP must be configured for Citrix Workspace. For details, see Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud.
- Citrix ADC release version 13.0 Build 82.109 or later.
- Smart access tags are configured on the Citrix Gateway appliance.

Understanding the flow of events

- User enters the Workspace URL into a browser or connects to a Workspace Store using a native Citrix Workspace App.
- User is redirected to the Citrix Gateway configured as an IdP.
- User is prompted to allow an EPA check to be performed on the device.
- Citrix Gateway performs an EPA check after the user consents to scan the device and writes the smart access tags to CAS against the device ID.
- User logs in to Citrix Workspace using Citrix Gateway IdP and the configured authentication mechanism.
- Citrix Gateway provides smart access policy information to Citrix Workspace and Secure Private Access.
- User is redirected to the Citrix Workspace home page.
- Citrix Workspace processes the smart access tags provided by the Citrix Gateway configured as an IdP, and then determines the apps that must be enumerated and displayed to the end user.

Configuration scenario – Enterprise Web, TCP, or SaaS app enumeration based on device posture scans

Step 1: Configure smart access policies using Citrix Gateway GUI

2. On the Profiles tab, click Add to create a profile.
1. In **Tags**, enter the smart access tag name. This is the tag that you must enter manually when creating the adaptive access policy.


3. Click **Add** to create a policy.

---

**Step 2: Create an adaptive access policy**

1. In **Action**, select the previously created profile and click **Add**.

2. In **Expression**, create the policy expression and click **OK**.
Perform the steps detailed in Create an adaptive access policy procedure with the following changes.

- In If the following condition is met, select Device posture check.
- If you have configured multiple smart access tags, then select one of the following as per your requirement.
  - **Matches all of** – The device ID matches all of the smart access tags written against the device ID when you log in to Citrix Workspace.
  - **Matches any of** – The device ID matches any of the tags written against the device ID when you log in to Citrix Workspace.
  - **Does not match any** - The device ID does not match against the device ID when you log into Citrix Workspace.
- In Enter custom tags, manually type the smart access tag. These tags must be similar to the tags configured in Citrix Gateway (Create Authentication Smart Access Profile > Tags).
Points to note

- Posture evaluation occurs only when you log on to Citrix Workspace (only during the authentication).
- In the current release, continuous device posture evaluation is not done. If the device context changes after the user logs on to Citrix Workspace, then the policy conditions do not have any impact on the device posture evaluation.
- Device ID is a GUID generated for each end user device. Device ID might change if the browser used to access Citrix Workspace is changed, cookies are deleted or incognito/private mode is used. However, this change does not impact the policy evaluation.

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 procedure with the following changes.

- In If the following condition is met, select User risk score.
- Configure the adaptive access policy based on the following three types of user risk conditions.
  - 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
Create a policy to enforce application access rules based on a user's context.

For these applications

If the following condition is met

Then do the following

Policy name

RiskScorePolicy
Route tables to resolve conflicts if the related domains in both SaaS and web apps are the same

July 16, 2022

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 Citrix Gateway connectors.

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 Citrix Gateway Connectors, as per the requirement.

Application Domains feature also enables admins to configure the Citrix Gateway connectors to by-
pass 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 Citrix Gateway connector.

**How the route table works**

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

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

![Image of a FQDN entry](image)

**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 Gateway Service user interface.

**To add routes to the mini route table**

The steps to add an app in the Citrix Gateway Service UI 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 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 Gateway Connector 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 Citrix Gateway Connector.
  – **Internal – bypass proxy** - Domain traffic is routed through Citrix Cloud Gateway Connectors, bypassing the customer’s web proxy configured on the Gateway Connector.
  – **External via Gateway Connector** – The apps are external but the traffic must flow via the Citrix Gateway Connector 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.

• **Gateway Connector Status:** Autopopulated, along with resource location, when you select the type Internal for an app.

**Note:**

You can also add a Gateway Connector in a new resource location using the “Install Gateway Connector” link and get the activation code for registration. For details, see [Ways to install Citrix Gateway Connector](#).

**Web filtering**

March 31, 2022
The web filtering feature evaluates the risk of each hyperlink selected within the SaaS application. Accessing these sites and monitoring changes in user behavior increases the user’s overall risk score because it signals the endpoint device is compromised and started to infect or encrypt data or the user and device are stealing intellectual property.

**How web filtering works**

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. 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.

**Note:** The block, redirect, and allow URL analysis is also performed at the category level.

**Configure website filtering**

March 31, 2022

Configure web filtering for internet access from SaaS apps.

**Configure web filtering for internet access from SaaS apps**

You are now ready to configure content access settings for your end users accessing the SaaS apps. For example, a link within a SaaS app can point to a malicious website. With content access settings, an administrator can take a specific website URL or a website category and allow access, block access, or redirect the request to a hosted, secure browser instance, helping to prevent browser-based
attacks. For more information about the secure browser service, see Secure Browser Standard Service documentation at [Secure Browser Standard Service](#).

**Note:**

A paid Secured Browser Standard Service customer (organization) gets 5,000 hours of use per year by default. For more hours, they need to buy secure browser add-on packs. You can track the usage of the Secure Browser Service. For more information, see [Monitor usage](#).

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, website categories are checked.

3. Does the request match the configured website category?
   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 website category filtering**

Website categorization restricts user access to specific website categories. Administrators can select from a preset list or customize the categories depending on the deployment. The preset list enables organizations to filter web traffic by using a commercial categorization database. The auto-updating database classifies billions of websites into different categories, such as social networking, gambling, adult content, new media, and shopping. In addition to categorization, each website has a reputation score kept up-to-date based on the site’s historical risk profile. Presets are classified as strict, moderate, lenient, none, and custom. Administrators can tweak presets to add or remove website categories.

- Strict preset minimizes the risk of accessing unsecured or malicious websites. End users can still access websites with low risk. Includes most business travel and social media websites.
- Moderate preset minimizes the risk while allowing more categories with low probability of exposure from unsecure or malicious sites. Includes most business travel, leisure, and social media websites.
- Lenient preset maximizes access while still controlling risk from illegal and malicious websites.
- None preset allows all categories.
- Custom allows configuring custom filtering of categories.

Perform the following steps to configure website category filtering.

1. In the Secure Private Access home page, click **Settings** in the navigation pane.
2. Click **Web Filtering** and then click **Edit**.
3. Enable **Filter website categories**. Click **Add** in the respective section to block website categories, allow website categories, or redirect the user to a secure browser. For example, to block categories, in the blocked categories section, click **Add**.

4. Select the categories to block from the list and click **Add**.

5. To allow categories, in the allowed categories section, click **Add**. Select the categories to allow from the list and click **Add**.

6. To redirect users to a secure browser, in the redirected to secure browser categories section, click **Add**. Select the categories from the list and click **Add**.

7. Click **Save**.

**Configure website lists filtering**

The website list feature enables you to control access to specific websites. 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.

Perform the following steps to configure website lists filtering.

1. In the Secure Private Access home page, click **Settings** in the navigation pane.

2. Click **Web Filtering** and then click **Edit**.

3. Enable **Filter website list**. Click **Add** in the respective section to block websites, allow websites, or redirect the user to a secure browser. For example, to block websites, in the blocked categories section, click **Add**.
4. Enter a website that users cannot access and click Add.

5. To allow websites, in the allowed websites section, click Add. Enter the website that users can access and click Add.

6. To redirect users to a secure browser, in the redirected to secure browser websites section, click Add. Enter a website that end users can access only from a Citrix hosted browser and click Add.

7. Click Save for the changes to take effect.

Available categories list for Citrix Secure Private Access

April 1, 2022

Categories restrict user access to specific websites and website categories. Enterprise customers can filter web traffic by using a commercial categorization database that is available in the Citrix Secure Private Access service. This database has many URLs classified into different categories, such as social networking, gambling, adult content, new media, and shopping. When you select categories to add, block, or redirect to a secure browser, advanced policies are created internally to filter your traffic.

For example, you might want to block access to dangerous sites, such as sites known to be infected with malware. You might want to selectively restrict access to content, such as adult content or entertainment streaming media for enterprise users.

List of third party categories and category groups:

- **Adult**
  - Adult/Porn
  - Nudity
  - Sexual Services
  - Adult Search/Links
  - Illegal Activities
  - Dating
  - Grotesque
- Adult Magazine/News
- Fetish
- Sexual Expression (text)
- Sex Education

- Business & Industry
  - Swimsuits & Lingerie
  - Business & Industry
  - Translators
  - Auctions
  - Shopping/Retail
  - Real Estate
  - IT Online Shopping
  - Side Business
  - Smoking
  - Alcoholic Products
  - Automotive
  - Business & Commercial
  - Ringtones
  - Emoticons
  - Mobile Operators
  - Agriculture
  - Associations/Trade Groups/Unions
  - Books/ebooks
  - Piracy & Copyright Theft
  - Transport Service & Freight

- Computing & Internet
  - Advertisements/Banners
  - Computing & Internet
  - Mobile Apps & Publishers
  - Content Delivery Networks & Infrastructure
  - Hosting Sites
  - Parked Domains
  - DDNS

- Downloads
  - Downloads
  - Program Downloads
  - Storage Services
  - Mobile App Stores

- Email
- Web-based Mail
- Email Subscriptions

**Finance**
- Market Rates
- Online Trading
- Insurance
- Financial Products

**Gambling**
- Gambling in general
- Lottery
- Sweepstakes/Prizes

**Health**
- Health
- Hate

**Illegal/Harmful**
- Illegal Activities
- Illegal Drugs
- Medication
- Marijuana
- Terrorism/Extremists
- Weapons
- Hate/Slander
- Violence/Suicide
- Advocacy in general

**Jobs & Resumes**
- LinkedIn
- LinkedIn: Updates
- LinkedIn: Mail
- LinkedIn: Connections
- LinkedIn: Jobs
- Employment
- Career Advancement

**Malware & SPAM**
- Hacking/Cracking
- Malware
- Malicious and Dangerous
- SPAM
- Spyware
- Botnets
- Infected Sites
- Phishing Sites
- Key loggers
- Mobile Malware
- BOT Phone Home

• Messaging/Chat/Telephony
  - Web based Chat
  - Instant Messages
  - Internet Telephony
  - Military
  - SMS $ Mobile Telephony Services

• News/Entertainment/Society
  - Online games
  - Games
  - Personal Web Pages/Blogs
  - Personal Web Pages/Blogs
  - Streaming Media
  - Special Events
  - Popular Topics
  - Drinking
  - Sexual Expression(text)
  - Costume Play/Enjoyment
  - Occult
  - Home & Family
  - Professional Sports
  - Sports in general
  - Life Events
  - Travel & Tourism
  - Public Agency Tourism
  - Public Transit
  - Accommodations
  - Music
  - Horoscope/Astrology/Fortune Telling
  - Entertainer/Celebrity
  - Dining/Gourmet
  - Entertainment/Venues/Activities
  - Traditional Religions
  - Religions
  - Politics
- News
- Education
- Government
- Military
- Recreation & Hobbies
- Reference
- Kids Sites
- Arts & Cultural Events
- Philanthropy & Non-Profit Organizations
- Fashion & Beauty
- No Content
- Unsupported URL
- Law
- Local Communities
- Miscellaneous
- Online Magazines
- Pets/Veterinarian
- Recycling/Environment
- Science
- Society & Culture
- Photography & Film
- Museums & History
- eLearning
- Wordpress
- Wordpress: Posting
- Wordpress: Upload

• **Private IP Address**
  - Private IP Addresses

• **Peer-to-Peer/Torrents**
  - Peer to Peer/Torrents

• **Remote Proxies**
  - Remote Proxies

• **Search**
  - Search Engine Caches
  - Ask.fm
  - Ask.fm: Ask
  - Ask.fm: Answer
  - Search Engines & Portals

• **Social Networking**
- Social Networks in General
- Facebook
  - Facebook: Posting
  - Facebook: Commenting
  - Facebook: Friends
  - Facebook: Photo Upload
  - Facebook: Events
  - Facebook: Apps
  - Facebook: Chat
  - Facebook: Questions
  - Facebook: Video Upload
  - Facebook: Groups
  - Facebook: Games
- Twitter
  - Twitter: Posting
  - Twitter: Mail
  - Twitter: Follow
- YouTube
  - YouTube: Commenting
  - YouTube: Video Upload
  - YouTube: Sharing
- Instagram
  - Instagram: Upload
  - Instagram: Commenting
  - Instagram: Private Message
- Tumblr
  - Tumblr: Posting
  - Tumblr: Commenting
  - Tumblr: Photo or Video Upload
- Google+
  - Google+: Posting
  - Google+: Commenting
  - Google+: Photo Upload
  - Google+: Video Upload
  - Google+: Video Chat
- Pinterest
  - Pinterest: Pin
  - Pinterest: Commenting
- Vine
Citrix Secure Private Access

- Vine: Upload
- Vine: Commenting
- Vine: Message
- YikYak
- YikYak: Posting
- YikYak: Commenting
- Photo Search & Photo Sharing Sites
- Bulletin Boards
- IT Bulletin Boards

Citrix Cloud Gateway Connector availability in Azure Marketplace

May 17, 2022

Important:

- Citrix Gateway Connector is planned to be deprecated in the upcoming release. Citrix recommends that you migrate to Connector Appliance that is a single Zero Trust Network Access connector. For details on Connector Appliance, see Connector Appliance for Cloud Services.

- To migrate your Gateway Connector to Connector Appliance, see Migrate Gateway Connector to Connector Appliance.

The Citrix Cloud Gateway connector is available in Azure Marketplace Offers.

To deploy the Citrix Gateway Connector instances in the Azure Marketplace:

1. Go to Azure > Marketplace and search for Citrix Cloud Gateway Connector.
2. Click Citrix Cloud Gateway Connector.
3. Click **Create** in the **Citrix Cloud Gateway Connector** page. Choose a size that has 2 vCPUs and 4 GB RAM minimum.
Create a virtual machine

Basics  Disks  Networking  Management  Advanced  Tags  Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more.

Project details
Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription *
- sees-dev-guyrags-shared

Resource group *
- (New)Resource group
- Create new

Instance details
Virtual machine name *

Region *
- (US) South Central US

Availability options *
- No infrastructure redundancy required

Image *
- Citrix Cloud Gateway Connector BYOL - Gen1
- See all images

Azure Spot instance
- 

Size *
- Standard A2s - 2 vcpus, 4 GB memory ($21.63/month)
- See all sizes

Administrator account
Authentication type
- SSH public key
- Password

Username *
- The value must not be empty.
- The value must be between 1 and 64 characters long.

Password *

Confirm password *

Review + create  < Previous  Next : Disks >
4. Enter the virtual machine details as per your requirement.

**Note:** The default OS disk is the Premium SSD and the minimum storage needed is 20 GB.

5. After the VM is created, update the **Networking** and **Inbound Port Rules** to allow ports 22 and 8443. You can access the admin UI at `<https://<ip>:8443>`.

6. Log on with default connector credentials and complete the registration.

**Note:**

- The offering, by default, comes up with and allows management access on port 8443 only for the default administrator with the default administrator password.
- Citrix recommends accessing the Gateway Connector admin user interface from inside the Azure Virtual Network.

**Create a virtual machine by using a pre-set configuration**

You can also create a virtual machine by using a pre-set configuration. However, Citrix recommends that you create a virtual machine with a new configuration. The pre-set configuration suggests using the D series virtual machine but it is not a mandatory requirement for the Citrix Gateway Cloud Connector.

To do so, click **create a virtual machine with a pre-set configuration** in the Citrix Cloud Gateway Connector page and complete the registration.
Choose recommended defaults that match your workload

To quickly customize your virtual machine, choose one of the following preset configurations. You can modify these configurations at any time.

Select a workload environment

- Dev/Test
  - Boot diagnostics
  - High availability
  - Azure backup (where available)
- Production
  - Boot diagnostics
  - High availability
  - Azure backup (where available)

Select a workload type

- General purpose (D-Series)
  - Example sizes
    DS2_v2: 2 CPU, 7 GB
    DS3_v2: 4 CPU, 14 GB
  - Fast CPUs with optimal CPU-to-memory configuration
  - Workload types
    Enterprise applications, relational databases, analytics
- Memory optimized (E-Series)
  - Example sizes
    E3s_v3: 2 CPU, 16 GB
    E4s_v3: 4 CPU, 32 GB
  - High memory-to-core ratio optimized for heavy in-memory applications
  - Workload types
    SAP HANA, SQL Hekaton, other large in-memory workloads
- Compute optimized (F-Series)
  - Example sizes
    F2s_v2: 2 CPU, 4 GB
    F4s_v2: 4 CPU, 8 GB
  - High CPU-to-memory ratio optimized for compute intensive workloads
  - Workload types
    Batch processing, web servers, gaming

Continue to create VM  Skip this step
Create a virtual machine

**Basics**  **Disks**  **Networking**  **Management**  **Advanced**  **Tags**  **Review + create**

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the basics tab then review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

**Project details**

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

**Instance details**

- **Virtual machine name**: [Field]
- **Region**: (US) South Central US
- **Availability options**: Availability zone
  - High availability is recommended for production workloads.
- **Availability zone**: [Field]
- **Image**: Citrix Cloud Gateway Connector BYOL - Gen1
  - See all images
- **Azure Spot instance**: [Check box]
  - Standard_B2s - 2 vCPUs, 4 GB memory ($21.83/month)
  - D-series is recommended for general purpose workloads.
- **Administrator account**
  - **Authentication type**: SSH public key, Password
  - **Username**: [Field]
    - The value must not be empty.
    - Username must only contain letters, numbers, hyphens, and underscores and may not start with a hyphen or number.
    - The value must be between 1 and 64 characters long.
  - **Password**: [Field]
  - **Confirm password**: [Field]

**Review + create**  **< Previous**  **Next: Disks**
Note: Citrix Gateway Connector can also be deployed using the VHD. For details, see Citrix Cloud Gateway Connector availability in Azure.

Citrix Cloud Gateway Connector availability in Azure

May 17, 2022

Applications hosted in an enterprise’s data center are securely accessed and connected to cloud using the Citrix Cloud Gateway connector. The Citrix Cloud Gateway connector is a virtual machine based on the Citrix ADC appliance hosted within the company’s data center. The Citrix Cloud Gateway connector creates a secure connection and registers to Citrix Cloud services to form a secure tunnel. The Citrix Cloud Gateway connector is hosted on public cloud for customers to purchase and deploy.

Note:

- The Gateway Connector can be deployed through the Azure Marketplace. However the instructions in this topic can also be followed.
- Citrix Gateway Connector is planned to be deprecated in the upcoming release. Citrix recommends that you migrate to Connector Appliance that is a single Zero Trust Network Access connector. For details on Connector Appliance, see Connector Appliance for Cloud Services.
- To migrate your Gateway Connector to Connector Appliance, see Migrate Gateway Connector to Connector Appliance.

Deploy a gateway connector in Azure

The high-level steps involved in deploying a gateway connector in Azure are as follows:

1. Upload VHD to Azure Storage
2. Create an image
3. Create a virtual machine.

A fixed size VHD image is used as a connector image. These images are published with the regular build artifacts. The following are the steps to create a VHD from an HyperV image.

1. Extract the HyperV zip file CONNECTOR-HyperV-.zip, and copy the dynamic.vhd file to your working folder.

2. Run the following Azure CLI commands.
   
   - Convert-VHD -Path C:\Users\Administrator\Downloads\Dynamic.vhd -DestinationPath C:\Users\Administrator\Downloads\Fixed.vhd -VHDType >Fixed
• Resize-VHD -Path C:\Users\Administrator\Downloads\Fixed.vhd -SizeBytes 20481 MB
  This step is necessary if the VHD generated is not greater than the whole number size.

Upload VHD to Azure Storage

1. Create a storage account. If you already have a storage account, in the left pane, under **Blob Service**, click **Containers**.

2. Create a container or click an existing container.
3. On the Container page, click **Upload**.

4. Use the **Upload** form to upload your VHD.
Create an Image

1. Go to Azure > Images and then click Add.
2. Create an image using the uploaded VHD.

Create an image

Name *

Subscription *

Resource group *

Create new

Location *

Zone resiliency

OS disk

OS type *

Linux

VM generation *

Gen 1

Gen 2

Storage blob *

Storage type *

Standard HDD

Host caching *

Read/write

Data disks

+ Add data disk

Encryption

You can encrypt the OS and data disks with a platform-managed or customer-managed key. Learn more about disk encryption.

Create

Automation options
Create a virtual machine

1. Go to the image you created in the previous step and click **Create VM**. Choose a size that has 2 vCPUs and 4 GB RAM minimum.
Create a virtual machine

Your resources
Subscription *
Resource group *
Instance details
Virtual machine name *
Region *(US) West US *
Availability options *(No infrastructure redundancy required) *
Image *
Azure Spot instance *
Size *
See all sizes
Administrator account
Authentication type *
Username *
Password *
Confirm password *
Inbound port rules
Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular access on the Networking tab.
Public inbound ports *
Select inbound ports *
Review + create
< Previous Next : Disks >
2. After the VM is created, update the Networking and Inbound Port Rules to allow ports 22 and 8443. You can access the admin UI at <https://<ip>:8443>.

3. Log on with default connector credentials and complete the registration.

Deploy a Citrix Gateway Connector instance on AWS - Preview

March 31, 2022

Citrix Gateway Connectors can be deployed in AWS to provide secure VPN-less access to internal web applications hosted in AWS. Citrix Gateway Connectors deployed in AWS support all functions including all SSO types - Basic, Forms based, Kerberos, and SAML.

High-level steps to deploy the Citrix Gateway Connector instance on AWS:

1. Create a key pair
2. Create a Virtual Private Cloud (VPC)
3. Add more subnets
4. Create security groups and security rules
5. Add route tables
6. Create an internet gateway
7. Create a Citrix Gateway Connector instance
8. Connect to the Gateway Connector

**Create a key pair**

Amazon EC2 uses a key pair to encrypt and decrypt logon information. To log on to your instance, you must do the following:

1. Create a key pair.
2. Specify the name of the key pair when you launch the instance.
3. Enter the private key when you connect to the instance.

When you review and launch an instance by using the AWS Launch Instance wizard, you are prompted to use an existing key pair or create a new key pair. For details on creating a key pair, see [Amazon EC2 Key Pairs](#).

**Create a virtual private cloud**

A Citrix Gateway Connector instance is deployed inside an AWS VPC. A VPC allows you to define the virtual network dedicated to your AWS account. For more information on AWS VPC, see [Getting Started With Amazon VPC](#).

While creating a VPC for your Citrix Gateway Connector instance, note the following:

- Use the VPC with a VPC with public and private subnets option to create an AWS VPC in an AWS availability zone.
- Citrix recommends having the Bastion VM (Jump Box) in the public subnet and the Citrix Gateway Connector VM in the private subnet.
- Access the Citrix Gateway Connector from the Bastion VM.
- All subnets must be in the same availability zone.

**Add more subnets**

When you used the VPC wizard, only two subnets (Public and Private) were created. Depending on your requirement, you might want to create more subnets. For more information about how to create more subnets, see [Adding a Subnet to Your VPC](#).

**Create security groups and security rules**

To control inbound and outbound traffic, create security groups and add rules to the groups. For more information about how to create groups and add rules, see [Security Groups for Your VPC](#).

To enable access to the Citrix Gateway Connector, open port 22 and 8443 must on the security group for SSH and HTTPS respectively.
Add route tables

Route table contains a set of rules, called routes, that are used to determine where the network traffic is directed. Each subnet in your VPC must be associated with a route table. For more information about how to create a route table, see Route Tables.

Create an internet gateway

Create an internet gateway for internet traffic flow in your public subnet and add it to the corresponding route table for the private subnet.

Create an NAT gateway for internet traffic flow in your private subnet and add it to the corresponding route table for the private subnet.

For more information about how to create an Internet Gateway, see Attaching an Internet Gateway.

Create a Citrix Gateway Connector instance

To create a Citrix Gateway Connector instance by using the AWS EC2 service, complete the following steps.

1. Search for the AMI ID shared with you by Citrix.
   a) Navigate to EC2 from main menu.
   b) Click AMI and search for the AMI ID in Private Images.
Important:
For technical preview, the Citrix Gateway Connector image is not available in AWS Marketplace. Contact Citrix to get access to the AMI.

2. **Launch Instance Type** - Choose instance type that has more than 2 vCPUs, 4 GB RAM minimum.

3. **Configure an instance** - Configure the Instance VPC, subnet, and network.

4. **Add storage** - Configure the storage device setting. The storage must be a minimum of 20 GB.
5. **Add tags** - Add tags to the VM.

6. **Configure the security group** - Configure the inbound and outbound firewall rules. You can create a security group or select an existing group to configure the rules.

   Inbound rules:
   - TCP Port 22 to SSH
   - TCP 8443 to access dashboard

   Outbound rules:
• All traffic

For more details, see System requirements.

7. **Review the settings** - Review your instance launch details and edit the details if necessary.
   a) Click **Launch**.
   b) Select and existing key pair or create a new key pair.
   c) Click **Launch Instances**.
8. **Select the Key Pair** - Select the created key pair for the Citrix Gateway Connector.

**Connect to Citrix Gateway Connector**

From the AWS management console, select the Citrix Gateway Connector instance and click **Connect**. Follow the instructions on the **Connect to Your Instance** page.

- You must be able to SSH to the Gateway Connector VM from the Bastion VM.
  
  `ssh -i <pem file> administrator@<ip_address>`

- To access GUI in browser from the Bastion VM use;
  
  `<https://<ip_address>:8443>`

  User name: administrator

  Password: administrator

  The default password is administrator and you are prompted to change the password after the first time you log on.

**ADFS integration with Secure Private Access**

April 8, 2022
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.
   
   ![Add Claims Provider Trust Wizard](image)

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

**Note:**

First add the app and from the app’s SSO configuration section, you can download the SAML metadata file, and then import the metadata file into ADFS.
a) Complete the steps to finish adding claim provider trust. After you complete adding the claim provider trust, a window to edit the claim rule appears.

b) Add a claim rule with **Transform An Incoming Claim.**
c) Complete the settings as shown in the following figure. If your ADFS accepts other claims, then use those claims and configure SSO in Secure Private Access also accordingly.
You have now configured the claim provider trust that confirms ADFS now trusts Citrix Secure Private Access for SAML.

**Claim Provider trust ID**

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

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

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

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

**To enable the RelayState parameter on your ADFS servers**

1. Open the file.
   - For ADFS 2.0, enter the following file in Notepad: %systemroot%\inetpub\adfs\ls\web.config
   - For ADFS 3.0, enter the following file in Notepad: %systemroot%\ADFS\Microsoft.IdentityServer.Servicehost.exe.config

2. In the microsoft.identityServer.web section, add a line for useRelayStateForIdpInitiatedSignOn as follows, and save the change:
   ```xml
   <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.
   ```powershell
   Set-AdfsProperties -EnableRelayStateForIdpInitiatedSignOn $true
   ```


**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.
     ```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.
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)


- **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/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 apps related issues

August 16, 2022

This topic provides information on some of the common issues that you might come across while configuring or accessing an app. Also, while testing the apps for security controls. These errors and the associated error codes are captured in diagnostic logs as well.

Secure Private Access service architecture

The following diagram illustrates the high level system architecture of the Secure Private Access service. The components listed in the diagram summarize the data flow across the various components involved in the app launch flow.

Secure Private Access cloud: A distributed multitenant service running across various regions in the globe. It includes various components mainly a cloud proxy component that draws all client traffic, applies various admin configured policies before making routing decisions to SaaS applications running on other public cloud or Desktops and Web applications running inside customer data centers.

On-premises Connector Appliance: The connectors run on the customer’s data center and include various components alongside the Secure Private Access provider. The appliance first registers to Citrix Cloud following which it registers itself to the nearest Secure Private Access cloud POP.

Clients: Clients are broadly classified into two categories.

- Citrix Workspace (CWA) - These clients are available both as native mobile and desktop apps or as web-based clients. These clients first connect to Citrix Cloud during user login. Citrix Cloud, in addition to the various operations, retrieve Web and SaaS apps from Secure Private Access cloud and displays them on the user dashboard.
- Citrix Secure Access client - This is a VPN agent that sets up an SSL VPN tunnel to the VPN proxy servers on the Secure Private Access service. Once the tunnel establishment is complete, it performs layer 3 interception of network traffic on the client machine and selectively tunnels certain TCP or UDP apps/FQDNs configured in the Secure Private Access cloud across the Connector appliance via the VPN proxy on the Secure Private Access cloud.
**Points to note**

- **Diagnostic tool:**
  - This topic complements the SPA diagnostic tool that is available as a PowerShell script today. Admins are required to first run the diagnostics when they come across an unexpected behavior for their users.
  - The diagnostics tool bundles analytic events from various components of the Secure Private Access system. This topic guides you to navigate to the diagnostics csv file to troubleshoot configuration related issues on the Secure Private Access cloud portal or on the customer managed on premises Connector Appliance.

- **Filtering events in the Secure Private Access diagnostics tool**

  Most components in Citrix Cloud including Secure Private Access server components send useful diagnostic information indexed as tables and include the timestamp, app info, user info, product or component type, error codes, failure reason, recommended fix and so on.

  1. Download and open the CSV file in Microsoft Excel or similar application.
  2. Enable the **Data > Filter** option.
1. In the Prod column, select WebSaas.

2. Add an additional filter in the userName column and select the affected user name. If a group of users are facing the issue, you can select any user in the group.

Adding these filters help you to narrow down to the diagnostic events to Secure Private Access’ first routing component on cloud for a specific user.

The reason column in the csv file provides detailed logs of the failure or success events which includes error code along with the app info such as App Name and App Id.

3. Copy the error code related to the app that you are troubleshooting and search for the same in the Secure Private Access error lookup table.

Secure Private Access error 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.

The table captures the following information:

- **Access Type** - Indicates the type of client software used. For all Web and SaaS app launches using the Citrix Workspace thick client or the browser based Citrix Workspace thin client, the Access Type is set to **Citrix Workspace App**. Similarly for TCP and UDP apps, the access type is set to **Citrix Secure Access**.

The difference between Citrix Workspace app and Citrix Secure Access is the underlying tunneling technology that is used to access the backend application running behind the corporate firewall. The Citrix Workspace app provides agentless access to Web and SaaS applications while...
Citrix Secure Access is an SSL VPN client that performs layer 3 routing of client traffic through the VPN server on cloud.

- **App Operation** - Indicates the high level functionality of Secure Private Access for Web/SaaS and TCP/UDP apps.

For Citrix Workspace app, as we are dealing with Web/SaaS apps, it is classified under the following categories:

- **App Enumeration** - This is the pre-launch operation which involves listing all the Applications the user is subscribed for, on the user’s dashboard immediately after the logging into the Citrix Workspace app.
- **App Access** - The operation performed by a user as part of launching the app by clicking the app’s icon.
- **Enhanced Security** - This operation is configured by the admin on the management console and the user sees the effect of it. Ex: enabling restrictions such as Cut/Copy/Paste and so on or enforcing conditional access such as redirecting the user to the Secure Browser Service instead of direct access if the user’s device does not meet certain compliance requirements.

For the Citrix Secure Access, as we are dealing with tunneling TCP-UDP traffic, the app operations are:

- **Tunnel Establishment** - the operation performed by a user as part of establishing a VPN connection on the Citrix Secure Access.
- **Packet Tunneling** - this operation happens once the VPN tunnel is established and the client forwards the IP packets to the VPN server.

<table>
<thead>
<tr>
<th>Access Type</th>
<th>App Operation</th>
<th>UI Behavior</th>
<th>Error Description</th>
<th>Error Code related</th>
<th>Recommended Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Workspace</td>
<td>App enumeration</td>
<td>One or more apps not listed on the</td>
<td>Apps restricted by contextual policy</td>
<td>0x180055</td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td>app</td>
<td></td>
<td>CWA dashboard</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>No apps listed on CWA dashboard)</td>
<td>Cache lookup errors</td>
<td></td>
<td>Contact Citrix Support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Policy evaluation errors</td>
<td></td>
<td>Contact Citrix Support</td>
</tr>
<tr>
<td>Access Type</td>
<td>App Operation</td>
<td>UI Behavior</td>
<td>Error Description</td>
<td>Error Code related</td>
<td>Recommended Steps</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>App access</td>
<td>User denied access to links inside an app</td>
<td>User not subscribed to the application</td>
<td>0x1800BC</td>
<td></td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Apps restricted by contextual policy</td>
<td>0x18000F</td>
<td></td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td>Slow backend</td>
<td></td>
<td>Apps restricted by contextual policy</td>
<td>0x18000F</td>
<td></td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td>App performance</td>
<td></td>
<td>Apps restricted by contextual policy</td>
<td>0x18000F</td>
<td></td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td>Apps are not</td>
<td></td>
<td>App FQDN length exceeded</td>
<td>0x180006</td>
<td></td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td>opening or</td>
<td></td>
<td>App details length exceeded</td>
<td>0x18000E</td>
<td></td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td>giving errors</td>
<td></td>
<td>App access is denied</td>
<td>0x18000A</td>
<td></td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Connection establishment failure between Citrix Cloud and on premises</td>
<td>0x1800EF</td>
<td></td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td>Access Type</td>
<td>App Operation</td>
<td>UI Behavior</td>
<td>Error Description</td>
<td>ErrorCode</td>
<td>Recommended Steps</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------</td>
<td>-------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>-----------</td>
<td>-------------------------------------</td>
</tr>
<tr>
<td>Connection establishment failure between Citrix Cloud and on premises connectors</td>
<td></td>
<td></td>
<td></td>
<td>0x1800EF</td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td>Single sign-on errors</td>
<td></td>
<td></td>
<td></td>
<td>0x180001, 0x18001A, 0x18001B</td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td>Authentication server down</td>
<td></td>
<td></td>
<td></td>
<td>0x180022</td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td>StoreFront errors</td>
<td></td>
<td></td>
<td></td>
<td>0x180002, 0x180003, 0x180004, 0x180005, 0x180033, 0x180034, 0x180037, 0x180035</td>
<td>Contact Citrix Support</td>
</tr>
<tr>
<td>Policy evaluation errors</td>
<td></td>
<td></td>
<td></td>
<td>0x18000F, 0x18001D, 0x18001E, 0x18001F, 0x180020, 0x18006E</td>
<td>Contact Citrix Support</td>
</tr>
<tr>
<td>Cache errors</td>
<td></td>
<td></td>
<td></td>
<td>0x18000C, 0x18000D, 0x180010, 0x180029, 0x18002A, 0x180036, 0x18004E</td>
<td>Contact Citrix Support</td>
</tr>
<tr>
<td>Access Type</td>
<td>App Operation</td>
<td>UI Behavior</td>
<td>Error Description</td>
<td>Error Code related</td>
<td>Recommended Steps</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------</td>
<td>-------------</td>
<td>-------------------</td>
<td>--------------------</td>
<td>-------------------------</td>
</tr>
<tr>
<td>Global cache (Ticketing Service) errors</td>
<td></td>
<td></td>
<td></td>
<td>0x180016, 0x180044, 0x180045</td>
<td>Contact Citrix Support</td>
</tr>
<tr>
<td>Pre-launch Secure Browser Service errors</td>
<td></td>
<td></td>
<td></td>
<td>0x180017, 0x180018</td>
<td>Contact Citrix Support</td>
</tr>
<tr>
<td>Internal Errors</td>
<td></td>
<td></td>
<td></td>
<td>0x180007, 0x180011, 0x180012, 0x180013, 0x180014, 0x180015, 0x180019, 0x180021, 0x180025, 0x180028, 0x18002B, 0x18002D, 0x18002E, 0x18003F, 0x180040, 0x180047, 0x180063, 0x180064, 0x180065, 0x180066, 0x180067, 0x180068, 0x18006A</td>
<td>Contact Citrix Support</td>
</tr>
<tr>
<td>Feature flag errors</td>
<td></td>
<td></td>
<td></td>
<td>0x18001C, 0x180087</td>
<td>Contact Citrix Support</td>
</tr>
<tr>
<td>Access Type</td>
<td>App Operation</td>
<td>UI Behavior</td>
<td>Error Description</td>
<td>Error Code related</td>
<td>Recommended Steps</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------</td>
<td>-------------</td>
<td>-------------------</td>
<td>--------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td>Auth internal errors</td>
<td></td>
<td></td>
<td>0x180021, 0x180022, 0x180023, 0x180024, 0x180026, 0x180027, 0x180039, 0x18003A, 0x18003B, 0x18003C, 0x18003D, 0x180042, 0x180043, 0x180046, 0x180049, 0x180049, 0x18006B, 0x180083, 0x180084, 0x180085, 0x180086</td>
<td>Contact Citrix Support</td>
<td></td>
</tr>
<tr>
<td>Clientless VPN - URL rewrite internal errors</td>
<td></td>
<td></td>
<td>0x180041, 0x180069, 0x1800C2, 0x1800C4, 0x1800C6, 0x1800C6, 0x1800C8, 0x1800C9, 0x1800CA</td>
<td>Contact Citrix Support</td>
<td></td>
</tr>
<tr>
<td>Access Type</td>
<td>App Operation</td>
<td>UI Behavior</td>
<td>Error Description</td>
<td>Error Code related</td>
<td>Recommended Steps</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------</td>
<td>-------------</td>
<td>-------------------</td>
<td>--------------------</td>
<td>-----------------------------------</td>
</tr>
<tr>
<td>OTT validation failed</td>
<td></td>
<td></td>
<td></td>
<td>0x180079, 0x18007A, 0x18007B, 0x18007C, 0x18007D, 0x18007E, 0x18007F, 0x180080, 0x180081, 0x180082, 0x180088, 0x180089</td>
<td>Contact Citrix Support</td>
</tr>
<tr>
<td>CVMS request forward failure</td>
<td></td>
<td></td>
<td></td>
<td>0x18006F, 0x180070, 0x180071, 0x180072, 0x180073, 0x180074, 0x180075, 0x180076, 0x180077, 0x180078</td>
<td>Contact Citrix Support</td>
</tr>
<tr>
<td>SAML SSO failure</td>
<td></td>
<td></td>
<td></td>
<td>0x18008A, 0x1800A9, 0x1800AA, 0x1800AB, 0x1800AC, 0x1800AD, 0x1800AE, 0x1800AF, 0x1800B0, 0x1800B1, 0x1800B2, 0x1800B3</td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td>Access Type</td>
<td>App Operation</td>
<td>UI Behavior</td>
<td>Error Description</td>
<td>Error Code related</td>
<td>Recommended Steps</td>
</tr>
<tr>
<td>---------------------</td>
<td>---------------------</td>
<td>----------------------</td>
<td>-------------------</td>
<td>--------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Invalid app FQDN</td>
<td>0x180048</td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td>Secure Browser</td>
<td>Backend app not loading</td>
<td>DNS lookup/Connection errors</td>
<td>0x18009D</td>
<td>See troubleshooting steps</td>
<td></td>
</tr>
<tr>
<td>Service redirect</td>
<td></td>
<td></td>
<td>Unexpected internal errors</td>
<td>0x18008B, 0x18008C, 0x18008D, 0x18008E, 0x18008F, 0x180090</td>
<td>Contact Citrix Support</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Some links not working</td>
<td>0x180092, 0x180093, 0x180094, 0x180095, 0x180096, 0x180097, 0x180098, 0x180099, 0x18009A, 0x18009B, 0x18009C, 0x18009D, 0x18009E, 0x18009F</td>
<td>Contact Citrix Support</td>
</tr>
<tr>
<td></td>
<td>CWA Web</td>
<td>Browser errors specific internal apps</td>
<td>DNS lookup/Connection errors</td>
<td>0x1800A0, 0x1800A2, 0x1800A3</td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Browser errors specific to SaaS apps</td>
<td>DNS lookup/Connection errors</td>
<td>0x1800A6</td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td>Access Type</td>
<td>App Operation</td>
<td>UI Behavior</td>
<td>Error Description</td>
<td>Error Code related</td>
<td>Recommended Steps</td>
</tr>
<tr>
<td>-------------</td>
<td>---------------</td>
<td>-------------</td>
<td>-------------------</td>
<td>---------------------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>App not loading on browser</td>
<td>Internal parsing errors</td>
<td>0x1800A4, 0x1800A8</td>
<td>Contact Citrix Support</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Feature flag error</td>
<td></td>
<td>0x1800B5</td>
<td>Contact Citrix Support</td>
<td></td>
</tr>
<tr>
<td></td>
<td>App FQDN length exceeded</td>
<td></td>
<td>0x1800B7</td>
<td>See troubleshooting steps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User not subscribed to the application</td>
<td></td>
<td>0x1800BC</td>
<td>See troubleshooting steps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Misconfigured as WebApp</td>
<td></td>
<td>0x1800BF</td>
<td>See troubleshooting steps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Disabled for clients other than Citrix Workspace</td>
<td></td>
<td>0x1800BD</td>
<td>See troubleshooting steps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Internal errors</td>
<td></td>
<td>0x1800B6, 0x1800B8, 0x1800B9, 0x1800B8, 0x1800B9, 0x1800BA, 0x1800BB, 0x1800C0</td>
<td>Contact Citrix Support</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Links within a webpage not working</td>
<td>App configuration or related domains not configured for this FQDN</td>
<td>0x1800C1, 0x1800C3, 0x1800C4, 0x1800CA</td>
<td>Contact Citrix Support</td>
<td></td>
</tr>
<tr>
<td>Access Type</td>
<td>App Operation</td>
<td>UI Behavior</td>
<td>Error Description</td>
<td>Error Code related</td>
<td>Recommended Steps</td>
</tr>
<tr>
<td>------------------</td>
<td>---------------</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>Enhanced security</td>
<td>App not opening in Secure Browser Service even though it was checked in App configuration</td>
<td>Contextual policy rule is likely conflicting with the Secure Browser Settings</td>
<td>0x1800C3</td>
<td>See troubleshooting steps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>App forced to open in Secure Browser Service even though it was not selected in app configuration</td>
<td></td>
<td>0x18006D</td>
<td>See troubleshooting steps</td>
<td></td>
</tr>
<tr>
<td></td>
<td>App incorrectly applying policies such as watermark clipboard access restricted printing and so on</td>
<td>Enhanced security policies are likely misconfigured</td>
<td>0x180091</td>
<td>See troubleshooting steps</td>
<td></td>
</tr>
<tr>
<td>Citrix Secure Access app</td>
<td>TCP/UDP Apps</td>
<td>Tunnel establishment failure</td>
<td>Config exceeds max allowed length</td>
<td>0x1800D0</td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td>Access Type</td>
<td>App Operation</td>
<td>UI Behavior</td>
<td>Error Description</td>
<td>Error Code related</td>
<td>Recommended Steps</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------</td>
<td>-------------</td>
<td>-------------------</td>
<td>-------------------</td>
<td>------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Malformed client requests</td>
<td>0x1800CD, 0x1800CE, 0x1800D6, 0x1800EA</td>
<td>See troubleshooting steps</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tunnel establishment failure because of Internal Errors</td>
<td>0x1800CC, 0x1800CF, 0x1800D1, 0x1800D2, 0x1800D3, 0x1800D4, 0x1800D5, 0x1800D7, 0x1800D8, 0x1800D9, 0x1800DA, 0x1800E1, 0x1800E2, 0x1800E4, 0x1800E5, 0x1800E6, 0x1800E7, 0x1800E8, 0x1800E9, 0x1800EE</td>
<td>Contact Citrix Support</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tunneling errors because of misconfigured App configurations</td>
<td>0x1800DC</td>
<td>See troubleshooting steps</td>
<td></td>
</tr>
</tbody>
</table>

Enhanced security control not allowed for TCP/UDP Apps

© 1999–2022 Citrix Systems, Inc. All rights reserved.
### Recommended Workarounds

**One or more apps not listed in the user dashboard**

Due to the contextual policy settings, apps may 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

---

<table>
<thead>
<tr>
<th>Access Type</th>
<th>App Operation</th>
<th>UI Behavior</th>
<th>Error Description</th>
<th>Error Code related</th>
<th>Recommended Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Secure Browser Service redirect not allowed for TCP/UDP Apps</td>
<td>0x1800DD</td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>No routing domain entry for given FQDN</td>
<td>0x1800DE</td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Access denied due to policy configuration</td>
<td>0x1800DF, 0x1800E3</td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>IPV6 unsupported</td>
<td>0x1800EB</td>
<td>See troubleshooting steps</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Access denied due to invalid IP</td>
<td>0x1800EC, 0x1800ED</td>
<td>See troubleshooting steps</td>
</tr>
</tbody>
</table>
• Incorrect matching default rule in policy - this is a fall-through case. Adjust the conditions accordingly.

**User not subscribed to the application**

User might have clicked the app link for which the user might not be subscribed.

Make sure that the user has subscriptions to the applications.

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

**Slow backend app performance**

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

1. Make sure that the connector appliance is positioned geographically close to the backend server to rule out network latencies.
2. Check if the backend 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 FQDN length exceeded**

App FQDNs must not exceed 512 characters in length. Check the application FQDN in the app configuration page. Make sure 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**

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 has been denied

This is related to contextual policy, 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.

Connection establishment failure between Citrix Cloud and on premises connectors

App routing fails due to 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 backend 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 backend 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. Make sure 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 backend URL through the proxy configuration. Check the proxy configuration for correctness.
   - `FailedToReadRequest` or `RequestReceivedForNonSecureBrowse` or `UnableToRetrieveUserCredentials` or `CCSPolicyIsNotLoaded` or `FailedToLoadBaseClient` or `ProcessConnectionFailure` or `WebAppUnSupportedAuthType` indicates tunneling failure. Contact Citrix Support.
   - `UnableToConnectTargetServer` indicates that the backend server is unreachable from the connector. Check the backend configuration again.
   - `IncorrectFormAppConfiguration` or `NoLoginFormFound` or `FailedToConstructForLoginActionURL` or `FailedToLoginViaFormBasedAuth` indicates form-based authentication failure.
Check the form SSO configuration section in App configuration in the Citrix management portal.

- **NTLMAuthNotFound** indicates NTLM based authentication failure. Check the NTLM SSO configuration section in the app configuration in the Citrix management portal.
- For further debugging, see Connector events.

**Authentication server down**

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**

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 additional 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**

Customer admin might have provided an invalid FQDN or an FQDN where DNS resolve fails at the backend 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 errors**

Broken browsing experience via Secure Browser Service. Check the backend server that the end user is trying to connect.

1. Go to the backend 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 backend server.

**CWA Web - DNS lookup/connection errors for Web apps**

Broken browsing experience of web applications running inside corporate network.

1. Filter through the diagnostic logs for the FQDNs that are not resolvable.
2. Check for reachability of the backend server from inside the corporate network.
3. Check the proxy settings to see if the connector is blocked from reaching the backend server.

**CWA Web - DNS lookup/connection errors for SaaS apps**

Broken browsing experience of SaaS applications running on public cloud.

1. Filter through the diagnostic logs for the FQDNs that are not resolvable.
2. Check for reachability of the backend 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. Cross-check the app FQDN inside the routing domain table if it has been marked as internal.
**Direct access disabled for clients other than Citrix Workspace**

App configuration disables direct access for traffic that originates from browser-based clients.

Make sure that the user has subscriptions 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**

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 that are 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.

**TCP/UDP apps - Configuration exceeds max allowed length**

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. Make sure that the maximum number of entries is well within the 16k limit.

**TCP/UDP apps - Malformed client requests**

Either the VPN tunnel is not established or certain FQDNs might not be tunneled.

1. Make sure that the requests are not being fabricated or reconstructed by proxies in the middle.
2. Suspected Man-in-Middle attacks.

**TCP/UDP apps - Enhanced security policy misconfiguration**

Enhanced Security controls can only be applied for the Web apps and not TCP/UDP apps. Review the app configuration in the Secure Private Access service GUI.
TCP/UDP Apps - Secure Browser Service redirect misconfiguration

Secure Browser 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.

TCP/UDP Apps - No routing domain entry for a given FQDN

Make sure that all the internal FQDNs that need to be tunneled by the Citrix Secure Access client must have a corresponding entry in the routing domain table.

TCP/UDP Apps - IPV6 not supported

Review the routing domain entries. Make sure that there are no IPV6 entries in the table.

TCP/UDP Apps - Invalid IP addresses

Review the routing domain entries. Make sure that the IP addresses are valid and are pointing to the correct back end.

Data Governance

March 31, 2022

This topic provides information regarding the collection, storage, and retention of logs by the Citrix Secure Private Access service. Any capitalized terms not defined in the Definitions sections carry the meaning specified in the Citrix End User Services Agreement.

Data residency

The Citrix Secure Private Access Service Customer Content data reside in the Amazon Web Services East region, and they are replicated to the following Azure regions for availability and redundancy:

- East US
- West US
- Brazil South
- Southeast Asia
- North Europe
- West Europe
- Australia East
- South India
The following are the different destinations for the service configuration and runtime logs.

- Splunk service for system monitoring and debug logs, in the US location only.
- Citrix Analytics Service for the diagnostics and user access logs, see Citrix Analytics Service Data Governance for more information.
- Citrix Application Delivery Management Service for the aggregated user access logs, see Citrix ADM Data Governance for more information.
- Citrix Cloud System Logs Service for admin audit logs, see the link below

For general information on Citrix Cloud Services, see Citrix Cloud Services Customer Content and Log Handling and Geographical Considerations.

Data collection

Citrix Secure Private Access Service allows the customer administrators to configure the service through the Admin UI, and the companion Connector Appliances through the console. The Customer Content collected are:

- For Secure Private Access Service
  - Customer private and SaaS applications
  - FQDNs and URLs for web apps or both
  - IP addresses/ranges, ports, and protocols
  - The associated resource locations
  - Single Sign-On parameters for Web and SaaS apps

- User identifiers for app entitlements
- Conditions for Adaptive Access policies
  - User identity
  - User/device geo location
  - User/device network location, through Citrix Cloud network location configuration. For details, see Optimize connectivity to workspaces with Direct Workload Connection.
  - User risk score
  - Device type

- For Connector Appliance Platform, see Connector Appliance for Cloud Services related to Secure Private Access.
  - IP addresses or FQDNs
  - Users, devices, and resource location identifiers
  - Internal proxy configuration

For runtime logs collected by the service components, the key information consists of the following:

- User name
Citrix Secure Private Access

- User Object ID
- User email address
- User UPN
- User group memberships
- Client IP address and port
- Destination FQDN/address and port
- Client User-Agent
- Application name
- Application URL path
- Application access time and duration
- Request byte count
- Response byte count
- Web Filtering decision for unsanctioned applications
- HTTP transaction ID

For the comprehensive list of data sent to Citrix Analytics Service, see Citrix Analytics Service Data Governance.

Data transmission

Citrix Secure Private Access sends logs to destinations protected by transport layer security.

Data control

Citrix Secure Private Access service does not currently provide options for the customer to turn off sending logs or to prevent Customer Content from being replicated globally.

Data retention

Based on the Citrix Cloud data retention policy, the customer configuration data are purged from the service 90 days after subscription has expired.

The log destinations maintain their service-specific data retention policy.

- For details, see Data Governance for the retention policy for the Analytics logs.
- For the events stored in Citrix Application Delivery Management, see Data governance.
- The Splunk logs are archived and eventually removed after 90 days.

Data export

There are different data export options for different types of logs.

- The admin audit logs are accessible from the Citrix Cloud System Log console.
Citrix Secure Private Access

- The Secure Private Access Service diagnostics logs can be exported from the Citrix Analytics Service as a CSV file.
- The Splunk logs are not for customers to consume. These events can also be exported from Splunk as a CSV file.

Definitions

- Customer Content means any data uploaded to a customer account for storage or data in a customer environment to which Citrix is provided access to perform Services.
- Log means a record of events related to the services, including records that measure performance, stability, usage, security, and support.
- Services mean that the Citrix Cloud services outlined earlier for the purposes of Citrix Analytics.