Citrix Cloud™

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

Citrix Cloud™ 5

What's new in Citrix Cloud™ 11

Service Level Agreement 13

Third Party Notifications 16

How to get help and support 16

Citrix Cloud™ service health 26

System and Connectivity Requirements 36

Plan your deployment 53

Citrix Cloud™ Service Trials 55

Extend Citrix Cloud™ service subscriptions 58

Geographical Considerations 61

Secure Deployment Guide for the Citrix Cloud™ Platform 68

Create a Citrix Cloud™ account 77

Verify your email for Citrix Cloud™ 87

Connect to Citrix Cloud™ 88

Citrix Cloud Connector™ 93

Citrix Cloud Connector system requirements 95

Citrix Cloud Connector™ Technical Details 102

Cloud Connector Proxy and Firewall Configuration 111

Cloud Connector Installation 113

Cloud Connector Advanced Connectivity Checks 127

Cloud Connector advanced health checks - Deprecated 132

Connector notifications 135

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Log Collection for Citrix Cloud Connector™ 138

Select a primary resource location 140

Connector Appliance for Cloud Services 142

Active Directory with Connector Appliance 185

Connector Appliance Network Connectivity Probe 198

Connector updates 202

Identity and access management 208

Manage administrator access to Citrix Cloud 213

Manage administrator groups 228

Register on-premises products with Citrix Cloud™ 241

Conditional Authentication 244

Connect Active Directory to Citrix Cloud™ 263

Connect Microsoft Entra ID to Citrix Cloud™ 268

Microsoft Entra ID Permissions for Citrix Cloud™ 273

Connect an on-premises Citrix Gateway as an identity provider to Citrix Cloud™ 278

Connect Google Cloud Identity as an identity provider to Citrix Cloud™ 286

Connect Okta as an identity provider to Citrix Cloud™ 293

Connect SAML as an identity provider to Citrix Cloud™ 306

Prerequisites 316

Which SAML Binding Mechanism should I choose to use? 320

Service Provider Initiated SSO vs Identity Provider Initiated SSO 321

Directly Connecting the SAML Provider to Citrix Cloud VS IDP Chaining 321

SAML Logout Considerations 322

Create a SAML Connection using Metadata URL Mode 325

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a SAML Connection using Metadata File Mode 329

Create a SAML Connection using Manual Mode 333

Troubleshooting 337

Configure a SAML application with a scoped Entity ID in Citrix Cloud™ 341

Sign in to stores with SAML using Multiple Custom URLs 354

Update the Service Provider SAML Signing Certificate 379

Update the Identity Provider SAML Signing Certificate 397

Advanced SAML Scenarios and correct use of cip_forest and cip_domain within the SAML Assertion 411

Configure ADFS as a SAML provider for store authentication 420

Configure Duo as a SAML provider for store authentication 427

SAML using Entra ID and AD identities for store authentication 437

SAML using Entra ID and Entra ID identities for store authentication 446

SAML using Entra ID for Guest and B2B identities for store authentication 457

Configure Okta as a SAML provider for store authentication 480

Configure an On-Premise PingFederate Server as the SAML Provider for stores and Citrix Cloud™ 491

Licensing for Citrix Cloud™ 513

Monitor licenses and active usage for cloud services 514

Monitor licenses and active usage for Citrix DaaS (User/Device) 519

Monitor licenses and peak usage for Citrix DaaS™ (Concurrent User) 527

Monitor licenses and usage for Citrix DaaS Standard for Azure 531

Monitor licenses and active usage for Endpoint Management 540

Monitor bandwidth usage for Gateway service 544

Monitor licenses and usage for Secure Private Access 551

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Monitor Citrix Managed Azure resource consumption for Citrix DaaS™ 556

Monitor licenses and usage for on-premises deployments 562

Licensing for Citrix Service Providers 569

Get started with License Usage Insights 570

Manage product usage, license servers, and notifications 573

Cloud service license usage and reporting for Citrix Service Providers 582

Customer license and usage monitoring for Citrix DaaS™ 587

Licensing for Citrix Platform Flex 590

Platform Flex Credit consumption and reporting 600

Citrix Cloud™ account management 602

Custom landing page 612

How to delete Citrix Cloud™ account and re-onboard 614

Network locations 617

Notifications 625

System Log 630

System Log Events Reference 633

System Log events for the Citrix Cloud™ platform 634

System Log events for connectors 640

System Log events for licensing in Citrix Cloud™ 642

System Log Events for Secure Private Access 645

System Log events for Citrix® StoreFront Cloud 653

SDKs and APIs 662

Citrix Cloud™ for Partners 665

Cloud Services 690

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Cloud™

July 17, 2026

> **Note:**
>
> Citrix Virtual Apps Essentials and Citrix Virtual Desktops Essentials have reached End of Sales and End of Life. For more information, see CTX583004.

Citrix Cloud is a platform that hosts and administers Citrix cloud services. It connects to your resources through connectors on any cloud or infrastructure you choose (on-premises, public cloud, private cloud, or hybrid cloud). It allows you to create, manage, and deploy stores with apps and data to your end users from a single console.

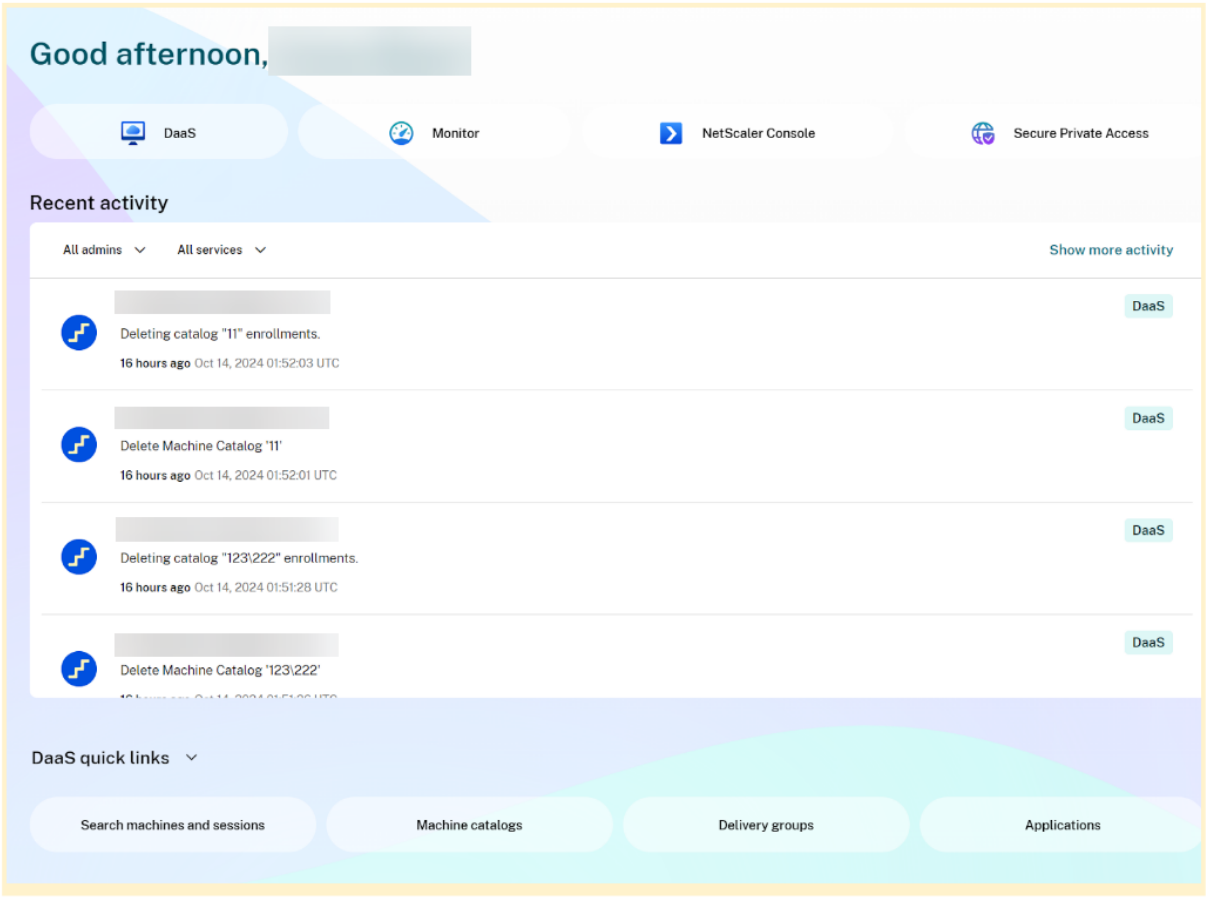
Try Citrix Cloud

Experience a full production environment in a proof-of-concept for one or more Citrix Cloud services. After signing up for Citrix Cloud, you can request service trials right inside the console. When the trial ends, you can convert to a production environment so you retain all your configurations. For more information, see Citrix Cloud Service Trials.

New modern Citrix Cloud™ home page and unified navigation experience

With the introduction of the Citrix Platform, we promised to present a simplified, unified platform that gives you zero-trust access, best-in-class app and desktop virtualization, and high-performance application delivery with comprehensive security.
As part of this commitment, a newly redesigned Citrix Cloud home page and a unified navigation experience are being introduced to elevate the way administrators manage and engage with their environments.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

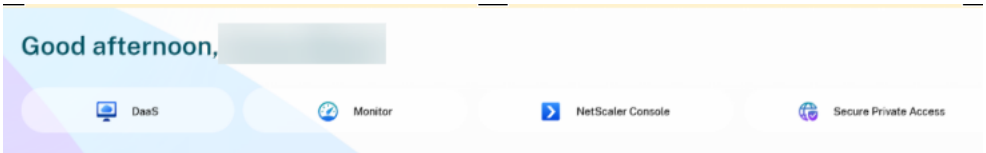


Key features

- Operational efficiency
  - Access key services directly
  - View recent activity at a glance
  - Quick links to actions within the product
- Educational hub
  - Citrix roadmap
  - Upcoming events
  - Quick links to training, community resources, and technical documentation
- Improved navigation
  - Consistent look and feel across all Citrix solutions
  - Simplified navigation with breadcrumbs and a page path
  - Customizable features like pinning

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Services Access

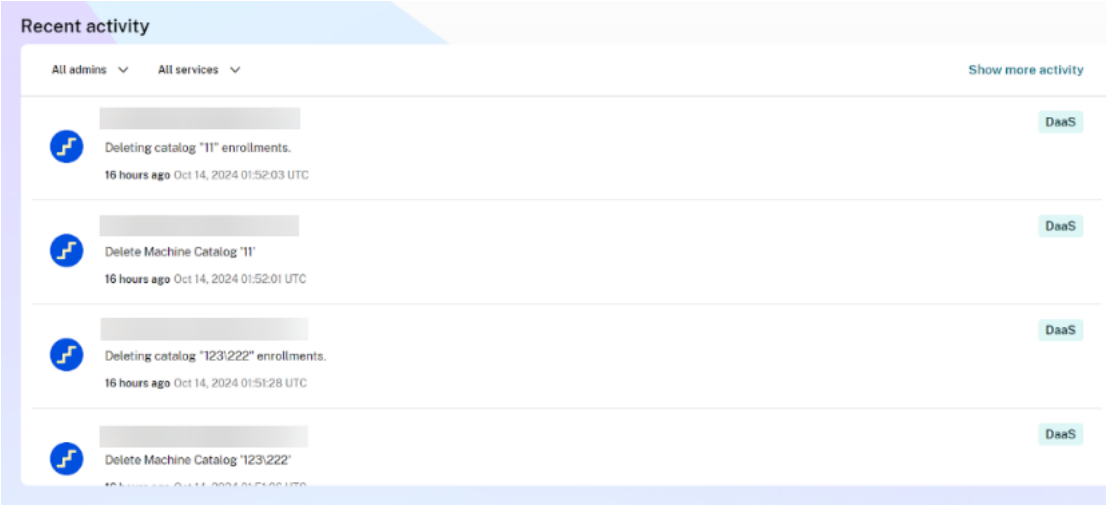


You can access all the key services through these options.

- DaaS
- Monitor
- NetScaler® Console
- Secure Private Access

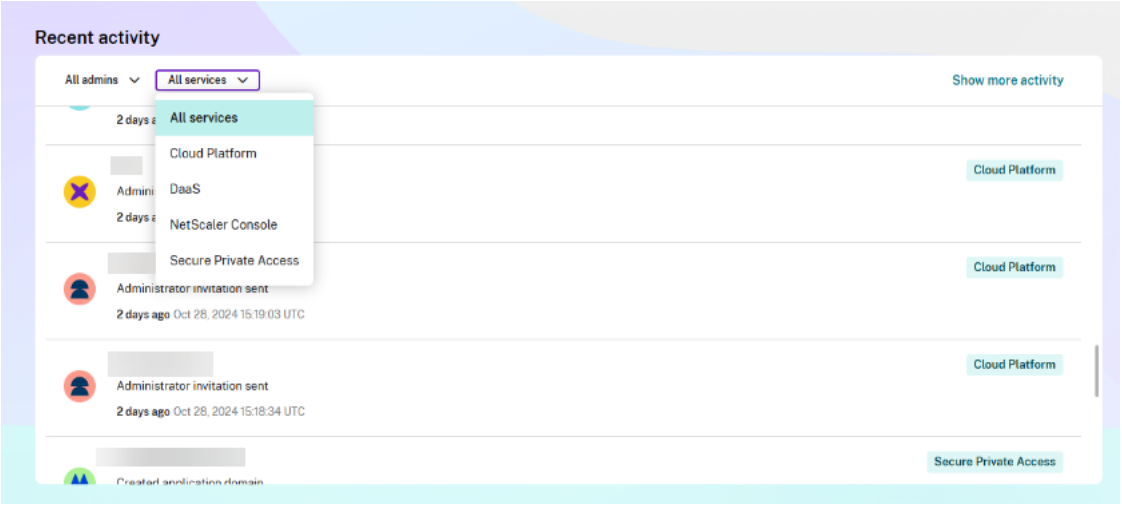
> **Note:**
>
> Additional services can be accessed using the waffle menu in the top left corner.

Recent Activity

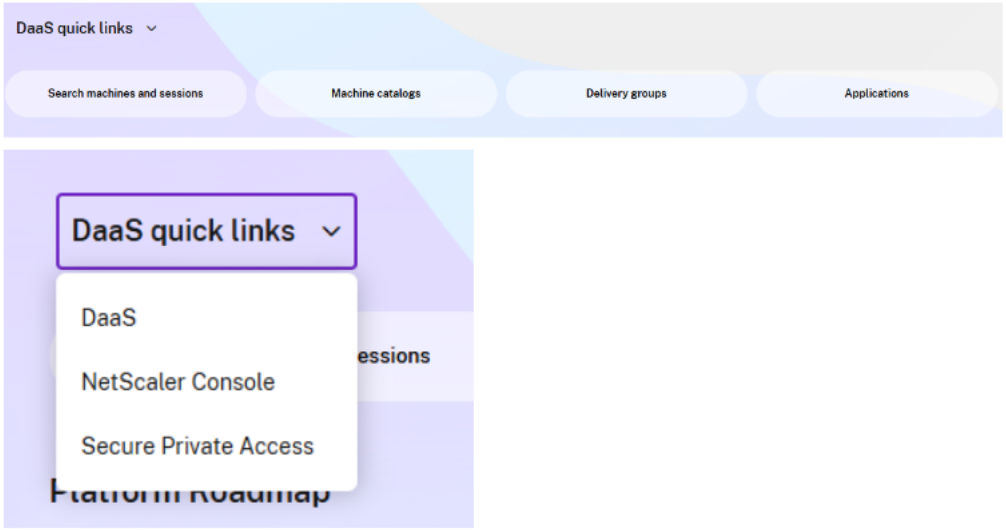


Recent Activity displays configuration changes made across the platform for services such as DaaS, NetScaler Console, Secure Private Access and Citrix Cloud, offering a quick overview. You can filter activity by service and choose to view changes made by all admins or just yourself. Selecting Show More Activity on the top right of the widget allows you to view up to 100 logs. For more information, you can click on the service to get detailed logs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



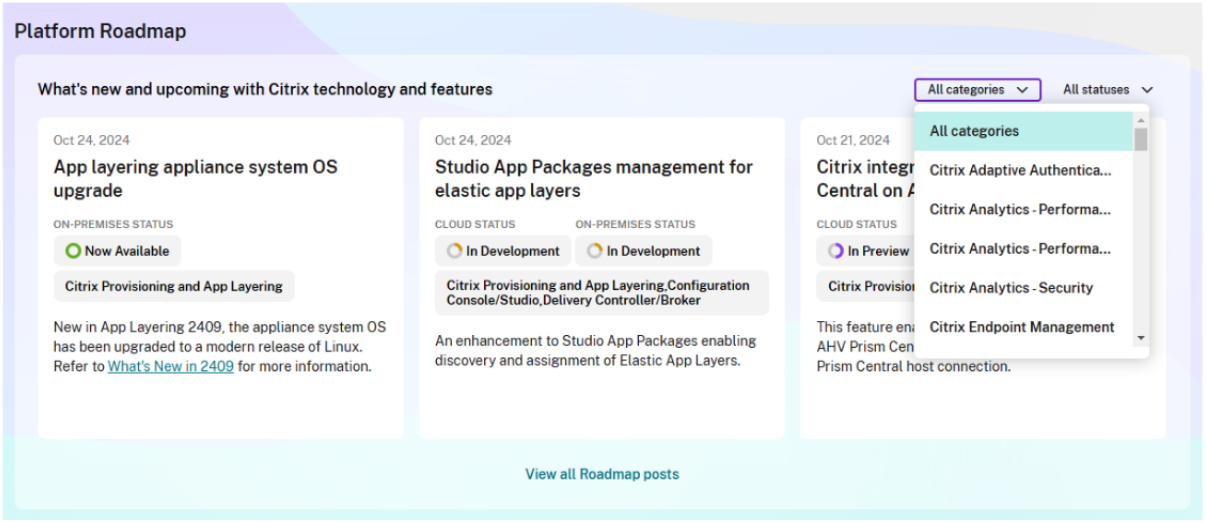
Quick links



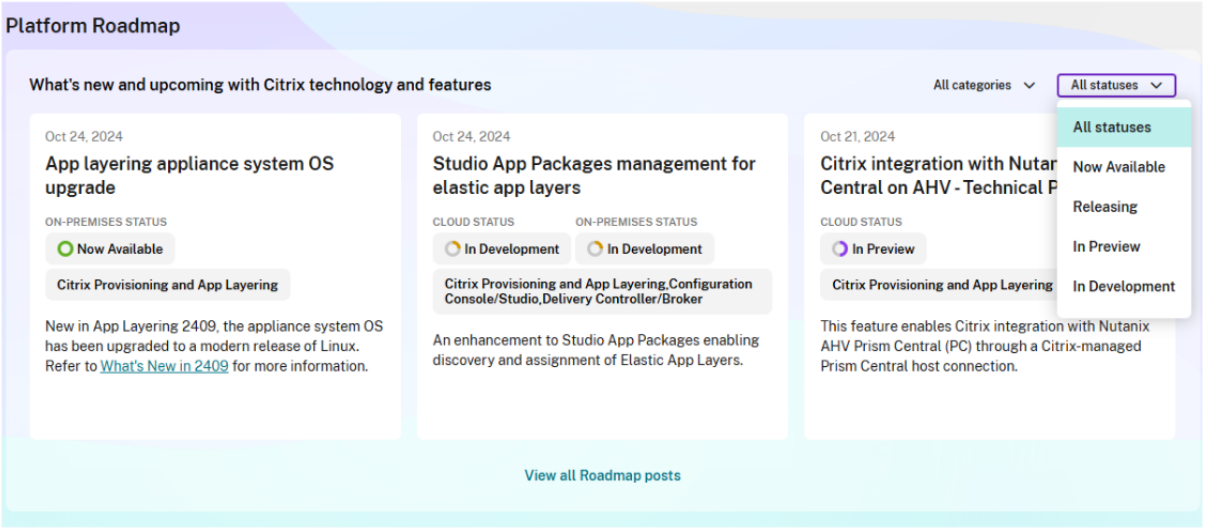
Quick links are designed to help you work more efficiently, allowing you to navigate directly to specific service sections with fewer clicks. Select the quick link for the service you wish to access, such as **DaaS**, **NetScaler Console**, or **Secure Private Access**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Platform Roadmap



Review all items currently in progress, releasing, in tech preview, or at general availability (GA). You can filter by categories like provisioning, secure private access, and/or by release status. To see the full list, click View all Roadmap posts.



Upcoming events

Stay updated with the latest events, and access the full list by clicking **View All**, which directs you to the Citrix Community page, Citrix Events.

Resources

Here are some essential resources to help you make the most of the platform:

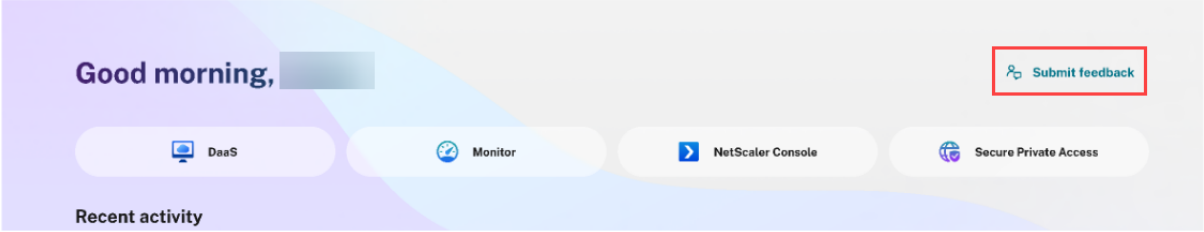
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Citrix Community**: Access discussion forums, videos, and upcoming events.
- **Training**: Find comprehensive training resources, including Pluralsight courses.
- **Automation**: Explore SDKs, REST APIs, migration tools, and more across the platform.
- **Techwire**: Our monthly platform newsletter featuring updates and top released features.

With these updates, Citrix Cloud now delivers a fully integrated, high-performance experience, setting a new standard for accessibility, usability, and productivity.

Feedback

Share feedback on bugs, enhancements, and your overall satisfaction by clicking **Submit Feedback** in the top right corner of the screen.



Citrix Cloud service documentation

Looking for information about setting up or managing Citrix Cloud services? Go to Citrix Cloud Services to find links to the product documentation for all cloud services.

Architectural and deployment resources

Citrix Tech Zone contains a wealth of information to help you learn more about Citrix Cloud and other Citrix products. Here you'll find reference architectures, diagrams, and technical papers that provide insights for designing, building, and deploying Citrix technologies.

To learn more about key service components in Citrix Cloud, see the following resources:

- Citrix® StoreFront Cloud conceptual diagram: Provides an overview of key areas such as identity, store intelligence, and single sign-on.
- Reference Architectures: Provides comprehensive guides for planning your StoreFront Cloud implementation, including use cases, recommendations, and related resources.
- Citrix DaaS reference architectures: Provides in-depth guidance for deploying Citrix DaaS (formerly Virtual Apps and Desktops service) with related services.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Education resources

The Citrix Cloud Learning Series portal offers education modules to get you up and running with Citrix Cloud and its services. You can view all of the modules sequentially, from overviews through planning and building services. Start your cloud journey with the following courses:

- Fundamentals of Citrix Cloud
- Intro to Citrix Identity and Authentication

The Citrix Education video library offers online video lessons that walk you through key deployment tasks and troubleshooting the components that you use with Citrix Cloud services. Learn more about tasks like installing Cloud Connectors and registering VDAs, as well as troubleshooting these components.

What's new in Citrix Cloud™

June 22, 2026

This article describes new features, enhancements, and fixes in Citrix Cloud releases.

May 2026

- **Licensing for Citrix Platform Flex**. Citrix Platform Flex is a managed, cloud-delivered platform designed to provide secure, resilient, and flexible delivery of digital stores and platform services across clouds. For more information, see:
  - Licensing for Citrix Platform Flex
  - Flex Credit consumption and reporting

April 2026

- **Configurable inactivity timeout for console**. Full-access administrators can now configure the duration of inactivity on the Citrix Cloud console before administrators are automatically signed out. The configurable inactivity timeout ranges from 10 minutes to 12 hours, with a default of 60 minutes. For more information, see System and Connectivity Requirements.
- **Conditional Authentication enhancements**. Conditional Authentication now supports additional identity providers and policy conditions. For more information, see Conditional Authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

January 2026

- **SAML using Entra ID for Guest and B2B identities**. Citrix Cloud now supports store authentication for guest and B2B user identities using Entra ID as a SAML provider. For more information, see SAML using Entra ID for Guest and B2B identities for store authentication.

December 2024

- **Conditional Authentication**. Citrix Cloud now supports Conditional Authentication, enabling administrators to enforce context-aware access policies. For more information, see Conditional Authentication.

September 2024

- **Onboard a new customer for partners**. Citrix partners can now onboard new customers directly from the Citrix Cloud console. For more information, see Onboard a new customer.
- **Account management updates**. The Licenses management section in Account management has been updated. For more information, see Account management.

June 2024

- **SAML using Microsoft Entra ID for Guest and B2B identities**. Citrix Cloud now supports store authentication for guest and B2B user identities. For more information, see SAML using Microsoft Entra ID for Guest and B2B identities for store authentication.

April 2024

- **SAML Signing Certificates**. You can now update both the Service Provider and Identity Provider SAML signing certificates. For more information, see:
  - Update the Service Provider SAML Signing Certificate
  - Update the Identity Provider SAML Signing Certificate

March 2024

- **Custom landing page**. Administrators can now configure a custom landing page for Citrix Cloud. For more information, see Custom landing page.
- **SAML with PingFederate**. Citrix Cloud now supports configuring an on-premises PingFederate server as a SAML provider. For more information, see SAML using PingFederate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

January 2024

- **Citrix identity provider support**. Added Citrix identity provider support in Identity and Access Management. For more information, see Identity and Access Management.
- **License Usage Insights as a new service**. License Usage Insights is now available as a new service in Supported services.

Service Level Agreement

June 22, 2026

Effective date: October 30, 2020

Citrix Cloud™ is designed using industry best practices to achieve a high degree of service availability.

> **Note:**
>
> - For information on SLA for Citrix Cloud Government, see Service Level Agreement.
> - For information on SLA for Citrix Platform Flex, see Service Level Agreement.

This Service Level Agreement (SLA) describes Citrix's commitment for Citrix Cloud Service availability. This SLA is part of the Cloud Software Group end user agreement (EULA) for covered services ("Services").

Citrix's service commitment ("Service Commitment") is to maintain at least 99.9% monthly uptime ("Monthly Uptime") on Services. Monthly Uptime is calculated by subtracting from 100% the percentage of minutes during a full month of a Service in which the Service instance was in the state of "Unavailable."Services and the measure of availability for each are set forth in the table below. Monthly Uptime percentage measurements exclude downtime resulting from:

- Regularly scheduled maintenance windows.
- Customer's failure to follow configuration requirements for the Service as documented on https://docs.citrix.com, or abusive behavior, or faulty input.
- Customer's use of a Service after Citrix® advised Customer to modify Customer's use of the Service, if Customer did not modify use.
- Caused by any component not managed by Citrix including, but not limited to, Customer controlled physical and virtual machines, Customer installed and maintained operating systems, Customer installed and controlled software, networking equipment or other hardware; Customer defined and controlled security settings, group policies and other configuration policies;

© 1997–2026 Citrix Systems, Inc. All rights reserved.

public cloud provider failures, Internet Service Provider failures; or other Customer support factors external to Citrix'control.
- Customer's employees, agents, contractors, or vendors, or anyone gaining access by means of Customer's passwords or equipment, or otherwise resulting from Customer's failure to follow appropriate security practices.
- Customer's attempts to perform operations that exceed Service entitlements.
- Service disruption due to Force Majeure, including, but not limited to, natural disasters, war or acts of terrorism, or government actions.

No Service Commitment is offered for any Citrix trial, tech preview, Labs or Beta service.

Citrix offers Service Commitments to customers that:

- Have purchased the Services using a term based subscription (1 year minimum subscription period).
- Have at least a 100 unit subscription (1,000 minimum for Citrix Service Providers), per the license model applicable to the Service, during the claim period.

Citrix Service Providers (CSPs) are eligible on October 1, 2018.

Per Service Availability Measures

Service	Measure for Monthly Uptime
Citrix Analytics for Performance™	Time users can access and improve apps and desktops performance.
Citrix Analytics for Security™	Time users can detect and mitigate user access and activity risks.
NetScaler® Console service	Average time the Service is available across all POPs.
Citrix Endpoint Management™	Time users can access their Citrix delivered mobile apps and enrolled devices through the Service.
Citrix Gateway Service for HDX™ Proxy	Time users can access their app or desktop session through the Service.
NetScaler SD-WAN Orchestrator	Time users can access their SD-WAN Orchestrator account and manage their SD-WAN network through the Service.
Citrix Secure Private Access™	Time users can access their SaaS or internal web app through the Service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service	Measure for Monthly Uptime
Citrix DaaS™	Time users can access their app or desktop session through the Service.
Citrix® StoreFront Cloud	Same as above for component services, but includes availability for each. Credits may be prorated if a claim relates to less than all components.
License Activation Service (LAS)	Time product activations are available to customers.

> **Note:**
>
> Citrix DaaS is the new name for Citrix Virtual Apps service, Citrix Virtual Desktops service, and Citrix Virtual Apps and Desktops™ service.

Service Commitment and Remedies

In the event Citrix fails to meet the Service Commitment in at least 3 out of any 5 consecutive months on or after the SLA Effective Date, the exclusive remedy is a 10% Service credit on a month-for-month basis, for those months that Citrix fails to meet the Service Commitment, applied to Customer's next annual Service extension in the immediate renewal period for the same Service and same number of units as impacted.

- Monthly Uptime Percentage: > 99.9%
- Service Credit: 10% off for applicable months (presented to the Customer as a voucher)

To receive the above remedy, the customer must be in compliance with the EULA and the failure must be reported by the customer within thirty (30) days of the end of the last month of the consecutive five-month period for which a credit claim is to be made. For instructions to report possible violations of this SLA, see CTX237141.

The request must identify the Service(s), define the dates, times and durations of Unavailability, along with supporting logs or records that corroborate the Unavailability, and identify the affected users and their locations, as well any technical support requested or remediation implemented. Only one service credit will be issued per Service, for the applicable number of months, with a maximum of a single 10% service credit for all months of the extension. Customer must present the voucher upon purchase of the extension.

If you purchase the extension through a reseller, you will receive a credit through the reseller. The credit we apply for a direct purchase, or pass to your reseller for an indirect purchase, will be based on the pro-rated, blended suggested retail price of the extension for the same number of units. Citrix

© 1997–2026 Citrix Systems, Inc. All rights reserved.

does not control resale pricing or resale credits. Credits do not include a right of offset on payments due to Citrix or a reseller. Citrix will occasionally update these terms. When updates occur, Citrix will also revise the publication date at the top of the Service Level Agreement. Any changes apply only to your new Service purchases or Service extensions on or after the current publication date.

Third Party Notifications

August 6, 2026

- Citrix Cloud Third Party Notifications (PDF)
- Citrix Analytics Service Third Party Notifications (PDF)
- Citrix DaaS Third Party Notifications (PDF)
- Citrix DaaS Standard for Azure Third Party Notifications (PDF)
- Remote Browser Isolation (formerly Secure Browser) (PDF)
- Citrix Endpoint Management Third Party Notifications (PDF)
- Citrix Cloud Linux VDA Image Service Third Party Notices (PDF)
- Connector Appliance for Cloud Services Third Party Notices (PDF)
- Citrix Gateway Service Third Party Notices (PDF)
- Citrix Device Posture Service Third Party Notices (PDF)
- Citrix Secure Private Access Third Party Notices (PDF)

> **Note:**
>
> Citrix DaaS was formerly Citrix Virtual Apps and Desktops service. Citrix DaaS Standard for Azure was formerly Citrix Virtual Apps and Desktops Standard for Azure.

How to get help and support

June 9, 2026

This article describes how to troubleshoot and get help if you experience a problem when creating an account or signing in to Citrix Cloud™ or another Citrix website. This article also includes other self-help resources and guided support options.

> **Important:**
>
> If you experience an issue with signing in to Citrix website or enrolling in multifactor authentication (MFA), review this article first for troubleshooting resources. If these resources don't help

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> you resolve your issue, contact Citrix Customer Service at https://www.citrix.com/contact/customer-service.html.

Creating an account

A Citrix account is required to access certain resources on the Citrix website, such as Citrix discussion forums, training courses, certain product downloads, and Citrix Technical Support.

To create a new Citrix account for your company, contact Citrix using one of the following methods:

- Contact Citrix Customer Service.
- Contact a Citrix Partner or Citrix Sales office in your area.

If you already have a Citrix account, you can create a Citrix Cloud account and complete the onboarding process by completing the tasks described in Create a Citrix Cloud account.

If you encounter an issue when signing up for Citrix Cloud, contact Citrix Customer Service.

Signing in to Citrix websites and Citrix Cloud

If you're having trouble signing in to a Citrix website with your Citrix account, use the following resource to troubleshoot:

- CTX228792: Troubleshooting login issues on Citrix websites

I can't set up MFA or I can't authenticate with MFA when signing in to my Citrix account

Refer to the following articles for troubleshooting information:

- CTX461297: How to Enroll into Multi Factor Authentication (MFA)
- CIX463758: How to reset Citrix MFA with recovery email address or backup codes

If you still can't sign in with MFA, contact Citrix Customer Service at https://www.citrix.com/contact/customer-service.html.

How do I find my Citrix account user name or reset my Citrix password?

Use the following steps to verify your Citrix account user name and reset your password.

1. Visit https://www.citrix.com/welcome/request-password.html.
2. To verify your Citrix account user name:
    a) Under **Find my account by**, select **Email**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b) Enter the email address associated with your Citrix account.

3. To reset your Citrix account password:

   a) Under **Find my account by**, select **User name**.
   b) Enter your Citrix account user name.

4. Click **Find my account**.

If Citrix finds your account using your email address, Citrix sends you an email with the user names and company names associated with your email address. If Citrix finds your account using your Citrix user name, Citrix sends you an email with instructions to reset your password.

If you don't receive an email after several minutes, see Citrix emails aren't appearing in my email inbox in this article.

I can't sign in to Citrix Cloud

- Make sure you sign in with the correct account credentials. To verify your account user name, visit https://citrix.cloud.com/, select **Forgot your username?**, and enter your email address. Citrix sends you an email with your account username.
- You might need to reset your password. Citrix Cloud prompts you to change your password if you haven't signed in recently or if your password isn't strong enough. For more information, see Changing your password in this article.
- You might need to sign in using a custom sign-in URL. If your Citrix Cloud account uses Microsoft Entra ID, Google Cloud Identity or SAML to authenticate administrators, select **Sign in with my company credentials** and enter your company's sign-in URL. You can then enter your company credentials to access your company's Citrix Cloud account. If you don't know your company's sign-in URL, contact your company's administrator for assistance.

If you still can't sign in to Citrix Cloud, contact Citrix Customer Service.

Citrix emails aren't appearing in my email inbox

When Citrix sends you emails to verify your identity for MFA, when finding your Citrix account, or when changing your password, the email typically arrives within a few minutes. If you don't receive these emails:

- Check the email address that's registered for your Citrix account and verify that it's correct. If you recently changed your email address, the verification email might be sent to your old address.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The email might have been accidentally filtered. Check the Spam and Trash folders in your email client. You can also search your email account for emails from donotreplynotifications@citrix.com or cloud@citrix.com.
- Your firewall might have blocked the email. Ensure that the following addresses are listed as trusted senders:
  - donotreplynotifications@citrix.com
  - cloud@citrix.com
  - CustomerService@citrix.com

If you don't receive the email after several minutes or you experience another issue with signing in, contact Citrix Customer Service.

Multifactor authentication for Citrix and Citrix Cloud accounts

Citrix customers are required to sign in to their Citrix account and Citrix Cloud using MFA. Enrolling in MFA occurs when:

- A new customer signs in to their Citrix account for the first time.
- A Citrix customer onboards a new Citrix Cloud account but hasn't yet enrolled in MFA.
- A new administrator joins an existing Citrix Cloud account.

If you're prompted to enroll in MFA when you sign in to your Citrix account or Citrix Cloud, follow the steps in CTX461297: How to Enroll into Multi Factor Authentication (MFA).

For more information about MFA for Citrix accounts, see CTX463482: Frequently asked questions when setting up Multi-Factor Authentication (MFA) on Citrix properties.

Account recovery

If you need help recovering your Citrix account credentials, see How do I find my Citrix account user name or reset my Citrix password? in this article.

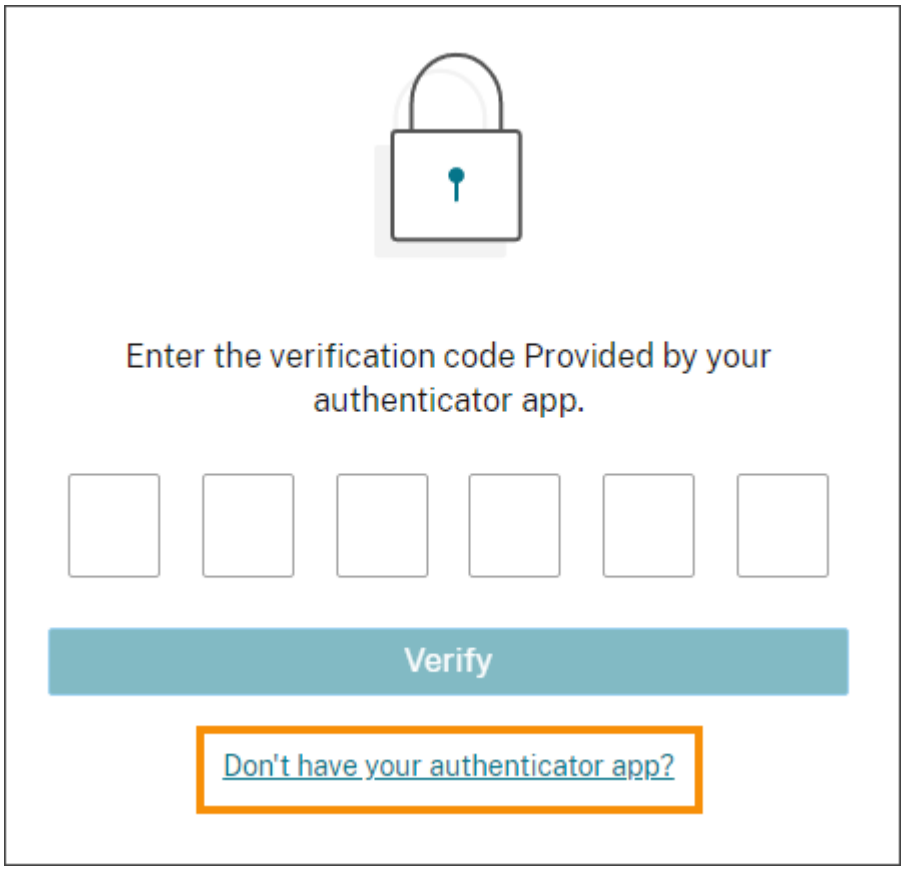
If you need help recovering access to your Citrix Cloud account, you can use the recovery methods you configured when you enrolled in MFA. These recovery methods include:

- A one-time code that Citrix sends to your recovery email address.
- A backup code from the list that you generated during MFA enrollment.
- A phone call from Citrix Support to your recovery phone number to verify your identity and help you access your account. Setting up a recovery phone number is required during MFA enrollment.

To sign in with a recovery method:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. From the Citrix account or Citrix Cloud sign-in page, enter your user name and password and then select **Sign in**.
2. When prompted for the code from your primary MFA method, select **Use a recovery method**.



3. Select the recovery method you want to use, if applicable. If you have only one other recovery method configured, besides a recovery phone number, Citrix prompts you to use that method automatically.
4. If using your recovery email address, enter the one-time code that Citrix sends and select **Verify**. If you don't receive the code for some time, select **Re-send email**. After verification, Citrix Cloud signs you in.
5. If using a backup code, enter the code when prompted and select **Verify and continue**. Citrix Cloud signs you in and sends you an email to notify you that a backup code has been used and the number of remaining valid backup codes. Note or delete the used backup code to ensure that you don't use it again.
6. If you're not able to use your recovery email or backup codes:
    a) Select **Contact Citrix Support**.
    b) Complete the form with the details of your issue. A Citrix Support representative contacts you using your recovery phone number to verify your identity. Afterward, the representa-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

tive sends you a recovery code you can use to sign in.

c) Return to the Citrix Cloud sign-in page and sign in using your Citrix Cloud credentials.

d) When prompted for a code, enter the recovery code you received from Citrix Support and select **Verify**.

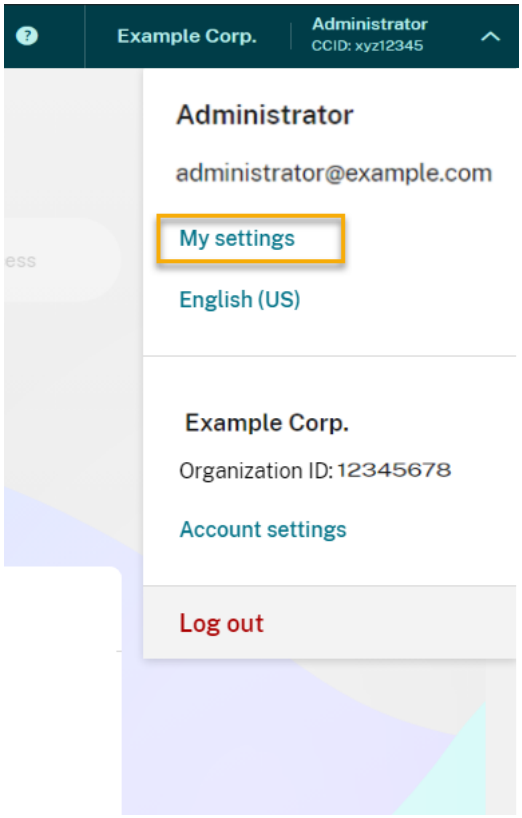
After you sign in, be sure to update your account recovery methods to avoid future sign-in delays.

Update your MFA settings

You can update your MFA access and recovery settings through your **My settings** page. You can access this page through your Citrix account or through Citrix Cloud.

To access your **My settings** page:

1. Sign in to your Citrix account or to Citrix Cloud.
2. From your Citrix account, visit https://accounts.cloud.com/core/profile.
3. In Citrix Cloud, select **My settings** from the top-right menu.



To change your MFA settings, refer to the following sections:

- Manage your primary MFA method
- Manage your MFA recovery methods

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Changing your password

If you've forgotten your account password, select **Forgot password?** and enter your account username when prompted. Citrix sends an email to the email address on your account with a link to set up a new password. If you don't receive this email after several minutes, or if you need further assistance, contact Citrix Customer Service.

Citrix Cloud might prompt you to reset your password when you attempt to sign in. This prompt occurs if:

- Your password doesn't meet Citrix Cloud's complexity requirements.
- Your password includes dictionary words.
- Your password is listed in a known database of compromised passwords.
- You haven't signed in to Citrix Cloud in the last 60 days.

Passwords must be between 8 and 128 characters long and include:

- At least one number
- At least one upper-case letter
- At least one symbol: ! @ # $ % ^ * ? + = -

When prompted, select **Reset Password** to create a new strong password for your account.

Cloud service health

The Citrix Cloud Health Dashboard (https://status.cloud.com) provides an overview of real-time availability of the Citrix Cloud platform and services in each geographical region. If you experience any issues with Citrix Cloud, check the Cloud Health Dashboard to verify that Citrix Cloud or specific services are operating normally.

For more information about the Cloud Health Dashboard, see Service health.

Citrix Cloud support forums

On the Citrix Cloud support forums you can get help, provide feedback and improvement suggestions, view conversations from other users, or start your own topics.

Citrix support staff members track these forums and are ready to answer your questions. Other Citrix Cloud community members can also offer help or join the discussion.

You don't need to sign in to read forum topics. However, you must sign in to post or reply to a topic. To sign in, use your existing Citrix account credentials, or use the email address and password you provided when you created your Citrix Cloud account.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support articles and documentation

Citrix provides substantial product and support content to help you get the most out of Citrix Cloud and resolve issues you might experience with Citrix products.

Citrix Support Knowledge Center

The Knowledge Center provides troubleshooting content as well as security bulletins and software update notices for all Citrix products. Simply enter a search string to find relevant content. You can filter results based on product and article type.

Citrix Tech Zone

Citrix Tech Zone contains a information to help you learn more about Citrix Cloud and other Citrix products. Here, you can find reference architectures, diagrams, videos, and technical papers that provide insights for designing, building, and deploying Citrix technologies.

User Help Center

The Citrix User Help Center provides Citrix product documentation just for the end-users in your organization. The User Help Center provides instructions in an easy-to-read format for end-user-facing products such as Citrix Workspace app and Citrix SSO. For end-user documentation for ShareFile, see Citrix Files apps on the ShareFile product documentation web site.

How to open a customer service case online

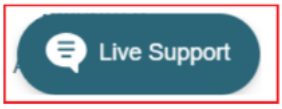
> **Note:**
>
> A customer service case can only be opened by customers or partners who are telemetry-compliant and have a valid, active entitlement.
> If the Create Case button is no longer available, customers must contact support using Chat. An advisor can help or start a Web-to-Case to create a support case.

To create a new case, follow these steps:

1. Visit the Citrix Support site.
2. Sign in using your Citrix credentials.
3. If you're having trouble signing in to a Citrix website with your Citrix account, refer to the article CTX228792: Troubleshooting login issues on Citrix websites

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Click **Live Support** to begin the virtual assistant flow.



5. Select the appropriate Case Type and then choose the **Related Issue** from the available options.



6. If you are following up on an existing case, select **My Support Cases** and follow the prompts to continue. The bot presents an article or document related to your issue.



7. If helpful, click **Yes**. You are prompted to return to the main menu or end the chat.
8. If the article was not helpful, click **No**. The bot asks you to describe the issue again and attempts to provide a more relevant article based on your new input.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

9. If the second article still does not help, click **No** again to get connected to support.
10. Click **Get Support** to proceed.



11. Click **New Case** to begin case creation.



12. Select **Account** from the drop-down list.
13. Select your **preferred language** from the available options.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



14. You are prompted with the message: **Would you like to get connected to a live agent after case creation?**
15. Select **Yes** to initiate a chat with a live agent. A case is created, and you are connected to an available advisor.
16. If **No** is selected, The bot asks for additional information and creates an offline case.

Submitting an Offline Case Through Live Support

If the virtual assistant is unable to resolve your issue, you may be prompted to provide additional details so that an offline case can be created.

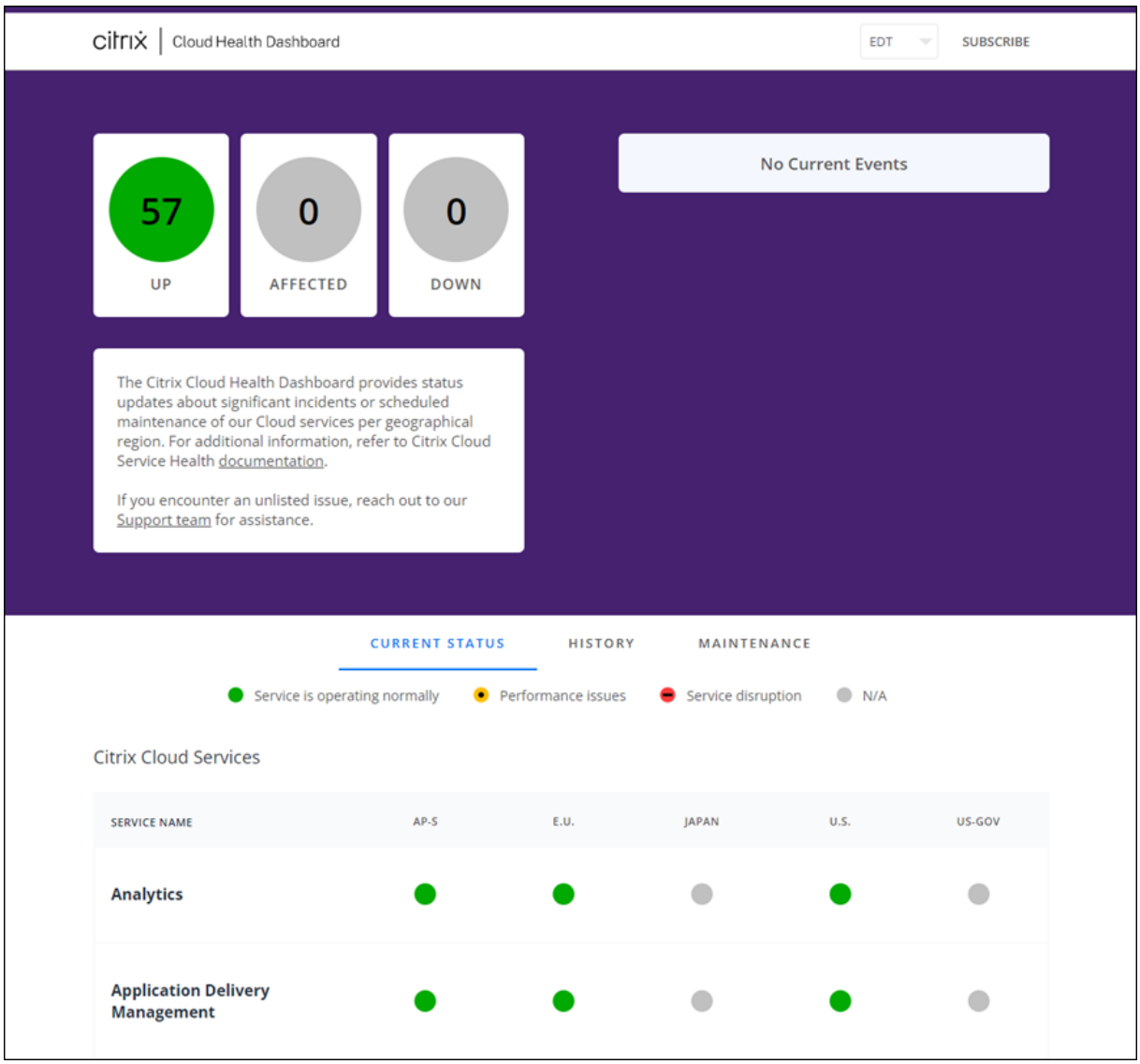
1. **Describe the issue in 10 words or less**: Provide a brief summary of the issue or request.
2. **Please enter a preferred callback number**: Provide a valid phone number where a Citrix Customer Service advisor can reach you.
3. After you submit the requested information. An offline case is generated and emailed to the chat initiator. The customer service advisor contacts the customer within two hours.

Citrix Cloud™ service health

September 6, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

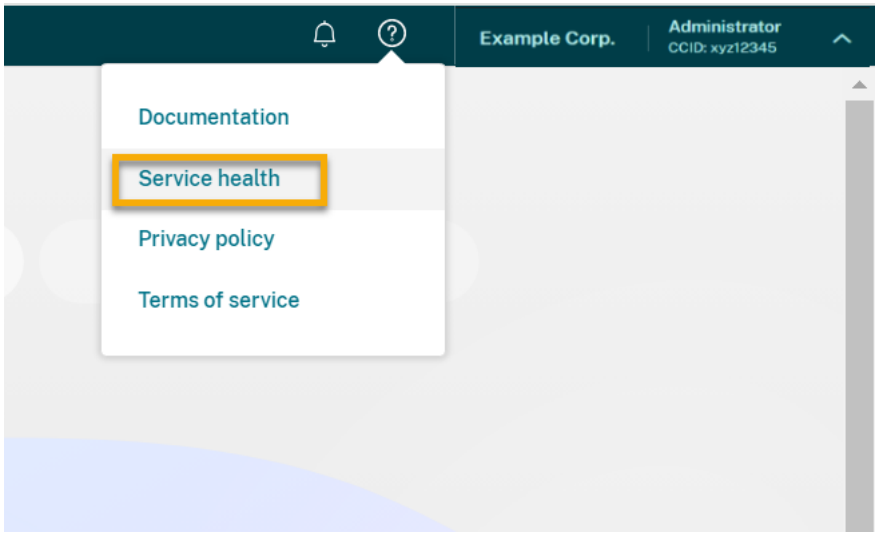
The Citrix Cloud Health Dashboard provides an overview of real-time availability of the Citrix Cloud platform and services in each geographical region. If you experience any issues with Citrix Cloud, check the Cloud Health Dashboard to verify that Citrix Cloud or specific services are operating normally.



You can access the Cloud Health Dashboard using the following methods:

- Navigate to https://status.cloud.com through your web browser.
- Select **Service Health** from the Help menu in Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



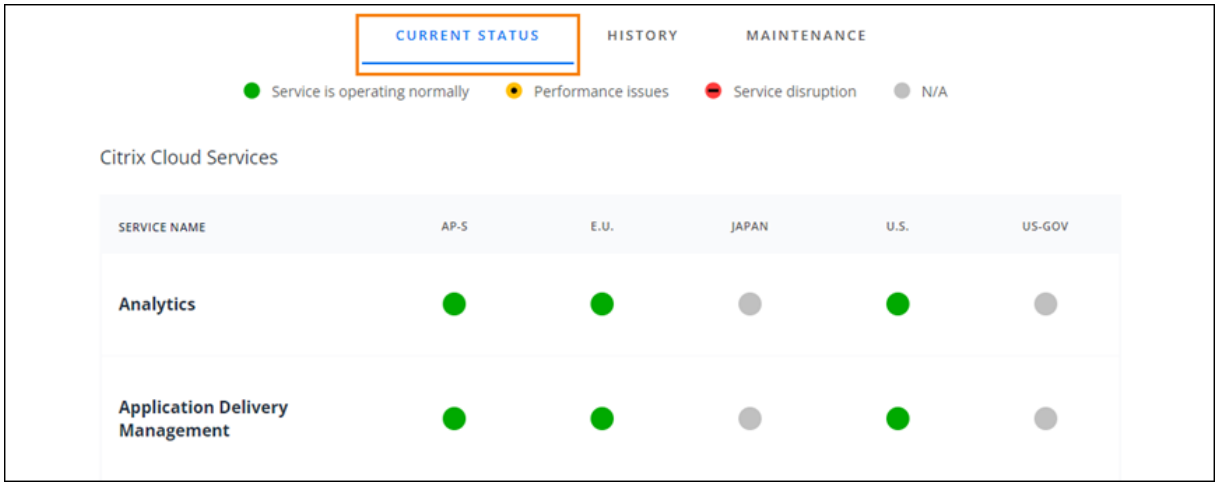
Use the dashboard to learn more about the following conditions:

- The current health status of all Citrix Cloud services, grouped by geographical region
- The health history of each service for the last seven days
- Maintenance windows for specific services

You can also subscribe to notifications about events like maintenance windows and service incidents.

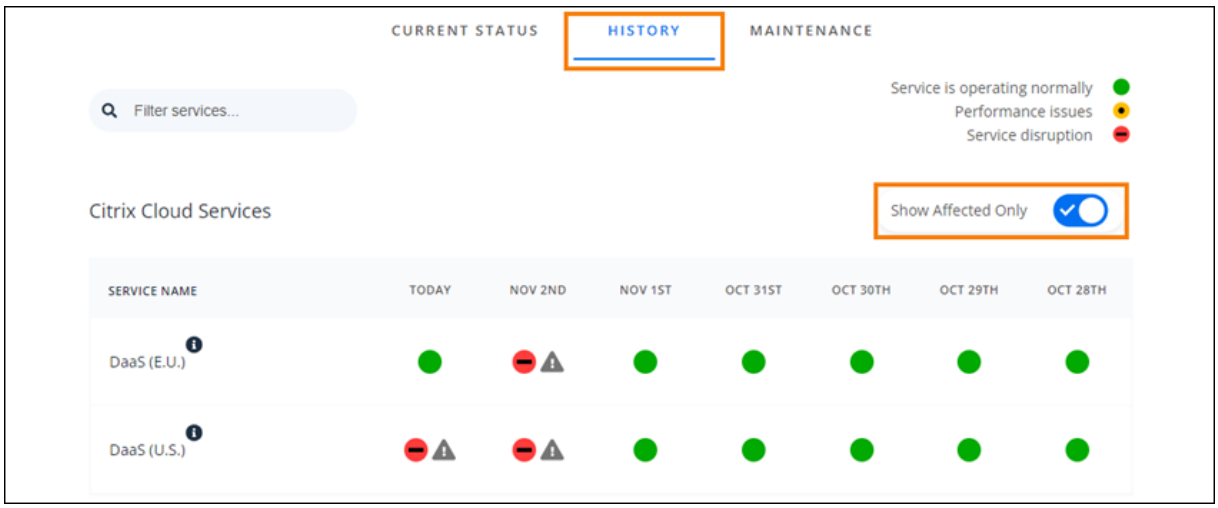
View health and maintenance status

Select **Current Status** to display the current health status of all Citrix Cloud services and platform components in each geographical region.

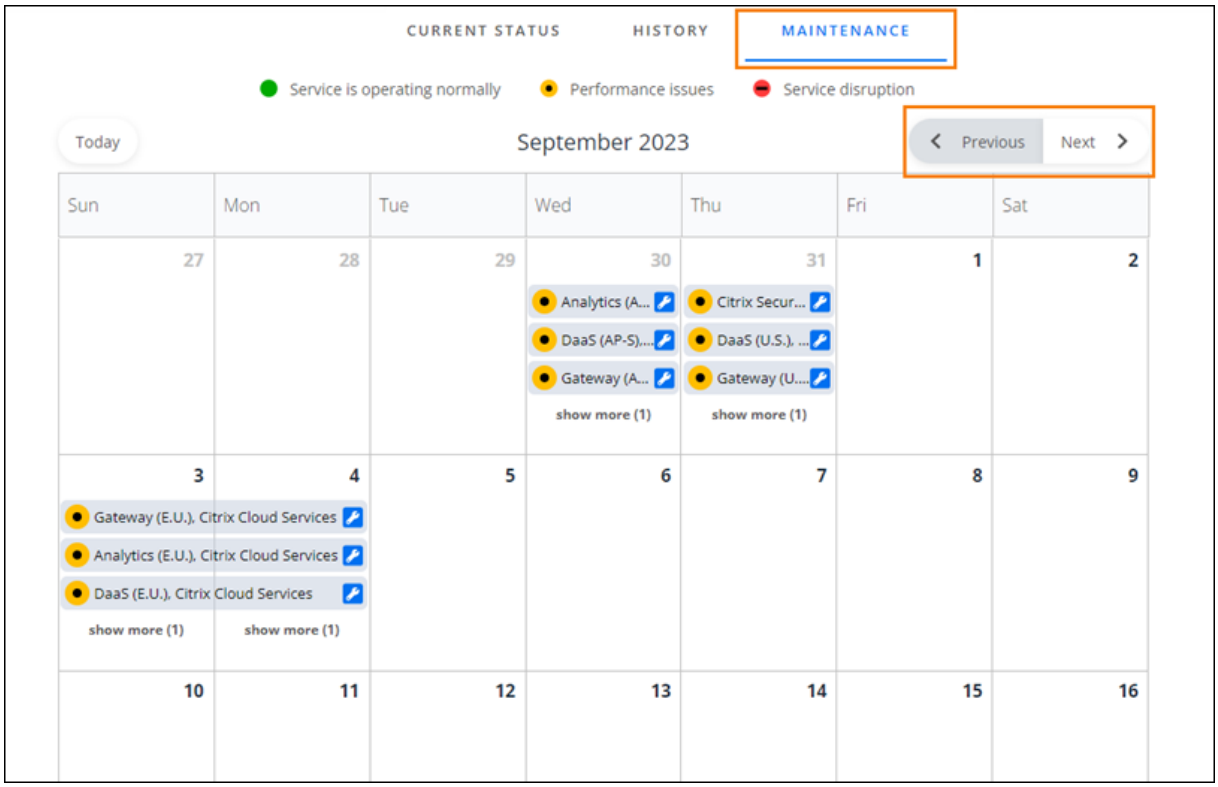


Select **History** to display the health status of all Citrix Cloud services and platform components for the last seven days. Select **Show Affected Only** to display only the services that have had maintenance or health events in the last seven days.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Select **Maintenance** to display a calendar view of service maintenance windows. Select **Next** to view maintenance events that are scheduled for future months. Select **Previous** to return to events for the current month.



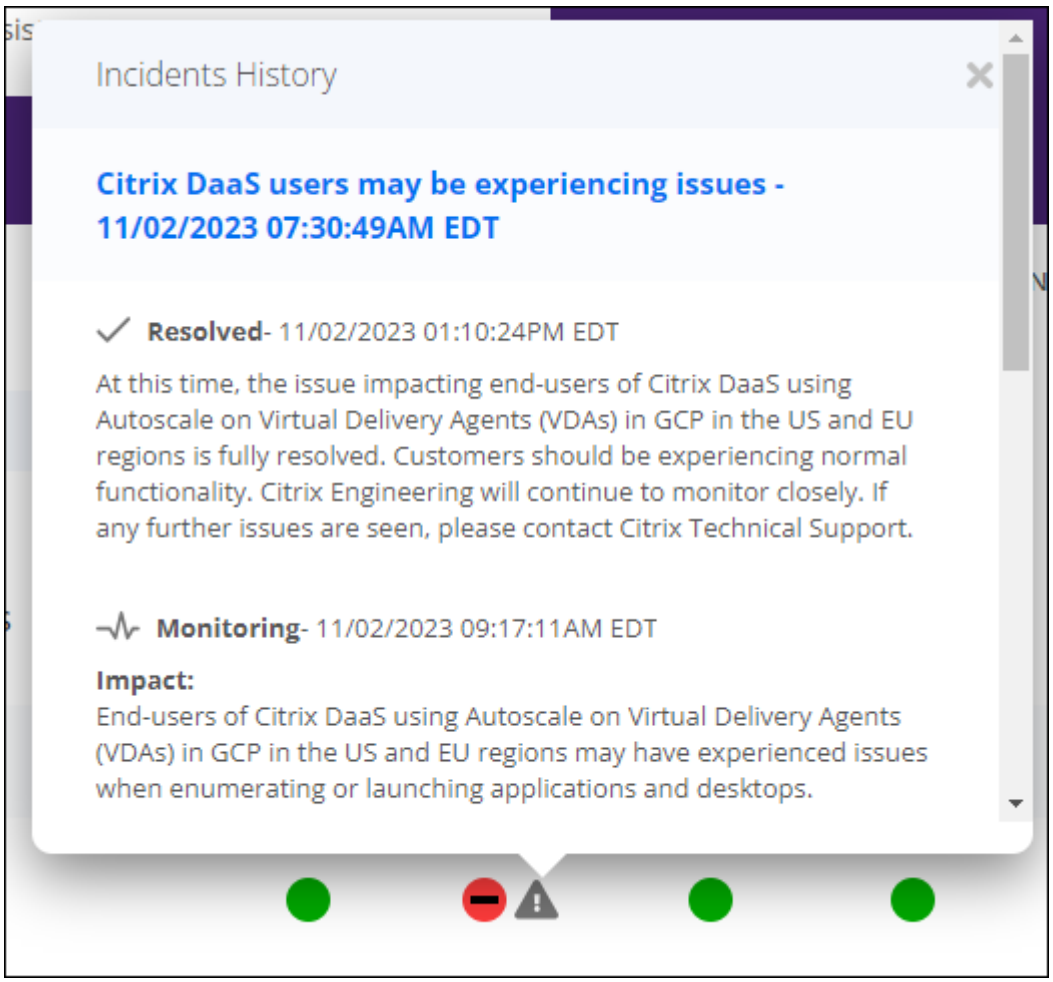
View service incident details

To view more detailed information about the service health incident for an affected service:

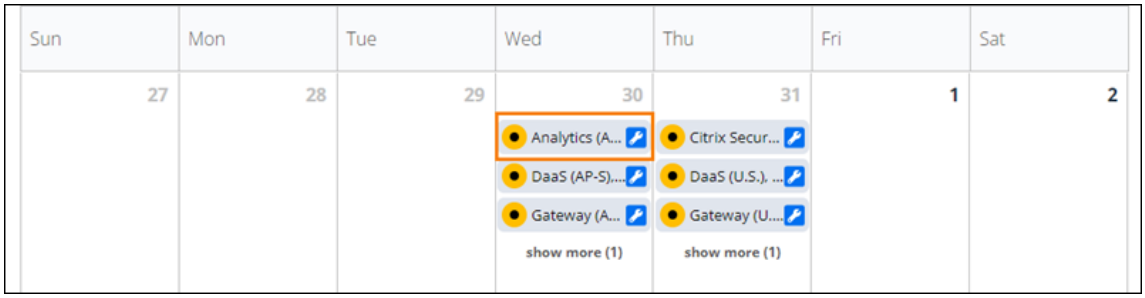
- From the History view, click the icon next to the service indicator to view more detailed infor-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

mation about the service health incident.



- From the Maintenance view, click the service entry to view the status page for the scheduled maintenance window.



Incident notification frequency

If a service health incident occurs, Citrix considers the following characteristics when posting to status.cloud.com:

- Duration of impact

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Frequency of impact

As the incident is being addressed, Citrix® posts the following types of notifications to the Cloud Health Dashboard:

- **Investigating:** This notification indicates that Citrix has identified the issue as urgent and is investigating the issue.
- **Monitoring:** This notification indicates that Citrix has identified the root cause and is mitigating the issue.
- **Resolved:** This notification indicates that Citrix has resolved the issue and the service is restored to a healthy state.

While investigating and monitoring an incident, Citrix posts updates at 60 to 120 minute intervals. These updates may include information such as:

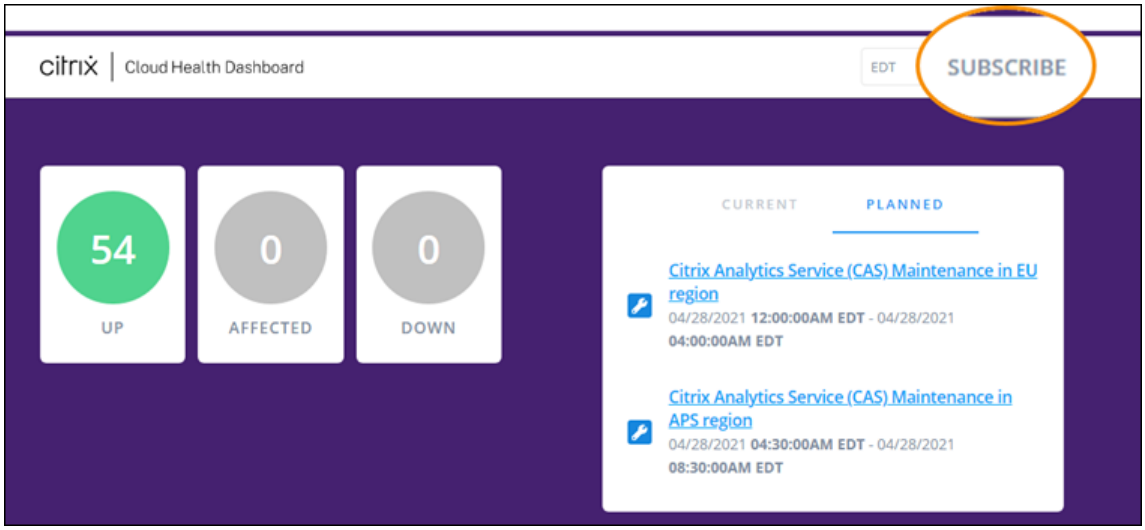
- Additional details about the incident.
- A description of the actions Citrix is taking to resolve the incident.
- An indication that no new changes occurred since the last update.

When an incident is resolved, Citrix posts a final update. This update might indicate the incident has been resolved and the service has been restored to a healthy state.

Subscribe to notifications

You can receive notifications about service health events using the following methods:

- Select **Subscribe** in the upper-right of the dashboard and select the notification method you want to use. You can select from several methods, including email and phone (as a text message).



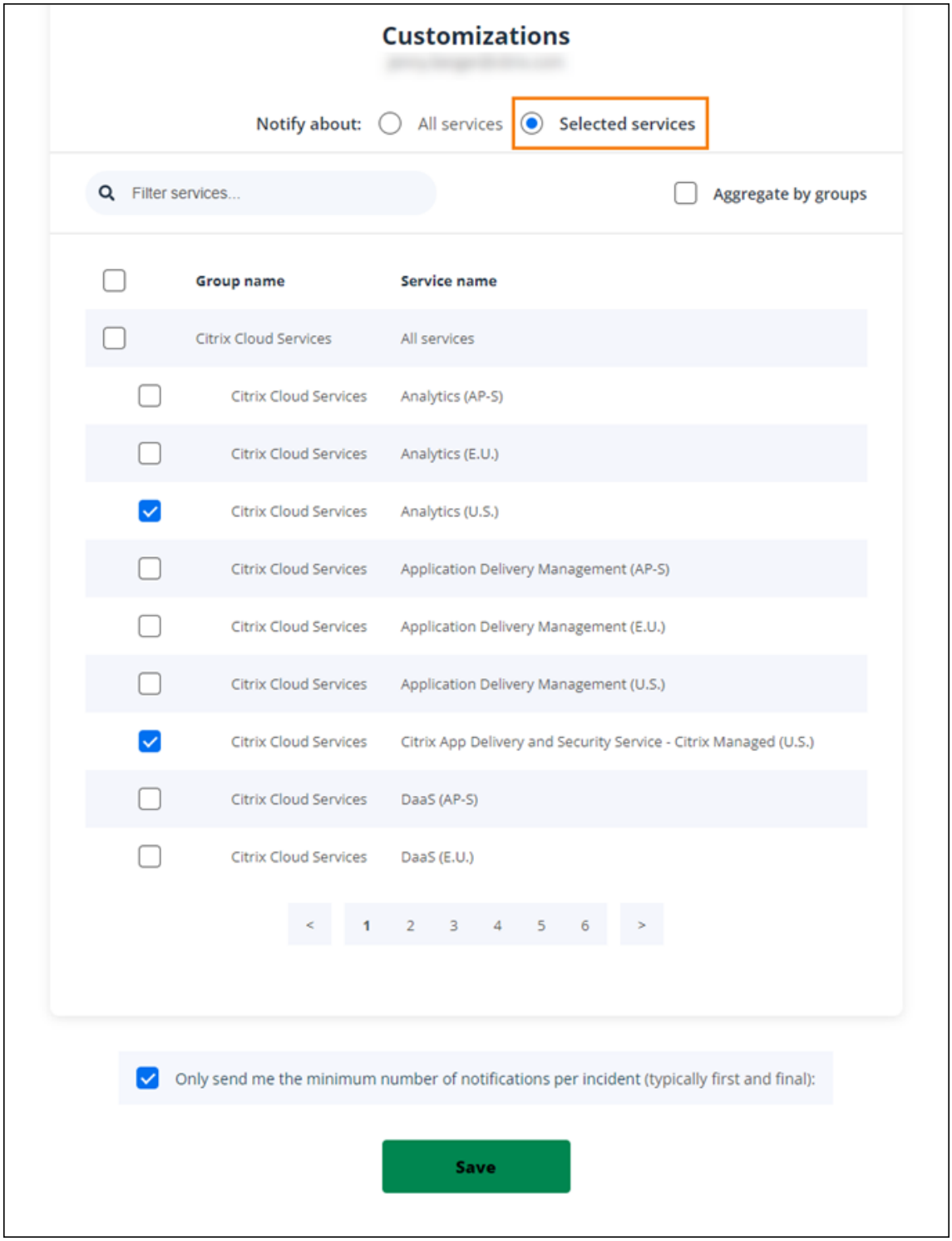
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Enter the following URLs in your RSS reader to subscribe to the Citrix Cloud Health RSS feed:
  - To receive service incident and maintenance notifications in a single feed, subscribe to `https://status.cloud.com/?format=atom`.
  - To receive only service incident notifications, subscribe to `https://status.cloud.com/atom/incidents`.
  - To receive only maintenance notifications, subscribe to `https://status.cloud.com/atom/maintenances`.

Subscribe to specific services in a region

1. Select **Subscribe** in the upper-right corner of the dashboard and then select the notification method you want to use.
2. Enter the contact details or URL for the chosen subscription method and select **I accept terms & services**. Select **Next**. The **Customizations** page appears with **Selected services** selected by default.
3. On the **Customizations** page, select the services in the regions that you want from the multi-page list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



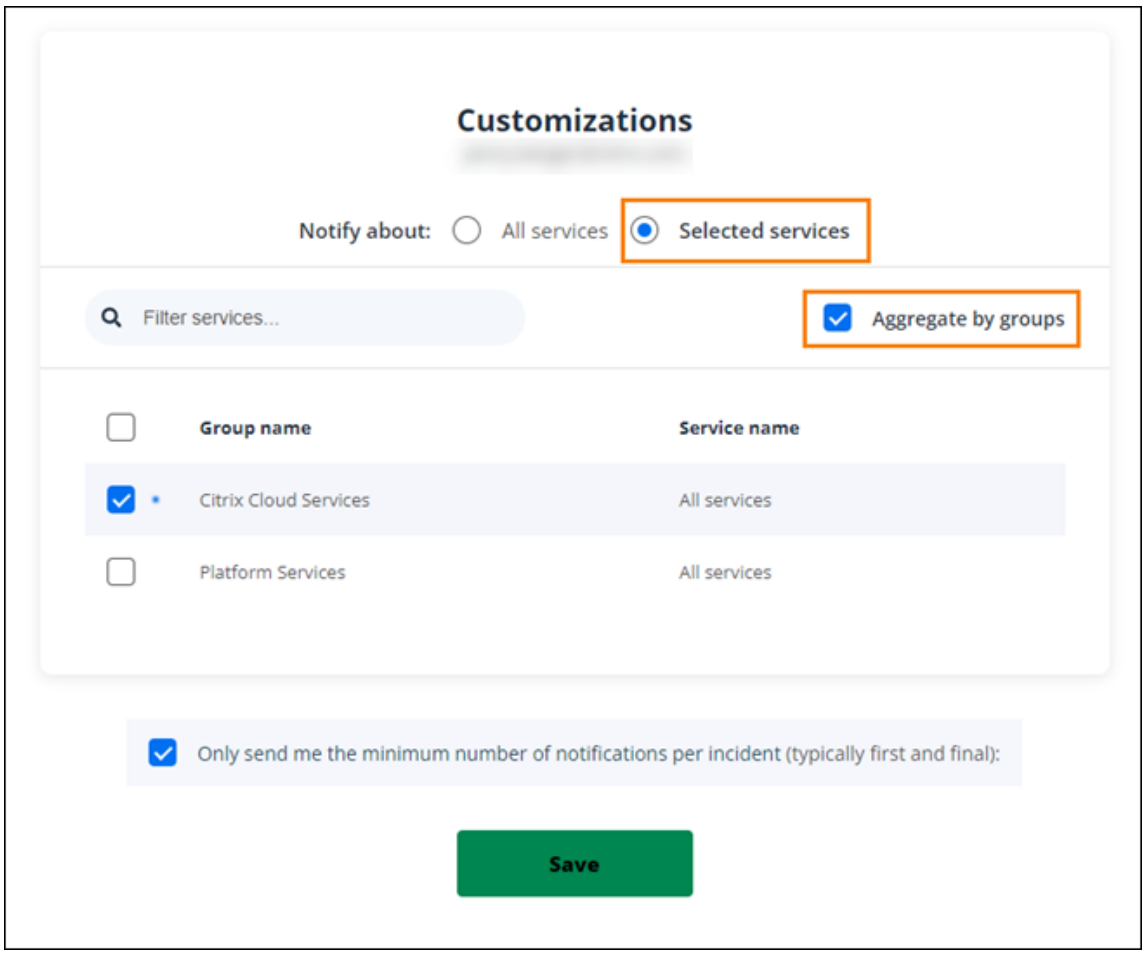
4. To receive only the first and last notifications for each incident, select **Only send me the minimum number of notifications per incident**.
5. Click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Subscribe to specific groups of services

You can subscribe to notifications for all cloud services (for example, Analytics and DaaS) or all platform services (for example, the control plane and cloud APIs) in all regions.

1. Select **Subscribe** in the upper-right corner of the dashboard and then select the notification method you want to use.
2. Enter the contact details or URL for the chosen subscription method and select **I accept terms & services**. Select **Next**. The **Customizations** page appears with **Selected services** selected by default.
3. On the **Customizations** page, select **Aggregate by groups**.
4. Select either **Citrix Cloud Services** or **Platform Services**.



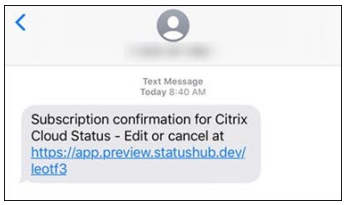
5. To receive only the first and last notifications for each incident, select **Only send me the minimum number of notifications per incident**.
6. Click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

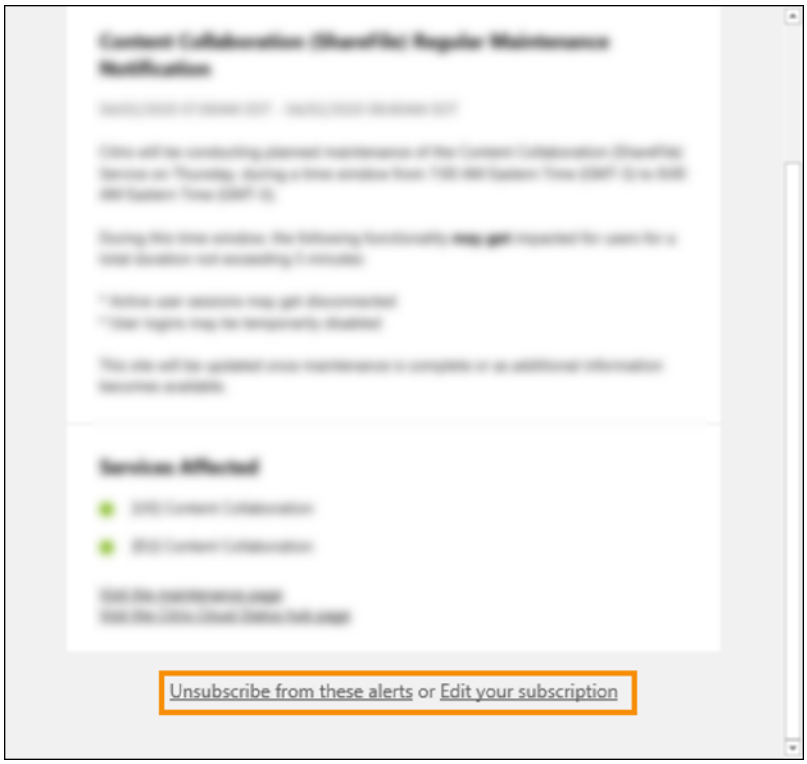
Unsubscribe from notifications

Depending on the subscription method, links to unsubscribe or change your subscription are included in the confirmation message you receive (for example, when subscribing to phone notifications) or in each notification message (for example, when you subscribe to email notifications). For example:

- Phone notification with subscription options:



- Notification email with subscription options



To unsubscribe from all notifications and remove all subscription methods:

1. Locate your subscription confirmation message or an existing notification and select the link to unsubscribe. Some subscription methods might provide a single link to edit or cancel your subscription.
2. Depending on your subscription method, use one of the following options on the **Edit Subscriptions** page:
    - Select **Remove all subscriptions**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Select **Unsubscribe**. From the **Unsubscribe methods** page, select **Remove all subscriptions**.

To unsubscribe from all notifications for a specific subscription method:

1. Locate your subscription confirmation message or an existing notification and select the link to unsubscribe. Some subscription methods might provide a single link to edit or cancel your subscription.
2. Depending on your subscription method, use one of the following options on the **Edit Subscriptions** page:
   - Select the subscription method you want to remove. Your subscription is removed immediately.
   - Select **Unsubscribe**. From the **Unsubscribe methods** page, select the subscription method you want to remove. Your subscription is removed immediately.

Change service notifications

1. Locate your subscription confirmation message or an existing notification and select the link to edit your subscription. Some subscription methods might provide a single link to edit or cancel your subscription.
2. From the **Edit Subscriptions page**, select the subscription method that you want to manage.
3. On the **Customizations** page, select the services you want to be notified about or clear the services you no longer want notifications for, as needed.
4. Select **Save**.

System and Connectivity Requirements

September 28, 2026

Citrix Cloud™ provides administrative functions (through a web browser) and operational requests (from other installed components) that connect to resources within your deployment. This article describes the system requirements, required contactable Internet addresses, and considerations for establishing connectivity between your resources and Citrix Cloud.

System requirements

Citrix Cloud requires the following minimum configuration:

- An Active Directory domain

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Two physical or virtual machines, joined to your domain, for the Citrix Cloud Connector. For more information, see Cloud Connector system requirements.
- Physical or virtual machines, joined to your domain, for hosting workloads and other components such as StoreFront. For more information about system requirements for specific services, refer to the Citrix® documentation for each service.

For information about scale and size requirements, see Scale and size considerations for Cloud Connectors.

Supported web browsers

- Latest version of Google Chrome
- Latest version of Mozilla Firefox
- Latest version of Microsoft Edge
- Latest version of Apple Safari

Transport Layer Security requirements

Citrix Cloud supports Transport Layer Security (TLS) 1.2 for TCP-based connections between components. Citrix Cloud doesn't allow communication over TLS 1.0 or TLS 1.1.

To access Citrix Cloud, you must use a browser that supports TLS 1.2 and have accepted cipher suites configured. For more information, see Encryption and key management.

Citrix Cloud management console

The Citrix Cloud management console is a web-based console that you can access after signing in at https://citrix.cloud.com. The web pages that make up the console might require other resources on the Internet, either when signing in or at a later point when carrying out specific operations.

Proxy configuration

If you're connecting through a proxy server, the management console operates using the same configuration applied to your web browser. The console operates within the user context, so any configuration of proxy servers that require user authentication should work as expected.

Firewall configuration

For the management console to operate, you must have port 443 open for outbound connections. You can test general connectivity by navigating within the console. For more information about required

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ports, see Inbound and outbound ports configuration.

Console notifications

The management console uses Pendo to display critical alerts, notifications about new features, and in-product guidance for some features and services.

To ensure you can view Pendo content within the management console, Citrix recommends that the following addresses are contactable:

- `https://citrix-cloud-content.customer.pendo.io/`
- `https://citrix-cloud-data.customer.pendo.io/`

If connectivity to Pendo services is restricted, in-product guidance, notifications, and related user experience features might be limited or unavailable. Pendo services are hosted in the United States (US), and data collected by Pendo is processed within this region. For more information, see Geographical Considerations.

> **Note:**
>
> Both URLs are required to fully enable messaging, including outage notices, new feature announcements, and customer feedback surveys.

Services that display Pendo content include:

- Citrix Cloud management console
- Citrix DaaS™ (including Workspace Environment Management™, Web Studio, and Session Recording)
- Citrix Studio (on-premises)
- Citrix Director and Monitor
- NetScaler (ADC)
- NetScaler Console (ADM) and NetScaler Console service
- Secure Developer Spaces
- Citrix® StoreFront Cloud (desktop, mobile, and tablet –cloud deployments only), including native iOS and Android applications

Pendo is a third-party sub-processor that Citrix uses to provide cloud and support services to Citrix customers. For a complete list of these sub-processors, see Sub-Processors for Citrix Cloud & Support Services and Citrix Affiliates.

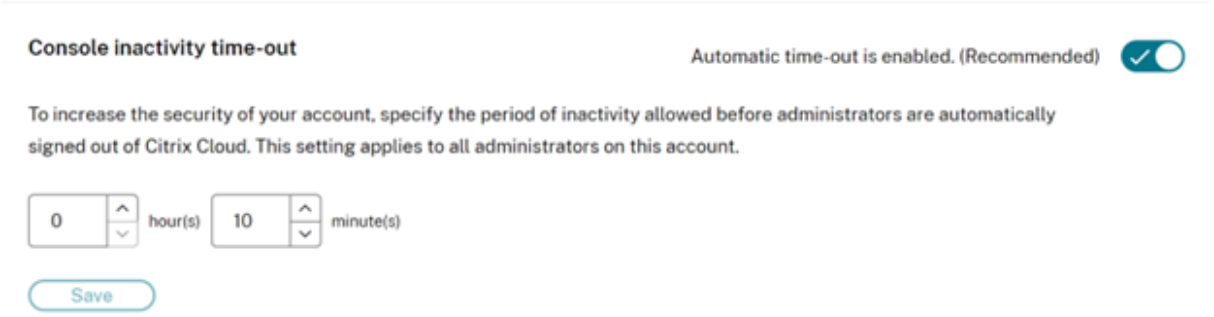
Session time-outs

After an administrator signs in to Citrix Cloud, the management console session times out after 72 hours have elapsed. This time-out occurs regardless of console activity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configurable inactivity timeout for console

As a full-access administrator, you can configure the duration of inactivity on the Citrix Cloud console before administrators are automatically signed out. Once configured, the specified timeout period will be applied to all administrators of the Citrix Cloud account.



When the feature is enabled, administrators will be logged out after the configured period of inactivity, and the session timeout will reset upon each subsequent login.

When the feature is disabled, there is no inactivity timer, and administrators will be logged out only when the 72-hour session limit is reached.

> **Note:**
>
> - By default this feature is disabled.
> - The configurable inactivity timeout is 10 minutes to 12 hours.
> - The default inactivity timeout is 60 minutes.

License Server connectivity to Citrix Cloud

If you are registering your on-premises Citrix License Server with Citrix Cloud to monitor usage of on-premises deployments, ensure that the following addresses are contactable:

- `https://trust.citrixnetworkapi.net` (for retrieving a code)
- `https://trust.citrixworkspacesapi.net/` (for confirming the license server is registered)
- `https://cis.citrix.com` (for data upload)
- `https://core.citrixworkspacesapi.net`
- `ocsp.digicert.com port 80`
- `crl3.digicert.com port 80`
- `crl4.digicert.com port 80`
- `ocsp.entrust.net port 80`
- `crl.entrust.net port 80`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If you are using a proxy server with Citrix License Server, ensure that the proxy server is configured as described in Configure a proxy server in the Licensing product documentation.

Citrix Cloud Connector™

The Citrix Cloud Connector is a software package that deploys a set of services that run on Microsoft Windows servers. The machine hosting the Cloud Connector resides within the network where the resources that you use with Citrix Cloud reside. The Cloud Connector connects to Citrix Cloud, allowing it to operate and manage your resources as needed.

For requirements for installing the Cloud Connector, see System requirements. To operate, the Cloud Connector requires outbound connectivity on port 443. After installation, the Cloud Connector might have additional access requirements depending on the Citrix Cloud service with which it is being used.

The machine hosting the Cloud Connector must have stable network connectivity with Citrix Cloud. Networking components must support HTTPS and long-lived secure web sockets. If a timeout is configured in the networking components, it must be greater than 2 minutes.

For help with troubleshooting connectivity between the Cloud Connector and Citrix Cloud, use the Cloud Connector Advanced Connectivity Checks

Cloud Connector common service connectivity requirements

Connecting to the Internet from your data centers requires opening port 443 to outbound connections. However, to operate within environments containing an Internet proxy server or firewall restrictions, further configuration might be needed. For more information, see Cloud Connector Proxy and Firewall Configuration.

The addresses for each service in this article must be contactable to properly operate and consume the service. The following list includes the addresses that are common to most Citrix Cloud services:

- `https://*.citrixworkspacesapi.net` (provides access to Citrix Cloud APIs that the services use)
- `https://*.cloud.com` (provides access to the Citrix Cloud sign-in interface)
- `https://*.blob.core.windows.net` (provides access to Azure Blob Storage, which stores updates for Citrix Cloud Connector)
- `https://*.servicebus.windows.net` (provides access to Azure Service Bus, which is used for logging and the Active Directory agent)

These addresses are provided only as domain names because Citrix Cloud services are dynamic and their IP addresses are subject to routine changes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

As a best practice, use Group Policy to configure and manage these addresses. Also, configure only the addresses that are applicable to the services that you and your end-users are consuming.

If you are using Citrix Cloud with Citrix License Server to register your on-premises products, see License Server connectivity to Citrix Cloud in this article for additional required contactable addresses.

Allowed FQDNs for Cloud Connector

To help you ensure that all the required fully qualified domain names (FQDNs) are allowed through your firewall, Citrix provides the following resources:

- Connector allowlist API
- Citrix Gateway Service –Points of Presence (PoPs)

When configuring your firewall, consult both of these resources to verify that the FQDNs that your service deployment requires are allowed.

Local Host Cache (High Availability Service) When using Local Host Cache (LHC) in Connectors, ensure that the Connectors can reach the election endpoint of every other connector in the resource location. The election endpoint is on port 80 and can be accessed through the following URL: `http://<FQDN_OR_IP_OF_PEER_CONNECTOR>/Citrix/CdsController/ISecondaryBrokerElection`.

If Connectors are unable to communicate at this address, multiple brokers are elected during an LHC event, which can result in intermittent virtual app and desktop launch failures. For more information, see Resource Locations with Multiple Cloud Connectors.

Adaptive Authentication When using the Cloud Connector for connectivity to an Adaptive Authentication service, you must allow your Citrix Cloud Connector to access the domain or URL you've reserved for the Adaptive Authentication instance. For example, allow `https://aauth.xyz.com`. For more information, see Adaptive Authentication.

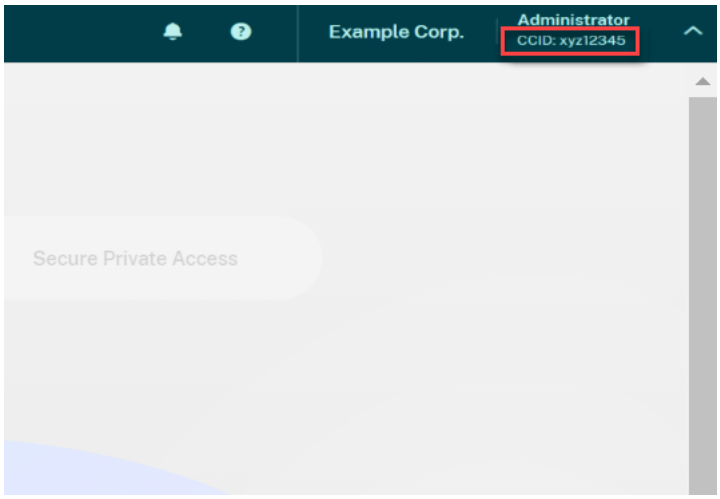
Connector allowlist API Where possible, use the wildcard addresses in the Cloud Connector common service connectivity requirements section. If your environment does not allow wildcards, use the Connector allowlist API to retrieve the current list of required FQDNs.

Retrieve the list from: `https://api.cloud.com/connectivity/v2/allowlist?customerId=<CUSTOMER_ID>`

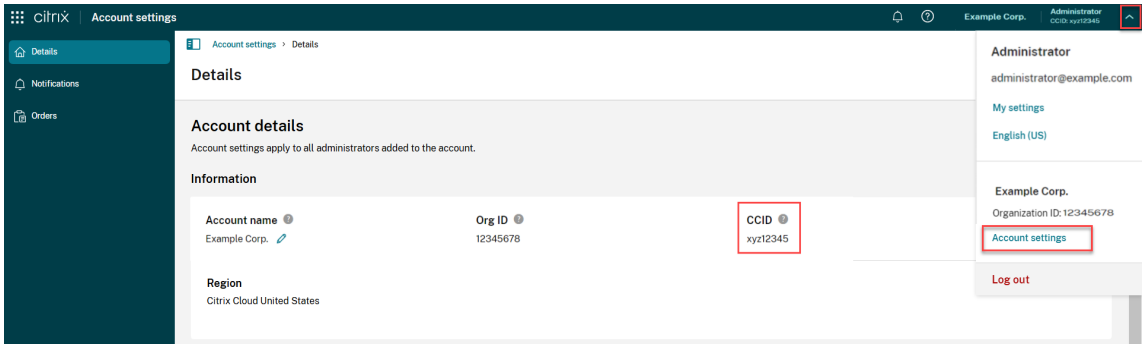
Replace `<CUSTOMER_ID>` with your Citrix Cloud Customer ID (CCID). You can find your CCID in the following locations in the Citrix Cloud console:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Top right of the console, below the customer name.



- On the Account Settings page, under **Citrix Cloud Customer ID (CCID)**.



Query parameters Add query parameters to the endpoint by separating each name-value pair with &. For example, to retrieve the outbound FQDNs for the EU geography, use the following URL:

```
https://api.cloud.com/connectivity/v2/allowlist?customerId=<CCUSTOMER_ID>&direction=outbound&geo=EU
```

The v2 API supports the following query parameters:

- **CustomerId:** your Citrix Cloud Customer ID (CCID). When you pass customerId, the API substitutes <CUSTOMER_ID> placeholders in returned FQDNs (for example, <CUSTOMER_ID>.xendesktop.net becomes abc123.xendesktop.net) before returning the list. You no longer need to substitute your CCID manually in each entry after downloading the file, as you did with the previous allowlist.json file.
- **Format:** Choose between `json` (default) or `zscaler`. If omitted, the response is returned as json(default). Set format=zscaler to receive the response pre-formatted for import into a Zscaler configuration.
- **Geo:** if omitted, defaults to `all` and returns FQDNs for every Citrix Cloud geography. To scope the response to a single geography your resource locations serve, set `geo` to one of `us`, `eu`, or

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`ap-s`. Scoping produces a shorter, more targeted list and avoids allowlisting regions that your deployment does not reach.

- **Direction:** if omitted, defaults to `all` and returns both inbound and outbound FQDNs. Set `direction=outbound` to retrieve only the FQDNs the Cloud Connector needs to reach (the typical firewall egress use case), or `direction=inbound` for the FQDNs from which Citrix Cloud contacts your environment.

> **Note:**
>
> The previous allowlist file at `https://fqdnallowlistsa.blob.core.windows.net/fqdnallowlist-commercial/allowlist.json` remains available for a limited transition period but is deprecated for customer use. Migrate to the API endpoint above. The blob URL is retained temporarily only for internal Connector connectivity checks and will be removed in a future release.
>
> The v2 API endpoint is currently available for Citrix Cloud commercial customers.

Gateway Service Points of Presence Some of the FQDNs included in the allowlist.json file are also included in Citrix Gateway Service –Points of Presence (PoPs). However, Citrix Gateway Service – Points of Presence (PoPs) also includes FQDNs that clients access, such as the following:

- global-s.g.nssvc.net
- azure-s.g.nssvc.net

Certificate validation

Cloud Connector binaries and endpoints that the Cloud Connector contacts are protected by X.509 certificates that are verified when the software is installed. To validate these certificates, each Cloud Connector machine must meet certain requirements. For a full list of these requirements, see Certificate validation requirements.

SSL Decryption

Enabling SSL decryption on certain proxies might prevent the Cloud Connector from connecting successfully to Citrix Cloud. For more information about resolving this issue, see CTX221535.

Citrix Connector™ Appliance for Cloud Services

The Connector Appliance is an appliance that you can deploy in your hypervisor. The hypervisor hosting the Connector Appliance resides within the network where the resources that you use with Citrix

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cloud reside. The Connector Appliance connects to Citrix Cloud, allowing it to operate and manage your resources as needed.

For requirements for installing the Connector Appliance, see System requirements.

To operate, the Connector Appliance requires outbound connectivity on port 443. However, to operate within environments containing an Internet proxy server or firewall restrictions, further configuration might be needed.

To properly operate and consume the Citrix Cloud services, the following addresses must be contactable:

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.citrixnetworkapi.net`
- `https://*.*.nssvc.net`

  Customers who can't enable all sub-domains can use the following addresses instead

  - `https://*.g.nssvc.net`
  - `https://*.c.nssvc.net`
- `https://*.servicebus.windows.net`
- `https://ctxccopspacrconnappprod.azurecr.io`
- `https://ctxccopspacrconnappprod.eastus.data.azurecr.io`

Network requirements

Ensure that your Connector Appliance environment has the following configuration:

- Either the network allows the Connector Appliance to use DHCP to get DNS and NTP servers, an IP address, a host name, and a domain name or you can manually set the network settings in the Connector Appliance console.
- The network is not configured to use the link-local IP ranges 169.254.0.1/24, 169.254.64.0/18 or 169.254.192.0/18, which are used internally by the Connector Appliance.
- Either the hypervisor clock is set to Coordinated Universal Time (UTC) and is synchronized with a time server or DHCP provides NTP server information to the Connector Appliance.
- If you use a proxy with Connector Appliance, the proxy must be unauthenticated or use basic authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Analytics service connectivity

- For in-product messages including new features and critical communications and customer surveys, the following addresses must be contactable:
  - `https://citrix-cloud-content.customer.pendo.io/`
  - `https://citrix-cloud-data.customer.pendo.io/`
- Additional requirements: Prerequisites

For more information about onboarding data sources to the service, see Supported data sources.

NetScaler® Console service connectivity

For complete Internet connectivity requirements, see Supported ports in the NetScaler product documentation.

Citrix DaaS connectivity

Cloud Connectors connectivity to DaaS

In addition to the Cloud Connector common service connectivity requirements, when used with DaaS, Cloud Connectors require connectivity to the following:

- `https://[customerid].xendesktop.net`, where `[customerid]` is the customer ID parameter displayed on the **Service principals** tab (**Identity and access management > API access > Service principals**) of the Citrix Cloud management console.
- Customers using Quick Deploy to install Citrix DaaS need to make these additional addresses contactable:
  - `https://*.apps.cloud.com`
  - The `AzureCloud` service tag
- `https://*.*.nssvc.net`
  - Customers who can't enable all subdomains can use the following addresses instead:
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`

For an overview of how the Cloud Connector communicates with the service, refer to the Citrix DaaS diagram on the Citrix Tech Zone website.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connectivity to DaaS Administration console

To administer DaaS, in addition to the Citrix Cloud Management Console you must be able to connect to the following:

- `https://*.citrixworkspacesapi.net` (Not required for Rendezvous protocol)
- `https://*.citrixnetworkapi.net` (Not required for Rendezvous protocol)
- `https://*.cloud.com` (Not required for Rendezvous protocol)
- `https://[customerid].xendesktop.net`, where `[customerid]` is the customer ID parameter displayed on the **Service principals** tab (**Identity and access management > API access > Service principals**) of the Citrix Cloud management console.
- `https://*.*.nssvc.net` (Not required for Citrix DaaS Standard for Azure)
  - Customers who can't enable all sub-domains can use the following addresses instead:
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`
- For in-product messages including new features and critical communications and customer surveys, the following addresses must be contactable:
  - `https://citrix-cloud-content.customer.pendo.io/`
  - `https://citrix-cloud-data.customer.pendo.io/`

Citrix DaaS Remote PowerShell SDK

To use the Citrix DaaS Remote PowerShell SDK, whitelist the following URLs:

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net/[customerid]`
- `https://[customerid].xendesktop.net:443`

VDAs connectivity when using Rendezvous protocol

When using the Citrix Gateway Service, the Rendezvous protocol allows VDAs to bypass the Citrix Cloud Connectors to connect directly and securely with the Citrix Cloud control plane.

Regardless of the protocol version you're using, VDAs must be able to contact the addresses for the administration console listed above, unless otherwise noted. For a complete list of the requirements for the Rendezvous protocol, refer to the following sections of the Citrix DaaS product documentation:

- Rendezvous V1
- Rendezvous V2

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Local Host Cache requirement

If your firewall performs packet inspection and you want to use the Local Host Cache feature, ensure that your firewall accepts XML and SOAP traffic. This feature requires the ability to download MDF files, which occurs when the Cloud Connector synchronizes configuration data with Citrix Cloud. These files are delivered to the Cloud Connector through XML and SOAP traffic. If the firewall blocks this traffic, the synchronization between the Cloud Connector and Citrix Cloud fails. If an outage occurs, users can't continue working because the configuration data residing on the Cloud Connector is out-of-date.

For more information about this feature, see Local Host Cache in the Citrix DaaS product documentation.

VDA upgrade requirement

Using the Full Configuration interface of Citrix DaaS, you can upgrade VDAs on a per-catalog or a per-machine basis. You can upgrade them immediately or at a scheduled time. For more information about the VDA upgrade feature, see Upgrade VDAs using the Full Configuration interface.

When using the feature, make sure that you meet the following connectivity requirements:

- The following Azure CDN URLs have been added to the allow list. The feature downloads the VDA installers from the Azure CDN endpoints.
  - Production - United States (US): `https://prod-us-vus-storage-endpoint.azureedge.net/*`
  - Production - European Union (EU): `https://prod-eu-vus-storage-endpoint.azureedge.net/*`
  - Production - Asia Pacific South (APS): `https://prod-aps-vus-storage-endpoint.azureedge.net/*`
  - Production - Japan (JP): `https://prod-jp-vus-storage-endpoint.azureedge.net/*`
- The feature verifies that the VDA installer is signed by a valid certificate. Make sure that the following URLs have been added to the allow list for certificate validity and revocation check:
  - `http://crl3.digicert.com/*`
  - `http://crl4.digicert.com/*`
  - `http://ocsp.digicert.com/*`
  - `http://cacerts.digicert.com/*`
- The feature requires VDA Upgrade Agent to work. The VDA Upgrade Agent running on the VDA communicates with Citrix DaaS. Make sure that the following URLs have been added to the allow list:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `https://[customerId].xendesktop.net/citrix/VdaUpdateService/*`, where `[customerid]` is the customer ID parameter displayed on the **Service principals** tab (**Identity and access management > API access > Service principals**) of the Citrix Cloud management console.
- `http://xendesktop.net/citrix/VdaUpdateService/*`

Endpoint Management service connectivity

Citrix resource location / Cloud Connector:

- Cloud Connector common service connectivity requirements
- Additional requirements: /en-us/citrix-endpoint-management/endpoint-management.html

Administration console:

- `https://*.citrix.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.cloud.com`
- `https://*.blob.core.windows.net`
- Additional requirements: /en-us/citrix-endpoint-management/endpoint-management.html

Citrix Gateway service connectivity

Cloud Connectors connectivity to Citrix Gateway Service

When using Citrix Gateway Service via Cloud connectors (i.e. without Rendezvous v2), in addition to Cloud Connector common service connectivity requirements, Cloud Connectors need access to:

- `https://*.*.nssvc.net`

Customers who can't enable all subdomains can use the following addresses instead:

- `https://*.g.nssvc.net`
- `https://*.c.nssvc.net`

> **Important:**
>
> SSL interception cannot be performed on Citrix Gateway addresses. Enabling SSL interception on certain proxies might prevent the Cloud Connector from connecting successfully to Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Client connectivity to Citrix Gateway Service

To use Citrix Gateway Service, client devices need access to:

- https://*.*.nssvc.net

Customers who can't enable all subdomains can use the following addresses instead:

- https://*.g.nssvc.net
- https://*.c.nssvc.net

SD-WAN Orchestrator service connectivity

For complete Internet connectivity requirements, see Prerequisites for Citrix SD-WAN Orchestrator service usage.

Remote Browser Isolation (formerly Secure Browser) service

Cloud Connector connectivity to Remote Browser Isolation service

Cloud Connectors do not need any additional connectivity beyond Cloud Connector common service connectivity requirements.

Connectivity to Administration console

- https://*.cloud.com
- https://*.citrixworkspacesapi.net
- https://browser-release-a.azureedge.net
- https://browser-release-b.azureedge.net

Client connectivity to Citrix Secure Private Access™

- https://*.netscalergateway.net
- https://*.*.nssvc.net
    - Customers who can't enable all subdomains can use the following addresses instead:
        - https://*.g.nssvc.net
        - https://*.c.nssvc.net

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Client connectivity to Global App Configuration service

`https://discovery.cem.cloud.us`

For more information about this service, see Customize Workspace app settings.

End user connectivity to stores

This section lists URLs that clients must be able to reach when accessing their cloud stores using Citrix Workspace app or a web browser.

Store URL

Users access the store through either a cloud URL, e.g. `https://<customername>.cloud.com`, or a custom URL. For more information, see Configure access to stores.

Authentication

Citrix Cloud:

- `https://accounts.cloud.com`
- `https://accounts-dsauthweb.cloud.com`
- `https://accounts-webassets.cloud.com` - for graphical interface assets
- `https://login.cloud.com` - only required if you are using Active Directory or Active Directory + Token as your identity provider

Citrix Cloud Japan:

- `https://accounts.citrixcloud.jp`
- `https://accounts-dsauthweb.citrixcloud.jp`
- `https://accounts-webassets.citrixcloud.jp` - for graphical interface assets
- `https://login.citrixcloud.jp` - only required if you are using Active Directory or Active Directory + Token as your identity provider

Citrix Cloud Government:

- `https://accounts.cloud.us`
- `https://accounts-dsauthweb.cloud.us`
- `https://login.cloud.us` - only required if you are using Active Directory or Active Directory + Token as your identity provider

© 1997–2026 Citrix Systems, Inc. All rights reserved.

https://accounts-webassets.cloud.us is not required for Citrix Cloud Government. https://accounts.cloud.us is used for graphical interface assets.

If you are using a third party identity provider, contact the vendor for required URLs.

Store graphical interface assets

- https://ctx-ws-assets.cloud.com

For Citrix Cloud Government, this may change in the future to https://ctx-ws-assets.cloud.us.

Personalization, notifications, and feature rollout

When using Citrix Workspace app, but not a web browser, the following URLs are required according to your organization's region.

US:

- https://customer-interface-personalization.us.wsp.cloud.com
- https://user-personalization.us.wsp.cloud.com
- https://admin-notification.us.wsp.cloud.com
- https://feature-rollout.us.wsp.cloud.com

EU:

- https://customer-interface-personalization.eu.wsp.cloud.com
- https://user-personalization.eu.wsp.cloud.com
- https://admin-notification.eu.wsp.cloud.com
- https://feature-rollout.eu.wsp.cloud.com

Asia Pacific South:

- https://customer-interface-personalization.ap-s.wsp.cloud.com
- https://user-personalization.ap-s.wsp.cloud.com
- https://admin-notification.ap-s.wsp.cloud.com
- https://feature-rollout.ap-s.wsp.cloud.com

Citrix Cloud Japan:

- https://customer-interface-personalization.jp.wsp.citrixcloud.jp
- https://user-personalization.jp.wsp.citrixcloud.jp
- https://admin-notification.jp.wsp.citrixcloud.jp
- https://feature-rollout.jp.wsp.citrixcloud.jp

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Cloud Government:

- https://customer-interface-personalization.us.wsp.cloud.us
- https://user-personalization.us.wsp.cloud.us
- https://admin-notification.us.wsp.cloud.us
- https://feature-rollout.us.wsp.cloud.us

Branding images

- US: https://cips-iws-prod-eus2-cip-cdn.azureedge.net
- EU: https://cips-iws-prod-weu-cip-cdn.azureedge.net
- AP-S https://cips-iws-prod-aue-cip-cdn.azureedge.net
- Citrix Cloud Japan https://cips-wspjp-prod-jpe-cip-cdn.azureedge.net
- Citrix Cloud Government https://cips-wspgov-prod-usgv-cip-cdn.azureedge.us

Profile pictures

If users upload profile pictures, access is required to the following URLs:

- US: https://wups-us-iws-cloud.azureedge.net
- EU: https://wups-eu-iws-cloud.azureedge.net
- AP-S: https://wups-ap-s-iws-cloud.azureedge.net
- Citrix Cloud Japan: https://wups-wspjp-jp-production.azureedge.net

Application Icons

Citrix Cloud:

- https://wscs-cdn.wsp.cloud.com/icons

Citrix Cloud Japan:

- https://wscs-cdn.wsp.citrixcloud.jp/icons

Citrix Cloud Government:

- https://wscs-cdn.wsp.cloud.us/icons

Pendo

For in-product messages including new features and critical communications.

- https://citrix-cloud-content.customer.pendo.io

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Analytics Service

- `locus.analytics.cloud.com`

Enable access to the appropriate URL from the following list, depending on the tenant's GEO:

- US: `citrixanalyticseh.servicebus.windows.net`
- EU: `citrixanalyticseheu.servicebus.windows.net`
- APS: `citrixanalyticsehaps.servicebus.windows.net`

Other Services

For other services that the client may need to connect to, see:

- Client connectivity to Citrix Gateway Service
- Client connectivity to Citrix Secure Private Access service
- Client connectivity to Global App Configuration service

Citrix Federated Authentication Service (FAS)

See Connections between Citrix Federated Authentication Service and Citrix Cloud.

Workspace Environment Management™ service connectivity

Citrix resource location / Cloud Connector / Agent:

`https://*.wem.cloud.com`

For complete requirements, see Connectivity prerequisites in the Workspace Environment Management service documentation.

Plan your deployment

September 6, 2025

This article outlines key considerations for planning your Citrix Cloud™ deployment. It provides an overview of service trials, cloud subscriptions, regions, and resources for deployment and migration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service trials and subscriptions

Citrix Cloud offers trials for most cloud services. Trials have the same features and functions as paid services, so they're suitable for a proof-of-concept or pilot deployment. For more information, see Citrix Cloud Service Trials.

In general, paid service entitlements can have a monthly, annual, or termed duration. As the entitlement nears its end, Citrix Cloud sends reminders so you can renew your entitlement without undue service interruptions. For more information about renewing your entitlements, see Extend Citrix Cloud service subscriptions.

Regions and service presence

Citrix Cloud provides services in three regions: United States, European Union, and Asia Pacific South. When you sign up for Citrix Cloud, you must choose the region that best suits your performance and business needs.

To learn more about selecting a region and the services that are available in each region, see Geographical Considerations.

Deployment resources

- Citrix Cloud Resiliency
- Tech Zone Proof of Concept guides
- Tech Zone Reference Architectures
- Scale and size considerations for Cloud Connectors
- Scale and size considerations for Local Host Cache
- On-premises StoreFront Authentication Reference Architectures for Citrix DaaS

Migration resources

- Proof of Concept: Automated Configuration Tool
- Migrating Citrix Virtual Apps and Desktops on-premises to Citrix Cloud
- Migrating Citrix Virtual Apps and Desktops from VMware vSphere to Citrix DaaS on Microsoft Azure
- Migration from Android Device Administrator to Android Enterprise with Citrix Endpoint Management

© 1997–2026 Citrix Systems, Inc. All rights reserved.

More information

- Citrix Discussions: Citrix Cloud: Community support forums for Citrix Cloud and Citrix cloud services
- Citrix Training:
  - Fundamentals of Citrix Cloud
  - Introduction to Citrix Identity and Authentication

Citrix Cloud™ Service Trials

June 22, 2026

Trials for individual Citrix Cloud services are delivered through the Citrix Cloud management console. The functionality in a service trial is the same as the purchased service, so they're suitable for a proof-of-concept (POC) or pilot deployment.

When you're ready to buy Citrix Cloud services, your trial is converted to a production service. There's no need to reconfigure anything or create a separate production account.

Service trial overview

The information in this section applies to most Citrix Cloud service trials. Services with different trial terms are described in separate sections.

		Citrix Cloud Trial
	Number of end users allowed	25
	Maximum length of trial	60 calendar days
	Data retention period	90 calendar days after trial expiration
	Availability	Restricted availability
	Resource location	Customer provided and configured
	User session length	Unlimited
	Local Microsoft Active Directory integration	Yes
	Choice of resource locations	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

		Citrix Cloud Trial
	Deploy to on-premises	Yes
	Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service)	Full feature set
	Endpoint Management	Full feature set
	Customizable	Yes

Requesting a service trial

Citrix Cloud trial access is managed on a per-service basis. For some services, you can request a trial as described in Request a service trial in this article. For other services, you must request a demo before you receive trial access, as described in Request a service demo in this article.

Service trial period

For most services, you have 60 days to try out the service after your trial request is approved. You can request a trial for a service only once.

Purchasing service subscriptions

You can buy a service subscription at any time during your trial or during the data retention period. For more information, see Buy Citrix Cloud services.

After you buy a subscription, your trial is converted to a production service. Administrators and users can access the service and any data that you added during the trial remains intact.

Citrix DaaS Standard for Azure

This section describes the following types of trials for Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure):

- **Auto-approved trial:** After you request the trial through the Citrix Cloud management console, the trial is approved automatically and ready to use.
- **Sales-approved trial:** After you contact a Citrix® sales representative to request a trial, the sales representative approves the trial. After approval, the trial is ready to use.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

		Auto-approved trial	Sales-approved trial
	Maximum length of trial	7 calendar days	14 calendar days
	Data retention period	30 calendar days after trial expiration	90 calendar days after trial expiration

Depending on the trial type, you have seven or 14 days to use the service. You can request a trial for the service only once.

Depending on the trial type, Citrix retains any data that you add to the service for 30 days or 90 days after the trial expires. If you buy a subscription to the service during this retention period, administrators and users can access the service with your data intact.

You can buy a subscription to the service through the Azure Marketplace or by contacting your Citrix sales representative.

Request a service demo

For some services, you must request a demo from a Citrix sales representative before you can try out the service. Requesting a demo allows you to discuss your organization's cloud service needs with a Citrix sales representative. Also, the sales representative ensures you have all the information needed to use the service successfully.

1. Sign in to your Citrix Cloud account.
2. From the management console, select **Request Demo** for the service that you want. The service's demo request page appears.
3. Complete and submit the form. A Citrix sales representative contacts you to provide more information and walk you through using the service.

Request a service trial

1. Sign in to your Citrix Cloud account.
2. From the management console, select **Request Trial** for the service that you want to try out.

When your trial is approved and ready to use, Citrix sends you an email notification.

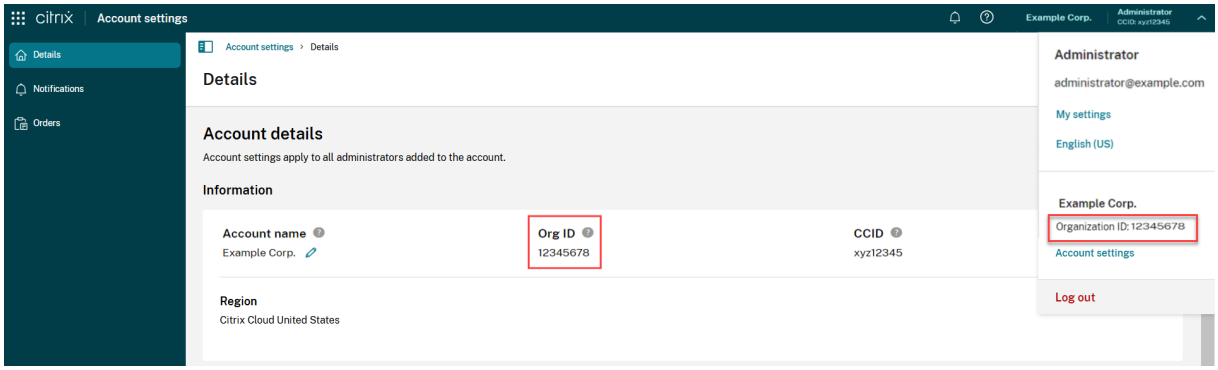
> **Note:**
>
> To provide the best customer experience, Citrix reserves the right to approve trials for a limited number of participants at any given time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Buy Citrix Cloud services

When you're ready to convert your trial to a production service, visit https://www.citrix.com/buy/ to find a local Citrix partner.

To buy the service, you need your Organization ID (OrgID). Your OrgID appears on the customer menu in the top-right corner of the Citrix Cloud management console. Your OrgID also appears on the **Account Settings** page.



More information

- Terms of Service for Citrix Cloud services
- The Fundamentals of Citrix Cloud course includes a short video that walks you through requesting a trial. The full course also covers the components of the Citrix Cloud platform and its services.

Extend Citrix Cloud™ service subscriptions

January 20, 2026

This article describes how purchased subscriptions for Citrix Cloud services expire and how you can extend your subscription.

In this article, *monthly subscriptions* refer to services that are purchased on a month-to-month basis. *Annual subscriptions* refer to services that are purchased on a yearly basis. *Multiannual subscriptions* refer to services that are purchased on a multi-yearly basis.

> **Note:**
>
> Citrix Service Providers (CSPs) can extend their subscriptions by submitting a zero-dollar purchase order to their CSP distributor. For more information about CSP product renewals and li-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> censing, refer to the *Citrix Service Provider Licensing Guide for Citrix Cloud*, available through the Citrix Partner Central web site.

Before expiration

For monthly subscriptions, Citrix Cloud does not send notifications prior to expiration.

For annual and multiannual subscriptions, Citrix Cloud notifies you at certain intervals when your existing subscription approaches expiration. These notifications alert you to extend the subscription and avoid service interruption. The following notifications appear in the Citrix Cloud management console:

- 90 days before expiration: A yellow banner appears, showing the services that need to be extended and their expiration dates. This notification appears in the console every seven days or until the service is extended.
- Seven days before expiration: A red banner appears, showing the services that need to be extended and their expiration dates. This notification appears in the console until the service is extended.

You can dismiss these notifications when they appear; however, they will reappear after seven days.

Citrix® also sends you an email notification that includes a list of the services that need to be extended and their expiration dates. Citrix sends this notification at the following intervals:

- 90 days before expiration
- 60 days before expiration
- 30 days before expiration
- Seven days before expiration
- One day before expiration

Additional warnings appear in the management console and for end users to alert them of the expiration status. These messages are triggered when all licenses in the subscription have expired (typically after the 12-month term is complete).

- Administrator warnings: Starting 30 days before the subscription expires, warnings appear within the Studio console alerting administrators of the upcoming expiration.
- End user warnings: After the subscription has expired, end users receive a warning message upon launching a session.
    - Message text: "Citrix Virtual Apps and Desktops warning: Your corporate Citrix environment is currently unsupported. Please contact your IT department to resolve."

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After expiration: Service block and data retention

- Access to Citrix Cloud services is suspended immediately upon contract expiration.
- To reinstate the services, customers must contact their dedicated Citrix representative or account team to initiate the renewal process.

Customer-managed Azure subscriptions

If you are using your own Azure subscription with a Citrix Cloud service, the service installs an app when you connect your Azure subscription to the service. If you don't extend your Citrix Cloud service subscription, Citrix does not remove this app from your Azure subscription after the 90-day retention period ends. You must delete this app to remove the service completely from your Azure subscription. You can delete the app using one of the following methods:

- If administrators are not yet blocked from accessing the service, delete this app from within the service.
- If administrators are blocked from accessing the service, delete this app from within the Azure portal.

Purchase service extensions

To extend your subscription to Citrix Cloud services, contact your Citrix sales representative. To find your sales representative, use the following steps:

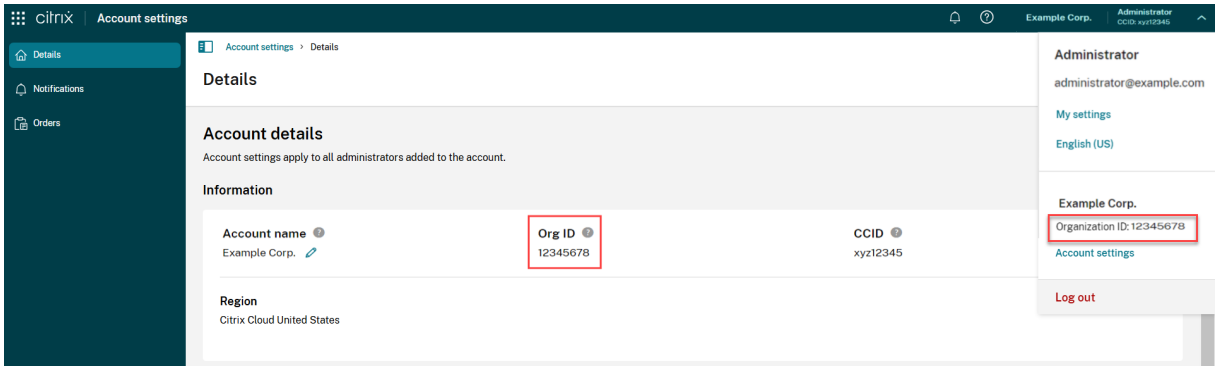
1. Sign in to your Citrix account.
2. Select **Quoting (DOTI)** and then select **Transactions**. Your sales representative and their email address are displayed near the top of this view.

Alternatively, visit the Citrix Customer Service page for contact information in your geographical region.

To complete the purchase, your sales representative needs the Organization ID for your Citrix Cloud account. To find your Organization ID, sign in to your Citrix Cloud account. Your Organization ID is displayed in the following places:

- In the customer menu, in the upper-right corner of the Citrix Cloud console.
- On the **Account Settings** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Geographical Considerations

June 12, 2026

This article discusses the commercial regions that Citrix Cloud™ uses and the presence of Citrix Cloud commercial services within each region.

For more information about the geographical regions and service presence for Citrix's public-sector and dedicated cloud platforms, see Other cloud platforms from Citrix.

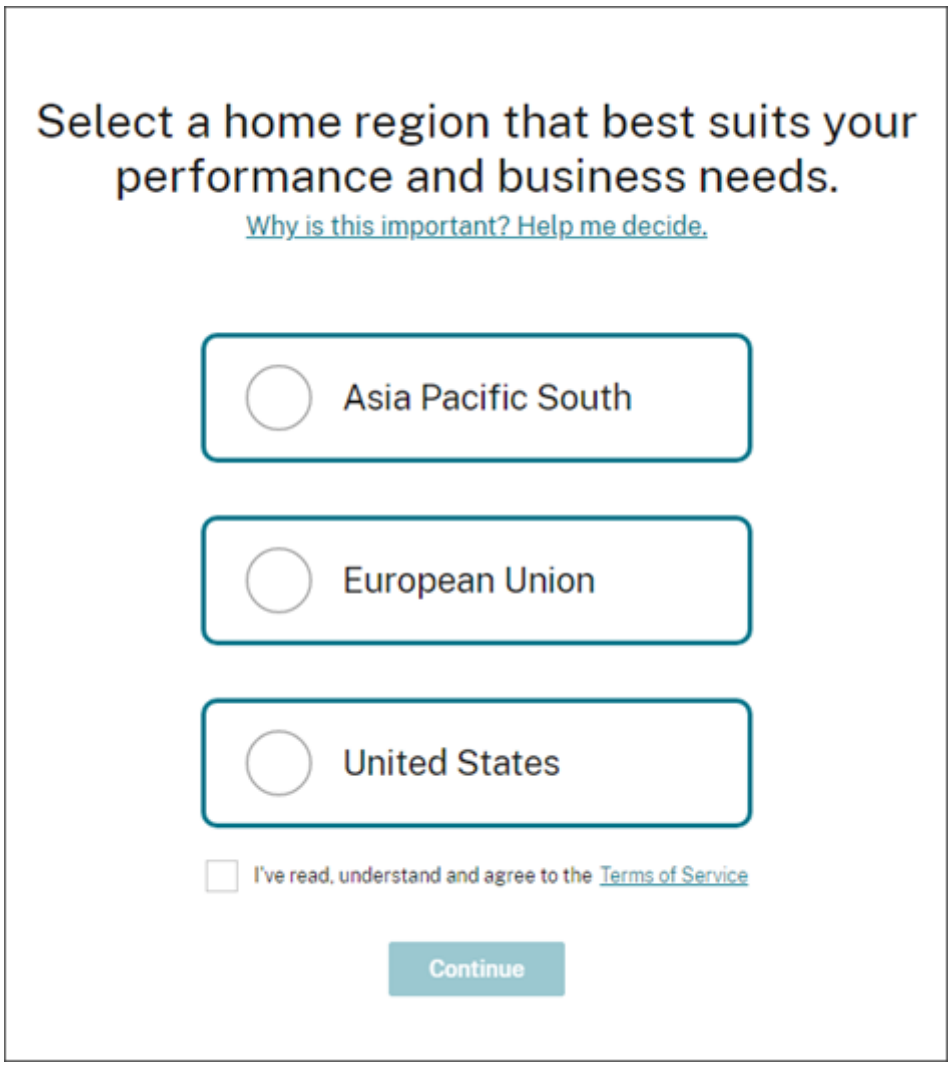
Choose a region

When your organization is onboarded to Citrix Cloud and you sign in for the first time, you are asked to choose one of the following regions:

- United States
- European Union
- Asia Pacific South

When you select a region, services hosted in that geographic region are used for actions associated with the organization where possible. Pick a region that maps to where most of your users and resources are located.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Important notes:

- You can choose a region only once, when your organization is onboarded. You cannot change your region later.
- If you are located in one region and use a service in another region, any performance impacts are minimal. Citrix Cloud services are designed to be used on a global basis. For example, customers in the US that have users and connectors in Australia will see minimal impact from latency.
- If Citrix Cloud is not supported in your region, pick a region that is closest to where most of your users and resources are located.

Service presence in each region

Most Citrix Cloud services are globally replicated. The region you select indicates a preference for where connections must be made. However, connections might still be made to other geographical

© 1997–2026 Citrix Systems, Inc. All rights reserved.

regions. When a service is globally replicated, all the data of that service is stored in all regions.

Similarly, your data might be processed on a global basis by Citrix affiliates or subprocessors as necessary to perform the services.

Certain services have dedicated regional instances. Some services have US-based instances only. In these cases, connections and data are contained within the geographic region.

Where a service is not available in the region that you selected for your organization, certain information (such as authentication data) might be transferred between regions as needed.

Service	US	EU	Asia Pacific South	Notes
Citrix Cloud control plane	Yes	Yes	Yes	
Citrix Analytics for Security™	Yes	Yes	Yes	
Citrix Analytics for Performance™	Yes	Yes	Yes	
NetScaler® Console (formerly Application Delivery Management)	Yes	Yes	Yes	See Low-touch onboarding of NetScaler instances using Console Advisory Connect in this article. For Console on-prem telemetry program, see here.
Citrix DaaS™ (formerly Virtual Apps and Desktops service)	Yes	Yes	Yes	Service uses the Citrix Cloud region.
Citrix DaaS Standard for Azure (formerly Virtual Apps and Desktops Standard for Azure)	Yes	Yes	Yes	Service uses the Citrix Cloud region.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service	US	EU	Asia Pacific South	Notes
Citrix DaaS Standard for Google Cloud (formerly Virtual Apps and Desktops Standard for Google Cloud)	Yes	No (Uses US region)	No (Uses US region)	
Citrix DaaS Premium for Google Cloud (formerly Virtual Apps and Desktops Premium for Google Cloud)	Yes	No (Uses US region)	No (Uses US region)	
Citrix Endpoint Management™	Yes	Yes	Yes	Select from multiple locations across multiple regions. See Endpoint Management service locations in this article.
Remote Browser Isolation Service	Yes	Yes	Yes	Service uses the Citrix Cloud region.
SD-WAN Orchestrator	Yes	Yes	Yes	
Citrix Secure Private Access™	Globally replicated	Globally replicated	Globally replicated	See Secure Private Access points of presence in this article.
Session Recording service	Yes	Yes	Yes	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service	US	EU	Asia Pacific South	Notes
Citrix Virtual Apps Essentials™	Yes	Yes	Yes	Service uses the Citrix Cloud region.
Citrix Virtual Desktops Essentials™	Yes	Yes	Yes	Service uses the Citrix Cloud region.
Web App Firewall	Yes	Yes	No (Uses US region)	
Workspace Environment Management™; Citrix Optimization Pack	Yes	Yes	Yes	
Networking services	Yes	No (Uses US region)	No (Uses US region)	
License Usage Insights (CSPs only)	Globally replicated	Globally replicated	Globally replicated	
Citrix Gateway Service Access Nodes/POP	Multiple WW nodes; traffic routed as needed to ensure the best experience	Multiple WW nodes; traffic routed as needed to ensure the best experience	Multiple WW nodes; traffic routed as needed to ensure the best experience	You can configure resource locations to enable user traffic routed to specific regions. For more information, see Geo-location Routing - Preview
License Activation Service	Yes	Yes	Yes	

> **Note:**
>
> Certain regional Services may be delivered with entitlements to non-regional component Services set forth elsewhere in the table above, and may be used at the customer's election.
>
> Citrix Cloud Services use the customer's designated region to store Customer Content and Logs,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> except with select Logs collected by Citrix sub-processors or for which non-regional storage is necessary for performance of the service, including for support or troubleshooting, monitoring performance, security, auditing, and to allow for cross-region authentication (such as when an EU-based support engineer needs to access a US-based environment). Customer Content and Logs may be accessed on a global basis as necessary to perform the services.

For more information about the data stored by individual services, refer to the Technical Security Overview for each service.

Low-touch onboarding of NetScaler Console instances using Console Advisory Connect

As a part of Console Advisory Connect-based low-touch onboarding of Console instances:

- If you are an existing Citrix Cloud customer, the Console service tenant is created in the same geographical region that you selected when you created your Citrix Cloud account.
- If you are not an existing Citrix Cloud customer, the address mentioned for that customer in the Citrix.com portal is referred. A placeholder Console service tenant is created in the geographical region that corresponds to the region of this referred address. If you choose to onboard to Citrix Cloud in the future, a new Console service tenant is created in the same region that you select when you create your Citrix Cloud account. Also, the data is migrated from the placeholder Console service tenant to the new Console service tenant.

Endpoint Management service locations

You can select one of the following Endpoint Management service locations from your home region:

- US East
- US West
- EU West
- SE Asia
- Sydney

Secure Private Access points of presence

For a list of the points of presence (PoPs) that Secure Private Access uses to ensure continuity and quality of service for customers, see What are all the Secure Private Access PoP locations? in the Secure Private Access service documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pendo data residency and regional considerations

Citrix uses Pendo to provide in-product guidance, feature announcements, and critical notifications across various products and services. All data collected by Pendo is processed and stored exclusively within the United States (US) region.

This data residency applies only to **Pendo-processed data** for the following Citrix products and services:

- Citrix Cloud management console
- Citrix DaaS (including Workspace Environment Management, Web Studio, and Session Recording)
- Citrix Studio (On-premises)
- Citrix Director and Monitor
- NetScaler (ADC)
- NetScaler Console (ADM) and NetScaler Console service
- Secure Developer Spaces
- Citrix Workspace app (Desktop, Mobile, and Tablet –Cloud deployments only)
- Citrix Workspace app for iOS (Native)
- Citrix Workspace app for Android (Native)

Other cloud platforms from Citrix

In addition to Citrix Cloud, Citrix offers other clouds that are isolated and separate from Citrix Cloud.

Citrix Cloud Government

Citrix Cloud Government allows US government agencies and other public-sector customers in the US to use Citrix cloud services according to regulatory and compliance requirements. Citrix Cloud Government is a geographical boundary within which Citrix operates, stores, and replicates services and data for delivery of Citrix Cloud Government services. Citrix may use multiple public or private clouds located in one or more states within the US to provide services.

Citrix Cloud Government and offered services are available only in the US region.

For more information, see the Citrix Cloud Government product documentation.

Citrix Cloud Japan

Citrix Cloud Japan allows Japanese customers to use certain Citrix Cloud services in a dedicated Citrix-managed environment. Citrix Cloud Japan and offered services are available only in Japan.

For more information, see the Citrix Cloud Japan product documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure Deployment Guide for the Citrix Cloud™ Platform

June 9, 2026

The Secure Deployment Guide for Citrix Cloud provides an overview of security best practices when using Citrix Cloud and describes the information Citrix Cloud collects and manages.

Technical security overviews for services

Consult the following articles for more information about data security within Citrix cloud services:

- Analytics Technical Security Overview
- Endpoint Management Technical Security Overview
- Remote Browser Isolation Technical Security Overview
- Citrix DaaS technical security overview
- Citrix DaaS Standard for Azure technical security overview

Guidance for administrators

- Use strong passwords and regularly change your passwords.
- All administrators within a customer account can add and remove other administrators. Ensure that only trusted administrators have access to Citrix Cloud.
- Administrators of a customer have, by default, full access to all services. Some services provide a capability to restrict the access of an administrator. Consult the per-service documentation for more information.
- Two-factor authentication for Citrix Cloud administrators is achieved using the default Citrix identity provider. When administrators sign up for Citrix Cloud or are invited to a Citrix Cloud account, they are required to enroll in multifactor authentication (MFA). If a customer uses Microsoft Azure to authenticate Citrix Cloud administrators, multifactor authentication can be configured as described in Configure Microsoft Entra ID Multi-Factor Authentication settings on the Microsoft website.
- By default, Citrix Cloud automatically terminates administrator sessions after 72 hours, regardless of console activity. This time-out cannot be changed.
- Administrator accounts can be associated with a maximum of 100 customer accounts. If an administrator needs to manage more than 100 customer accounts, they must create a separate administrator account with a different email address to manage the additional customer accounts. Alternatively, they can be removed as an administrator from customer accounts that they no longer need to manage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Password compliance

Citrix Cloud prompts administrators to change their passwords if one of the following conditions exists:

- The current password hasn't been used to sign in for more than 60 days.
- The current password has been listed in a known database of compromised passwords.

New passwords must meet all of the following criteria:

- At least 8 characters long (128 characters maximum)
- Includes at least one upper-case and lower-case letter
- Includes at least one number
- Includes at least one special character: ! @ # $ % ^ * ? + = -

Rules for changing passwords:

- The current password can't be used as a new password.
- The previous 5 passwords can't be reused.
- The new password can't be similar to the account user name.
- The new password must not be listed in a known database of compromised passwords. Citrix Cloud uses a list provided by https://haveibeenpwned.com/ to determine if new passwords violate this condition.

Encryption and key management

The Citrix Cloud control plane does not store sensitive customer information. Instead, Citrix Cloud retrieves information such as administrator passwords on-demand (by prompting the administrator explicitly).

For data-at-rest, Citrix Cloud storage is encrypted using keys that are AES-256 bit or higher. These keys are managed by Citrix.

For data-in-flight, Citrix uses industry standard TLS 1.2 with the strongest cipher suites. Customers cannot control the TLS certificate in use, as Citrix Cloud is hosted on the Citrix-owned cloud.com domain. To access Citrix Cloud, customers must use a browser capable of TLS 1.2, and must have accepted cipher suites configured.

The following strong ciphers are recommended: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

> **Note:**
>
> While TLS 1.2 is required, some services can negotiate TLS 1.3 for enhanced security and performance. Customers are encouraged to allow both TLS 1.2 and TLS 1.3 to be negotiated by their

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> clients. The following strong ciphers are recommended:
>
> - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
> - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

For more information about how Citrix Cloud services data is protected, see Citrix Cloud Services Data Protection Overview on the Citrix web site.

For more information about encryption and key management within each cloud service, consult the service's documentation.

Data sovereignty

The Citrix Cloud control plane is hosted in the United States, the European Union, and Australia. Customers do not have control over this.

The customer owns and manages the resource locations that they use with Citrix Cloud. A resource location can be created in any data center, cloud, location, or geographic area the customer desires. All critical business data (such as documents, spreadsheets, and so on) are stored in resource locations and are under customer control.

Other services may have an option to store data in different regions. Consult the Geographical Considerations topic or the Technical Security Overviews (listed at the beginning of this article) for each service.

Security issues insight

The website status.cloud.com provides transparency into security issues that have an ongoing impact on the customer. The site logs status and uptime information. There is an option to subscribe for updates to the platform or individual services.

Citrix Cloud Connector™

Installing the Cloud Connector

For security and performance reasons, Citrix® recommends that customers do not install the Cloud Connector software on a domain controller.

Also, Citrix strongly recommends that the machines on which the Cloud Connector software is installed be inside the customer's private network and not in the DMZ. For network and system requirements and instructions for installing the Cloud Connector, see Citrix Cloud Connector.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuring the Cloud Connector

The customer is responsible for keeping the machines on which the Cloud Connector is installed up-to-date with Windows security updates.

Customers can use antivirus alongside the Cloud Connector. Citrix supports customers who use industry standard AV products.

In the customer's Active Directory (AD) Citrix strongly recommends that the Cloud Connector's machine account be restricted to read-only access. This is the default configuration in Active Directory. Also, the customer can enable AD logging and auditing on the Cloud Connector's machine account to monitor any AD access activity.

Logging on to the machine hosting the Cloud Connector

The Cloud Connector allows sensitive security information to pass through to other platform components in Citrix Cloud services, but also stores the following sensitive information:

- Service keys for communicating with Citrix Cloud
- Hypervisor service credentials for power management in Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service)

This sensitive information is encrypted using the Data Protection API (DPAPI) on the Windows server hosting the Cloud Connector. Citrix strongly recommends allowing only the most privileged administrators to log on to Cloud Connector machines (for example, to perform maintenance operations). In general, there is no need for an administrator to log on to these machines to manage any Citrix product. The Cloud Connector is self-managing in that respect.

Do not allow end users to log on to machines hosting the Cloud Connector.

Installing other software on Cloud Connector machines

Customers can install antivirus software and hypervisor tools (if installed on a virtual machine) on the machines where the Cloud Connector is installed. However, Citrix recommends that customers do not install any other software on these machines. Other software creates possible security attack vectors and might reduce the security of the overall Citrix Cloud solution.

Inbound and outbound ports configuration

The Cloud Connector requires outbound port 443 to be open with access to the internet. Citrix strongly recommends that the Cloud Connector have no inbound ports accessible from the Internet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Customers can locate the Cloud Connector behind a web proxy for monitoring its outbound Internet communications. However, the web proxy must support SSL/TLS encrypted communication.

The Cloud Connector might have other outbound ports with access to the Internet. The Cloud Connector negotiates across a wide range of ports to optimize network bandwidth and performance if other ports are available.

The Cloud Connector must have a wide range of inbound and outbound ports open within the internal network. The following table lists the base set of open ports required.

Client Port	Server Port	Service
49152 -65535/UDP	123/UDP	W32Time
49152 -65535/TCP	135/TCP	RPC Endpoint Mapper
49152 -65535/TCP	464/TCP/UDP	Kerberos password change
49152 -65535/TCP	49152-65535/TCP	RPC for LSA, SAM, Netlogon (*)
49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
49152 -65535/TCP	3268/TCP	LDAP GC
53, 49152 -65535/TCP/UDP	53/TCP/UDP	DNS
49152 -65535/TCP	49152 -65535/TCP	FRS RPC (*)
49152 -65535/TCP/UDP	88/TCP/UDP	Kerberos
49152 -65535/TCP/UDP	445/TCP	SMB

The Cloud Connector uses LDAP signing and sealing to secure connections to the domain controller. This means that LDAP over SSL (LDAPS) is not required. For more information on LDAP signing, see How to enable LDAP signing in Windows Server and Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing.

Each of the services used within Citrix Cloud extends the list of open ports required. For more information, consult the following resources:

- Technical Security Overviews for each service (listed at the beginning of this article)
- Internet Connectivity Requirements for Citrix Cloud services
- Console service port requirements
- Endpoint Management port requirements

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Monitoring outbound communication

The Cloud Connector communicates outbound to the Internet on port 443, both to Citrix Cloud servers and to Microsoft Azure Service Bus servers.

The Cloud Connector communicates with domain controllers on the local network that are inside the Active Directory forest where the machines hosting the Cloud Connector reside.

During normal operation, the Cloud Connector communicates only with domain controllers in domains that are not disabled on the **Identity and Access Management** page in the Citrix Cloud user interface.

Each service within Citrix Cloud extends the list of servers and internal resources that the Cloud Connector might contact during normal operations. Also, customers cannot control the data that the Cloud Connector sends to Citrix. For more information about services' internal resources and data sent to Citrix, consult the following resources:

- Technical Security Overviews for each service (listed at the beginning of this article)
- Internet Connectivity Requirements for Citrix Cloud services

Viewing Cloud Connector logs

Any information relevant or actionable to an administrator is available in the Windows Event Log on the Cloud Connector machine.

View installation logs for the Cloud Connector in the following directories:

- %AppData%\Local\Temp\CitrixLogs\CloudServicesSetup
- %windir%\Temp\CitrixLogs\CloudServicesSetup

Logs of what the Cloud Connector sends to the cloud are found in %ProgramData%\Citrix\WorkspaceCloud\Logs.

The logs in the WorkspaceCloud\Logs directory are deleted when they exceed a specified size threshold. The administrator can control this size threshold by adjusting the registry key value for HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CloudServices\AgentAdministration\MaximumLogSpaceMegabytes.

SSL/TLS Configuration

The Windows Server hosting the Cloud Connector must have the ciphers detailed in Encryption and key management enabled.

The Cloud Connector must trust the certification authority (CA) that the Citrix Cloud SSL/TLS certificates and Microsoft Azure Service Bus SSL/TLS certificates use. Citrix and Microsoft might change certificates and CAs in the future, but always use CAs that are part of the standard Windows Trusted Publisher list.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Each service within Citrix Cloud might have different SSL configuration requirements. For more information, consult the Technical Security Overviews for each service (listed at the beginning of this article).

Security compliance

To ensure security compliance, the Cloud Connector self-manages. Do not disable reboots or put other restrictions on the Cloud Connector. These actions prevent the Cloud Connector from updating itself when there is a critical update.

The customer is not required to take any other action to react to security issues. The Cloud Connector automatically applies any security fixes.

Citrix Connector™ Appliance for Cloud Services

Installing the Connector Appliance

The Connector Appliance is hosted on a hypervisor. This hypervisor must be inside your private network and not in the DMZ.

Ensure that the Connector Appliance is within a firewall that blocks access by default. Use an allow list to allow only expected traffic from the Connector Appliance.

Ensure that the hypervisors that host your Connector Appliances are installed with up-to-date security updates.

For network and system requirements and instructions for installing the Connector Appliance, see Connector Appliance for Cloud Services.

Logging on to the hypervisor hosting a Connector Appliance

The Connector Appliance contains a service key for communicating with Citrix Cloud. Allow only the most privileged administrators to log on to a hypervisor hosting the Connector Appliance (for example, to perform maintenance operations). In general, there is no need for an administrator to log on to these hypervisors to manage any Citrix product. The Connector Appliance is self-managing.

Inbound and outbound ports configuration

The Connector Appliance requires outbound port 443 to be open with access to the internet. Citrix strongly recommends that the Connector Appliance have no inbound ports accessible from the internet.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can locate the Connector Appliance behind a web proxy for monitoring its outbound internet communications. However, the web proxy must support SSL/TLS encrypted communication.

The Connector Appliance might have other outbound ports with access to the internet. The Connector Appliance negotiates across a wide range of ports to optimize network bandwidth and performance if other ports are available.

The Connector Appliance must have a wide range of inbound and outbound ports open within the internal network. The following table lists the base set of open ports required.

Connection Direction	Connector Appliance Port	External Port	Service
Inbound	443/TCP	Any	Local Web UI
Outbound	49152-65535/UDP	123/UDP	NTP
Outbound	53, 49152-65535/TCP/UDP	53/TCP/UDP	DNS
Outbound	67/UDP	68/UDP	DHCP and broadcast
Outbound	49152 -65535/UDP	123/UDP	W32Time
Outbound	49152 -65535/TCP	464/TCP/UDP	Kerberos password change
Outbound	49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
Outbound	49152 -65535/TCP	3268/TCP	LDAP GC
Outbound	49152 -65535/TCP/UDP	88/TCP/UDP	Kerberos
Outbound	49152 -65535/TCP/UDP	445/TCP	SMB
Outbound	137/UDP	137/UDP	NetBIOS Name Service
Outbound	138/UDP	138/UDP	NetBIOS Datagram
Outbound	139/TCP	139/TCP	NetBIOS Session

Each of the services used within Citrix Cloud extends the list of open ports required. For more information, consult the following resources:

- Technical Security Overviews for each service (listed at the beginning of this article)
- System and Connectivity Requirements for Citrix Cloud services

Monitoring outbound communication

The Connector Appliance communicates outbound to the Internet on port 443 to Citrix Cloud servers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Each service within Citrix Cloud extends the list of servers and internal resources that the Connector Appliance might contact during normal operations. Also, customers cannot control the data that the Connector Appliance sends to Citrix. For more information about services' internal resources and data sent to Citrix, consult the following resources:

- Technical Security Overviews for each service (listed at the beginning of this article)
- System and Connectivity Requirements for Citrix Cloud services

Viewing Connector Appliance logs

You can download a diagnostic report for your Connector Appliance that includes various log files. For more information about getting this report, see Connector Appliance for Cloud Services.

SSL/TLS Configuration

The Connector Appliance does not need any special SSL/TLS configuration.

The Connector Appliance trusts the certification authority (CA) used by Citrix Cloud SSL/TLS certificates. Citrix might change certificates and CAs in the future, but always use CAs that the Connector Appliance trusts.

Each service within Citrix Cloud might have different SSL configuration requirements. For more information, consult the Technical Security Overviews for each service (listed at the beginning of this article).

Security compliance

To ensure security compliance, the Connector Appliance self-manages and you cannot log in to it through the console.

You are not required to take any other action to react to connector security issues. The Connector Appliance automatically applies any security fixes.

Ensure that the hypervisors that host your Connector Appliances are installed with up-to-date security updates.

In your Active Directory (AD) we recommend that the Connector Appliance machine account be restricted to read-only access. This is the default configuration in Active Directory. Also, the customer can enable AD logging and auditing on the Connector Appliance machine account to monitor any AD access activity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Guidance for handling compromised accounts

- Audit the list of administrators in Citrix Cloud and remove any who are not trusted.
- Disable any compromised accounts within your company's Active Directory.
- Contact Citrix and request rotating the authorization secrets stored for all the customer's Cloud Connectors. Depending on the severity of the breach, take the following actions:
  - **Low Risk:** Citrix can rotate the secrets over time. The Cloud Connectors continue to function normally. The old authorization secrets become invalid in 2-4 weeks. Monitor the Cloud Connector during this time to ensure that there are no unexpected operations.
  - **Ongoing high risk:** Citrix can revoke all old secrets. The existing Cloud Connectors will no longer function. To resume normal operation, the customer must uninstall and reinstall the Cloud Connector on all applicable machines.

Create a Citrix Cloud™ account

June 22, 2026

This article walks you through the process of creating a Citrix Cloud account and completing the required tasks for onboarding your account successfully.

Customers with an existing relationship with Citrix® and are new to Citrix cloud services can use the tasks in this article to complete the onboarding process.

Sign-up process for new Citrix customers

If you're new to Citrix and Citrix Cloud, you must contact Citrix to create a new Citrix account for your company. Use one of the following contact methods:

- Contact Citrix Customer Service.
- Contact a Citrix Partner or Citrix Sales office in your area.

When you contact Citrix, you can discuss your business needs with a Citrix representative. The representative helps you complete the sign-up process and provides you with your Citrix sign-in credentials.

After you receive your Citrix account credentials, you can use the tasks in this article to sign in and get started with Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What is a Citrix account?

A Citrix account, also known as a Citrix.com account or My Citrix account, enables you to manage access to the licenses you have purchased. Your Citrix account uses an organization ID (OrgID) as a unique identifier. You can access your Citrix account by logging in at https://www.citrix.com with a user name (also known as a web login) or your email address, if one is linked to your account.

> **Important:**
>
> A user name maps to a single, unique Citrix account, but an email address can map to multiple Citrix accounts.

What is an OrgID?

An OrgID is the unique identifier assigned to your Citrix account. Your OrgID is associated with a physical site address, typically your company's business address. Companies usually have a single OrgID. However, in some cases, such as having different branch offices or having different departments managing their assets separately, Citrix may allow a single company to have multiple OrgIDs.

Citrix routinely cleans up certain OrgIDs, merging duplicates in some cases. If your company has OrgIDs that you want to merge with a valid and active OrgID, you can contact Citrix Customer Support with the OrgIDs you want merged.

> **Note:**
>
> Companies have already set up OrgIDs based on how they want to manage their assets, so if you don't know what OrgID you need to use or how many OrgIDs you have, contact the IT department or Citrix administrator in your company. If you need help, contact Citrix Customer Service at https://www.citrix.com/support/ to locate your OrgID.

What is a Citrix Cloud account?

A Citrix Cloud account enables you to use one or more Citrix cloud services to securely deliver your apps and data. A Citrix Cloud account is identified by a customer ID and is associated with an OrgID. An OrgID can be associated with multiple Citrix Cloud customer IDs, but a customer ID can be associated with only one OrgID.

It's important to use the right Citrix Cloud account, based on how your organization has set up OrgIDs, so that your purchases and administrator access can continue on the same OrgIDs. For example, if a company's design department using OrgID 1234 has been using Virtual Apps and Desktops on-premises and wants to try Citrix Cloud, one of the administrators of OrgID 1234 can sign up for Citrix Cloud on that OrgID using their Citrix account sign-in credentials or an email address associated with

© 1997–2026 Citrix Systems, Inc. All rights reserved.

that OrgID. When the company decides to purchase a Citrix DaaS™ subscription, the order can be placed correctly on OrgID 1234.

> **Important:**
>
> Users who have access to a particular Citrix account do not automatically have access to the Citrix Cloud account associated with that Citrix account's OrgID. Because Citrix Cloud access enables users to potentially impact service, it's important to control who accesses the Citrix Cloud account.



Multifactor authentication

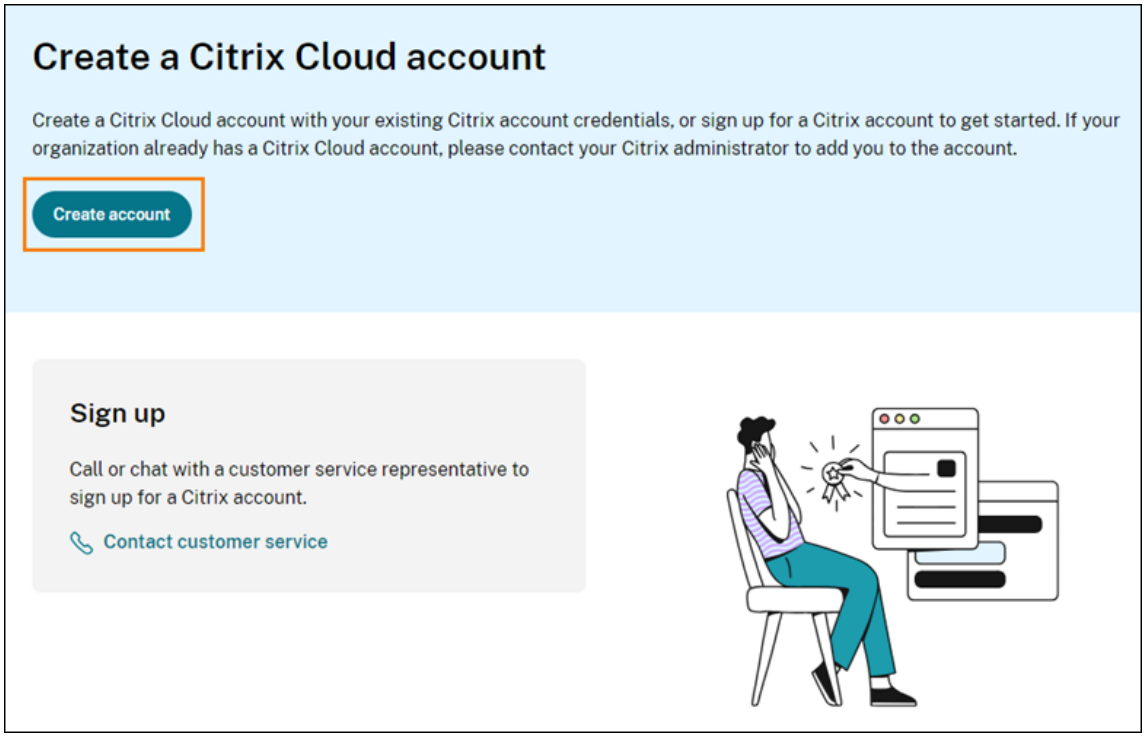
To keep your Citrix Cloud account safe and secure, Citrix requires all customers to enroll in multifactor authentication (MFA). To enroll, you need only a device, such as a computer or mobile device, and an authenticator app installed, such as Citrix SSO. If using a device with an authenticator app isn't possible, you can use an email address instead.

If you're not already enrolled in MFA, Citrix prompts you to enroll when you sign in with your Citrix account credentials. For requirements and instructions, see Step 2: Set up multifactor authentication in this article.

Step 1: Visit the Citrix Cloud web site

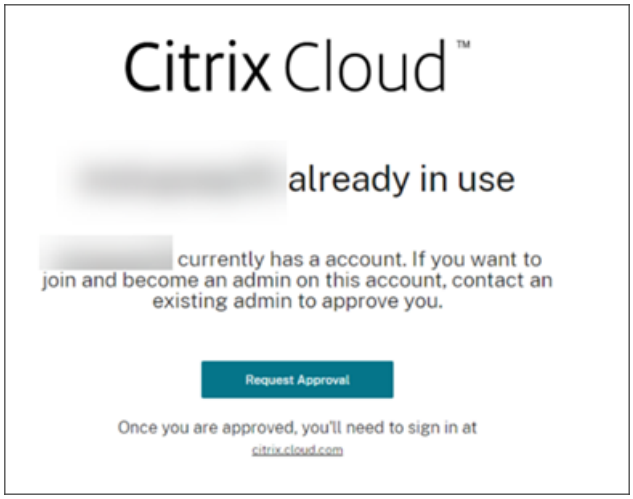
1. Using a web browser, visit https://onboarding.cloud.com.
2. Select **Create account**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Enter your user name and password or the email address and password associated with your Citrix.com account.

What happens if the account is already in use?



If you see a message indicating a Citrix Cloud account for your organization is already in use, it means that another administrator from your Citrix account has already created the Citrix Cloud account. Before you can access the account, an existing administrator needs to invite you to be an administrator, even if you're already a member of the Citrix account.

Since a Citrix Cloud account allows administrators much greater control on the service, we expect that

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the first administrator who creates the Citrix Cloud account has to explicitly give access to another administrator, even if the other administrator is already a member of the Citrix account.

To request an invitation to join the Citrix Cloud account, select **Request Approval**. All existing administrators on the account receive an email notifying them of your request. If the existing administrators are no longer with your organization, please contact Citrix Support.

When an administrator receives your approval request, they invite you to be an administrator as described in Invite individual administrators.

When you receive the invitation email, click the **Sign in** link to accept the invitation. When your browser opens, Citrix Cloud prompts you to create a password and sign in to the Citrix Cloud account.

Step 2: Set up multifactor authentication

If you're not enrolled in MFA, Citrix Cloud prompts you to enroll before signing in. You can choose to enroll in MFA using an authenticator app (recommended) or your email address.

> **Notes:**
>
> - Only administrators under the Citrix identity provider can set up MFA through Citrix Cloud. If you use Microsoft Entra ID to manage Citrix Cloud administrators, you can configure MFA using the Azure portal. For more information, see Configure Azure Multi-Factor Authentication settings on the Microsoft web site.
> - After you complete the setup process, MFA is used for all customer organizations that you belong to in Citrix Cloud. You can't disable MFA after completing the setup process.
> - You can enroll only one device. If you enroll a different device later, Citrix Cloud deletes the current device enrollment and replaces it with the new device. For more information, see Manage your primary MFA method.

Email as an authentication method

If you can't use an authenticator app to access Citrix Cloud, MFA using email is a convenient alternative. However, Citrix strongly recommends that you take precautions to ensure access to your email address is secure.

MFA requirements

To set up MFA with an authenticator app, you must install an app that follows the Time-Based One-Time Password standard on your device, such as a smartphone or desktop computer. Depending on

© 1997–2026 Citrix Systems, Inc. All rights reserved.

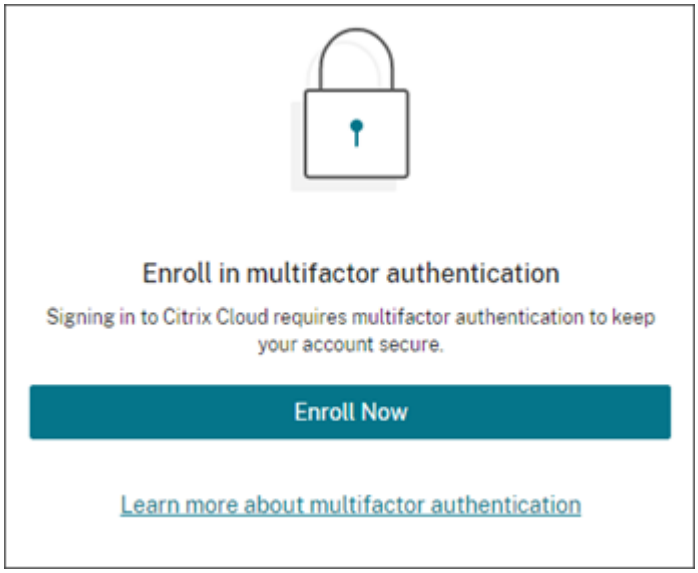
the device you're enrolling, the app might need to access your device's camera to scan a QR code. If your device doesn't have a camera, you can enter a key that Citrix Cloud provides.

To set up MFA with an email address, you must use an email address that meets the following requirements:

- The email address is different from the email address you're using for your Citrix account.
- The email address is an address that you can access to receive verification emails from Citrix.

To enroll in multifactor authentication

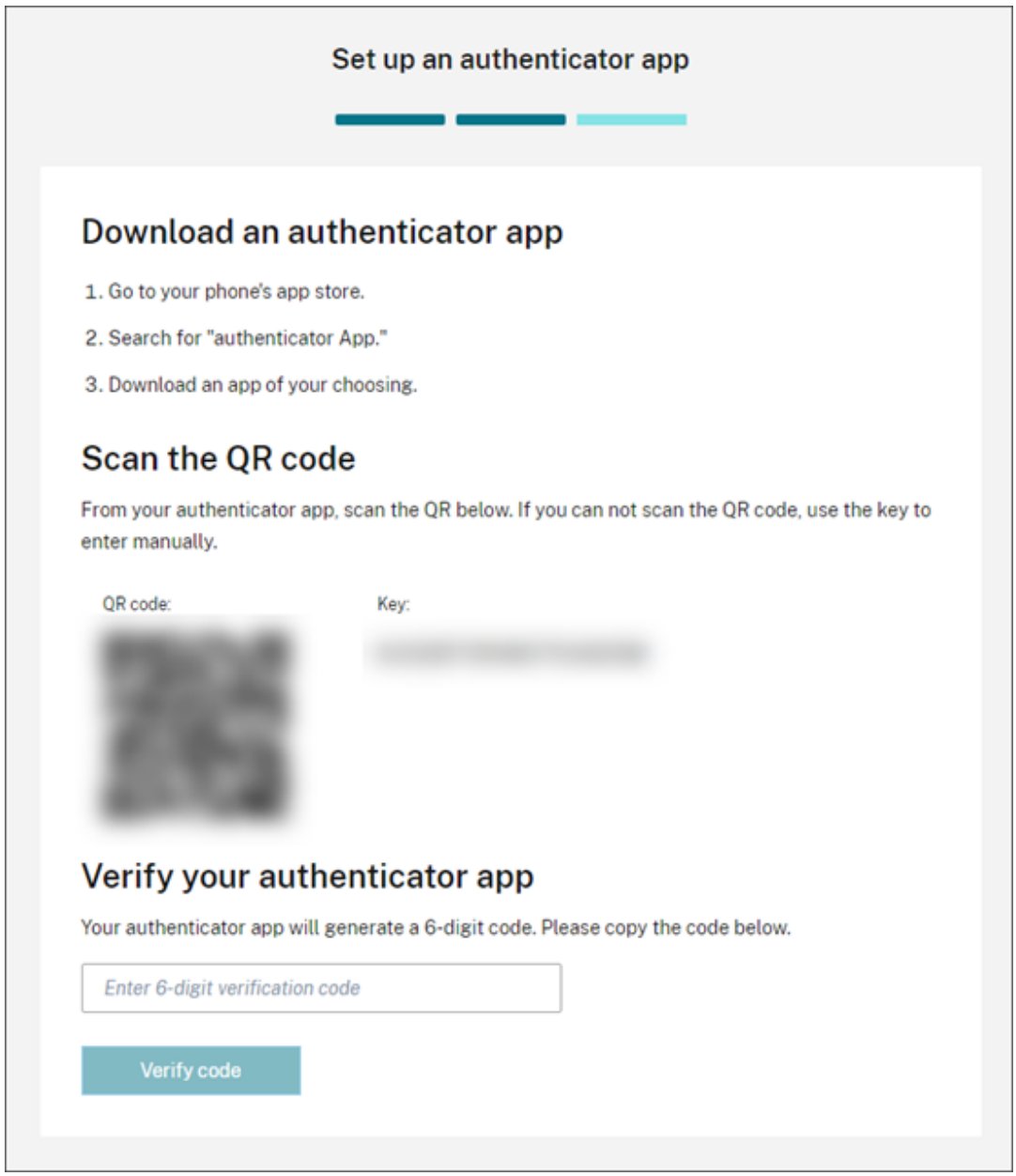
1. When prompted to enroll in MFA, select **Enroll now**.



2. When prompted, enter your email address and select **Send email**. Citrix Cloud sends you an email with a verification code.
3. Enter the verification code from the email and your Citrix account password. Click **Verify and continue**.
4. Select the authentication method you want to use, either authenticator app or email.
5. If you selected **Authenticator app**, perform the following actions:

    a) From your authenticator app, scan the QR code or enter the key manually. Your authenticator app displays an entry for Citrix Cloud and generates a 6-digit code.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



b) Under **Verify your authenticator app**, enter the code from your authenticator app and select **Verify code**.

6. Click **Next: Recovery Methods**.
7. Select **Add recovery phone** and enter a recovery phone number that Citrix Support can use to call you and verify your identity. Citrix recommends using a landline phone number. When finished, click **Save recovery phone number**.
8. Select **Next**.
9. Select **Add recovery email** and enter an email address that you can access that's different from the one you use with Citrix Cloud. Citrix uses this address to send you a verification code to verify

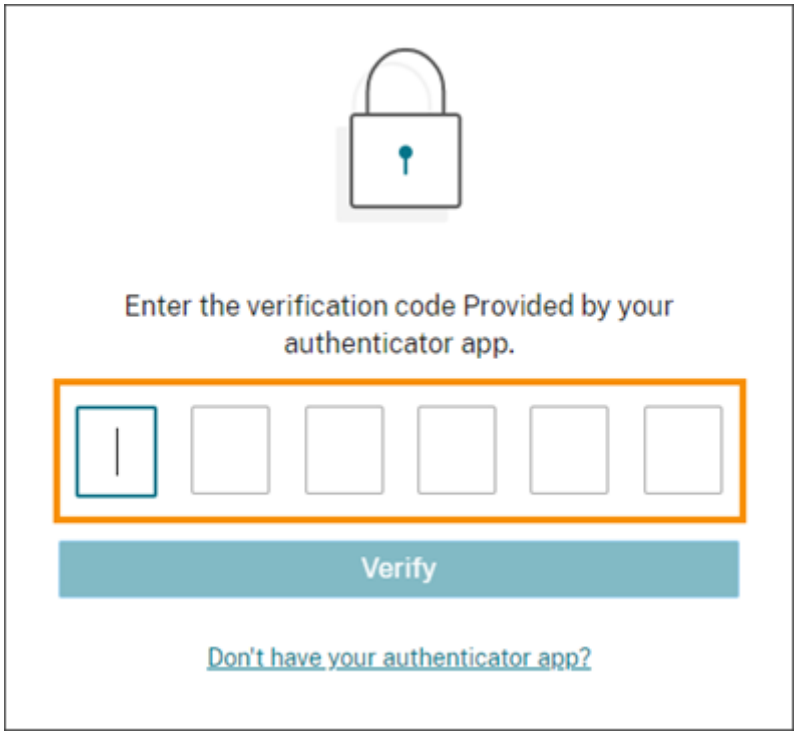
© 1997–2026 Citrix Systems, Inc. All rights reserved.

your identity.

If you don't have a different email address, select **Don't have a recovery email?** to generate a list of backup codes instead. Backup codes aren't recommended because they can be lost easily. If you choose this option, download the codes and keep them in a location where you can access them when needed.

10. Select **Finish** to complete the enrollment.

The next time you sign in with your Citrix Cloud administrator credentials, Citrix Cloud prompts you for the verification code from your chosen MFA method.



Manage your MFA enrollment

To change your device, switch to a different MFA method, or update your recovery methods, see the following articles:

- Manage your primary MFA method
- Manage your MFA recovery methods

Step 3: Verify your OrgID

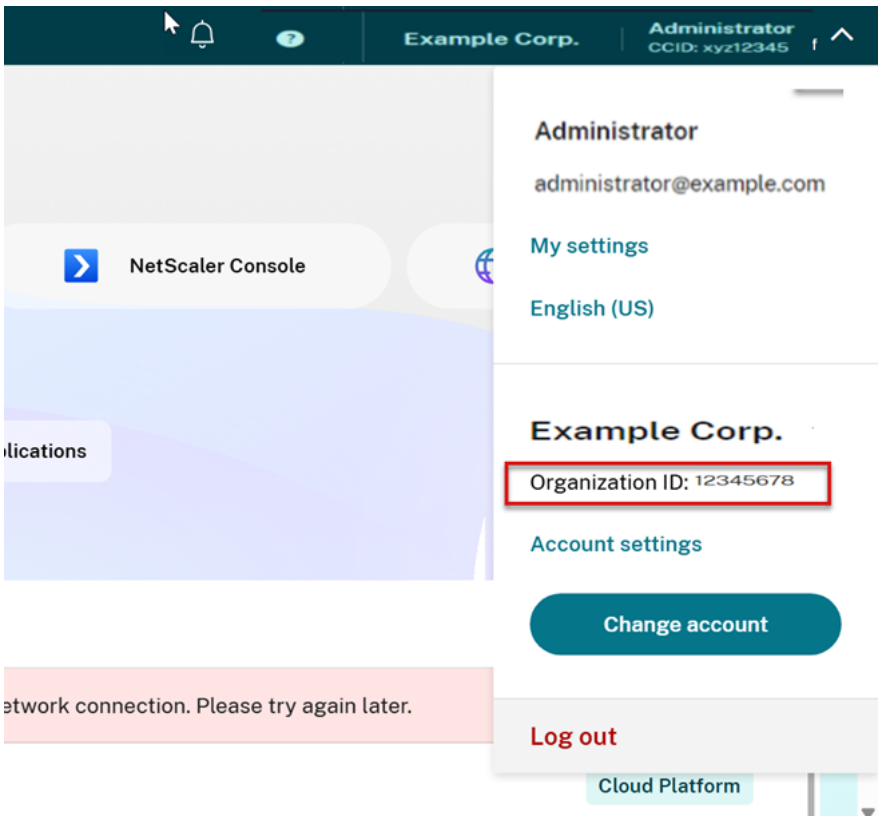
Before you start using Citrix Cloud, take a moment to verify your OrgID.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Make sure your account OrgID matches the OrgID that you use to place orders. One of the benefits of Citrix Cloud is that if you try a service and decide to purchase it, then all the configurations you made in the trial are retained in the purchased service, since the purchase occurs in the same account. So, making sure that the trial starts in the right OrgID saves effort when you decide to purchase.

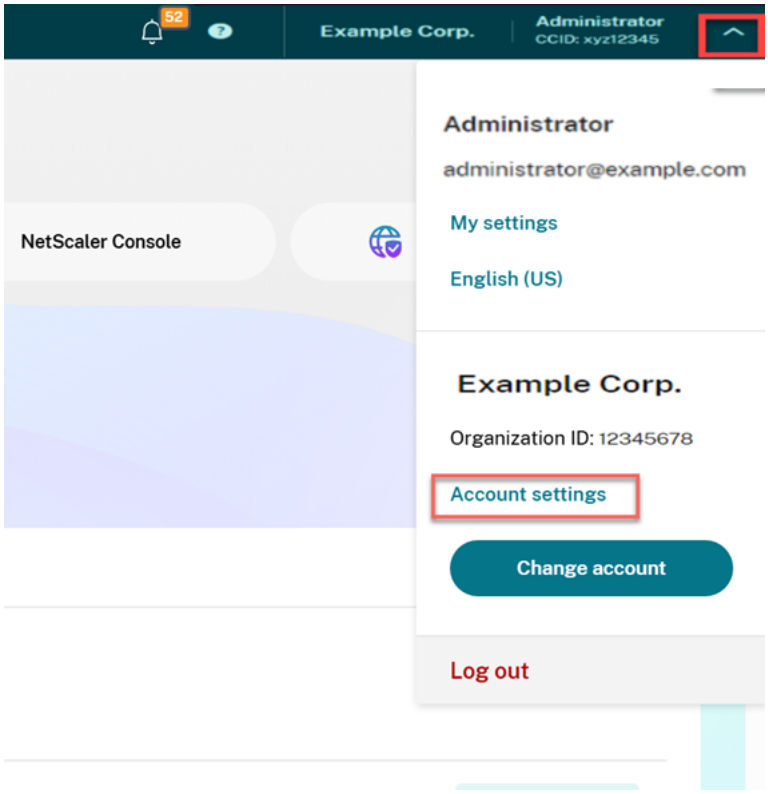
Your OrgID appears in the following locations in the management console:

- In the menu beneath your customer name. Click on your customer name in the top-right corner to reveal the menu.



- On your **Account Settings** page. Select **Account Settings** from the customer menu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Next steps

After onboarding, you can move on to the following tasks:

- Add an identity provider to authenticate administrators or end users.
- Add administrators to your Citrix Cloud account. Even if your other administrators have access to your Citrix account on Citrix.com, you still need to add them to your Citrix Cloud account.
- Request cloud service trials. Trials are designed to be tested with your choice of on-premises infrastructure or public cloud, your applications, and your Microsoft Active Directory.
- Allocating licenses to an account. This procedure assists you in allocating licenses to the users.

More information

- Citrix Training: Fundamentals of Citrix Cloud
- Citrix channel on YouTube: Citrix Cloud Master Class

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Verify your email for Citrix Cloud™

September 6, 2025

From time to time, Citrix might ask you to verify your Citrix Cloud account. Some reasons why you might be asked to verify your email:

- You haven't logged in to Citrix Cloud in a while.
- You changed your email address.
- You added a new administrator to your Citrix Cloud account.
- Due to security system updates to Citrix Cloud, you are required to re-verify your Citrix Cloud account.

FAQ

How often will I be asked for verification?

Verifying your account is a one-time event. Citrix Cloud won't ask you for verification every time you sign in or when something in your account changes. If you're asked to verify frequently, contact Citrix Technical Support.

Has something happened to my account?

No, being asked to verify your account doesn't mean that anything is wrong with either your account or any of your Citrix Cloud services. It's simply a part of how Citrix keeps your information safe and secure.

I haven't received a verification email. What do I do?

Perform the following steps:

1. Search your inbox for a verification email from 'Citrix'. The verification email expires after 24 hours. To trigger a new verification email, sign in to Citrix Cloud again. This is a one-time process for each web login.
2. If it's not in your inbox, check your folders. If a spam filter or email rule moved the email, it might be in your spam or junk folders. Check any firewalls.
3. Ensure that you're checking the correct email account. Citrix sends the verification email to the email address currently on file for your account. Often, this is the email address you originally signed up with for Citrix Cloud or the one with which you were invited to join the Citrix Cloud account.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Confirm that the email address on record is valid by signing in to your Citrix account at https://www.citrix.com/account. If the email is invalid, update your email address and sign in to Citrix Cloud again to trigger a new verification email. For more information, see CTX120355 in the Citrix Support Knowledge Center.
5. If you still have not received a verification email, contact Citrix Support to open a support case. For education sites (see **Partner Services Delivery > eLearning > Citrix Training**), open a case with the education team for further investigation. To open a case, request **General Support** on the Contact Us page.

If you have successfully verified your email but you are still unable to sign in to Citrix Cloud, see Troubleshooting login issues on Citrix websites.

Contact Citrix Support

If you are experiencing an issue that's not covered here, contact Citrix Support to open a support case.

Connect to Citrix Cloud™

June 22, 2026

Connecting your resources to Citrix Cloud involves deploying connectors in your environment and creating *resource locations*.

Resource Locations

Resource locations contain the resources required to deliver cloud services to your end users. Resource locations contain different resources depending on which Citrix Cloud services you are using and the services that you want to provide to your users.

Your resource location is wherever your resources reside, whether that's a public or private cloud, a branch office, or a data center. If you already have resources in your own cloud or data center, your resources remain where they are. There's no need to move them elsewhere to use them with Citrix Cloud.

Your choice of location might be impacted by the following factors:

- Proximity to end users
- Proximity to data
- Scale requirements
- Security attributes

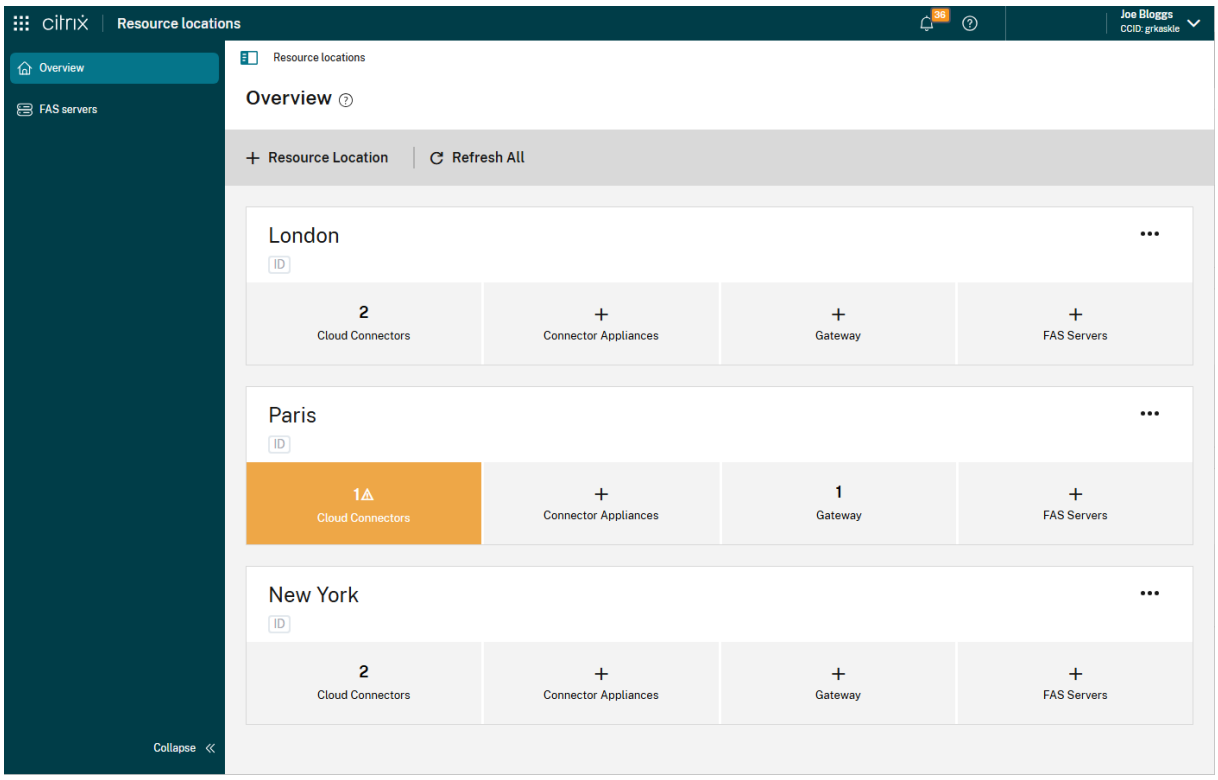
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example of a resource location deployment

- Build your first resource location in your data center for the head office based on users and applications that need to be close to the data.
- Add a second resource location for your global users in a public cloud. Alternatively, build separate resource locations in branch offices to provide the applications best served close to the branch workers.
- Add another resource location on a separate network that provides restricted applications. This provides restricted visibility to other resources and users without the need to adjust the other resource locations.

View and manage resource locations

To manage Resource Locations, log into Citrix Cloud and from the main menu choose **Resource Locations**.



For each resource location you can add:

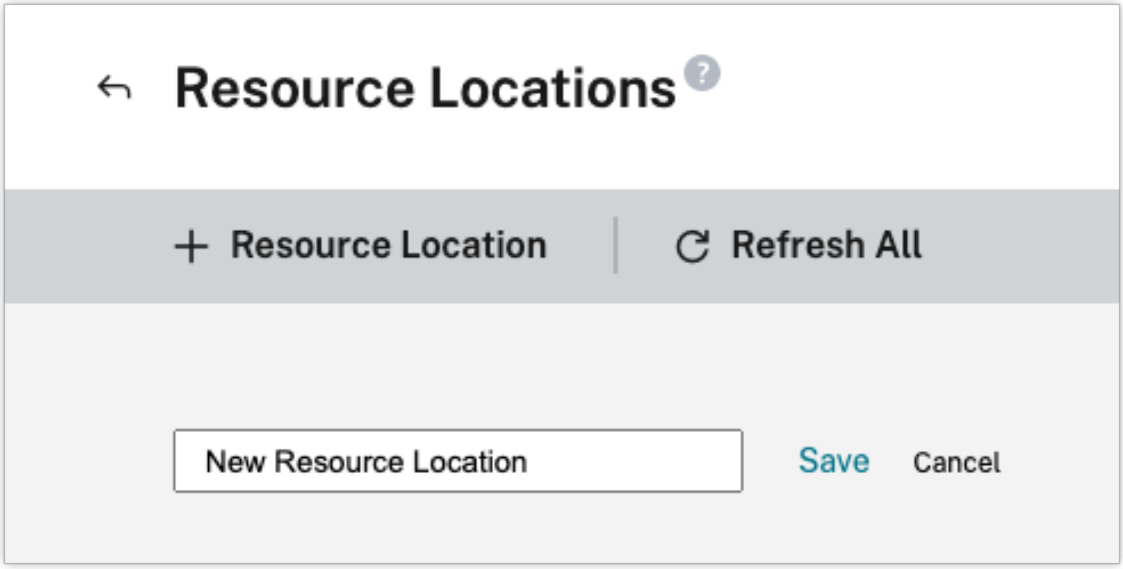
- Cloud connectors
- Connector appliances
- Citrix Gateways
- FAS servers

© 1997–2026 Citrix Systems, Inc. All rights reserved.

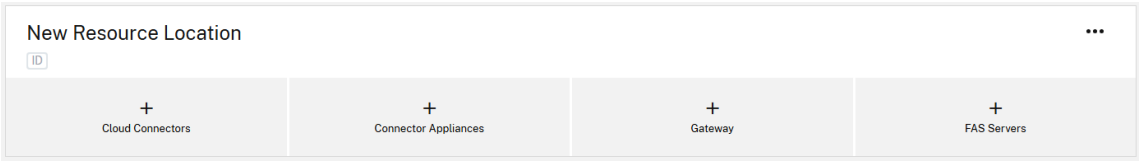
Create a resource location

To create a resource location:

1. Select **+ Resource Location**



2. Enter the name of the resource location. See Naming restrictions.
3. Press **Save**. The new resource location is created.



4. Install at least two connectors in the resource location. Depending on the cloud services you're using, either Cloud Connectors or Connector Appliances are required for enabling communication between Citrix Cloud and your resources. For more information about choosing the appropriate connector, see Resource type. To deploy the connectors, see the following articles:

   - Cloud Connector Installation
   - Connector Appliance for Cloud Services

Resource types

Resource locations contain different resources depending on which Citrix Cloud services you are using and the services that you want to provide to your end users. Different resources use different types of connector. Most services make use of the Citrix Cloud Connector™, but some specific services need a Connector Appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Services that use Citrix Cloud Connector

- **Citrix DaaS** (formerly Citrix Virtual Apps and Desktops service) requires the Cloud Connector for publishing apps and desktops and provisioning machine catalogs in your resource locations. For an overview of how the Cloud Connector communicates with this service, refer to the Citrix DaaS diagram in Citrix Tech Zone.
- **Citrix DaaS Standard for Azure** (formerly Citrix Virtual Apps and Desktops Standard for Azure) requires the Cloud Connector for delivering Citrix-hosted Azure virtual desktops and apps from multi-session machines.
- **Endpoint Management** requires the Cloud Connector for managing app and device policies and delivering apps to users.

Services that use Connector Appliance

- **Image Portability Service** simplifies the management of images across platforms. This feature is useful for managing images between an on-premises resource location and one in a public cloud. The Citrix Virtual Apps and Desktops™ REST APIs can be used to automate the administration of resources within a Citrix Virtual Apps and Desktops site.

  The Image Portability workflow begins when you use Citrix Cloud to initiate the migration of an image from your on-premises location to your public cloud subscription. After preparing your image, Image Portability Service helps you transfer the image to your public cloud subscription and prepare it to run. Finally, Citrix Provisioning or Machine Creation Services™ provisions the image in your public cloud subscription.

  For more information, see Image Portability Service.

- **Citrix Secure Private Access** enables administrators to provide a cohesive experience that integrates single sign-on, remote access, and content inspection into a single solution for end-to-end access control. For more information, see Secure Private Access with Connector Appliance.

There might be other services in preview that also depend on the Connector Appliance.

Resource location limits

You can have a maximum of 50 resource locations in your Citrix Cloud account.

Naming restrictions

Names that you assign to resource locations must conform to the following restrictions:

- Maximum length: 64 characters

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Disallowed characters:
  - #, $, %, ^, &, ?, +
  - Braces: [], { }
  - Pipes (|)
  - Less-than symbol (<) and greater-than symbol (>)
  - Forward and backward slashes (/, \)
- Must not match any other resource location name (case-insensitive) in the Citrix Cloud account

Primary resource locations

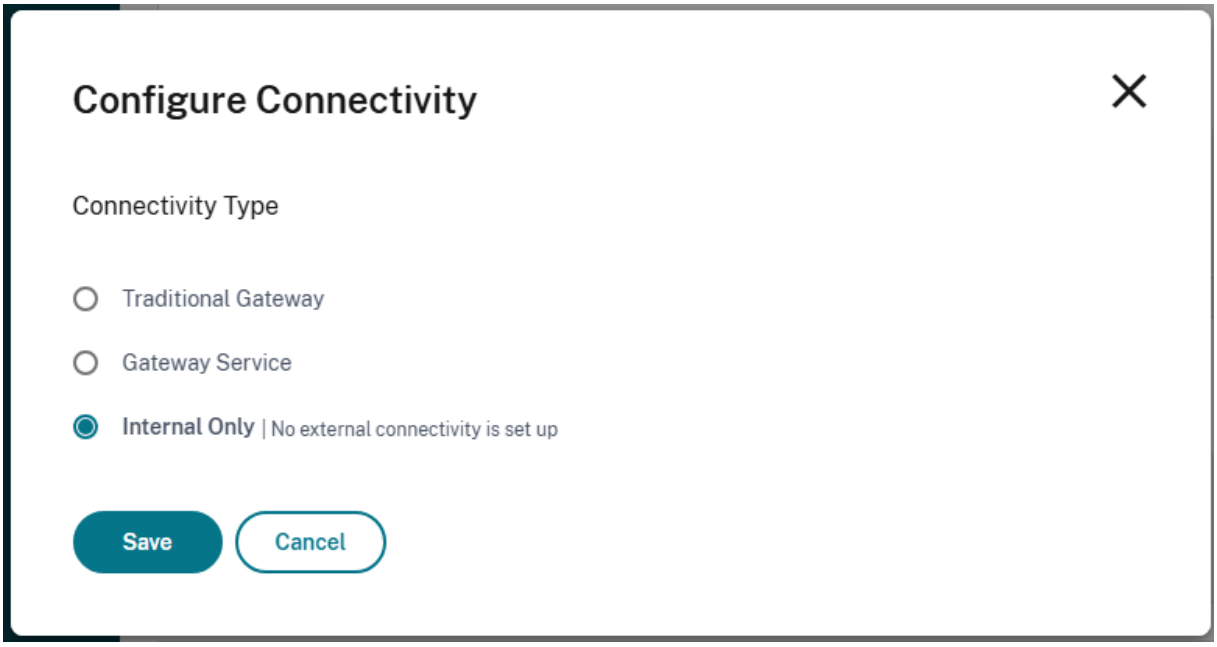
A primary resource location is a resource location that you designate as "most preferred" for certain communications between your domain and Citrix Cloud. The Cloud Connectors in a primary resource location are used for user logons and provisioning operations. The resource location you select as "primary" should have Cloud Connectors that have the best performance and connectivity to your domain. This enables your users to log on quickly to Citrix Cloud.

For more information, see Select a primary resource location.

Gateways

By default, clients must be able to directly reach the machines hosting your virtual apps and desktops. You can enable remote access by using a gateway. You can either use the Citrix Gateway Service or by using your own NetScaler® gateway.

To configure remote access, select the **Gateway** tile for a resource location.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alternatively, you can reach the same configuration screen from **StoreFront Cloud**.

For more information on configuring gateways, see Configure access to stores - External connectivity.

Citrix Cloud Connector™

July 17, 2026

The Citrix Cloud™ Connector is a Citrix component that serves as a channel for communication between Citrix Cloud and your resource locations, enabling cloud management without requiring any complex networking or infrastructure configuration. This removes all the hassle of managing delivery infrastructure. It enables you to manage and focus on the resources that provide value to your users.

> **Note:**
>
> Do not install the Citrix DaaS Remote PowerShell SDK on a Citrix Cloud Connector machine. It can be installed on any domain joined machine within the same resource location.
>
> Citrix® recommends that you do not run this SDK's cmdlets on Cloud Connectors. The SDK's operation does not involve the Cloud Connectors.

Services that require the Cloud Connector

Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) requires the Cloud Connector. For an overview of how the Cloud Connector communicates with the service, refer to the Citrix DaaS diagram in Tech Zone.

Citrix Endpoint Management™ requires the Cloud Connector for enterprise connectivity to the Endpoint Management service. The Remote Browser Isolation service requires the Cloud Connector for authenticated external web apps.

Cloud Connector functions

- **Active Directory (AD)**: Enables AD management, allowing the use of AD forests and domains within your resource locations. It removes the need for adding any additional AD trusts.
- **Virtual apps and desktops publishing**: Enables Citrix DaaS™ publishing from resources in your resource locations.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Endpoint Management**: Enables a mobile device management (MDM) and mobile application management (MAM) environment for managing device and app policies and delivering apps to users.
- **Machine catalog provisioning**: Enables provisioning of machines directly into your resource locations.

Cloud Connector communication

The Cloud Connector authenticates and encrypts all communication between Citrix Cloud and your resource locations. Once installed, the Cloud Connector initiates communication with Citrix Cloud through an outbound connection. All connections are established from the Cloud Connector to the cloud using the standard HTTPS port (443) and the TCP protocol. No incoming connections from the public internet are accepted.

Cloud Connector availability and load management

For continuous availability and to manage load, install multiple Cloud Connectors in each of your resource locations. At least two Cloud Connectors in each resource location are required for ensuring a highly available connection with Citrix Cloud. If one Cloud Connector is unavailable for any period of time, the other Cloud Connectors can maintain the connection. Since each Cloud Connector is stateless, the load can be distributed across all available Cloud Connectors. There is no need to configure this load balancing function. It is completely automated.

As long as there is one Cloud Connector available, there will be no loss in communication with Citrix Cloud. The end user's connection to the resources in the resource location does not rely on a connection to Citrix Cloud, wherever possible. This enables the resource location to provide users access to their resources regardless of a connection being available to Citrix Cloud.

Where to obtain the Cloud Connector

You can download the Cloud Connector software from within Citrix Cloud.

1. Sign in to Citrix Cloud.
2. From the menu in the top-left of the screen, select **Resource Locations**.
3. If you have no existing resource locations, click **Download** on the Resource Locations page. When prompted, save the **cwcconnector.exe** file.
4. 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How many Cloud Connectors do I need?

A minimum of two (2) Cloud Connectors are required to create a highly available connection between Citrix Cloud and your resource location. Depending on your environment and the workloads you're supporting, you might need more Cloud Connectors to ensure the best experience for your users.

As a best practice, Citrix recommends using the N+1 redundancy model when determining the number of Cloud Connectors you need to deploy. Determine the number of Cloud Connectors that you need in a resource location based on your environment, workloads, Active Directory configuration, and services. To this number, add at least one more Cloud Connector to provide resiliency. For example, if you determine that you need five Cloud Connectors, add one more to this total and install six Cloud Connectors in your resource location.

For additional scale and sizing guidelines, see Scale and size considerations for Cloud Connectors.

Where to install the Cloud Connector

Install the Cloud Connector on a dedicated machine that is joined to your domain and able to communicate with the resources that you want to manage from Citrix Cloud. For more information, see system requirements.

For more deployment information, see the following articles:

- Deployment scenarios for Cloud Connectors in Active Directory
- Cloud Connector Installation

Citrix Cloud Connector system requirements

July 21, 2026

The machines hosting the Citrix Cloud Connector™ must meet the following requirements. At least two Cloud Connectors in each resource location are required for production environments to ensure high availability. As a best practice, Citrix® recommends using the N+1 redundancy model when deploying Cloud Connectors to maintain a highly available connection with Citrix Cloud.

Host Resource requirements

Each Cloud Connector requires a minimum of:

- 2 vCPU
- 4 GB memory

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 20 GB disk space

For Cloud Connectors which will be used for Local Host Cache, Citrix recommends a minimum of 4 vCPU and 6 GB memory for Cloud Connectors.

More vCPU memory enables a Cloud Connector to scale up for larger sites. For recommended configurations, see Scale and size considerations for Cloud Connectors.

Operating systems

The following operating systems are supported:

- Windows Server 2025
- Windows Server 2022
- Windows Server 2019
- Windows Server 2016

The Cloud Connector is not supported for use with Windows Server Core.

.NET requirements

You must install both of the following on each server.

- Microsoft .NET Framework 4.7.2 or later. This is already installed by default on Windows Server 2019 and higher. On Windows Server 2016, Download the latest version from the Microsoft website.
- Microsoft .NET 8.0. Download the latest version from the Microsoft website.

Citrix strongly recommends configuring Windows Update to "Receive updates for other Microsoft products"to ensure these packages are kept up to date.

Server requirements

If you're using Cloud Connectors with Citrix DaaS™ (formerly Citrix Virtual Apps and Desktops service), refer to Scale and size considerations for Cloud Connectors for machine configuration guidance.

The following requirements apply to all machines where the Cloud Connector is installed:

- Use dedicated machines for hosting the Cloud Connector. Do not install on the same machine as any other Citrix products, or other applications.
- The server is not an Active Directory domain controller or any other machine critical to your resource location infrastructure. Regular maintenance on the Cloud Connector performs machine operations that cause an outage to these additional resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Server clock is set to the correct UTC time.
- If you are using the graphical installer, you must have a browser installed and the default system browser set.
- The Cloud Connector installer is downloaded from Citrix Cloud so your browser must allow downloading executable files.

Windows Update guidance

Citrix strongly recommends enabling Windows Update on all machines hosting the Cloud Connector, including the "Install updates for other Microsoft products"policy. The Cloud Connector performs regular checks for pending reboots, which can be triggered by various factors, including Windows Updates, every five minutes. Any detected reboot is promptly executed, irrespective of the preferred day schedule set on the Resource location. This proactive approach ensures that the Cloud Connector isn't left in a pending update state for an extended period, thereby maintaining system stability.

Citrix Cloud manages restarts to maintain availability, permitting only one Cloud Connector to restart at a time. When setting up Windows Update, ensure that Windows is set to automatically download and install updates during non-business hours. However, the automatic restarts are not allowed for at least four hours to allow the Cloud Connector ample time to manage the restart process. Additionally, you can establish a fallback restart mechanism using Group Policy or a system management tool for situations where a machine must be restarted following an update. For more information, see Manage device restarts after updates.

> **Note:**
>
> - If the customer does not intend their Cloud Connector to reboot during business hours, we suggest that the customer schedule Windows Updates accordingly outside of business hours.
> - Each Cloud Connector requires approximately 10 minutes to reboot, and this includes the time needed to synchronize with the Citrix Cloud Platform to ensure that only one Cloud Connector reboots at any given point of time. Hence, the recommended minimum delay of four hours for automatic restarts, as mentioned earlier, can be adjusted accordingly to a lesser or greater duration depending on the number of Cloud Connectors in the tenant.

Antivirus configuration

The article Tech Paper: Endpoint Security, Antivirus, and Antimalware Best Practices provides guidelines to help you determine the appropriate balance between security and performance for the Cloud Connectors in your environment. Citrix strongly recommends reviewing these guidelines with your organization's antivirus and security teams, and performing rigorous lab-based testing before applying them to a production environment.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Certificate validation requirements

The Cloud Connector depends on X.509 certificates to validate the integrity of software packages it installs and Citrix Cloud endpoints that it contacts. These certificates are issued by widely respected enterprise certificate authorities (CAs).

To perform this validation, Cloud Connectors have the following requirements:

- The root certificates must be present in the host certificate store.
- The intermediate certificates must be present in the host certificate store.
- The Cloud Connector must be able to verify the certificate's Certificate Revocation List (CRL).

For complete instructions for downloading and installing the certificates, see CTX223828.

Root Certificate Requirements

The following root certificates must be installed on Cloud Connector hosts:

- https://cacerts.digicert.com/DigiCertGlobalRootG3.crt
- https://cacerts.digicert.com/DigiCertGlobalRootG2.crt
- https://cacerts.digicert.com/DigiCertGlobalRootCA.crt
- https://cacerts.digicert.com/DigiCertTrustedRootG4.crt
- https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt
- https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_2009.crt
- https://www.microsoft.com/pkiops/certs/Microsoft%20RSA%20Root%20Certificate%20Authority%202017.crt
- https://www.microsoft.com/pkiops/certs/Microsoft%20EV%20ECC%20Root%20Certificate%20Authority%202017.crt
- https://www.microsoft.com/pkiops/certs/Microsoft%20ECC%20Root%20Certificate%20Authority%202017.crt

Root certificates are usually packaged as part of the Operating System or distributed by the Windows Root Certificate Program, unless:

- The Turn off Automatic Root Certificate Update group policy is in place to block the root certificate update; and
- Connectivity from the Connector host server to the internet is restricted, preventing the update from being downloaded

If any certificate is missing, the Cloud Connector installer will attempt to download it from http://cacerts.digicert.com.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Where this is not possible, the root certificates will need to be manually installed on all Cloud Connector hosts.

Intermediate Certificate Requirements

The following intermediate certificates must be installed on Cloud Connector hosts:

- https://cacerts.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA3842021.crt

Intermediate certificates are usually downloaded on demand when the server is presented with a certificate issued by an intermediate authority that is missing from the Windows Certificate store.

If connectivity from the connector host server to the internet is restricted, this download may not happen. In these cases the intermediate certificates will need to be manually installed on all Cloud Connector hosts.

Certificate Revocation List (CRL) Requirements

It is important to verify that certificates used to validate components have not been compromised. This is implemented with Certificate Revocation Lists (CRLs). When a client uses a certificate to validate the integrity of a file or endpoints, the client checks whether it trusts the CA that issued the certificates and whether the certificate has been revoked. If the certificate is on a CRL, the certificate is revoked and cannot be trusted.

The CRL servers use HTTP on port 80 instead of HTTPS on port 443. Cloud Connector components, themselves, do not communicate over external port 80. The need for external port 80 is a byproduct of the certificate verification process that the operating system performs.

The following CRL endpoints must be available for the Cloud Connector to contact on HTTP port 80:

- http://cacerts.digicert.com/
- http://dl.cacerts.digicert.com/
- http://crl3.digicert.com
- http://crl4.digicert.com
- http://ocsp.digicert.com
- http://www.d-trust.net
- http://root-c3-ca2-2009.ocsp.d-trust.net
- http://crl.microsoft.com
- http://oneocsp.microsoft.com
- http://ocsp.msocsp.com

For more information about how to test for CRL and OCSP connectivity, see https://www.digicert.com/kb/util/utility-test-ocsp-and-crl-access-from-a-server.htm.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Customer Managed Certificates

In addition to the Citrix-managed certificates required for communicating with Citrix Cloud services, customers can deploy additional certificates on Cloud Connectors to secure communication with other on-premises components. These certificates will be customer-managed and need to be monitored and renewed by the customer.

The following table provides a summary of the communication flows which can be secured with customer-managed certificates.

Component	Traffic Flow from Connector	Further Documentation
StoreFront	Inbound	HTTPS Configuration
NetScaler® Gateway	Inbound	HTTPS Configuration
Hypervisor	Outbound	Securing connections to the VMware Environment

Citrix DaaS

Utilizing the Cloud Connector for connectivity to DaaS resources necessitates the installation of additional certificates and granting access to extended PKI infrastructure. Each Cloud Connector machine is required to fulfill the following requirements:

- HTTP port 80 is open to the following addresses:
  - `crl.*.amazontrust.com`
  - `ocsp.*.amazontrust.com`
  - `*.ss2.us`
- Communication with the following addresses is enabled
  - `https://*.amazontrust.com`
  - `https://*.ss2.us`
- The following root certificates are installed:
  - `https://www.amazontrust.com/repository/AmazonRootCA1.cer`
  - `https://www.amazontrust.com/repository/AmazonRootCA2.cer`
  - `https://www.amazontrust.com/repository/AmazonRootCA3.cer`
  - `https://www.amazontrust.com/repository/AmazonRootCA4.cer`
  - `https://www.amazontrust.com/repository/SFSRootCAG2.cer`
- The following intermediate certificates are installed:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- https://www.amazontrust.com/repository/G2-RootCA4.orig.cer
- https://www.amazontrust.com/repository/R3-ServerCA3A.cer
- https://www.amazontrust.com/repository/SFC2CA-SFSRootCAG2.cer
- https://www.amazontrust.com/repository/SFC2CA-SFSRootCAG2.v2.cer
- https://www.amazontrust.com/repository/G2-RootCA1.orig.cer
- https://www.amazontrust.com/repository/R1-ServerCA1A.cer
- https://www.amazontrust.com/repository/G2-RootCA3.cer
- https://www.amazontrust.com/repository/R3-ServerCA3A.orig.cer
- https://www.amazontrust.com/repository/G2-RootCA2.orig.cer
- https://www.amazontrust.com/repository/G2-RootCA4.cer
- https://www.amazontrust.com/repository/R2-ServerCA2A.cer
- https://www.amazontrust.com/repository/R4-ServerCA4A.cer
- https://www.amazontrust.com/repository/R1-ServerCA1A.orig.cer
- https://www.amazontrust.com/repository/G2-RootCA1.cer
- https://www.amazontrust.com/repository/G2-RootCA2.cer
- https://www.amazontrust.com/repository/G2-RootCA3.orig.cer
- https://www.amazontrust.com/repository/R4-ServerCA4A.orig.cer
- https://www.amazontrust.com/repository/G2-ServerCA0A.cer
- https://www.amazontrust.com/repository/G2-ServerCA0A.orig.cer
- https://www.amazontrust.com/repository/SFSRootCA-SFSRootCAG2.cer

If any certificate is missing, the Cloud Connector will download it from https://www.amazontrust.com

For complete instructions for downloading and installing the certificates, see CTX223828.

Active Directory requirements

- The server must be joined to an Active Directory domain that contains the resources and users that you use to create offerings for your users. For multi-domain environments, see Deployment scenarios for Cloud Connectors in Active Directory.
- Each Active Directory forest you plan to use with Citrix Cloud must always be reachable by two Cloud Connectors.
- The Cloud Connector must be able to reach domain controllers in both the forest root domain and in the domains that you intend to use with Citrix Cloud. For more information, see the following Microsoft support articles:
  - How to configure domains and trusts

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - “Systems services ports”section in Service overview and network port requirements for Windows
- Use universal security groups instead of global security groups. This configuration ensures that user group membership can be obtained from any domain controller in the forest.

Supported Active Directory functional levels

The Cloud Connector supports the currently supported Microsoft versions and functional levels.

> **Note:**
>
> Windows Server 2025 functional level is only supported with Database 32k pages disabled.

Network requirements

- Connected to a network that can contact the resources you use in your resource location. For more information, see Cloud Connector Proxy and Firewall Configuration.
- Connected to the Internet. For more information, see the following sections in System and Connectivity Requirements:
    - Cloud Connector common service connectivity requirements
    - Allowed FQDNs for Cloud Connector

Federal Information Processing Standard (FIPS) support

The Cloud Connector supports the FIPS-validated cryptographic algorithms that are used on FIPS-enabled machines.

Citrix Cloud Connector™ Technical Details

July 17, 2026

The Citrix Cloud™ Connector is a component that establishes a connection between Citrix Cloud and your resource locations. This article describes deployment requirements and scenarios, Active Directory and FIPS support, and troubleshooting options.

System requirements

See System requirements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cloud Connector installed services

This section describes the services that are installed with the Cloud Connector and their system privileges.

During installation, the Citrix Cloud Connector executable installs and sets the necessary service configuration to the default settings required to function. If the default configuration is manually altered, the Cloud Connector might not perform as expected. In this case, the configuration resets to the default state when the next Cloud Connector update occurs, assuming the services that handle the update process can still function. At times, services are released in a 'disabled' state to support the addition or removal of services.

Citrix Cloud Agent System facilitates all elevated calls necessary for the other Cloud Connector services to function and does not communicate on the network directly. When a service on the Cloud Connector needs to perform an action requiring Local System permissions, it does so through a predefined set of operations that the Citrix Cloud Agent System can perform.

Service Name	Description	Runs As
Citrix Cloud Agent System	Handles the system calls necessary for the on-premises agents. Includes installation, reboots, and registry access. Can only be called by Citrix Cloud Services Agent WatchDog.	Local System
Citrix Cloud Services Agent WatchDog	Monitors and upgrades the on-premises agents (evergreen).	Network Service
Citrix Cloud Services Agent Logger	Provides a support logging framework for the Citrix Cloud Connector services.	Network Service
Citrix Cloud Services AD Provider	Enables Citrix Cloud to facilitate management of resources associated with the Active Directory domain accounts in which it is installed.	Network Service

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service Name	Description	Runs As
Citrix Cloud Services Agent Discovery	Enables Citrix Cloud to facilitate management of XenApp and XenDesktop® legacy on-premises Citrix products.	Network Service
Citrix Cloud Services Credential Provider	Handles storage and retrieval of encrypted data.	Network Service
Citrix Cloud Services WebRelay Provider	Enables HTTP Requests received from WebRelay Cloud service to be forwarded to On-Premises Web Servers.	Network Service
Citrix CDF Capture Service	Captures CDF traces from all configured products and components.	Network Service
Citrix Config Synchronizer Service	Copies brokering configuration locally for high availability mode.	Network Service
Citrix Connection Lease Exchange Service	Enables Connection Lease files to be exchanged between Workspace app and Cloud Connector for Service Continuity for Citrix® StoreFront Cloud	Network Service
Citrix High Availability Service	Provides continuity of service during outage of central site.	Network Service
Citrix ITSM Adapter Provider	Automates provisioning and management of virtual apps and desktops.	Network Service
Citrix NetScaler® CloudGateway	Provides Internet connectivity to on-premises desktops and applications without the need to open in-bound firewall rules or deploying components in the DMZ.	Network Service
Citrix Remote Broker Provider	Enables communication to a remote Broker Service from local VDAs and StoreFront™ servers.	Network Service

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service Name	Description	Runs As
Citrix Remote HCL Server	Proxies communications between the Delivery Controller™ and the Hypervisors.	Network Service
Citrix WEM Cloud Authentication Service	Provides authentication service for Citrix WEM agents to connect to cloud infrastructure servers.	Network Service
Citrix WEM Cloud Messaging Service	Provides service for Citrix WEM cloud service to receive messages from cloud infrastructure servers.	Network Service
Citrix Secure Private Access™	Zero Trust Network Access to all enterprise applications	Network Service
Citrix Cloud Services Message Broker	Handles messages between Citrix Cloud providers and Citrix Cloud services	Network Service
Citrix Secure Ticketing Authority Service	Provides secure ticketing authority for Citrix Cloud services	Network Service
Citrix Monitor Service	Enables Citrix Monitor cloud service to monitor and communicate with on-premises Citrix components	Network Service

Deployment scenarios for Cloud Connectors in Active Directory

You can use both Cloud Connector and Connector Appliance to connect to Active Directory controllers. The type of connector to use depends on your deployment.

For more information about using Connector Appliances with Active Directory, see Deployment scenarios for Connector Appliances in Active Directory

Install Cloud Connector within your secure, internal network.

If you have a single domain in a single forest, installing Cloud Connectors in that domain is all you need to establish a resource location. If you have multiple domains in your environment, you must consider where to install the Cloud Connectors so your users can access the resources you make available.

If the trust between the domains is not Parent/Child, you might have to install Cloud Connectors for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

each separate domain or forest. This configuration might be required to handle resource enumeration when using security groups to assign resources or for registrations for VDAs from either domain.

> **Note:**
>
> The below resource locations form a blueprint that you might have to repeat in other physical locations depending on where your resources are hosted.

Single domain in a single forest with a single set of Cloud Connectors

In this scenario, a single domain contains all the resource and user objects (forest1.local). One set of Cloud Connectors is deployed within a single resource location and joined to the forest1.local domain.

- Trust relationship: None - single domain
- Domains listed in **Identity and Access Management**: forest1.local
- User logons to cloud stores: Supported for all users
- User logons to on-premises stores: Supported for all users

> **Note:**
>
> If you have a hypervisor instance in a separate domain, you can still deploy a single set of Cloud Connectors as long as the hypervisor instance and the Cloud Connectors are reachable through the same network. Citrix Cloud uses the hosting connection and an available network to establish communication with the hypervisor. So, even though the hypervisor resides in a different domain, you don't need to deploy another set of Cloud Connectors in that domain to ensure that Citrix Cloud can communicate with the hypervisor.

Parent and child domains in a single forest with a single set of Cloud Connectors

In this scenario, a parent domain (forest1.local) and its child domain (user.forest1.local) reside within a single forest. The parent domain acts as the resource domain and the child domain is the user domain. One set of Cloud Connectors is deployed within a single resource location and joined to the forest1.local domain.

- Trust relationship: Parent/child domain trust
- Domains listed in **Identity and Access Management**: forest1.local, user.forest1.local
- User logons to cloud stores: Supported for all users
- User logons to on-premises stores: Supported for all users

> **Note:**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> You might need to restart the Cloud Connectors to ensure Citrix Cloud registers the child domain.

Users and resources in separate forests (with trust) with a single set of Cloud Connectors

In this scenario, one forest (forest1.local) contains your resource domain and one forest (forest2.local) contains your user domain. A one-way trust exists where the forest containing the resource domain trusts the forest containing the user domain. One set of Cloud Connectors is deployed in a single resource location and joined to the forest1.local domain.

- Trust relationship: One-way forest trust
- Domains listed in **Identity and Access Management**: forest1.local
- User logons to cloud stores: Supported for forest1.local users only
- User logons to on-premises stores: Supported for all users

> **Note:**
>
> The trust relationship between the two forests needs to permit the user in the user forest to be able to log on to machines in the resource forest.

Because Cloud Connectors can't traverse forest-level trusts, the forest2.local domain is not displayed on the **Identity and Access Management** page in the Citrix Cloud console and can't be used by any cloud-side functionality. This carries the following limitations:

- Resources can only be published to users and groups located in forest1.local in Citrix Cloud. However, if you're using on-premises stores, forest2.local users may be nested into forest1.local security groups to mitigate this issue.
- Cloud stores can't authenticate users from the forest2.local domain.
- The Monitor console in Citrix DaaS can't enumerate the users from the forest2.local domain.

To work around these limitations, deploy the Cloud Connectors as described in Users and resources in separate forests (with trust) with a set of Cloud Connectors in each forest.

Users and resources in separate forests (with trust) with a set of Cloud Connectors in each forest

In this scenario, one forest (forest1.local) contains your resource domain and one forest (forest2.local) contains your user domain. A one-way trust exists where the forest containing the resource domain trusts the forest containing the user domain. One set of Cloud Connectors is deployed within the forest1.local domain and a second set is deployed within the forest2.local domain.

- Trust relationship: One-way forest trust
- Domains listed in **Identity and Access Management**: forest1.local, forest2.local

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- User logons to cloud stores: Supported for all users
- User logons to on-premises store: Supported for all users

In this scenario Connector Appliances can been used in place of Cloud Connectors in user forests with no resources to reduce cost and management overheads, particularly if there are multiple user forests. For more information see Users and resources in separate forests (with trust) with a single set of Connector Appliances for all forests

View the health of the Cloud Connector

The Resource Locations page in Citrix Cloud displays the health status of all the Cloud Connectors in your resource locations. You can also view advanced health check data for each individual Cloud Connector. For more information, see Cloud Connector advanced health checks.

Windows event logs

The Cloud Connector generates certain Windows event logs that you can view through the Windows Event Viewer. If you want to enable your preferred monitoring software to look for these logs, you can download them as a ZIP archive. The ZIP download includes these logs in the following XML files:

- Citrix.CloudServices.Agent.Core.dll.xml (Connector Agent Provider)
- Citrix.CloudServices.AgentWatchDog.Core.dll.xml (Connector AgentWatchDog Provider)

Citrix.CloudSerivces.AgentWatchDog During normal operations, the following events can occur:

Event ID	Event	Description
10000	ConnectedToMessagingService	This event is raised when the Connector establishes its long-lived, outbound websocket connection with Citrix Cloud, allowing a two-way communication with Citrix Cloud.
10001	ConnectedToMessagingServiceWithWebProxy	Connected to messaging service through web proxy with address "{0}". The websocket connection was set up using the configured proxy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event ID	Event	Description
10002	UnableToConnectToMessagingService	Unable to connect to messaging service “{0}”. The Cloud Connector was unable to establish its websocket to Citrix Cloud.
10003	UnableToConnectToMessagingServiceWithWebProxy	Unable to connect to messaging service through web proxy with address “{0}”. The Cloud Connector was unable to establish its websocket to Citrix Cloud when using the configured proxy.
10004	ClockOutOfSyncError	There was a problem communicating with Citrix Cloud. Ensure that the clock on this machine has the correct time and timezone (UTC). You might need to restart the machine to resolve the issue.
10005	ConnectivityCheckHealthyToFailedStatus	The Cloud Connector’s hourly health check reported a failure after previously being healthy.
10006	ConnectivityCheckFailedStatus	The Cloud Connector’s hourly health check reported a failure, having also experienced a failure in the past.
10007	ConnectivityCheckFailedToHealthyStatus	The Cloud Connector’s hourly health check reported a healthy status after previously experiencing a failure.
10008	ConnectivityCheckHealthyStatus	The Cloud Connector’s hourly health check reported a healthy status after previously being healthy.

Citrix.CloudServices.Agent During normal operations, the following events can occur:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

10100	ConnectedToForest	Connected to the forest with a domain controller.
10101	UnableToConnectToForest	Unable to connect to the forest. Ensure that the host computer is joined to a domain and has network connectivity.
10102	UnableToConnectToForestWithDomainName	Unable to connect to the forest associated with the domain.
10103	ClockOutOfSyncError	There was a problem communicating with Citrix Cloud. Ensure that the clock on this machine has the correct time and timezone (UTC). You might need to restart the machine to resolve the issue.

For more information on Broker or LHC event logs, see Event logs

Download Cloud Connector event messages.

Connector log files

By default, event logs are located in the `C:\ProgramData\Citrix\WorkspaceCloud\Logs` directory of the machine hosting the Cloud Connector.

Troubleshooting

The first step in diagnosing any issues with the Cloud Connector is to check the event messages and event logs. If you don't see the Cloud Connector listed in your resource location or it is "not in contact," the event logs provide some initial information.

Cloud Connector connectivity

If the Cloud Connector is "disconnected,"the Cloud Connector Advanced Connectivity Check Tool can help verify that the Cloud Connector can reach Citrix Cloud and its related services.

For more information, see Cloud Connector Advanced Connectivity Check Tool.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Installation

If the Cloud Connector is in an "error"state, there might be a problem hosting the Cloud Connector. Install the Cloud Connector on a new machine. If the issue persists, contact Citrix Support. To troubleshoot common issues with installing or using the Cloud Connector, see CTX221535.

Cloud Connector Proxy and Firewall Configuration

September 6, 2025

The Cloud Connector supports connection to the Internet through an unauthenticated web proxy server. Both the installer and the services it installs need connections to Citrix Cloud.
Internet access needs to be available at both of these points.

Connectivity requirements

Use port 443 for HTTP traffic, egress only. For a list of required contactable addresses, see the following resources:

- System and Connectivity Requirements
- Cloud Connector common service connectivity requirements

The required contactable addresses for Citrix Cloud are specified as domain names, not IP addresses. Because IP addresses might change, allowing domain names ensures that the connection to Citrix Cloud remains stable.

For a list of required ports, see Inbound and outbound ports configuration.

> **Important:**
>
> - Enabling SSL interception on certain proxies might prevent the Cloud Connector from connecting successfully to Citrix Cloud.
> - SSL interception cannot be performed on Citrix Gateway addresses. For more information, see Citrix Gateway Services connectivity requirements.
> - SSL interception must not impact the network connectivity or stability. For more information, see Citrix Cloud Connector
> - If you are using a proxy, it is the following traffic flows must bypass the proxy:
>   - Communication between Connectors (for example, during LHC events).
>   - Communication between Connectors and VDA (WCF connection).
>   - Communication between Connectors and Domain Controllers (AD requests).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Furthermore, it is important to note that the connector utilizes the WinHTTP proxy settings. For configuration settings, see CTX222727.

Check Cloud Connector connectivity

The Cloud Connector Advanced Connectivity Check Tool can help verify connectivity between the Cloud Connector and Citrix Cloud using a series of connectivity checks.

For more information, see Cloud Connector Advanced Connectivity Check Tool.

Installer

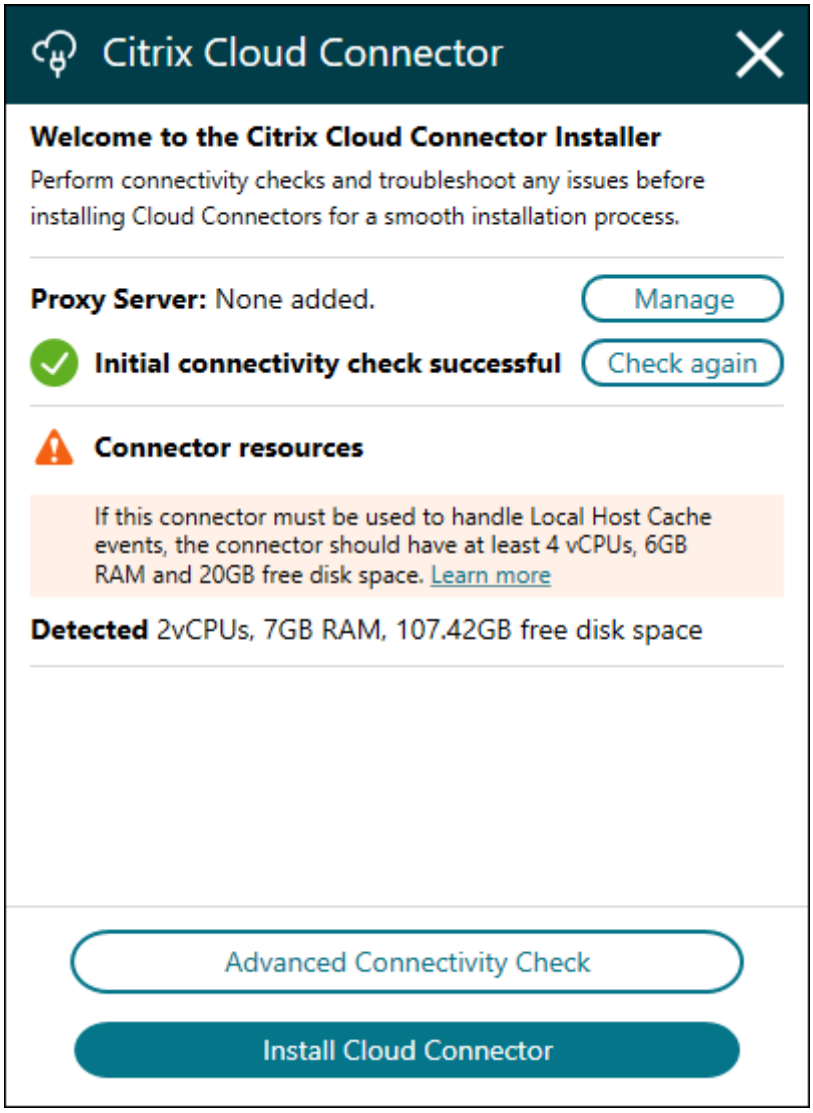
The installer uses the settings configured for Internet connections. If you can browse the Internet from the machine then the installer should also function.

Services at Runtime

The runtime service operates in the context of a local service. It does not use the settings defined for the user (as described above).

You can configure the proxy settings during the installation process.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



After the installer starts, before logging into Citrix Cloud, click **Configure Proxy**. You are prompted to add the proxy information and addresses to bypass the proxy. Both fully qualified domain names (FQDNs) and wildcard addresses are supported when specifying bypass addresses.

> **Note:**
>
> If you are using a proxy server, you must use manual proxy setup. Automatic proxy setup, through either automatic detection or PAC/setup scripts is not supported.

Cloud Connector Installation

September 28, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

You can install the Cloud Connector software interactively or using the command line.

The installation occurs with the privileges of the user who begins the install. The Cloud Connector requires access to the cloud to:

- Authenticate the user that performs the installation
- Validate the installer's permissions
- Download and configure the Cloud Connector services

Information to review before installation

Review the System requirements before installation.

Post-deployment guidance

After installation, keep all Cloud Connectors powered on continuously to ensure an always-on connection to Citrix Cloud.

Upgrades

Upgrades are normally automatically managed by Citrix Cloud. To do a manual upgrade, first uninstall the old Cloud Connector before installing the new version. Don't upgrade a previously installed Cloud Connector with a newer version. Do not upgrade individual components of the Cloud Connector separately.

Renaming machines

After installation, don't rename the machine hosting the Cloud Connector. If you need to change the server name later on, perform the following tasks:

1. Remove the machine from the resource location:
    a) From the Citrix Cloud menu, select **Resource Locations**.
    b) Locate the resource location you want to manage and then select the **Cloud Connectors** tile.
    c) Locate the machine you want to manage and then click the ellipsis menu. Select **Remove Connector**.
2. Uninstall the Cloud Connector software.
3. Rename the machine.
4. Install the latest version of the Cloud Connector software, as described in this article.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Moving machines to a different domain

After installation, don't move the machine hosting the Cloud Connector into a different domain. If you need to join the machine to a different domain later on, perform the following tasks:

1. Remove the machine from the resource location.
2. Uninstall the Cloud Connector software.
3. Unjoin the machine from its current domain and rejoin the machine to the new domain.
4. Install the latest version of the Cloud Connector software, as described in this article.

Considerations for cloned machines

Each machine hosting the Cloud Connector must have a unique SID and connector ID so that Citrix Cloud can communicate reliably with the machines in your resource location. If you intend to host the Cloud Connector on multiple machines in your resource location and you want to use cloned machines, perform the following steps:

1. Prepare the machine template according to the requirements for your environment.
2. Provision the number of machines that you intend to use as Cloud Connectors.
3. Install the Cloud Connector on each machine, either manually or using the silent installation mode.

Installing the Cloud Connector on a machine template (before cloning) isn't supported. If you clone a machine with the Cloud Connector installed, the Cloud Connector services won't run and the machine can't connect to Citrix Cloud.

Considerations for services

The installation steps in this article describe the process for deploying Cloud Connectors, regardless of the service for which they are used.

When deploying Cloud Connectors for Citrix DaaS, verify that the AD domains where the connectors reside are active and are not showing as "unused"in the Citrix Cloud console. If you specify an unused domain during machine catalog setup in Citrix DaaS, an error might occur. For more information, see Add a resource type or activate an unused domain in Citrix Cloud in the Citrix DaaS product documentation.

For additional considerations for other services, consult the service's documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Default resource locations

If you have no resource locations in your Citrix Cloud account and you install Cloud Connectors in your domain, the resource location that Citrix Cloud creates becomes the default resource location. You can have only one default resource location in your account. If needed, you can create additional resource locations in Citrix Cloud and then select the one you want when you install Cloud Connectors in other domains.

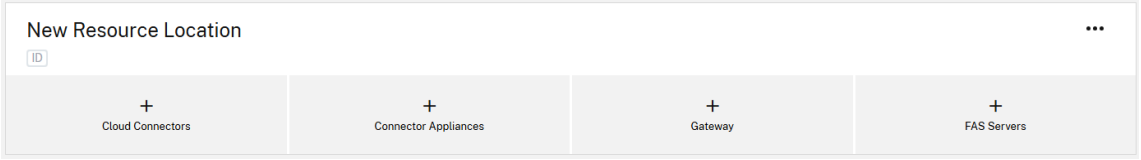
Alternatively, you can first create the resource locations you need in the console, before you install Cloud Connectors in your domains. The Cloud Connector installer prompts you to select the resource location you want during installation.

Interactive installation

You can download and install Cloud Connectors using the graphical installer interface. Before you do this, you must create one or more resource locations in the Citrix Cloud management console to deploy Cloud Connectors on. For more information on resource locations, see Resource locations.

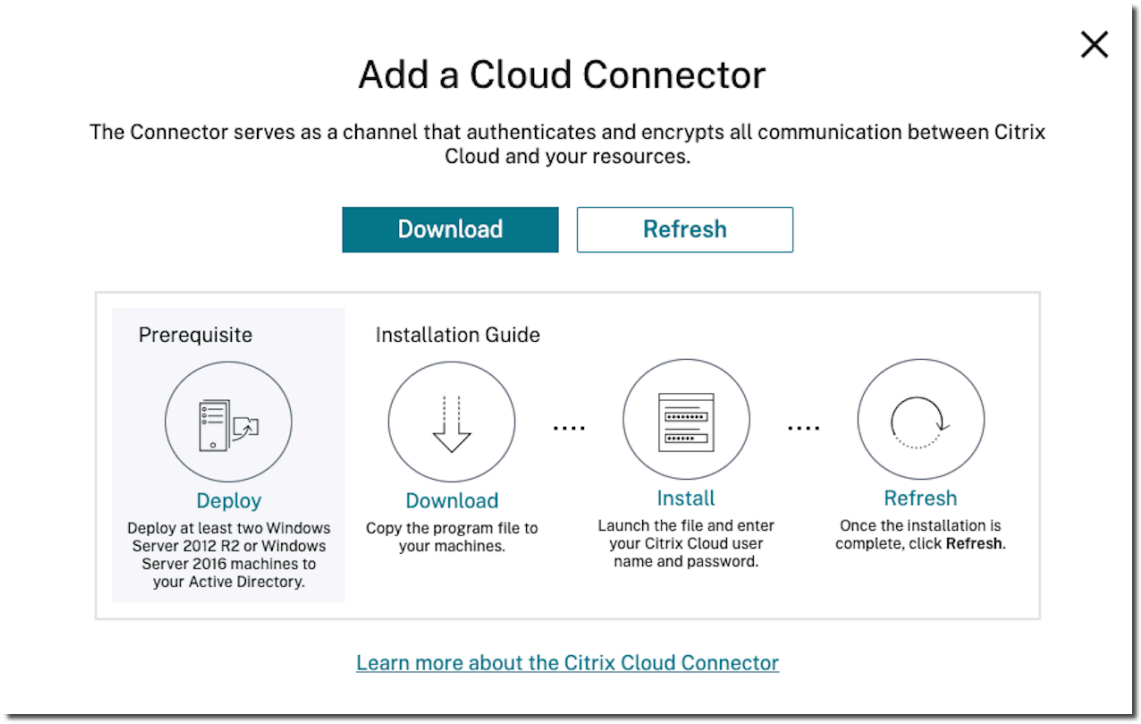
Download the Citrix Cloud Connector™ software

1. Sign in as a Windows administrator to the machine you intend to install Citrix Cloud Connectors on.
2. Visit https://citrix.cloud.com and sign in to your administrator account.
3. In the Citrix Cloud console, navigate to **Resource Locations** from the main menu.
4. If you do not already have a resource location, click the plus icon (+) or select **Add a Resource Location**. For more information, see create a resource location.
5. Locate the resource location you want to manage and select **+ Cloud Connectors**.



6. Select **Download** in the window that opens. Save the **cwcconnector.exe** file to a local file location on your connector machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

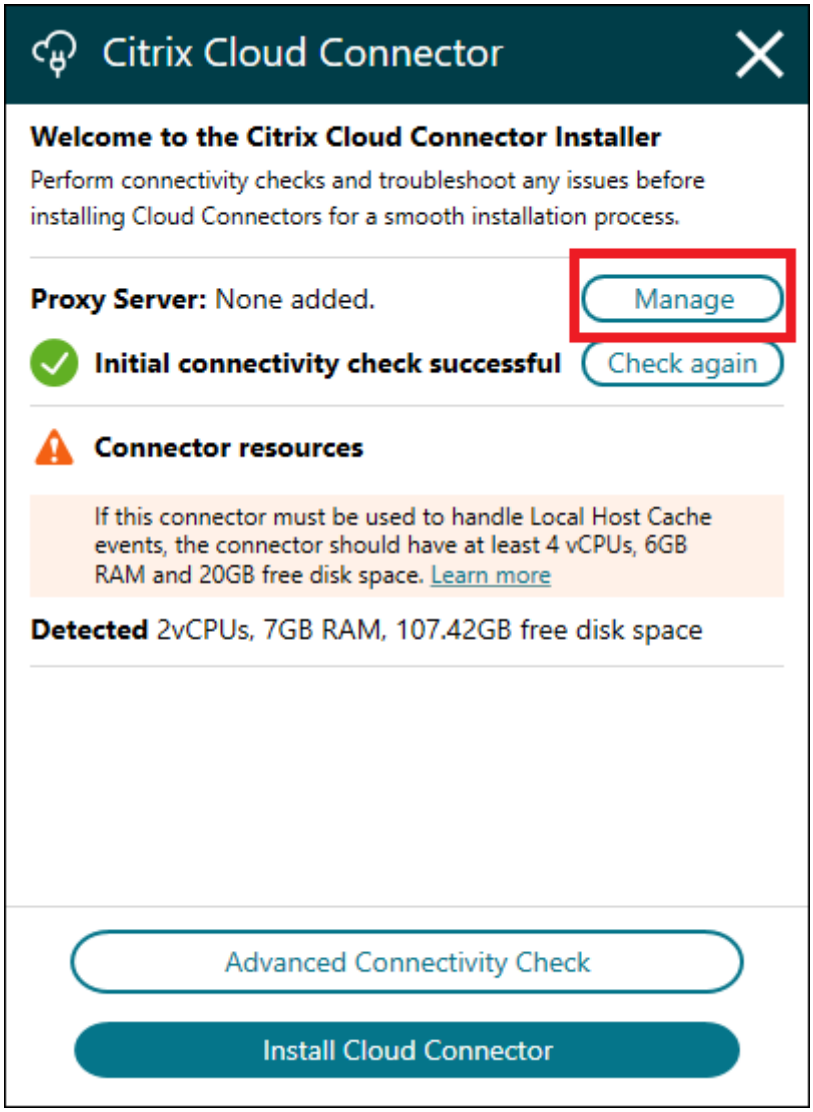


Install the Citrix Cloud Connector software

Prerequisites

1. Right-click on the `cwcconnector.exe` installer file and select **Run as administrator**. The installer performs an initial connectivity check to ensure you can connect to Citrix Cloud before installing the Cloud Connector.
2. Click **Manage** to update Proxy Server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

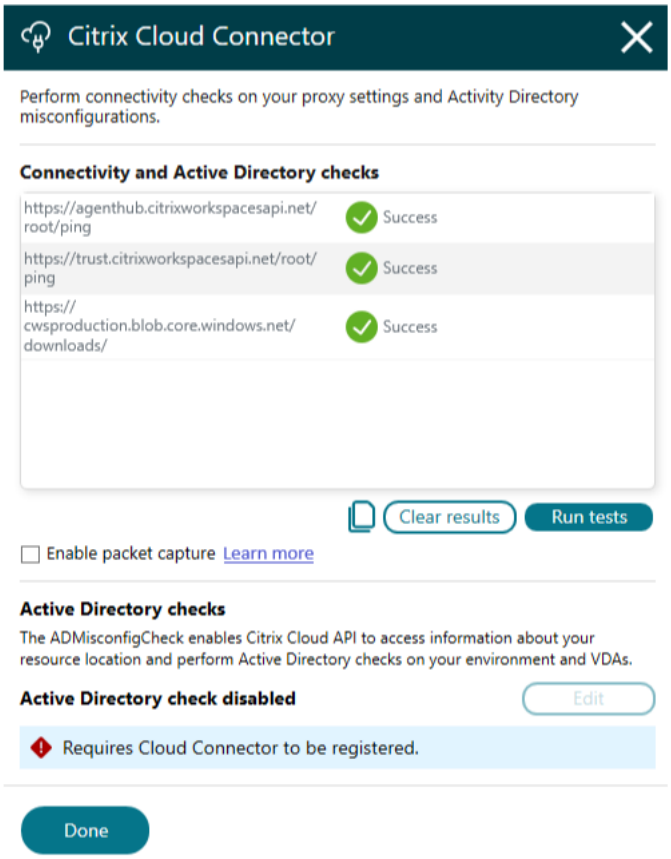


Note:

There is only one proxy server supported due to a limitation in Microsoft WinHTTP. For more information, see AutoProxy Issues in WinHTTP

1. Click **Advanced Connectivity Check** to run a verbose check to ensure that the basic connectivity requirements for Connector installation are met on the machine.

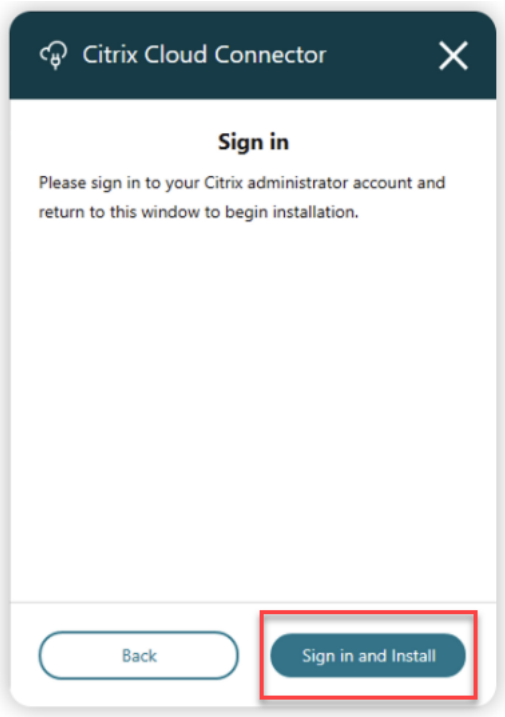
© 1997–2026 Citrix Systems, Inc. All rights reserved.



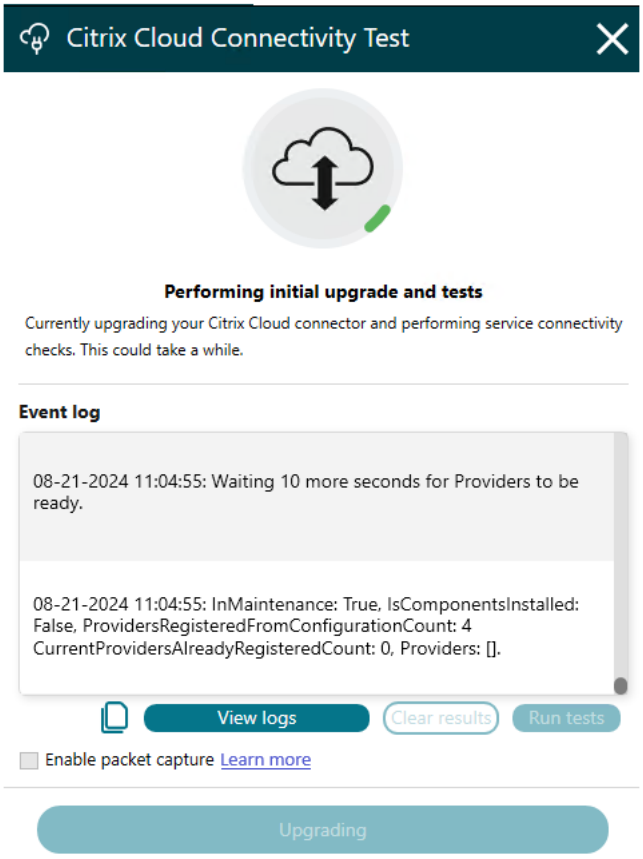
Initial upgrade and tests

1. After updating the **Proxy Server** and checking the **Advanced Connectivity Check**, click **Install Cloud Connector**.
2. On the **Sign-in** page, click **Sign in and Install**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

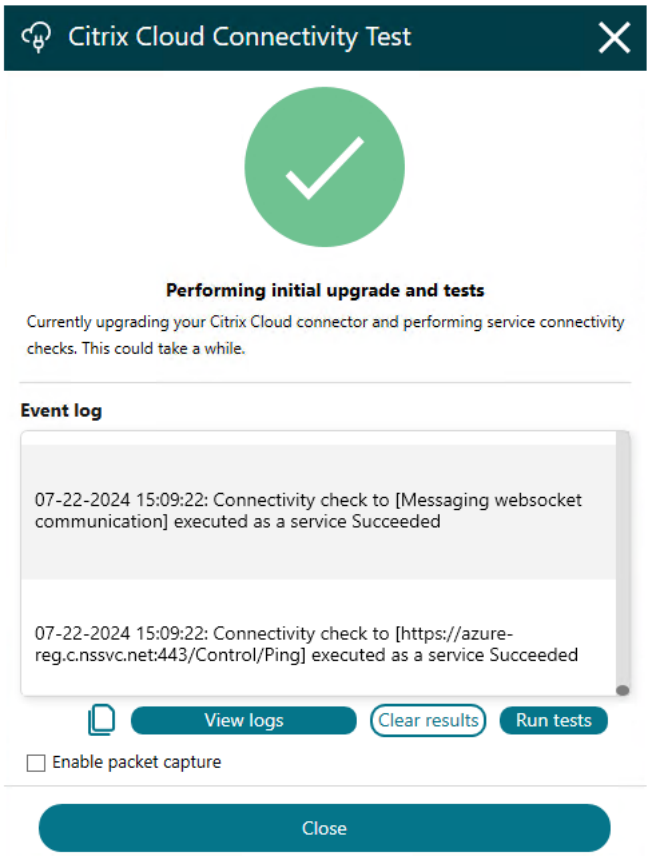


3. The **Citrix Cloud Connectivity Test** window appears and the status of the Initial upgrade and tests are displayed along with Event logs.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Click **View logs** to open the directory (`C:\ProgramData\Citrix\WorkspaceCloud\InstallLogs`) that includes all connectivity check debug logs.
5. Once the Initial upgrade and tests are completed, you'll see the Citrix Cloud Connectivity Test is **Successful** as shown in the following image. The connectivity check results are displayed in the Event log box after the first upgrade.



Activate unused domains

If you're creating resource locations and deploying Cloud Connectors for Citrix DaaS™, verify that the AD domains that you're using with Citrix DaaS are active and are not considered unused. If you specify an unused domain when setting up machine catalogs in Citrix DaaS, an error could occur.

For more information, see Add a resource type or activate an unused domain in Citrix Cloud in the Citrix DaaS product documentation.

Create additional resource locations

1. From the Citrix Cloud management console, click the menu button and select **Resource Locations**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click **+ Resource Location** and enter a meaningful name.
3. Click **Save**. Citrix Cloud displays a tile for the new resource location.
4. Click **Cloud Connectors** and then click **Download** to acquire the Cloud Connector software.
5. On each prepared machine, install the Cloud Connector software using either the installation wizard or the command-line installation. Citrix Cloud prompts you to select the resource location you want to associate with the Cloud Connector.

Installation with multiple customers and existing resource locations

If you're an administrator for multiple customer accounts, Citrix Cloud prompts you to select the customer account you want to associate with the Cloud Connector.

If your customer account has multiple resource locations already, Citrix Cloud prompts you to select the resource location you want to associate with the Cloud Connector.

Command-line installation

Silent or automated installation is supported. However, the connector installer is regularly updated and so it is recommended to download the latest installer for each installation. Download a new Cloud Connector installer from the Resource Locations page in the Citrix Cloud console.

Requirements

To use the command line installation with Citrix Cloud, you need to supply the following information:

- The customer ID of the Citrix Cloud account for which you are installing the Cloud Connector. This ID appears at the top of the **API Access** tab in **Identity and Access Management**.
- The ID and secret of the service principal you want to use to install the Cloud Connector. To acquire these values, you must first create a service principal. The service principal must be created with "Full Access". For more information on creating a service principal, see Create a Service Principal. Once you have the ID and secret of the service principal you can continue with Cloud Connector installation.
- The resource location ID for the resource location that you want to associate with the Cloud Connector. To retrieve this value, select the **ID** button located beneath the resource location name on the **Resource Locations** page. If you don't supply this value, Citrix Cloud uses the ID of the default resource location.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Supported parameters

To ensure the security of the service principal ID and secret, a JSON configuration file must be provided to the installer. This file must be deleted after the installation has completed. Supported values for the configuration file are:

- **customerName** Required. The customer ID shown on the API Access page in the Citrix Cloud console (within Identity and Access Management).
- **clientId** Required. The service principal ID an administrator can create, located on the API Access page.
- **clientSecret** Required. The service principal secret that can be downloaded after the service principal is created. Located on the API Access page.
- **resourceLocationId** Recommended. The unique identifier for an existing resource location. Select the ID button to retrieve the resource location ID on the Resource Locations page in the Citrix Cloud console. If no value is specified, Citrix Cloud uses the ID of the first resource location in the account.
- **acceptTermsOfService** Required. Must be set to **true**.

Sample configuration file

```
{

"customerName": "CustomerID",
"clientId": "clientID",
"clientSecret": "ClientSecret",
"resourceLocationId": "ResourceLocationId",
"acceptTermsOfService": "true"
 }
```

Sample command

The following command silently installs the Cloud Connector software using a JSON configuration file:

```
CWCConnector.exe /q /ParametersFilePath:c:\cwcconnector_install_params.
   json
```

Use `/q` to specify a silent install.

Use **Start /Wait CWCConnector.exe /ParametersFilePath:value** to examine a potential error code in the case of a failure. You can use the standard mechanism of running **echo %ErrorLevel%** after the installation completes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

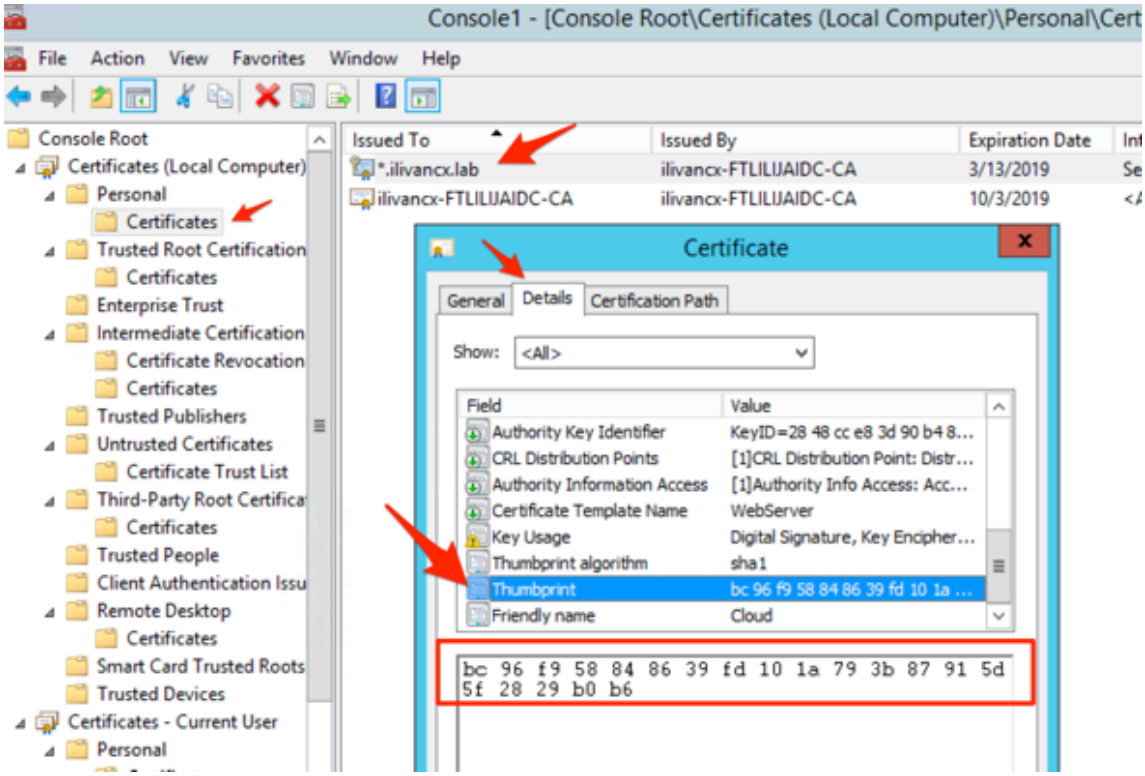
HTTPS Configuration

To allow StoreFront™ and NetScaler Gateway appliances to securely connect to the Cloud Connector and encrypt all data, it is strongly recommended that you enable HTTPS. This requires an SSL certificate.

- The certificate must include the FQDN used to reach the connector as the Common Name or Subject Alternative Name. If you have deployed a load balancer in front of the connector then use the load balancer's FQDN.
- The certificate can be signed by an enterprise CA or public CA.
- Any StoreFront and gateway servers that connect to the Cloud Connector must trust the certificate.

To enable HTTPS:

1. Open the Certificates MMC snap-in.
2. Create or import a suitable certificate in the Personal Certificates store. For more information on managing certificates, see Manage certificates.
3. Open the certificate, go to the **Details** tab and take a note of the **Thumbprint**, ignoring any spaces.



4. Determine which IP address to bind the certificate to. Normally you can use IP address of `0.0.0.0` to apply to all IPv4 addresses. If IPv6 is enabled then use `[::]` to apply to all IPv6

© 1997–2026 Citrix Systems, Inc. All rights reserved.

addresses. If you only want to apply the change to a specific network adapter then make a note of the IP address of the network adapter.

5. In an elevated command prompt run

```
netsh http add sslcert ipport=<IP address>:<Port number> certhash
   =<Certificate Hash Number> appid={
 Any GUID }
```

You can use any valid GUID for the AppId. It's purpose is to record which application added the binding. However the binding applies to all applications using that port.

For example:

```
C:\> netsh http add sslcert ipport=0.0.0.0:443 certhash=
   BC96F958848639FD101A793B87915D5F2829B0B6 appid={
 6DE9BEFD-F4CB-4D63-8681-E88012D6F5F1 }


SSL Certificate successfully added
```

6. To disable HTTP, in the registry go to `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\DesktopServer` and create a `DWORD` with name `XMLServicesEnableNonSSL` and value 0.

Next steps

1. Set up the Citrix Cloud Connector update schedule. For information on Citrix Cloud Connector updates and managing update schedules, visit Connector updates.
2. If you are using StoreFront, configure StoreFront so it can use the connector to reach DaaS to enumerate and launch resources. If this is the first connector in a new DaaS deployment then create a new resource feed. If this is an additional connector then it is recommended for resiliency that you add all Cloud Connectors to the server list for your existing DaaS resource feed. For more information, see Manage the resources made available in stores.
3. If you are using StoreFront with a NetScaler gateway, you can use the connector to reach the Citrix Cloud Secure Ticket Authority (STA). For more information, see Configure Citrix Gateways.
4. If this is the first connector on a particular Active Directory domain then you can connect that domain to Citrix Cloud. For more information, see To connect your Active Directory to Citrix Cloud.

Troubleshooting installation issues

This section details some ways of diagnosing and fixing problems you might encounter during installation. For more guidance about troubleshooting installation issues, see the Citrix Cloud Connector

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting Guide.

Installation logs

You can troubleshoot issues encountered with installation by first consulting the available log files.

Events that occurred during installation are available in the **Windows Event Viewer**. You can also review Cloud Connector installation logs, which are located at **%LOCALAPPDATA%\Temp\CitrixLogs\CloudServices**. Logs are also added to **%ProgramData%\Citrix\WorkspaceCloud\InstallLogs** after installation.

Exit codes

The following exit codes might be returned depending on the success or failure of the installation process:

- 1603 - An unexpected error occurred
- 2 - A prerequisite check failed
- 0 - Installation completed successfully

Installation error

If you install the Citrix Cloud Connector software by double-clicking the installer, you might receive the following error message:

```
Can't reach this page.
```

This error can occur even if you are logged in to the machine as an administrator to install the Citrix Cloud Connector. To avoid this error, run the Citrix Cloud Connector software as an administrator by right-clicking the installer and selecting Run as administrator.

Connectivity failures

To ensure that the Cloud Connector can communicate with Citrix Cloud, confirm that the following Citrix services are in a **Started** state:

- Citrix Cloud AD Provider
- Citrix Cloud Agent Logger
- Citrix Cloud Agent System
- Citrix Cloud Agent Watchdog
- Citrix Cloud Credential Provider
- Citrix Config Synchronizer Service

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix High Availability Service
- Citrix NetScaler® CloudGateway
- Citrix Remote Broker Provider
- Citrix Remote HCL Server
- Citrix Session Manager Proxy

For more information about these services, see Installed Services.

The Cloud Connector Advanced Connectivity Check Tool can help verify that the Cloud Connector can reach Citrix Cloud and its related services.

For more information, see Cloud Connector Advanced Connectivity Check Tool.

For more information on how to resolve a failed connectivity check, see CTX224133: Cloud Connector Connectivity Check Failed.

Cloud Connector Advanced Connectivity Checks

July 21, 2026

The Cloud Connector packages two tools to assist admins in diagnosing and troubleshooting connectivity issues. These are the `Advanced Connectivity Checks` available in the Cloud Connector Installer, and the `Citrix Cloud Services Connectivity Test Tool` installed alongside the Cloud Connector software.

Both tools include tests for:

- Proxy and Firewall configuration in line with the Cloud Connector connectivity requirements
- Certificate requirements in line with the Certificate Validation Requirements

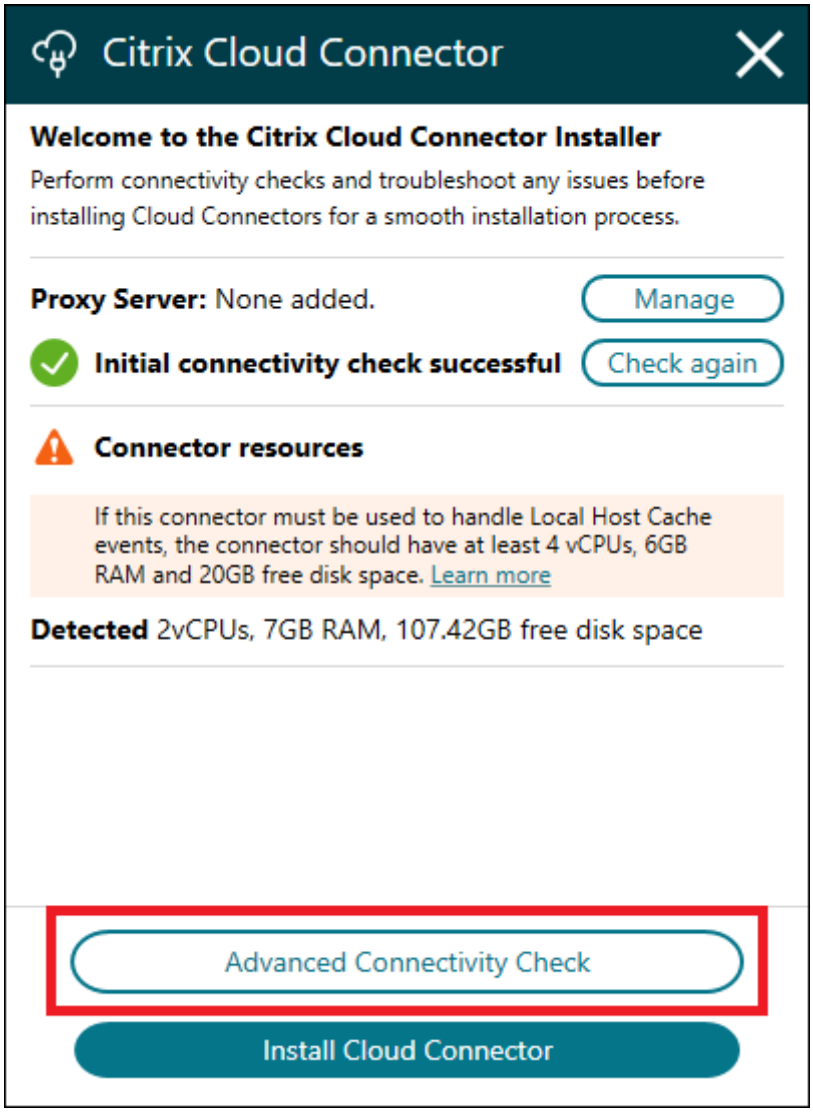
The tools can also be used to perform network packet capture to aid in diagnosing and troubleshooting connectivity issues.

Cloud Connector Installer Advanced Connectivity Checks

The `Advanced Connectivity Checks` are included in the Cloud Clonnecter `cwcconnector.exe` installer.

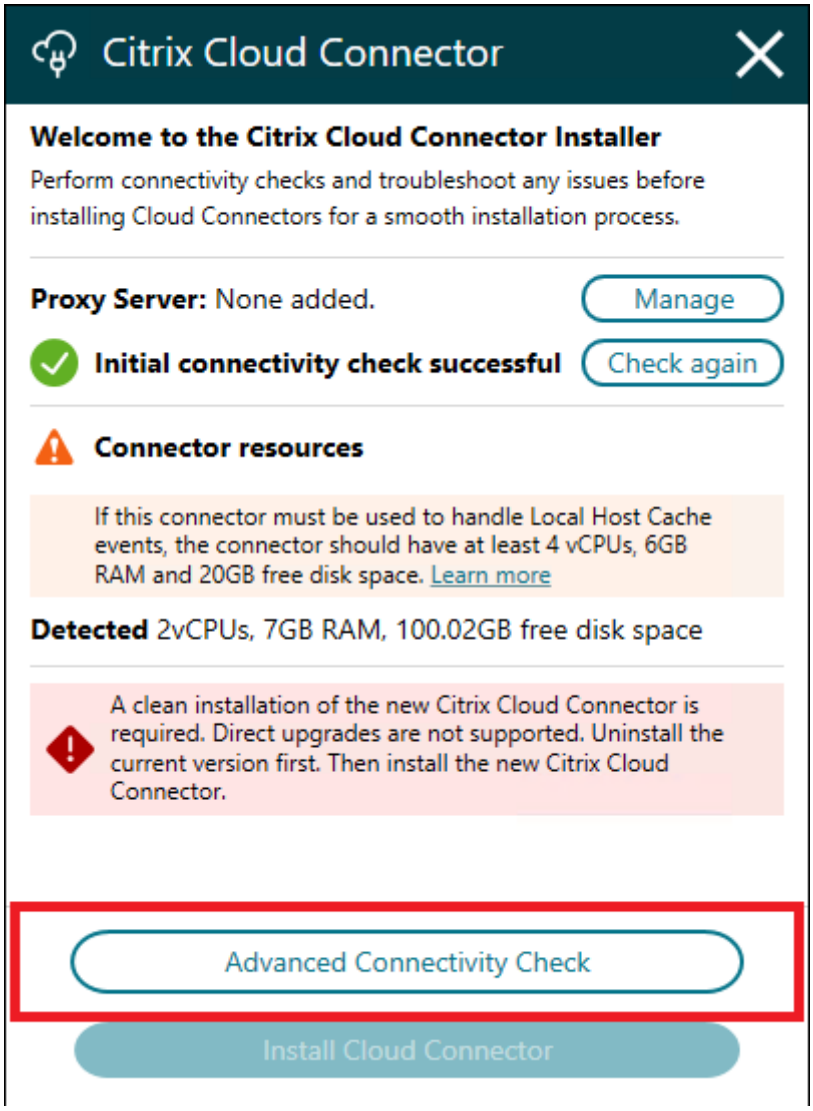
To access the checks, right-click on the `cwcconnector.exe` installer file and select run as administrator. The Advanced Connectivity Check Tool can then be accessed by clicking "Advanced Connectivity Check".

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If the Cloud Connector software has already been installed on the host machine then there will be a warning and the `Install Cloud Connector` option disabled, however the "Advanced Connectivity Check"option will still be available.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Checks Performed by the Installer Advanced Connectivity Check

The checks performed by the Advanced Connectivity Check tool are grouped into three categories.

- **Initial Checks:** These are the checks for the platform services required to install and register the Cloud Connector. They cover connectivity to the services related to Cloud Connector orchestration, authentication, and upgrades.
- **Certificate Checks:** These tests validate the presence of necessary root and intermediate certificates in order to validate secure connectivity to Citrix Cloud (TLS Certificates) and check the integrity of upgrade packages (code signing certificates). See Certificate Validation Requirements for more information on Cloud Connector certificate requirements.
- **FQDN Checks:** These checks cover connectivity to the remaining services described in the fully-qualified domain name (FQDN) AllowList.json published in the Cloud Connector Common Ser-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

vice requirements.

Citrix Cloud Services Connectivity Test Tool

The `Citrix Cloud Services Connectivity Test Tool` is only available on host machines where the Cloud Connector software is already installed. It can be accessed by navigating to the `Start Menu` > `Citrix` > `Citrix Cloud Services Connectivity Test Tool` .

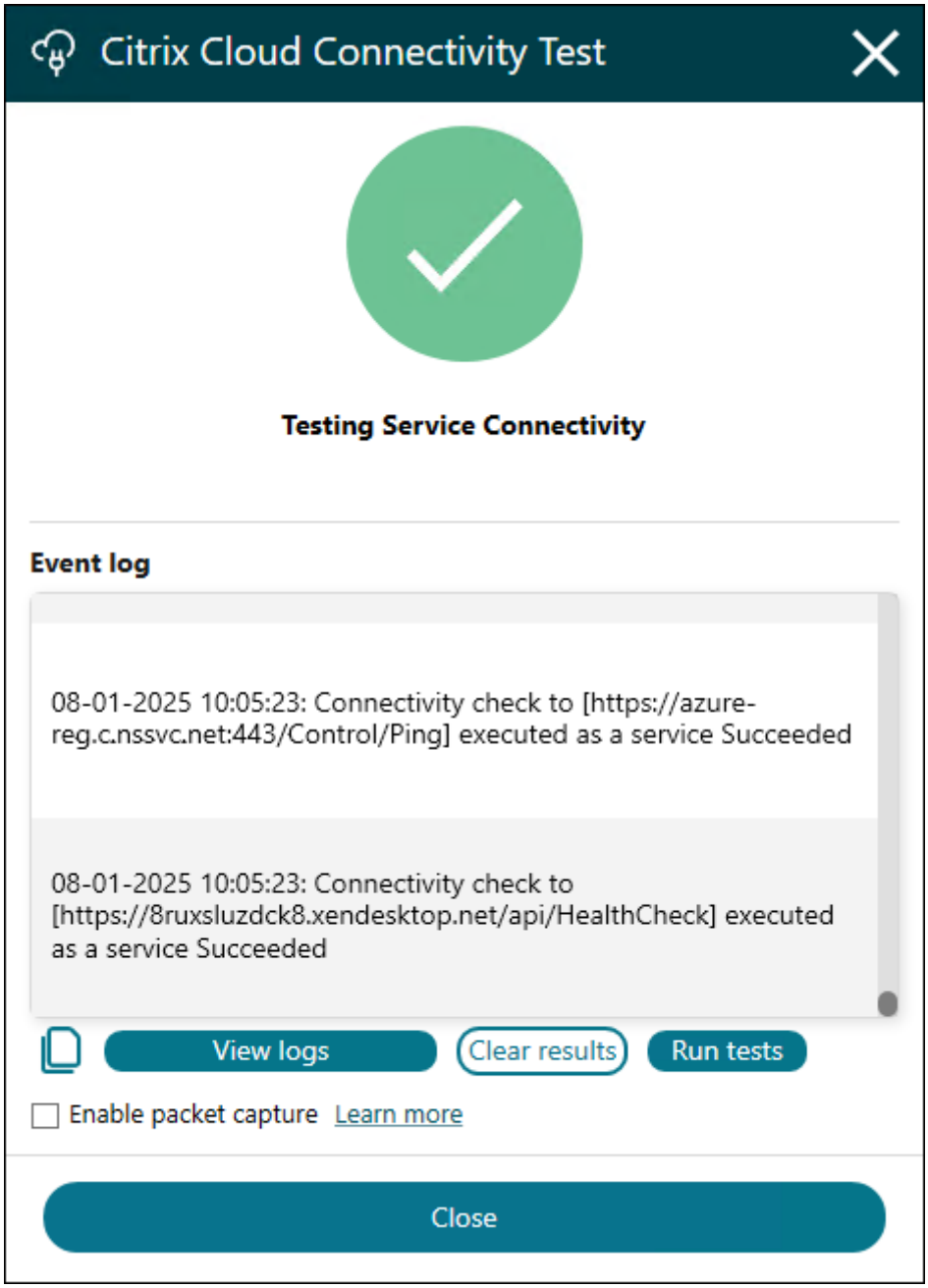
Checks Performed by the Citrix Cloud Services Connectivity Test Tool

The standalong `Citrix Cloud Services Connectivity Test Tool` performs the same set of Initial, Certificate, and FQDN checks described above. In addition, it performs an additional set of use-case specific tests.

The Citrix Cloud Connector™ installs a number of services relevant for each of its use-cases. Each of these services implement a set of Connectivity Checks related to its specific use-case. The Citrix Cloud Services Connectivity Test Tool performs tests by querying each service to perform the tests implemented for its specific use-case.

The details of these tests can be found by running the tool. It is also possible to access the log file with the same content.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



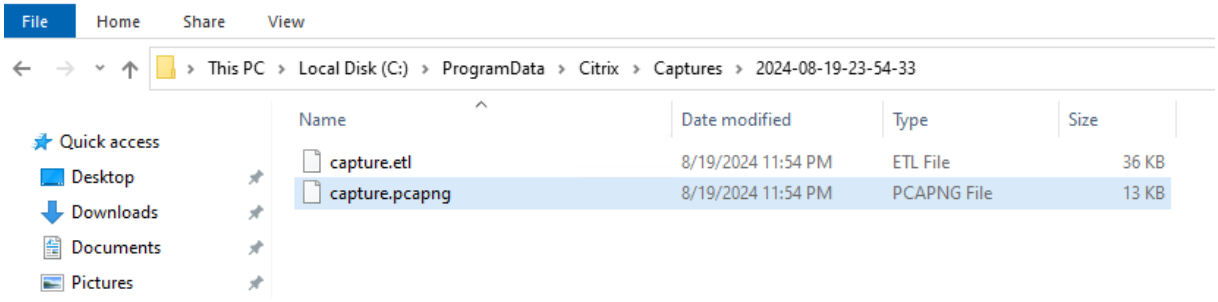
Packet Capture

Both the `Advanced Connectivity Checks` and `Citrix Cloud Services Connectivity Test Tool` include functionality to perform a packet capture alongside the Connectivity Checks they perofrm. By default, this checkbox is not selected, so packet capture is not performed unless explicitly enabled.

When activated, this feature utilizes the built-in `pktmon` utility on Windows to capture network traffic during connectivity checks. Once the checks are complete, the captured data will be saved locally

© 1997–2026 Citrix Systems, Inc. All rights reserved.

under `C:\ProgramData\Citrix\Captures` in a timestamped subdirectory. The files will be stored in both .etl and .pcapng formats. The .pcapng is the widely used format compatible with tools like Wireshark. These files remain on your local machine and are not uploaded to Citrix Cloud.



For customers requiring additional assistance, these packet captures can be shared with our support team to aid in diagnosing connectivity issues.

> **Note:**
>
> When the packet capture feature is activated in either the Advanced Connectivity Check screen of the installer or the Citrix Cloud Connectivity Test tool, all network traffic occurring during the connectivity check will be recorded. This includes traffic generated not only by the connectivity check and its related Cloud Connector components but also by any other network activity on the Cloud Connector VM. For instance, any unencrypted HTTP traffic, such as login attempts, that takes place during the connectivity check will also be captured in the resulting packet capture files.

Cloud Connector advanced health checks - Deprecated

September 6, 2025

> **Note:**
>
> Cloud Connector Health Metrics and Alerts have been added to Citrix DaaS™ Infrastructure Monitoring. This should be the primary location for analyzing and troubleshooting issues proactively regarding your infrastructure.
>
> For more information see Infrastructure Monitoring.

Before and after updates, Cloud Connectors perform health checks to ensure that updates cause no unnecessary downtime for providers. You can see the connectivity and health status of the Connector and of each service or provider on the Connector.

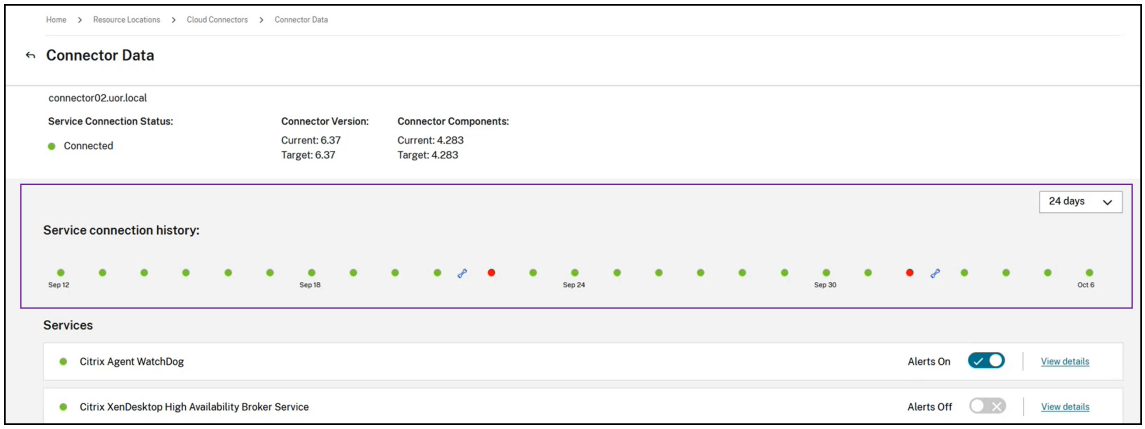
© 1997–2026 Citrix Systems, Inc. All rights reserved.

View Connector health check data

1. From the Citrix Cloud™ menu, select **Resource Locations**.
2. Select the Connector for which you want to view health check data.
3. On the Connectors page, go to the ellipsis menu next to the Connector and select **View Connector data**.

The Connector Data page appears, showing the following information.

- **Service Connection Status**. This area of the Connector data page shows:
  - Whether your Connector is connected to the Cloud
  - For the Connector and its components, the currently installed version and the target version to be installed in the next update
- **Service connection history**. 24 status indicators show the health status of the Connector over time. By default, service connection history shows status for the previous 24 hours, in one-hour intervals. To see more history, select **24 days** from the drop-down menu. The view shows status for the previous 24 days, in one-day intervals.
  - A green dot indicates healthy status during the time interval.
  - A red dot indicates a failure or exception status during the time interval. Hover over the dot for more information.
  - A wrench icon indicates that an update occurred during the time interval. Hover over the wrench icon for more information.
  - A gray dot indicates that no health status information was received during the time interval.



- **Services**. This area lists each service running on the Connector.
  - The dot next to each service indicates the current status of the service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

    - Use **Alerts On** and **Alerts Off** to control whether you are notified of alerts from the service. If alerts are set to On, failures in the service cause a failure in the overall Connector connection status.
    - Select **View Details** to view details of health status the service over time.

- **Connector Metrics**. This area shows Connector usage of memory usage, CPU, network data, and disks space for the previous 24 hours or 24 days. Use the drop-down menu in the **Service connection history** area to control the time period shown.

View service details

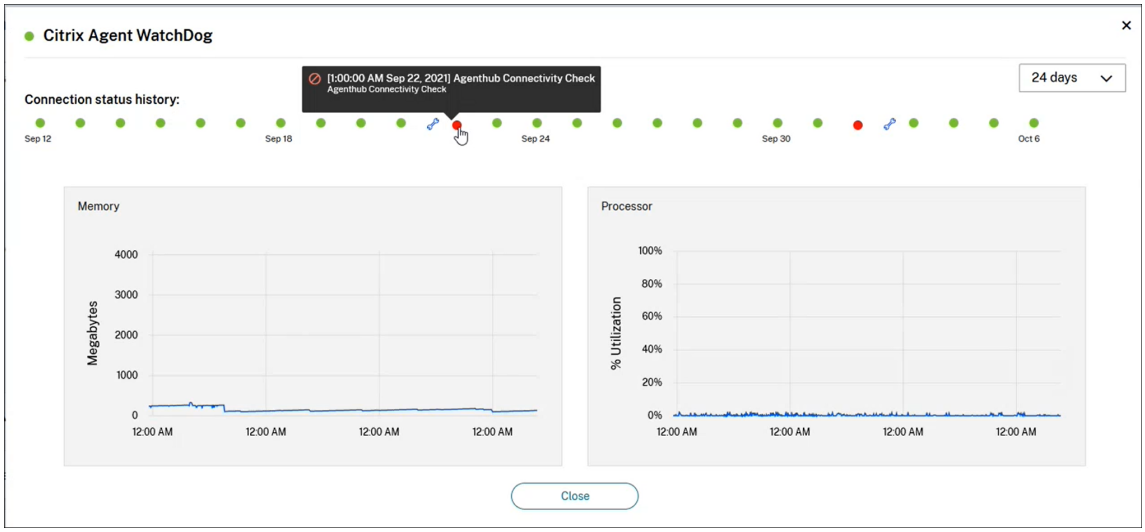
To view connection status history and metric for each service:

1. Use the drop-down menu in the **Service connection history** section to select the time period. You can view the previous 24 hours, in one-hour intervals, or the previous 24 days, in one-day intervals.
2. On the Connector Data page, select **View Details** next to the service.

The page that appears shows:

- 24 status indicators that show the health status of the service over time.
    - A green dot indicates healthy status during the time interval.
    - A red dot indicates a failure or exception status during the time interval. Hover over the dot for more information.
    - A wrench icon indicates that an update occurred during the time interval. Hover over the wrench icon for more information.
    - A gray dot indicates that no health status information was received during the time interval.
- Charts that show memory and processor usage for the service during the specified time period.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Connector notifications

September 6, 2025

Your connectors generate notifications within 2 hours of a warning or error condition occurring. You can see new notifications on the bell icon in the Citrix Cloud™ header.



Click this icon to view the notifications or select **Notifications** from the console menu.

For more information, see Notifications.

> **Note:**
>
> When a Notification is raised for a Cloud Connector it is important to understand the underlying cause before performing any reinstall of the Cloud Connector software. Failure to do so may result in the issue recurring.
>
> If reinstallation is necessary then it is important to ensure other Cloud Connectors in the Resource Location are healthy and will not be affected by the issue once the first Cloud Connector is removed. Failure to do so may result in service interruption.

Cloud Connector

The following table lists the notifications that Cloud Connector can raise:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alert message	Alert Type	Details	Resolution
Connector *CONNECTOR_NAME* is offline and out of date after failing to perform regular maintenance. Outdated connectors will impact service availability and prevent maintenance.	Error	If a connector has been offline for a long time and later comes back online, it might be an old version that cannot be updated to the latest version. Outdated connectors cannot perform maintenance and may impact the maintenance process of other connectors in the environment.	Install a fresh Cloud Connector before uninstalling the outdated Cloud Connector.
Connector *CONNECTOR_NAME* is not in sync with UTC time. Connectors in this state may impact service availability, functionality, or performance.	Error		How Do I Synchronize the Cloud Connector Time
Maintenance on connector *CONNECTOR_NAME* has failed. Failed maintenance on this connector will prevent maintenance for other connectors in the environment. Connectors with failed maintenance may impact service availability, functionality or performance.	Error	A connector upgrade or other maintenance operation has failed on this connector.	How Do I Resolve a Failed Cloud Connector Maintenance

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alert message	Alert Type	Details	Resolution
Connector *CONNECTOR_NAME* has been offline for *NUMBER* or more hours. Offline connectors will impact service availability and prevent maintenance.	Warning	If the connector has been uncontactable for a certain number of hours, it is considered offline.	How Do I Restore an Offline Cloud Connector to an Online State
Connector *CONNECTOR_NAME* has failed a recent connectivity check. A failed connectivity check may impact service availability or functionality.	Warning	A connectivity check has failed with error code *HEALTH_CHECK_CODE*. This connector was unable to contact certain web or IP addresses that are listed in the notification message.	Cloud Connector Connectivity Check Failed
Connector *CONNECTOR_NAME* is experiencing high CPU utilization. Connectors operating with constrained resources may impact service availability, functionality, or performance.	Warning	This connector has exceeded 80% CPU utilization over a one hour sample period.	How Do I Resolve a Cloud Connector Resource Availability Alert
Connector *CONNECTOR_NAME* is low on free disk space. Connectors operating with constrained disk space will impact service performance and maintenance.	Warning	This connector has less than 2 GB free disk space.	How Do I Resolve a Cloud Connector Resource Availability Alert

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alert message	Alert Type	Details	Resolution
Connector *CONNECTOR_NAME* has detected a critical process or service is no longer running. This state may impact service availability, functionality, or performance.	Warning		

Log Collection for Citrix Cloud Connector™

September 6, 2025

CDF logs are used for troubleshooting purposes within Citrix products. Citrix Support uses CDF traces to identify issues with application and desktop brokering, user authentication, Virtual Delivery Agent (VDA) registration. This article discusses how to capture Cloud Connector data that can be used to troubleshoot and resolve issues you might experience in your environment.

> **Important notes:**
>
> - Enable logging on all Cloud Connector machines in your resource locations.
> - To ensure that you're capturing the full spectrum of data, Citrix recommends using the CDFControl capturing tool that resides on the VDA. For more information, see CTX111961 in the Citrix Support Knowledge Center. For more information about log collection for Citrix Workspace app, CTX141751.
> - To submit CDF traces to Citrix, you must have an open Citrix Support case. Citrix Support technicians can't review CDF traces that are not attached to an existing support case.

Step 1: Recreate the issue

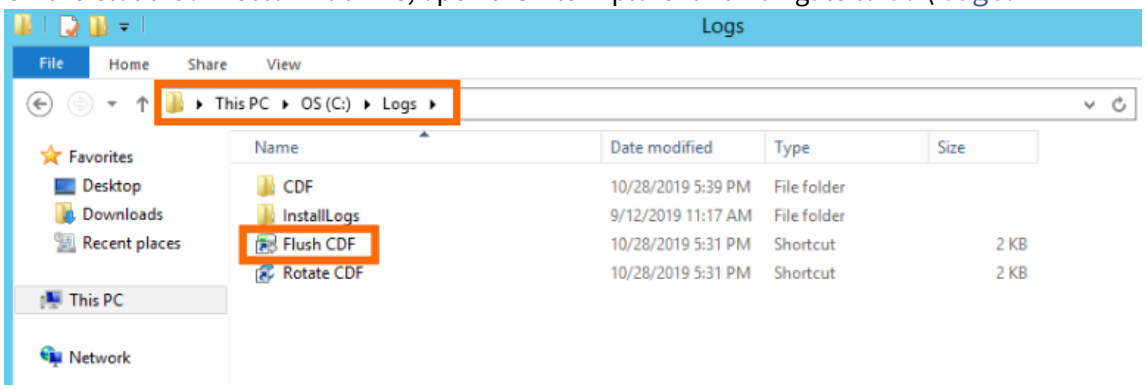
In this step, recreate the issue you're experiencing in your environment. If the issue is related to app launches or brokering, recreate the launch failure. If the issue is related to VDA registration, recreate the VDA registration attempt by manually restarting the Citrix Desktop Service on the VDA machine.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

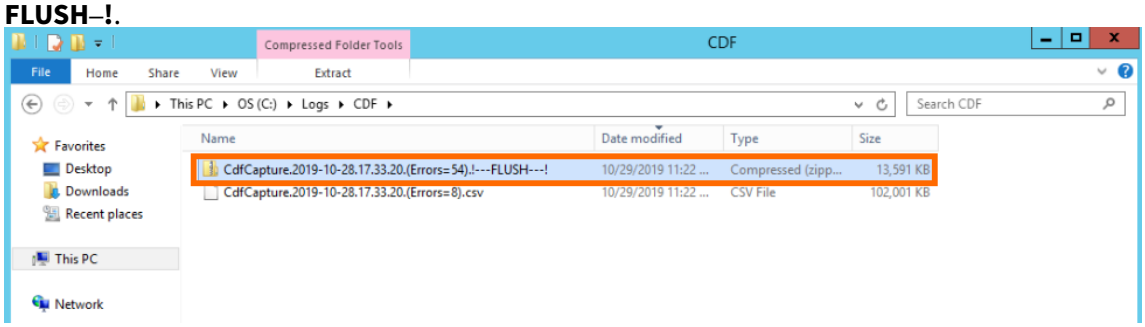
Step 2: Collect CDF traces

In this step, you collect CDF flush traces from each Cloud Connector in your resource location.

1. Access the Cloud Connector machine by initiating an RDP connection using a Domain Admin or Local Administrator account.
2. On the Cloud Connector machine, open the File Explorer and navigate to `C:\logs`.



3. Run **Flush CDF**. An icon appears briefly on the Taskbar of the Cloud Connector machine and then disappears.
4. From the File Explorer, navigate to C:\logs\CDF and identify the most recent folder ending in **!–FLUSH–!**.



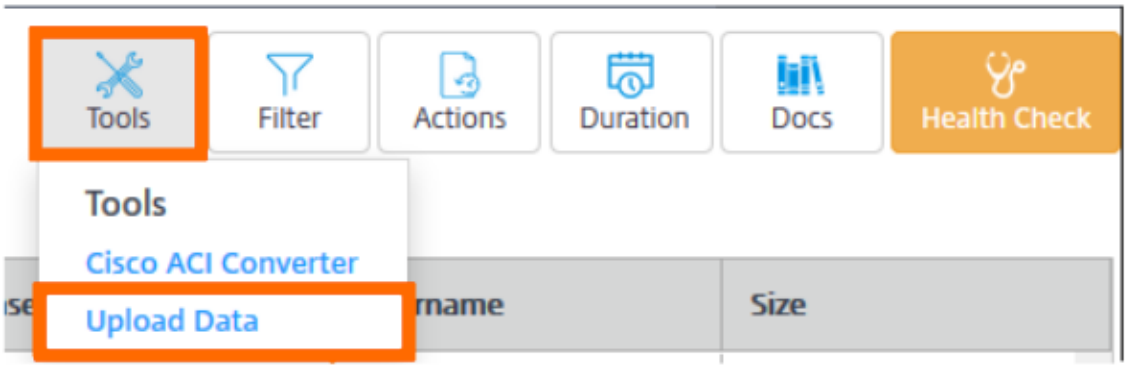
5. Perform Steps 1-5 on every Cloud Connector machine in your resource location and combine all Cloud Connector flush traces into a single ZIP archive. If you don't create a ZIP archive of the flush traces from all your Cloud Connector machines, you will need to submit them one at a time to Citrix.

Step 3: Submit data to Citrix

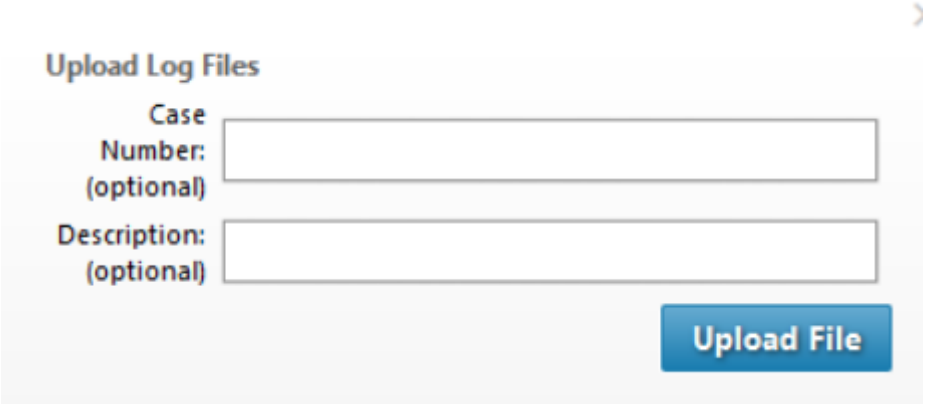
In this step, you attach your traces to your Citrix support case and submit them for review.

1. Visit https://cis.citrix.com/ and sign in using your Citrix.com credentials.
2. Select **Diagnostics**.
3. Select **Tools** and then select **Upload Data**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. In **Case Number**, enter the Citrix Support case number of the existing support case. Citrix Support technicians can't review CDF traces appropriately without a case number attached to the data upload.



5. In **Description** (optional), you can enter a brief description or leave this field blank.
6. Select **Upload File** and select the ZIP archive you created earlier. If you didn't create a ZIP archive of flush traces from all your Cloud Connector machines, repeat Steps 3-6 to attach each flush trace you want to submit.

After you submit your flush traces, Citrix Insight Services processes them and attaches them to the support case you specified. This process can take up to 24 hours, depending on the size of the files.

Select a primary resource location

June 22, 2026

If you have multiple resource locations in your domain, you can choose one to be the "primary"or "most preferred"location for Citrix Cloud. The primary resource location provides the best performance and connectivity between Citrix Cloud and your domain, enabling users to sign in quickly.

When you select a primary resource location, the Cloud Connectors in that resource location are used for user logons and provisioning operations where possible. If the Cloud Connectors in the primary

© 1997–2026 Citrix Systems, Inc. All rights reserved.

resource location are unavailable, these operations are performed using another Cloud Connector in the domain. Logons using a User Principal Name (UPN) might not contain the domain name and might not use the primary resource location.

> **Note:**
>
> To ensure that Cloud Connectors are always available in any resource location, install at least two Cloud Connectors in each resource location.

To decide which resource location you want to use for your primary resource location, consider the following:

- Does the resource location have the best connectivity to your domain?
- Is the resource location the closest to the geographical region in which you use the Citrix Cloud management console? For example, if your Citrix Cloud console is at https://us.cloud.com, the resource location you choose would be the closest one to the US region.

To select a primary resource location

1. From the Citrix Cloud management console, click the menu button and select **Identity and Access Management**.
2. Click **Domains** and then expand the domain containing the resource location you want to use.
3. Click **Set Primary Resource Location** and then select the resource location you want to designate as primary.
4. Click **Save**. Citrix Cloud displays "Primary"next to the resource location you selected.

> **Note:**
>
> Be sure to save your selections in one domain before expanding a different domain. When you expand a domain and then expand another domain, the previously expanded domain collapses and discards any unsaved selections.

Select a different primary resource location

1. From the Citrix Cloud management console, click the menu button and select **Identity and Access Management**.
2. Click **Domains** and then expand the domain that contains the primary resource location you want to change.
3. Click **Change Primary Resource Location** and then select the resource location you want to use.
4. Click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Reset a primary resource location

Resetting the primary resource location allows you to remove the "Primary"designation from a resource location without selecting a different one. When you remove the "Primary"designation, any of the Cloud Connectors in the domain can handle user logon operations. As a result, some users might experience slower logons.

1. From the Citrix Cloud management console, click the menu button and choose **Identity and Access Management**.
2. Choose **Domains** and then expand the domain that contains the primary resource location you want to change.
3. Choose **Change Primary Resource Location** and then choose **Reset**. A notification appears, warning you that logon performance might be affected.
4. Select **I understand the potential impact to end users** and then click **Confirm Reset**.

Connector Appliance for Cloud Services

October 8, 2026

The Connector Appliance is a Citrix component hosted in your hypervisor or cloud provider. It serves as a channel for communication between Citrix Cloud™ and your resource locations, enabling cloud management without requiring any complex networking or infrastructure configuration. The Connector Appliance enables you to manage and focus on the resources that provide value to your users.

> **Note:**
>
> The Connector Appliance cannot be used for VDA registration, Storefront XML traffic, Netscaler STA traffic, hypervisor management for MCS, or any other use cases related to DaaS resources. Use the Cloud Connector for these use cases.

Connector Appliance functions

- **Connecting Active Directory to Citrix Cloud** enables AD management, allowing the use of AD forests and domains within your resource locations. It removes the need for adding any additional AD trusts. Unlike the Cloud Connector, a single Connector Appliance can be used to provide connectivity to multiple Active Directory domains. For more information, see Active Directory with Connector Appliance.
- **Image Portability Service** simplifies the management of images across platforms. This feature is useful for managing images between an on-premises resource location and one in a public

© 1997–2026 Citrix Systems, Inc. All rights reserved.

cloud. The Citrix Virtual Apps and Desktops™ REST APIs can be used to automate the administration of resources within a Citrix Virtual Apps and Desktops site.

The Image Portability workflow begins when you use Citrix Cloud to initiate the migration of an image from your on-premises location to your public cloud subscription. After preparing your image, the Image Portability Service helps you transfer the image to your public cloud subscription and prepare it to run. Finally, Citrix Provisioning or Machine Creation Services™ provisions the image in your public cloud subscription.

For more information, see Image Portability Service.

- **Citrix Secure Private Access** enables administrators to provide a cohesive experience that integrates single sign-on, remote access, and content inspection into a single solution for end-to-end access control. For more information, see Secure Private Access with Connector Appliance.

There might be other services in preview that also depend on the Connector Appliance.

The Connector Appliance platform is part of Citrix Cloud Platform and Citrix Identity Platform and can process data, including the following information:

- IP addresses or FQDNs
- Device, user, and resource location identifiers
- Timestamps
- Event data
- User and group details from Active Directory (for example, used for authenticating and searching for users and groups)

Details of specific information processed by the Connector Appliance are available in the *Data Collected by Citrix Cloud Platform* table in the Citrix Cloud Services Data Protection Overview.

Connector Appliance availability and load management

For continuous availability and to manage load, install multiple Connector Appliances in each of your resource locations. Citrix recommends at least two Connector Appliances in each resource location. If one Connector Appliance is unavailable for any time, the other Connector Appliances can maintain the connection. Since each Connector Appliance is stateless, the load can be distributed across all available Connector Appliances. There is no need to configure this load balancing function. It is automated. If at least one Connector Appliance is available, there is no loss in communication with Citrix Cloud.

If you have only one connector configured for a resource location, Citrix Cloud shows a warning on the **Resource Locations** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connector Appliance updates

The Connector Appliance is updated automatically. You are not required to take any actions to update your connector.

You can configure your resource location to apply updates either immediately as they become available or after a scheduled time.

For more information about configuring updates, see Connector updates

As part of the update, the Connector Appliance becomes temporarily unavailable. Updates are applied to only one Connector Appliance in a tenant at a time. For this reason, register at least two Connector Appliances in each Resource Location to ensure that at least one Connector Appliance is always available.

Connector Appliance communication

The Connector Appliance authenticates and encrypts all communication between Citrix Cloud and your resource locations. Once installed, the Connector Appliance initiates communication with Citrix Cloud through an outbound connection. All connections are established from the Connector Appliance to the cloud using the standard HTTPS port (443) and the TCP protocol. No incoming connections are allowed.

The following table lists the ports that the Connector Appliance requires access to:

Service	Port	Supported Domain Protocol	Configuration details
DNS	53	TCP/UDP	This port must be open to the local setup
NTP	123	UDP	This port must be open to the local setup
HTTPS	443	TCP	Connector Appliance requires outbound access to this port

To configure the Connector Appliance, IT administrators must be able to access the administration interface on port 443 (HTTPS) of the Connector Appliance.

> **Note:**
>
> To access the administration interface you must include `https://` at the start of the IP address.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The Connector Appliance can communicate with both on-premises systems in your resource location and with external systems. If you define one or more web proxies on the Connector Appliance administration interface, only traffic from the Connector Appliance to external systems is routed through this web proxy. If your on-premises system is located in a private address space, traffic from Connector Appliance to this system is not routed through the web proxy.

The Connector Appliance defines private address spaces as the following IPv4 address ranges:

- 10.0.0.0 –10.255.255.255
- 172.16.0.0 –172.31.255.255
- 192.168.0.0 –192.168.255.255

Internet connectivity requirements

Connecting to the Internet from your data centers requires opening port 443 to outbound connections. However, to operate within environments containing an Internet proxy server or firewall restrictions, further configuration might be needed.

To properly operate and consume the Citrix Cloud services, the following addresses must be contactable with unmodified HTTPS connections:

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.citrixnetworkapi.net`
- `https://*.nssvc.net`
    - Customers who can't enable all subdomains can use the following addresses instead:
        - `https://*.g.nssvc.net`
        - `https://*.c.nssvc.net`
- `https://*.servicebus.windows.net`
- `https://ctxccopspacrconnappprod.azurecr.io`
- `https://ctxccopspacrconnappprod.eastus.data.azurecr.io`

Network requirements

Ensure that your environment has the following configuration:

- Either the network allows the Connector Appliance to use DHCP to get DNS and NTP servers, an IP address, a host name, and a domain name or you can manually set the network settings in the Connector Appliance console.
- The network is not configured to use the link-local IP ranges 169.254.0.1/24, 169.254.64.0/18 or 169.254.192.0/18, which are used internally by the Connector Appliance.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Either the hypervisor clock is set to Coordinated Universal Time (UTC) and is synchronized with a time server or DHCP provides NTP server information to the Connector Appliance.
- If you use a proxy with Connector Appliance, the proxy must be unauthenticated or use basic authentication.

System requirements

The Connector Appliance is supported on the following hypervisors:

- VMware ESXi version 7 update 2
- VMware ESXi version 8
- Hyper-V on Windows Server 2016, Windows Server 2019, Windows Server 2022, or Windows Server 2025.
- Nutanix AHV
- Microsoft Azure
- AWS
- Google Cloud Platform
- XenServer® 8.4
- XenServer® 9

Your hypervisor must provide the following minimum capabilities:

- 20 GB root disk
- 2 vCPUs
- 4 GB memory
- An IPv4 network

You can host multiple Connector Appliances on the same hypervisor host. The number of Connector Appliances on the same host is only constrained by the hypervisor and hardware limitations.

> **Note:**
>
> Cloning, suspending, and taking snapshots of the Connector Appliance VM are not supported.

Obtain the Connector Appliance

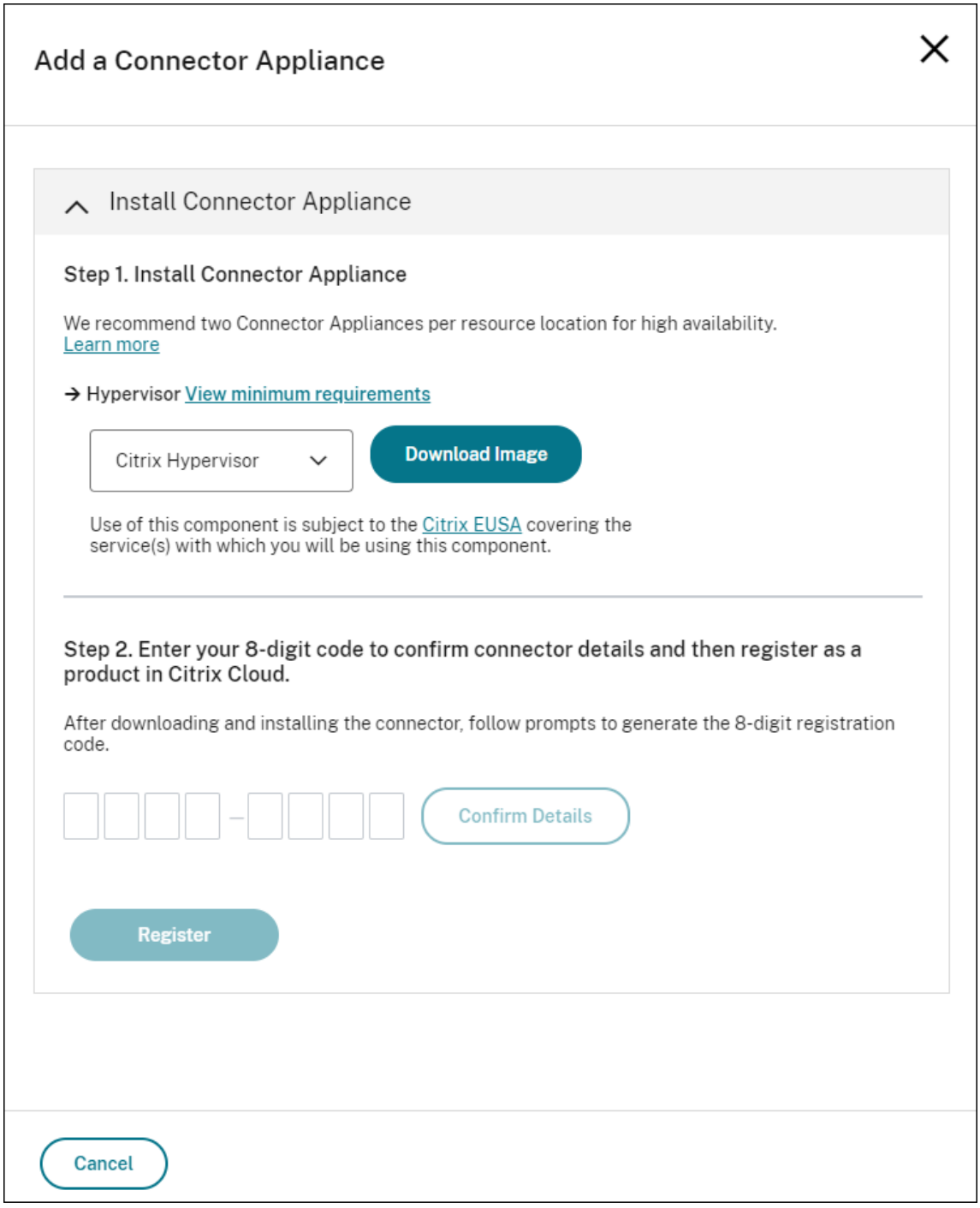
Download the Connector Appliance software from within Citrix Cloud.

1. Sign in to Citrix Cloud.
2. From the menu in the top left of the screen, select **Resource Locations**.
3. If you do not already have a resource location, click the plus icon (+) or select **Add a Resource Location**. For more information, see create a resource location.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. In the resource location where you want to register the Connector Appliance, click the **Connector Appliances** plus icon (+).

   The **Add a Connector Appliance** task opens.



5. From the **Hypervisor** list in **Step 1**, choose the type of hypervisor or cloud provider that you use to host your Connector Appliance.

   - For on-premises hypervisors and cloud environments, you can download the Connector

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Appliance within Citrix Cloud:

a) Click **Download Image**.

b) Review the Citrix End User Service Agreement and, if you agree, select **Agree and Continue**.

c) When prompted, save the provided Connector Appliance file.

The file name extension of the Connector Appliance file depends on the hypervisor that you choose.

- For some cloud environments, you can get the Connector Appliance from the marketplace:
  - AWS
  - Microsoft Azure
  - Google Cloud

6. Keep the **Install Connector Appliance** task open. After installing the Connector Appliance, you input your registration code into **Step 2**.

You can also get to the **Install Connector Appliance** task from the **Connectors** page. Select the plus icon (+) to add a connector and choose to add a Connector Appliance.

Install Connector Appliance on your hypervisor

- XenServer™
- VMware ESXi
- Hyper-V
- Nutanix AHV
- Microsoft Azure
- Google Cloud Platform
- AWS

XenServer

This section describes how to import the Connector Appliance to a XenServer host by using XenCenter.

1. Connect to your XenServer host or pool by using XenCenter on a system that has access to the downloaded Connector Appliance XVA file.
2. Select **File** > **Import**.
3. Specify or browse to the path where the Connector Appliance XVA file is located. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Select the XenServer host where you want to host the Connector Appliance. Alternatively, you can select the pool to host the Connector Appliance in and XenServer chooses a suitable available server. Click **Next**.
5. Specify the storage repository to use for your Connector Appliance. Click **Import**.
6. Click **Add** to add a virtual network interface. From the **Network** list, select the network for the Connector Appliance to use. Click **Next**.
7. Review the options to use to deploy the Connector Appliance. If any are incorrect, use **Previous** to change these options.
8. Ensure that **Start the new VM(s) automatically as soon as the import is complete** is selected. Click **Finish**.

After the Connector Appliance is deployed and has successfully started up, its console displays a landing page that contains the Connector Appliance IP address. Use this IP address to connect to the Connector Appliance administration page and complete the registration process.

By default, the Connector Appliance uses DHCP to set its network configuration. If DHCP is not available in your environment, you must set the network configuration at the Connector Appliance console before you can access the Connector Appliance management console. For more information, see Set the network configuration by using the Connector Appliance console.

Next step: Register your Connector Appliance with Citrix Cloud.

VMware ESXi

This section describes how to deploy Connector Appliance on a VMware ESXi host by using the VMware vSphere Client.

1. Connect to your ESXi host by using the vSphere Client on a system that has access to the downloaded Connector Appliance OVA file.
2. Select **File** > **Deploy OVF Template…**.
3. Specify or browse to the path where the Connector Appliance OVA file is located. Click **Next**.
4. Review the template details. Click **Next**.
5. You can specify a unique name for your Connector Appliance instance. By default, the name is set to **Connector Appliance**. Ensure that you choose a name that distinguishes this instance of the Connector Appliance from other instances hosted on this ESXi host. Click **Next**.
6. Specify the destination storage for your Connector Appliance. Click **Next**.
7. Choose the format to store the virtual disks in. Click **Next**.
8. Review the options to use to deploy the Connector Appliance. If any are incorrect, use **Back** to change these options.
9. Select **Power on after deployment**. Click **Finish**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After the Connector Appliance is deployed and has successfully started up, its console displays a landing page that contains the Connector Appliance IP address. Use this IP address to connect to the Connector Appliance administration page and complete the registration process.

By default, the Connector Appliance uses DHCP to set its network configuration. If DHCP is not available in your environment, you must set the network configuration at the Connector Appliance console before you can access the Connector Appliance UI. For more information, see Set the network configuration by using the Connector Appliance console.

Next step: Register your Connector Appliance with Citrix Cloud.

Hyper-V

This section describes how to deploy Connector Appliance on a Hyper-V host. You can deploy the VM by using the Hyper-V Manager or by using the included PowerShell script.

Deploy the Connector Appliance by using the Hyper-V Manager

1. Connect to your Hyper-V host.
2. Copy or download the Connector Appliance ZIP file to the Hyper-V host.
3. Extract the contents of the ZIP file. The ZIP file contains a PowerShell script and the connector-appliance.vhdx file.
4. Copy the VHDX file to where you want to keep your VM disks. For example, `C:\ConnectorApplianceVMs`.
5. Open Hyper-V Manager.
6. Right-click on your server name and select **New > Virtual Machine**.
7. In the **New Virtual Machine Wizard**, on the **Specify Name and Location** panel, enter a unique name to identify your Connector Appliance. Click **Next**.
8. On the **Specify Generation** panel, select **Generation 1**. Click **Next**.
9. On the **Assign Memory** panel, configure the following settings and then click **Next**:
    a) Assign 4 GB of RAM.
    b) Disable dynamic memory.
10. On the **Configure Networking** panel, select a switch from the list (for example, Default Switch). Click **Next**.
11. On the **Connect Virtual Hard Disk** panel, select **Use an existing virtual hard disk**.
12. Browse to the location of the connector-appliance.vhdx file and select it. Click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

13. On the **Summary** panel, review the values you have chosen and click **Finish** to create the VM.
14. On the **Virtual Machines** panel, right-click on the Connector Appliance VM and select **Settings**.
15. In the **Settings** window, select **Hardware > Processors** and perform the following actions:
    a) In **Number of virtual processors**, change the value to **2**.
    b) Click **Apply**.
    c) Click **OK**.
16. On the **Virtual Machines** panel, right-click on the Connector Appliance VM and select **Start**.
17. Right-click on the Connector Appliance VM and select **Connect** to open the console.

After the Connector Appliance is deployed and has successfully started up, connect to the console using the Hyper-V Manager. The console displays a landing page that contains the Connector Appliance IP address. Use this IP address to connect to the Connector Appliance administration page and complete the registration process.

By default, the Connector Appliance uses DHCP to set its network configuration. If DHCP is not available in your environment, you must set the network configuration at the Connector Appliance console before you can access the Connector Appliance UI. For more information, see Set the network configuration by using the Connector Appliance console.

Next step: Register your Connector Appliance with Citrix Cloud.

Deploy the Connector Appliance by using a PowerShell script The connector-appliance.zip file contains a PowerShell script that creates and starts a new VM.

> **Note:**
>
> To run this unsigned PowerShell script, you might have to change the execution policies on the Hyper-V system. For more information, see https://go.microsoft.com/fwlink/?LinkID=135170. Alternatively, you can use the provided script as the basis to create or amend your own local script.

1. Connect to your Hyper-V host.
2. Copy or download the Connector Appliance ZIP file to the Hyper-V host.
3. Extract the contents of the ZIP file: A PowerShell script and a VHDX file.
4. In a PowerShell console, change the current directory to where the ZIP file contents are located and run the following command:

```
.\connector-appliance-install.ps1
```

5. When prompted, type a name for your VM or select **Enter** to accept the default value of **Connector Appliance**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

6. When prompted, type a destination for the root disk or press Enter to use the system default directory for VHDs.
7. When prompted, type a file name for the root disk or select **Enter** to accept the default value of connector-appliance.vhdx.
8. When prompted, select the switch to use. Select **Enter**.
9. Review the summary of the VM import information. If the information is correct, select **Enter** to continue. The script creates and starts the Connector Appliance VM.

After the Connector Appliance is deployed and has successfully started up, its console displays a landing page that contains the Connector Appliance IP address. Use this IP address to connect to the Connector Appliance and complete the registration process.

Next step: Register your Connector Appliance with Citrix Cloud.

Nutanix AHV

This section describes how to deploy Connector Appliance from the `connector-appliance.vhdx` file onto a Nutanix AHV host by using the Nutanix Prism web console.

1. On the main menu of the Nutanix Prism web console, select the **Storage** view.
2. Click **+ Storage Container** to create a storage container to hold the Connector Appliance image file. Alternatively, you can use an existing storage container.
3. Upload the `connector-appliance.vhdx` file to your storage container.
    a) On the main menu of the web console, select **Settings**.
    b) Select the **Image Configuration** tab and click **+ Upload Image**
    c) In **Create Image**, specify a **Name** for your image.
    d) From the **Image Type** list, select **DISK**.
    e) From the **Storage Container** list, select the storage container you created.
    f) Select **Upload a file**.
    g) Click **Choose file** and navigate to the `connector-appliance.vhdx` file on your local system.
    h) Click **Save**.
4. Wait until the image is created and its state shows as **ACTIVE** in the **Image Configuration** page.
5. Select the **Network Configuration** tab.
6. Click **+ Create Network** to create a network for the Connector Appliance to use.
7. In the **Create Network** page, specify the following information:
    - The network name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The network VLAN ID.

8. On the main menu of the web console, select the **VM** view.
9. Click **+ Create VM** to create a Connector Appliance instance.
10. In **Create VM**, specify the following information:

    - The VM name
    - The number of vCPUs
    - The amount of memory in GiB

11. Select to use **Legacy BIOS**.
12. Click **+ Add New Disk** to add a disk to the VM.
13. In **Add Disk**, complete the following information:

    a) For **Type**, select **DISK**.
    b) For **Operation**, select **Clone from Image Service**.
    c) For **Bus Type**, select **SCSI**
    d) For **Image**, select the image you created when you uploaded the Connector Appliance file.

14. Click **Add** to finish adding the disk.
15. In **Create VM**, click **+ Add New NIC**.
16. In **Create NIC**, select the network to add the VM to.
17. For **Network Connection State**, select **Connected**.
18. Click **Add** to finish adding the NIC.
19. Click **Save** to create the VM.

    By default, the new VM is powered off.

20. In the **VM** view, select the VM and click **Power on**.
21. Wait for the VM to start up. This process can take several minutes.

After the Connector Appliance is deployed and has successfully started up, you can find the Connector Appliance IP address in one of the following places:

- In the **VM** view of the Nutanix Prism web console.
- In the Connector Appliance console.

Use this IP address to connect to the Connector Appliance administration page and complete the registration process.

Next step: Register your Connector Appliance with Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Azure

This section describes how to deploy Connector Appliance in Microsoft Azure. You can deploy the Connector Appliance from the Azure Marketplace or from the downloaded disk image by using the included PowerShell script.

Deploy the Connector Appliance from the Azure Marketplace To deploy the Connector Appliance from the Azure Marketplace complete the following steps:

1. Go to the Connector Appliance in the Azure Marketplace. (Azure Marketplace)

   Alternatively, you can search for "Connector Appliance for Cloud Services"in the marketplace search.

2. Click **Get It Now** and then **Create**.
3. On the **Create Citrix Connector™ Appliance for Cloud Services** page, complete the following information:

   - Select the **Subscription** to use.
   - Select the **Resource group** to use.
   - Select the **Region** to locate the Connector Appliance in.
   - Specify a **VM name**.
   - Select a **Virtual network** to add the Connector Appliance to. This network is used to access Citrix Cloud, the local resources, and the Connector Appliance administration page. This network cannot be changed later.
   - Specify a value for **Subnet**.

   Click **Next : Tags >**.

4. On the **Tags** tab, add required tags if needed.

   Click **Next : Review + create >**.

5. After you have reviewed the deployment details, click **Create**.

After the Connector Appliance is deployed and has successfully started up, its console displays a landing page that contains the Connector Appliance IP address. Use this IP address to connect to the Connector Appliance administration page and complete the registration process.

Next step: Register your Connector Appliance with Citrix Cloud.

Deploy the Connector Appliance VM by using a PowerShell script The `connector-appliance-azure.zip` file contains a PowerShell script that creates and starts a new VM. You can use the provided script as the basis to create or amend your own local script.

Before running the script ensure that you have the following prerequisites:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Install the Az PowerShell module into your local PowerShell environment.
- Run the PowerShell script in the directory where the VHD file is located.

Complete the following steps:

1. Copy or download the Connector Appliance ZIP file to your Windows system.
2. Extract the contents of the ZIP file: A PowerShell script and a VHD file.
3. Open a PowerShell console as Administrator.
4. Change the current directory to where the ZIP file contents are located and run the following command:

```
.\connector-appliance-upload-Azure.ps1
```

5. A dialog appears, prompting you to log into Microsoft Azure. Enter your credentials.
6. When prompted by the PowerShell script, select the subscription to use. Press Enter.
7. Follow the prompts in the script, which guide you through uploading the image and creating a virtual machine.
8. After you have created the first VM, the script asks if you want to create another VM from the uploaded image.
    - Type `y` to create another VM.
    - Type `n` to exit the script.

After the Connector Appliance is deployed and has successfully started up, its console displays a landing page that contains the Connector Appliance IP address. Use this IP address to connect to the Connector Appliance administration page and complete the registration process.

Next step: Register your Connector Appliance with Citrix Cloud.

AWS

This section describes how to deploy Connector Appliance in AWS. Connector Appliance is available as an AMI in the AWS marketplace and we recommend that you install the Connector Appliance from the AMI. Alternatively, you can deploy a downloaded disk image by using the AWS UI or by using the included PowerShell script.

Networking prerequisites To deploy the Connector Appliance on AWS, ensure that you have access to Citrix Cloud from the subnet in which the Connector Appliance is created.

We recommend using a private IP address for the appliance, which requires specific configuration to provide access to Citrix Cloud. To achieve this configuration, complete the following steps in the **AWSManagement Console**:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Create the NAT gateway.
    a) In the top navigation bar, select **Services > VPC > NAT Gateways**.
    b) On the top right, click **Create NAT Gateway**. Enter the following information:
        - Enter **Name**.
        - Select **subnet** from the list.
        - Set **Connectivity type** as **Public**.
        - Select an **Elastic IP allocation ID** from the list. If there is no available Elastic IP, click **Allocate Elastic IP** and follow the instructions to create one.
    c) Click **Create NAT Gateway**.
2. Create a route table entry including the NAT gateway.
    a) In the top navigation bar, select **Services > VPC > Route Tables**.
    b) On the top right, click **Create route table**. Enter the following information:
        - Enter **Name**.
        - From the list, select the VPC that contains the subnet you selected when creating the NAT gateway.
    c) Click **Create route table**.
    d) In the **Routes** tab of the route table you created, click **Edit routes > Add route**.
    e) Input the **Destination** and **Target** for the new route entry.
        - Set the destination as 0.0.0.0/0.
        - For the target, select the **NAT Gateway** you created from the list.
    f) Click **Save change**.
3. Attach the subnet to be used for the Connector Appliance to this route table.
    a) In the top navigation bar, **Select Services > VPC > Route Tables**.
    b) Select the route table that contains the NAT gateway.
    c) In the display page, go to the **Subnet Associations** tab.
    d) Click **Edit subnet associations**.
    e) Select the subnet or subnets to attach to the route table.
    f) Click **Save Associations**.

Deploy the Connector Appliance from the AWS Marketplace Before beginning, ensure you meet the following prerequisites:

- You have permissions to operate EC2 resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You have completed the configuration in Networking prerequisites.
- (Optional) You can create a security group that restricts which IP addresses are permitted to access your Connector Appliance.

Complete the following steps:

1. Log in to the **AWSManagement Console**.
2. Find the Connector Appliance AMI in the AWS marketplace. You can do this in one of the following ways:
   - Follow the marketplace link provided in Citrix Cloud. (AWS Marketplace)
   - Search for the AMI in the AWS Management Console:
     a) Go to **Services > Compute > EC2 > AMIs**
     b) Ensure that you are in the US East (Ohio) region.
     c) In **Public images**, search for "Citrix Connector Appliance"or for the AMI ID "ami-026eaf9b3b232577f".
3. Verify that you have the correct AMI by checking the AMI ID (ami-026eaf9b3b232577f) and owner ID (414337923189).
4. Copy the AMI to your subscription:
   a) Go to **Actions > Copy AMI**.
   b) In the **Copy AMI** dialog, you can select the **Destination Region** that you require.
   c) Click **Copy AMI**
5. From your copied AMI summary page, click **Launch instance from AMI**.
6. In the **Launch an instance** dialog, complete the following steps:
   a) Select the number of instances to create. For resiliency, we recommend that you have two or more Connector Appliances in each resource location.
   b) Specify a name for the instance.
   c) For the **Instance type**, select **t2.medium**. The instance type must have at least 4 GB and 2 CPUs.
   d) For the **Key pair (login)**, select **Proceed without a key pair**. SSH login to the Connector Appliance is not permitted, so a key pair is not needed.
   e) For the **Network settings**, in the **Firewall (security group)** section, configure the following settings:
      i. Choose whether to **Create security group** or **Select existing security group**.
      ii. Deselect **Allow SSH traffic from the internet**
      iii. Select **Allow HTTPs traffic from the internet**
      iv. Select **Allow HTTP traffic from the internet**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Click **Launch instance**.

7. After the instance is created, in the **Success** section, click the instance ID link to view your Connector Appliance instance.

   Alternatively, you can click the **View All Instances** button on this page or go to **Services > EC2 >Instances** in the AWS Management Console to see a list of your instances.

8. When your **Instance state** has changed to **Running**, go into the instance details and use the **Private IPv4 address** to connect to the Connector Appliance administration page and complete the registration process.

You might need to use a bastion host to go to the Connector Appliance administration page at the internal IP address from your browser and complete the registration process.

By default, the Connector Appliance uses DHCP to set its network configuration. You can edit this network configuration using the Connector Appliance web interface. For more information, see Configuring network settings on the Connector Appliance administration page.

Next step: Register your Connector Appliance with Citrix Cloud.

Deploy the Connector Appliance by using the AWS UI Before beginning, ensure you meet the following prerequisites:

- You have permissions to operate S3 and EC2 resources.
- You have created a service role and policy that has VM import access. For more information, see https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role.

  > **Note:**
  >
  > To create a service role, you must create an S3 bucket. When creating the policy, set the S3 bucket you have created with VM import access.

- You have access to AWS CloudShell. It is only available in certain regions. For the list of regions where AWS CloudShell is supported, see https://docs.aws.amazon.com/cloudshell/latest/userguide/supported-aws-regions.html.
- You have completed the configuration in Networking prerequisites.

Complete the following steps:

1. On your local system, extract the contents of `connector-appliance-aws.zip`.
2. Log in to the **AWSManagement Console**.
3. Create a storage bucket by completing the following steps. (Alternatively, you can skip these steps and use an existing storage bucket.)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a) In the top navigation bar, select **Services** > **S3** > **Create bucket**.
b) Enter a unique name for your bucket. For naming conventions for buckets in Amazon S3, see https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html.
c) Select the region for your bucket. Ensure that you choose the same region as your AWS Region, because you cannot use the files in the bucket if these regions are different.
d) Keep the remaining settings set to the defaults, then click **Create bucket**.

4. Click the name of the bucket that you have created. Click **Upload** > **Add files**, then select the `connector-appliance.vhd` file. Keep the remaining settings set to the defaults then click **Upload**.
5. Click the file you uploaded. Click **Copy S3 URI**.
6. Click the **AWS CloudShell icon** in the top navigation bar and run the following commands:

a) Create a task to convert your VHD file to a snapshot:

```
aws ec2 import-snapshot --disk-container Format=VHD,Url="<
    S3_URI>"
```

Replace the placeholder value with your S3 URI that you copied from the previous step. For example, `aws ec2 import-snapshot --disk-container Format=VHD, Url="s3://my-aws-bucket/connector-appliance.vhd"`.

This command is complete when the following command returns a JSON string containing `"Status": "completed"`. Make note of the `ImportTaskId` value in the JSON output.

b) Run the following command:

```
aws ec2 describe-import-snapshot-tasks --import-task-ids <
    ImportTaskId>
```

Replace the placeholder value with the `ImportTaskId` copied from the previous step. For example, `aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-0273h2836153itg5`.

7. On the **AWSManagement Console**, in the top navigation bar, select **Services** > **EC2**.
8. From the menu on the left of the screen, click **Snapshots**.
9. Right-click on the snapshot that you created and click **Create Image**.
10. In the pane that opens, complete the following steps:

a) Enter a name for your AMI.
b) Select **Hardware-assisted virtualization**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Click **Create**.

11. From the menu on the left of the screen, click **AMIs**.
12. Right-click on the AMI that you created and click **Launch**.
13. In the pane that opens, complete the following steps:

    a) Choose the instance type.
    b) (Optional) Customize the network on the **Configure Instance** tab.
    c) (Optional) Attach another volume on the **Add Storage** tab.
    d) Set security group rules on the **Configure Security Group** tab.

    After you have reviewed the instance launch, click **Review and Launch**.

After the Connector Appliance is deployed and has successfully started up, go to **Services** > **EC2** > **Instances** and select the instance you have created. Use the **Private IPv4 address** to connect to the Connector Appliance administration page and complete the registration process. You might need to use a bastion host to go to the Connector Appliance administration page at the internal IP address from your browser to continue the installation process.

By default, the Connector Appliance uses DHCP to set its network configuration. You can edit this network configuration using the Connector Appliance web interface. For more information, see Configuring network settings on the Connector Appliance administration page.

Next step: Register your Connector Appliance with Citrix Cloud.

Deploy the Connector Appliance by using a PowerShell script The `connector-appliance-aws.zip` file contains a PowerShell script that creates and starts a new VM. Before running the script ensure that you have the following prerequisites:

- You have either AWS.Tools, AWSPowerShell.NetCore or AWSPowerShell installed on your system. For more information, see https://docs.aws.amazon.com/powershell/latest/userguide/pstools-getting-set-up.html.
- You have created a service role and policy that has VM import access. Both the service role and the policy must be named `vmimport` for this PowerShell script to work. For more information, see https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role.

  > **Note:**
  >
  > To create a service role, you must create an S3 bucket. When creating the policy, set the S3 bucket you have created with VM import access.

- You have created an Amazon EC2 security group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You have S3 permissions and API access.
- You have completed the configuration in Networking prerequisites.

Complete the following steps:

1. On your local system, extract the contents of `connector-appliance-aws.zip` to a folder.
2. In PowerShell, run the following commands:

   a) To be able to run an AWS cmdlet in your local environment, run the following command to add a new profile to the AWS SDK store:

   ```
   Set-AWSCredential -AccessKey <access_key_ID> -SecretKey <
       secret_key> -StoreAs MyProfile
   ```

   Replace the placeholder values with your access key and secret key. Provide a unique profile name. In the example we have provided, it is `MyProfile`.

   b) Set the profile to the default:

   ```
   Initialize-AWSDefaultConfiguration -ProfileName MyProfile
   ```

   c) Change the current directory to the folder where the extracted files are located and run the following command:

   ```
   .\connector-appliance-upload-aws.ps1
   ```

3. Follow the prompts in the script, which guide you through selecting the region for your Connector Appliance deployment, uploading the image to your chosen bucket, and entering a name for your VM.

   - You must use the bucket with VM import access that you created earlier.
   - When asked to select the VPC to use, select the VPC where the NAT gateway and route tables are configured.
   - When asked to select the subnet to use, select the subnet attached to the route table containing the NAT gateway.

   For more information, see Networking prerequisites.

After the Connector Appliance is deployed and has successfully started up, the script displays the private IP address of the Connector Appliance. You might need to use a bastion host to go to the Connector Appliance administration page at the internal IP address from your browser and complete the registration process.

By default, the Connector Appliance uses DHCP to set its network configuration. You can edit this network configuration using the Connector Appliance web interface. For more information, see Configuring network settings on the Connector Appliance administration page.

Next step: Register your Connector Appliance with Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Google Cloud Platform

This section describes how to deploy Connector Appliance on the Google Cloud Platform. You can install the Connector Appliance from the Google Cloud Marketplace. Alternatively, you can deploy a downloaded disk image by using the Google Cloud Platform Console or by using the included PowerShell script.

The file `connector-appliance-gcp.zip` contains:

- `connector-appliance.tar.gz`, which is a disk image of the Connector Appliance
- `connector-appliance-upload-gcp.ps1`, which is a PowerShell script that can be used to automatically deploy the Connector Appliance

Deploy the Connector Appliance from the Google Cloud marketplace

1. Log in to your Google account.
2. Follow the marketplace link provided in Citrix Cloud. (Google Cloud Marketplace)

   Alternatively, you can search for "Connector Appliance for Cloud Services"in the marketplace search.
3. Click **Launch**.
4. On the **New Citrix Connector Appliance for Cloud Services deployment** page, complete the following information:

   - Specify a **Deployment name** for the deployment job.
   - Select the **Zone** to locate the Connector Appliance in.
   - Select the **Machine family**, **Series**, and **Machine type** to use.
   - Select the **Boot disk type** and **Boot disk size in GB** to use.
   - In the **Networking** section, specify the networking interface to be used by the Connector Appliance. If you want to be able to connect to the administration page from a public network, specify an **External IP**.

   Click **Deploy**. You are directed to the **Deployment Manager** page.

   > **Note:**
   >
   > After the Connector Appliance is deployed and has successfully started up, you receive an email to confirm that the Connector Appliance is deployed on Google Cloud Platform.

5. On the **Deployment Manager** page, click on the instance name. Alternatively, you can search for the Connector Appliance instance that you created in the **Compute Engine**.
6. If you previously specified an **External IP** when setting up the networking interface for your Connector Appliance, copy the **External IP address** in the **Network interfaces** section in the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Details tab. Use this IP address to connect to the Connector Appliance administration page and complete the registration process. Alternatively, you can use the **Primary internal IP address** to visit the Connector Appliance administration page from another machine that is in the same subnet as your Connector Appliance.

Next step: Register your Connector Appliance with Citrix Cloud.

Deploy the Connector Appliance by using the Google Cloud Platform console

1. On your local system, extract the contents of `connector-appliance-gcp.zip`.
2. In your Google Cloud Platform project, create a storage bucket. (Alternatively, you can use an existing storage bucket.)
   a) From the main menu, select **Cloud Storage**.
   b) On the main pane, select **Create bucket**.
   c) Specify a name for your bucket.
   d) Configure the data storage and access settings that you require. You can leave these settings as the defaults.
   e) Click **Create**.
3. Inside your storage bucket, select **Upload files** and choose the file `connector-appliance.tar.gz`. Wait while the file uploads.
4. Select the uploaded file to view its details. Copy the value of **gsutil URI** to the clipboard.
5. Open the Cloud Shell by clicking the **Activate Cloud Shell** icon in the header bar.
6. In your Cloud Shell, run the following command to create an image:

```
gcloud compute images create "Image name" --guest-os-features=
    MULTI_IP_SUBNET --source-uri="gsutil URI of uploaded connector-
    appliance.tar.gz file"
```

7. From the main menu, select **Compute Engine** > **VM Instances**.
8. Select **Create Instance**. In the pane that opens, specify the following information:
   a) In the **Name** field, specify a name for the Connector Appliance instance.
   b) Choose a region to locate the Connector Appliance in.
   c) Choose the machine configuration.
   d) In the **Boot disk** section, click **Change**.
   e) In the section that opens, go to the **Custom images** tab.
   f) From the **Image** list, select the image you created.
   g) Click **Select**.
   h) In the **Firewall** section, enable HTTPS traffic to allow access to the Connector Appliance administration page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

i) Specify any additional configuration required. For example, you might not want to use the default networking configuration.

Click **Create**.

9. In the **VM Instances** section, select your newly created VM to view its details.

After the Connector Appliance is deployed and has successfully started up, the **VM Instances** section displays the Connector Appliance IP addresses.

If the Connector Appliance has an external IP address, you can use this IP address to go to the Connector Appliance administration page from your browser and complete the registration process.

If the Connector Appliance has only an internal IP address, use a bastion host to go to the Connector Appliance administration page from your browser and complete the registration process. For more information, see https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host.

Next step: Register your Connector Appliance with Citrix Cloud.

Deploy the Connector Appliance by using a PowerShell script To use the provided PowerShell script to deploy the Connector Appliance, you must have the Google Cloud SDK installed on your system.

1. On your local system, extract the contents of `connector-appliance-gcp.zip` to a folder.
2. In PowerShell, change the directory to the folder where the extracted files are located.
3. Run the command `.\connector-appliance-upload-GCP.ps1`.
4. In the browser window that opens, authenticate with the Google Cloud SDK with an account that has access to the project you want to deploy the Connector Appliance to.
5. In Google Cloud Tools for PowerShell, when prompted by the PowerShell script, select the project to use. Press Enter.
6. Follow the prompts in the script, which guide you through uploading the disk, creating an image, and creating a virtual machine.
7. After you have created the first VM, the script asks if you want to create another VM from the uploaded image.

    - Type `y` to create another VM.
    - Type `n` to exit the script.

After the Connector Appliance is deployed and has successfully started up, the script displays the internal IP address of the Connector Appliance. Alternatively, you can go to the Google Cloud Platform console to find the Connector Appliance internal IP address. The **Compute Engine** > **VM Instances** section displays the Connector Appliance IP address.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use a bastion host to go to the Connector Appliance administration page at the internal IP address from your browser and complete the registration process. For more information, see https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host.

Next step: Register your Connector Appliance with Citrix Cloud.

Register your Connector Appliance with Citrix Cloud

Register a Connector Appliance with Citrix Cloud to provide a channel for communication between Citrix Cloud and your resource locations.

After you install your Connector Appliance on the hypervisor and start it, the console displays the IP address of the Connector Appliance. The console also displays an SSL fingerprint that you can use to validate your connection to the Connector Appliance UI.



1. Copy the Connector Appliance IP address to your browser address bar.

   > **Note:**
   >
   > You may have to include `https://` at the start of the IP address.

   The Connector Appliance UI uses a self-signed certificate, which is valid for five years. As a result, you might see a message about the connection not being secure. To verify the connection to your Connector Appliance, you can compare the SSL fingerprint in the console with the fingerprint the browser receives from the webpage.

   For example, in the Google Chrome browser, complete the following steps:

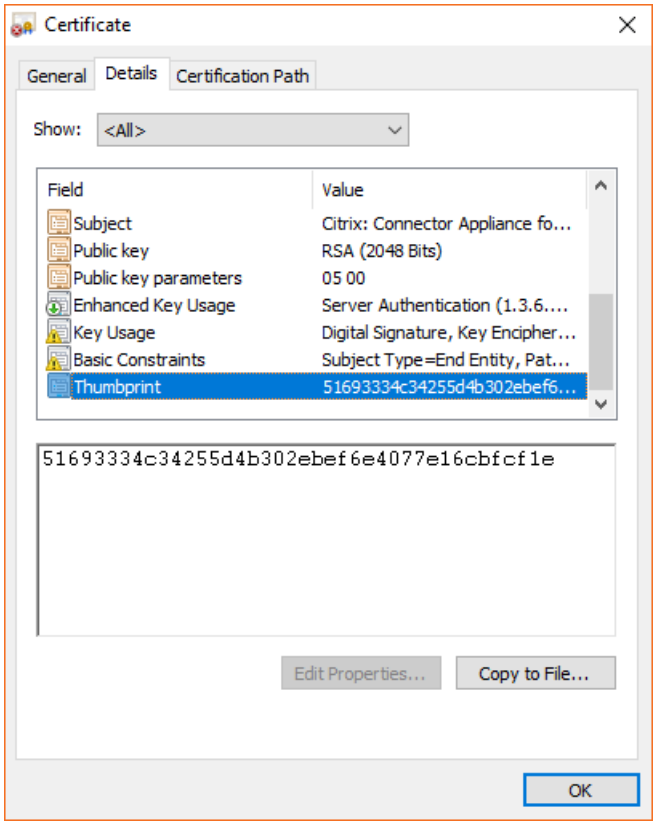
© 1997–2026 Citrix Systems, Inc. All rights reserved.

a) Click the **Not Secure** marker next to the address bar.

b) Select **Certificate**. The **Certificate** window opens.

c) Go to the **Details** tab and find the **Thumbprint** field.

If the value of the **Thumbprint** field and the SSL fingerprint provided in the console match, you can confirm that your browser is connecting directly to the Connector Appliance UI.



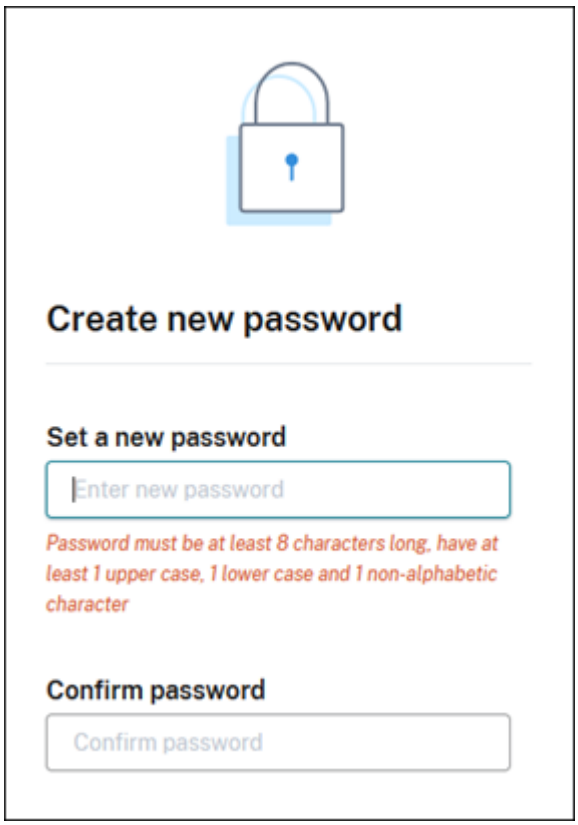
You can replace this self-signed certificate with one of your own that is signed by your organization or generated by using your organization's chain of trust. For more information, see Managing certificates.

2. If your browser requires an extra step to confirm that you want to continue to the site, complete this step now.

   The **Create new password** webpage opens.

3. Create a password for your Connector Appliance UI and click **Set password**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



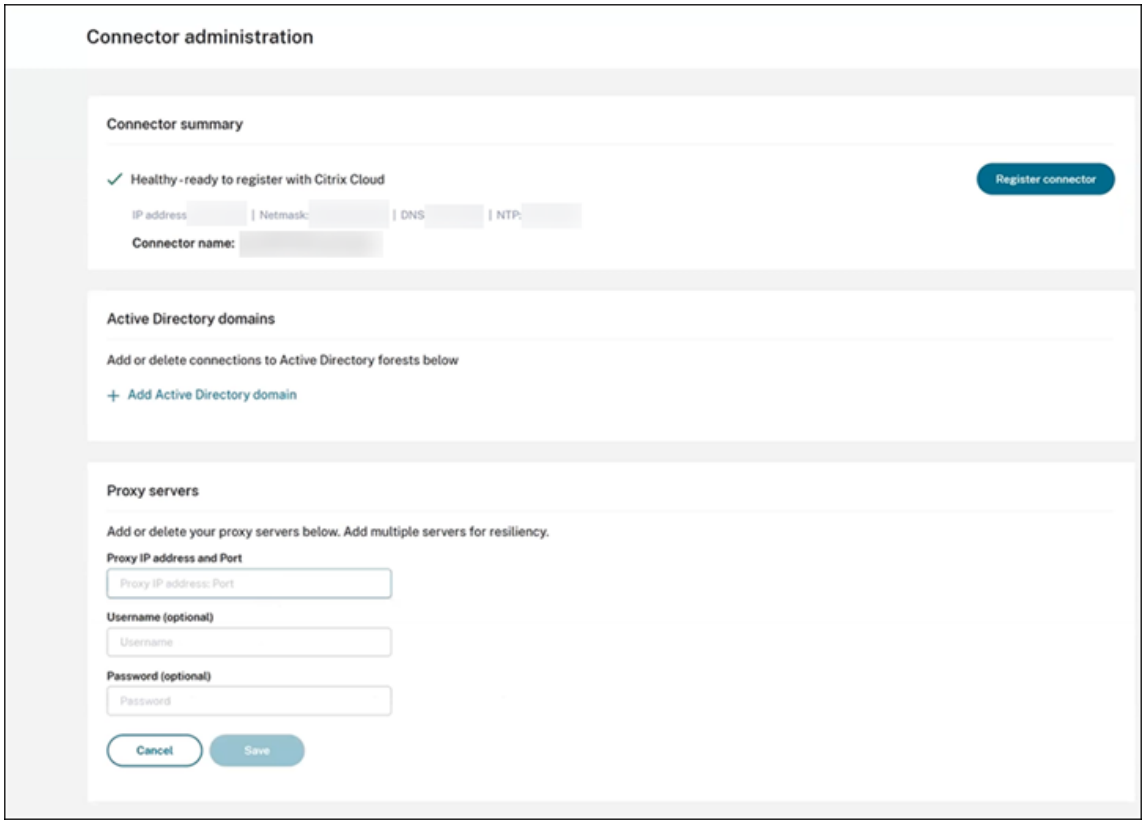
The password you set must meet the following requirements:

- 8 or more characters long
- Contains both upper and lower case letters
- Contains at least one non-alphabetic character

Ensure that you store this password in a safe place for future use.

4. Sign in with the password you set. The **Connector administration** page opens.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. (Optional) If you use one or more web proxies, you can add the proxy addresses in the **Proxy servers** section. Both unauthenticated and authenticated proxies are supported. To add an unauthenticated proxy, provide a valid **Proxy IP Address and Port**. To add an authenticated proxy, provide a valid **Username** and **Password** as well.

   > **Note:**
   >
   > Only basic proxy authentication is supported. Other forms of authentication are not supported.

   Only traffic to external systems is routed through the web proxy. For more information, see Connector Appliance communication.

6. (Optional) If your network uses TLS intercepting web proxies to access the internet you may require your Connector to trust its Root Certificate Authority to successfully communicate with the cloud.

   a) Under **Root certificate authorities**, select **Add certificate**.

   b) Copy the contents of the certificate in PEM format:

   ```
   -----BEGIN CERTIFICATE-----
   <certificate-base64-bytes>
   -----END CERTIFICATE-----
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c) In **Full Certificate Details**, paste the certificate contents.

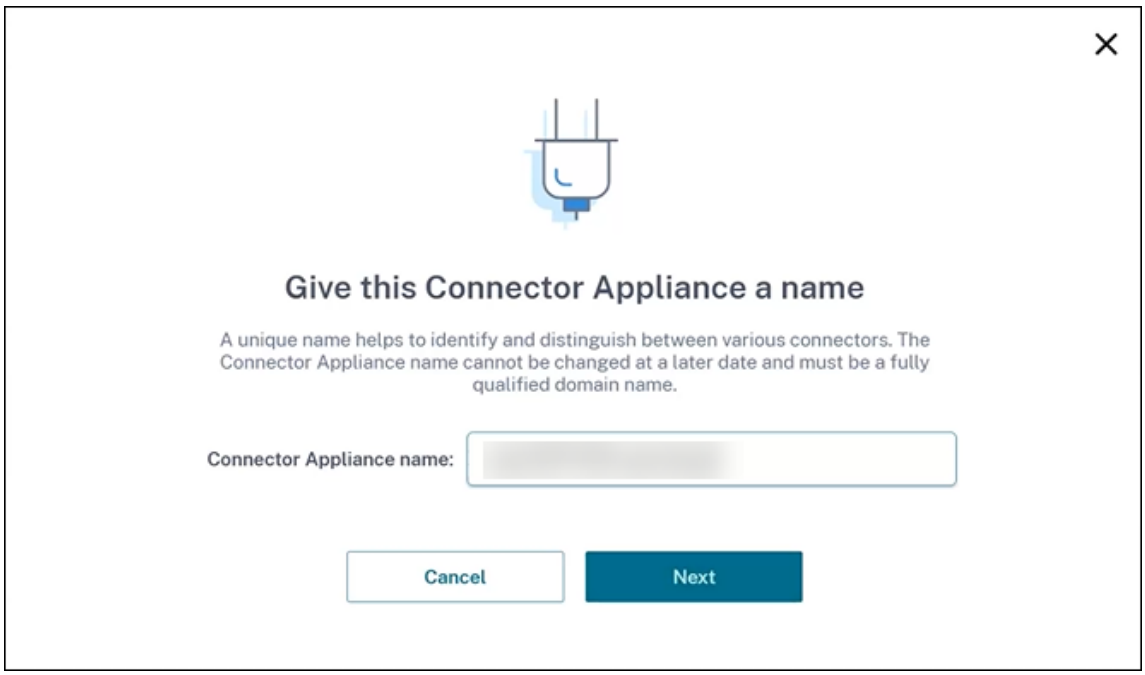
d) Select **Add Certificate**.

To add a RootCA using the Connector Appliance APIs, see Managing root certificate authorities in the Citrix Developer documentation.

> **Note:**
>
> Certificates which are expired or will expire in the next 30 days will show a warning.

7. Click **Register Connector** to open the registration task.
8. Choose a name for your Connector Appliance. This name can help you distinguish between the various Connector Appliances that exist in your resource location. After you register your Connector Appliance, the name cannot be changed.

   Enter the name in the **Connector Appliance name** field and click **Next**.



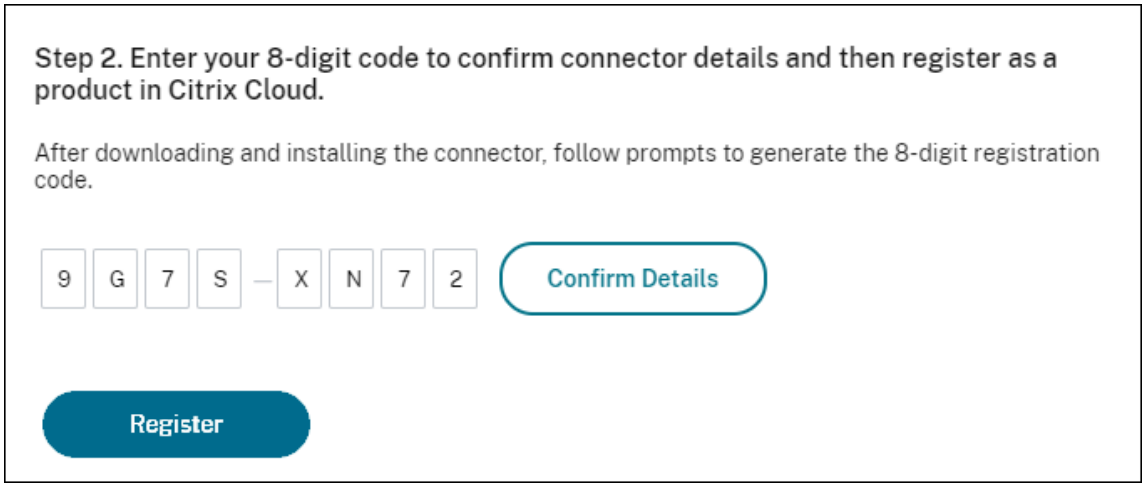
   The webpage provides a code to use to register with Citrix Cloud. This code expires in 15 minutes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



9. Use the **Copy** button to copy the code to the clipboard.
10. Return to the **Resource Locations** webpage.
11. Paste the code into **Step 2** of the **Install Connector Appliance** task. Click **Confirm Details**.

    Citrix Cloud verifies that the Connector Appliance is present and can be contacted. If the registration code has expired, you are prompted to generate a new code.



12. Click **Register**.

    The page shows whether the registration was successful. If the registration failed, you are prompted to try again.

13. Click **Close**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The **Connector Appliance administration page** also enables you to download a diagnostic report for the Connector Appliance. For more information, see Generating a diagnostic report.

After registering your Connector Appliance

For each resource location, we advise that you install and register two or more Connector Appliances. This configuration ensures continuous availability and enables the connectors to balance the load.

You cannot directly manage your Connector Appliance.

The Connector Appliance is updated automatically. You are not required to take any actions to update your connector. You can specify the time and day that you want Connector Appliance updates to be applied in your resource location. For more information, see Connector updates.

Do not clone, suspend, or take a snapshot of your Connector Appliance VMs. These actions are not supported.

You are only presented with the **Create new password** page the first time that you connect to the Connector Appliance UI. Ensure that you store this password in a safe place for future use. This password cannot be reset. If you forget the password, you must reinstall the Connector Appliance. On subsequent connections to the UI, you are asked to input the password you set when registering the Connector Appliance.



Connector Appliance Connectivity Checks

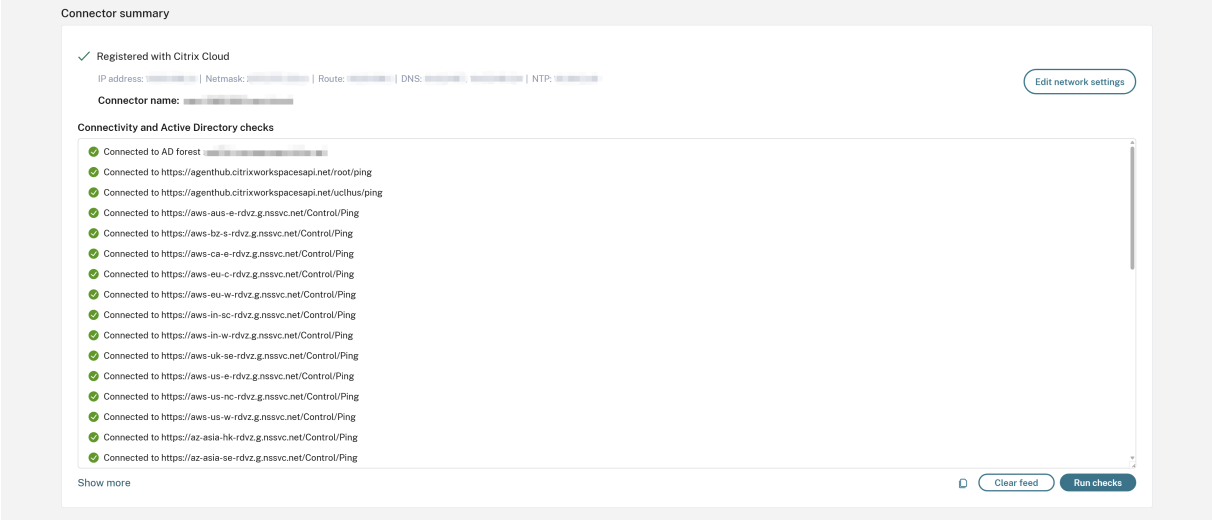
The Connector Appliance implements a set of automated connectivity checks to ensure that all requirements for Connector Appliance connectivity are met. For more information on the connectivity requirements, see Internet connectivity requirements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

These checks can be manually triggered, and the results can be viewed from the Connector Appliance Admin user interface.

Steps to Access and Run Connectivity Checks

1. From the Connector Appliance console in your hypervisor, copy the IP address to your browser's address bar.
2. Enter the password that you set when you registered your Connector Appliance.
3. The tests automatically run upon loading the page.
4. To rerun the tests, click **Run Checks**.
5. To copy the results to the clipboard, click the **Copy** icon.



Active Directory Checks The checks related to Active Directory are grouped by domain. If the appliance has not been joined to any domains then no Active Directory tests will be run.

For each joined domain, the following checks are run:

- Domain connectivity
- Query time synchronization with the domain
- Validate the ability to handle requests to the domain from Citrix Cloud

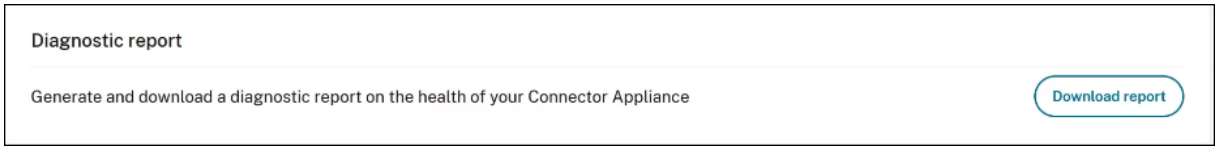
Gateway Service Provider For the gateway service, the connector performs a query for the list of points of presence and validates connectivity.

Core Connector Services For the core connector services, the Connector Appliance performs HTTP GET requests to a range of Cloud Services used as part of core functionality. The appliance also tests connectivity to the Azure Container Registry (ACR), which is used for downloading new versions of the connector.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Generating a diagnostic report

You can generate and download a diagnostic report from the **Connector Appliance administration page**.



1. From the Connector Appliance console in your hypervisor, copy the IP address to your browser address bar.
2. Enter the password that you set when you registered your Connector Appliance.
3. In the **Diagnostic report** section of the page, click **Download Report**.

The diagnostic reports are provided in a `.zip` file.

Verify your network connection

You can check your network connection from the **Connector Appliance administration page** by using the **TCP Capture** diagnostic check.

1. On the **Connector Appliance administration page**, click your account name in the header bar and select **Network Diagnostics**.
2. (Optional) In the **TCP Capture** section, enter the target IP address, host name, or port to restrict the TCP capture.
3. From the **Trace Duration** menu, select the duration for which you want your trace to run.
4. (Optional) Enable **Packet Tracing** to capture the contents of the packets.

   When packet tracing is disabled, the TCP capture functionality uses a best-effort approach to capture the headers for diagnosis. This best-effort approach captures the first 512 bytes of each packet. However, as headers are not a fixed size, this approach might not capture all of the header.
5. Click **Start trace**.
6. Wait until the trace has completed. After the trace has completed, you can download a trace report or start a new trace.

   - Click **Download** to download the trace report. The trace report is provided in a `.pcap` file.
   - Click **Start new trace** to begin another trace.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Network Connectivity Probe Tool

The Connector Appliance Network Connectivity Probe provides an on-demand way to test connectivity to supported network targets using multiple protocols, with optional proxy selection and packet capture. For details on supported protocols, proxy behavior, allowed targets, and interpreting probe results, see the Connector Appliance Network Connectivity Probe page.

Connecting Active Directory to Citrix Cloud

You can use Connector Appliance to connect a resource location to forests which do not contain Citrix Virtual Apps and Desktops resources. For example, in the case of Citrix Secure Private Access™ customers or Citrix Virtual Apps and Desktops customers with some forests only used for user authentication.

For more information, see Active Directory with Connector Appliance.

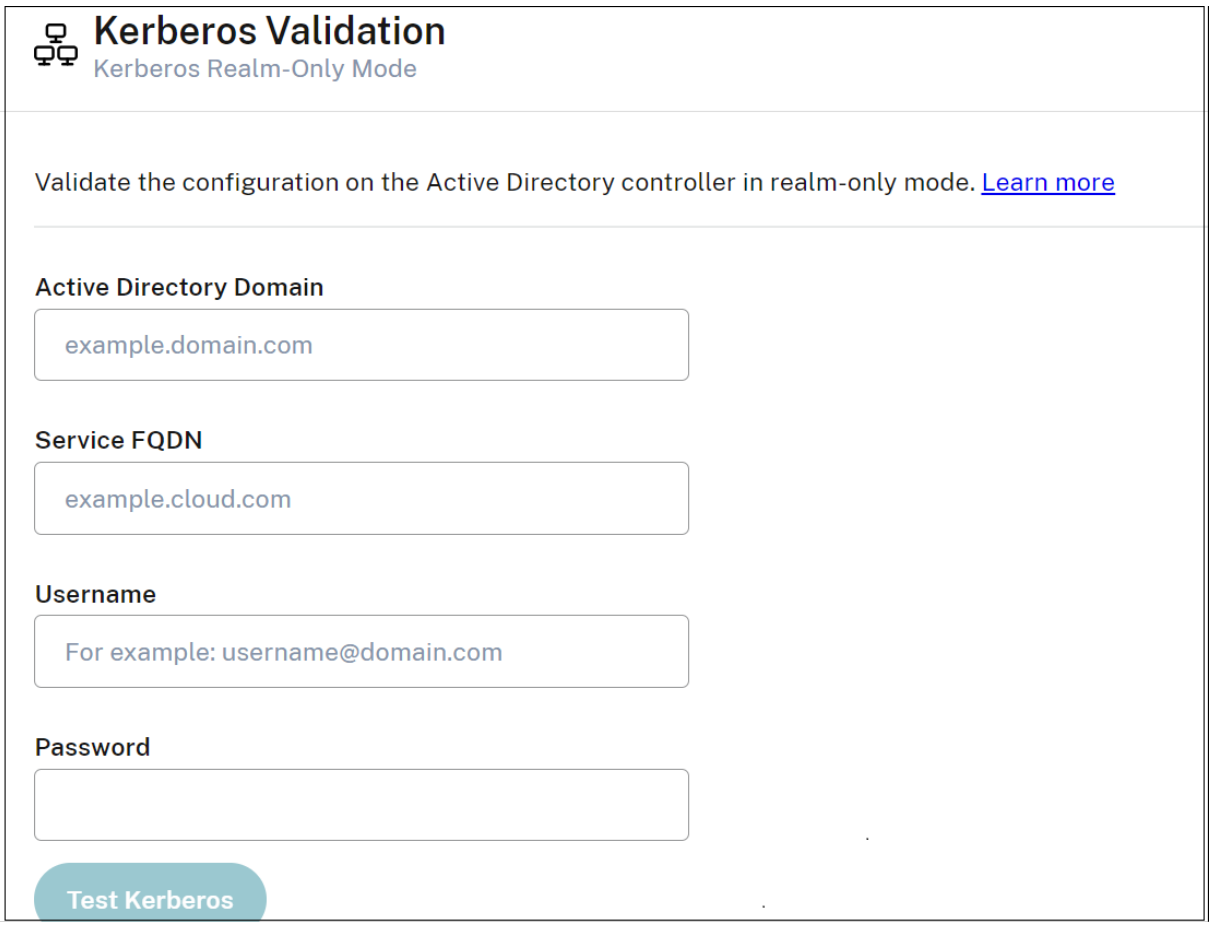
Validating your Kerberos configuration

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) mode configuration.

Validate Kerberos realm-only configuration:

1. Go to the **Connector Appliance administration** page.
2. From the Connector Appliance console in your hypervisor, copy the IP address to your browser address bar.
3. Enter the password that you set when you registered your Connector Appliance.
4. To validate your realm-only Kerberos configuration select the **Kerberos Validation Realm-Only** in the **Active Directory domains** section.
5. Specify the **Active Directory Domain**.
    - If you're validating a Kerberos realm-only mode configuration, you can specify any Active Directory domain. This mode doesn't depend on being joined to the domain.
6. Specify the **Service FQDN**. The default service name is assumed to be "https". If you specify "computer.example.com", this value is considered the same as "https://computer.example.com".
7. Specify the **Username**.
8. Specify the **Password**.
9. Click **Test Kerberos**.

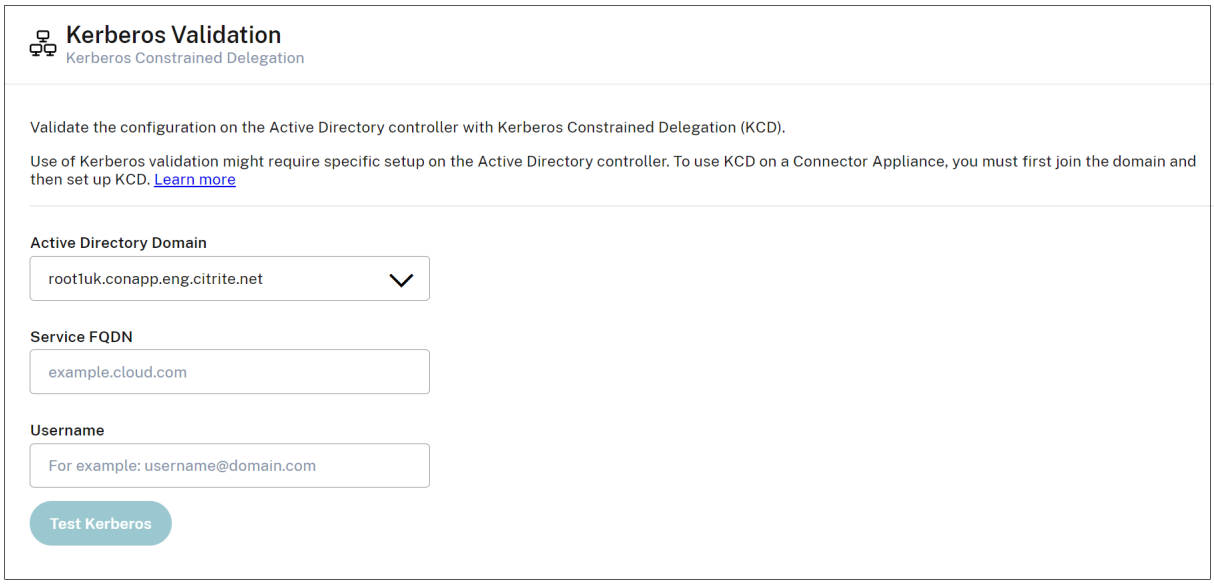
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Validate Kerberos Constrained Delegation (KCD) configuration:

1. Go to the **Connector Appliance administration** page.
2. To validate **Kerberos Constrained Delegation (KCD)** mode for domains to which the Connector Appliance has been joined, select **Kerberos validation** from the ellipsis menu (…) of the relevant domain.
3. Specify the **Active Directory Domain**.
    - If you're validating a Kerberos Constrained Delegation configuration, you must select from a list of joined domains.
4. Specify the **Service FQDN**. The default service name is assumed to be "https". For example, specify "computer.example.com", this value is considered the same as "https://computer.example.com%E2%80%9D.
5. Specify the **Username**.
    - For the Kerberos Constrained Delegation mode, you can also validate the kerberos setup using service accounts by selecting the **Service Accounts** tab.
6. Click **Test Kerberos**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

For more information about Kerberos, see the Microsoft documentation.

Network settings for your Connector Appliance

By default, the IP address and network settings of your Connector Appliance are automatically assigned by using DHCP.

After registering your Connector Appliance by using DHCP, you can edit its network settings in the **Connector Appliance administration page**.

However, if DHCP is not available in your environment or if you do not have access to the **Connector Appliance administration page**, you can set the network configuration directly on the Connector Appliance console.

Configuring network settings on the Connector Appliance administration page

After registering your Connector Appliance by using DHCP, you can edit its network settings in the **Connector Appliance administration page**.

To manually configure your network settings:

1. In the **Connector Summary** section, select **Edit network settings**.
2. In the **Network settings** dialog, choose **Configure your own network settings**.
3. Enter the **IP address**, **Subnet mask**, and **Default gateway**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Add one or more **DNS servers**.
5. Add one or more **NTP servers**.
6. Click **Save**.

When you save changes to your network settings, the Connector Appliance restarts. During the restart, the Connector Appliance is temporarily unavailable. You are logged out of the **Connector Appliance administration page** and the URL of this page changes. You can find the new URL in the Connector Appliance console or by looking at the network information in your hypervisor.

To change your network configuration to use automatically assigned values:

1. In the **Connector Summary** section, select **Edit network settings**.
2. In the **Network settings** dialog, choose **Obtain IP address automatically**.
3. Click **Save**.

When you save changes to your network settings, the Connector Appliance restarts. During the restart, the Connector Appliance is temporarily unavailable. You are logged out of the **Connector Appliance administration page** and the URL of this page changes. You can find the new URL in the Connector Appliance console or by looking at the network information in your hypervisor.

Set the network configuration by using the Connector Appliance console

By default, the IP address and network settings of your Connector Appliance are automatically assigned by using DHCP. However, if DHCP is not available in your environment or if you do not have access to the **Connector Appliance administration page**, you can set the network configuration directly on the Connector Appliance console.

To set the network configuration:

1. In your hypervisor, restart the Connector Appliance.
2. While the Connector Appliance starts up, watch the console for the message `Welcome to GRUB!`.
3. When you see this message, press **Esc** to enter the GRUB menu.
4. To edit the boot parameters, press **e**.

   You see a view that looks like the following image:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Edit the line that begins with `linux` to include your required network configuration.
   - To specify DHCP networking, append `network=dhcp` to the end of the line.
   - To specify static networking, append the following parameters to the end of the line:

     ```
     network=static:ip=<static_ip_address>:netmask=<netmask>:route
        =<default_gateway>:dns=<dns_server_1>,<dns_server_2>:ntp=<
        ntp_server_1>,<ntp_server_2>
     ```

     Replace the placeholder values with the values for your configuration.
6. Press **Ctrl+X** to start the Connector Appliance with the new configuration.

Change the administrator user password for the Connector Appliance

1. From the user menu in the top-right of the console, select **Change password**.

   The change password page is displayed.
2. Enter your current password and then enter and confirm the new password. The new password you set must meet the following requirements:
   - 8 or more characters long
   - Contains both upper and lower case letters
   - Contains at least one non-alphabetic character
   - Must not be the same as current password
3. Select **Change password** to save your changes.

Citrix Cloud signs you out automatically and redirects you to the sign-in page.

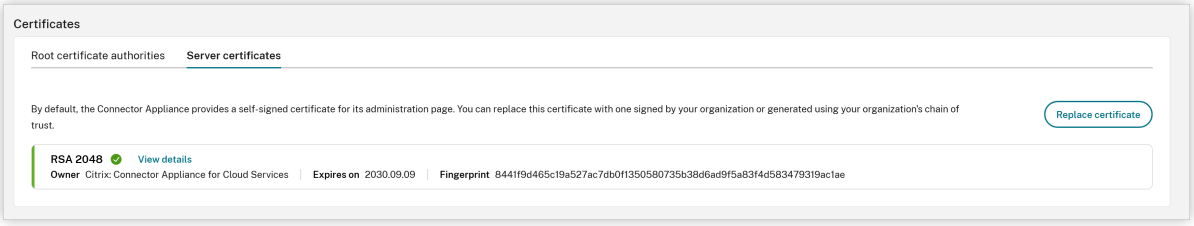
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Replace Server Certificate

The Connector Appliance allows administrators to replace the default self-signed SSL or TLS certificate used by its administration web interface. Administrators can use a custom certificate signed by their organization or generated using their organization's chain of trust.

To access the server certificate management interface, go to the Connector Appliance administrator interface. Navigate to **Certificates** and select the **Server certificates** tab.

By default, the Connector Appliance uses a self-signed certificate. After you replace it with a custom certificate, a trusted certificate authority must issue the certificate for the browser to trust the administration page.

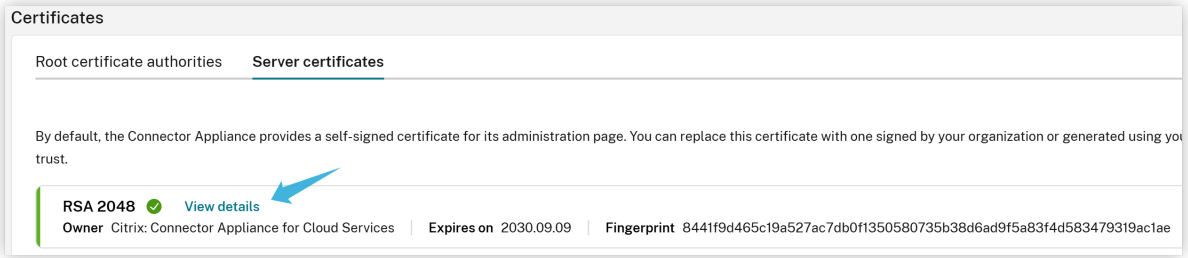


Viewing the current server certificate

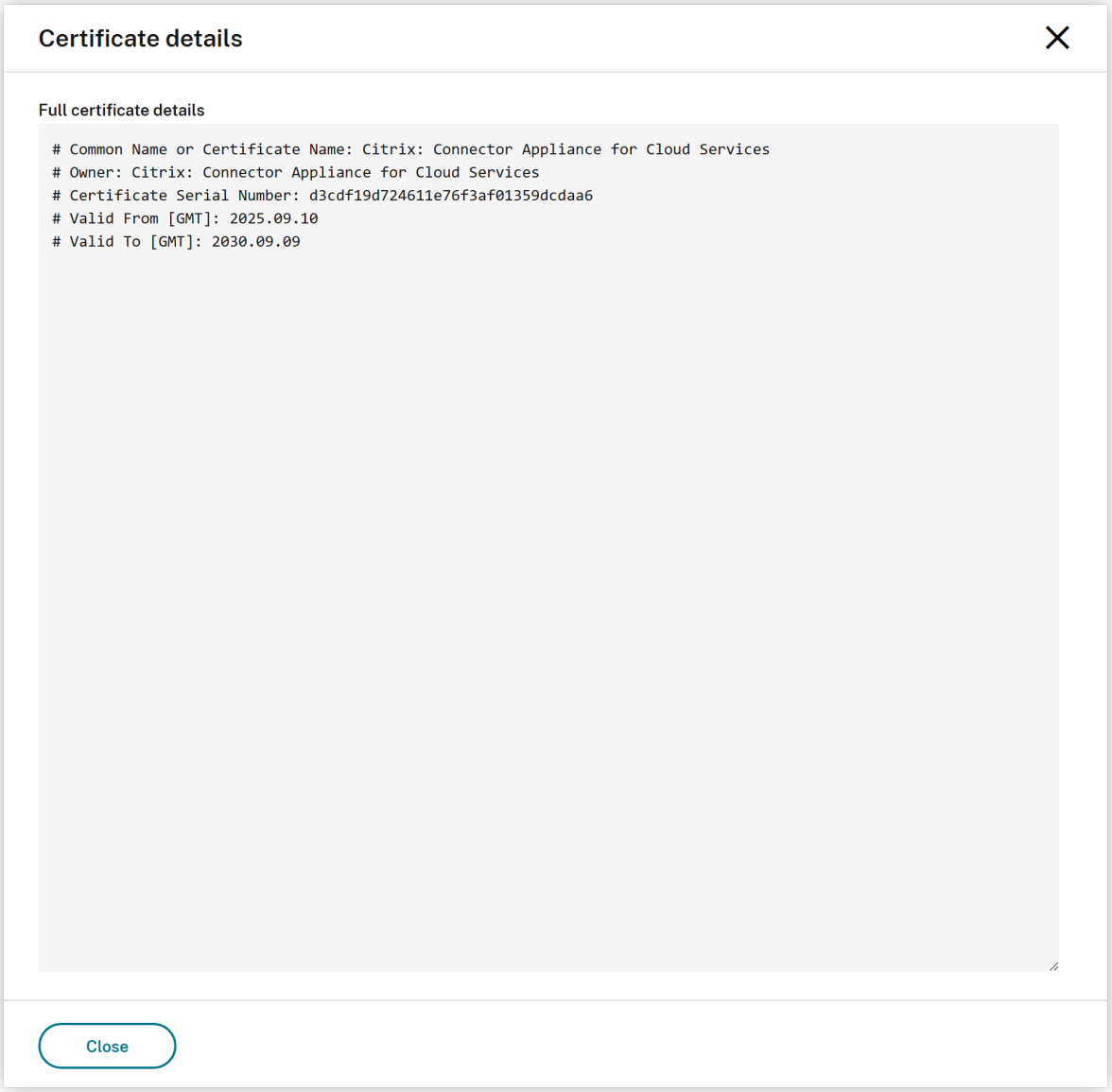
The **Server certificates** tab displays a card with information about the current certificate:

- **Subject** —the certificate algorithm and key length (for example, RSA 2048).
- **Owner** —the certificate issuer or owner, if available.
- **Expires on** —the certificate expiry date.
- **Fingerprint** —the SHA-256 fingerprint of the certificate.

To view full certificate details, click the **View details** link on the certificate card. A side panel opens and displays the complete parsed certificate information. Click **Close** to dismiss the details panel.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



Replacing the server certificate

You can replace the server certificate with a custom certificate signed by your organization.

Prerequisites: Before replacing the certificate, ensure that you have the following

- A certificate file in **PEM format**. The certificate should be issued by a certificate authority trusted by the browsers that access the Connector Appliance administration page.
- The corresponding **private key** in **PEM format**.
- The **passphrase** for the private key, if the key is encrypted (optional).

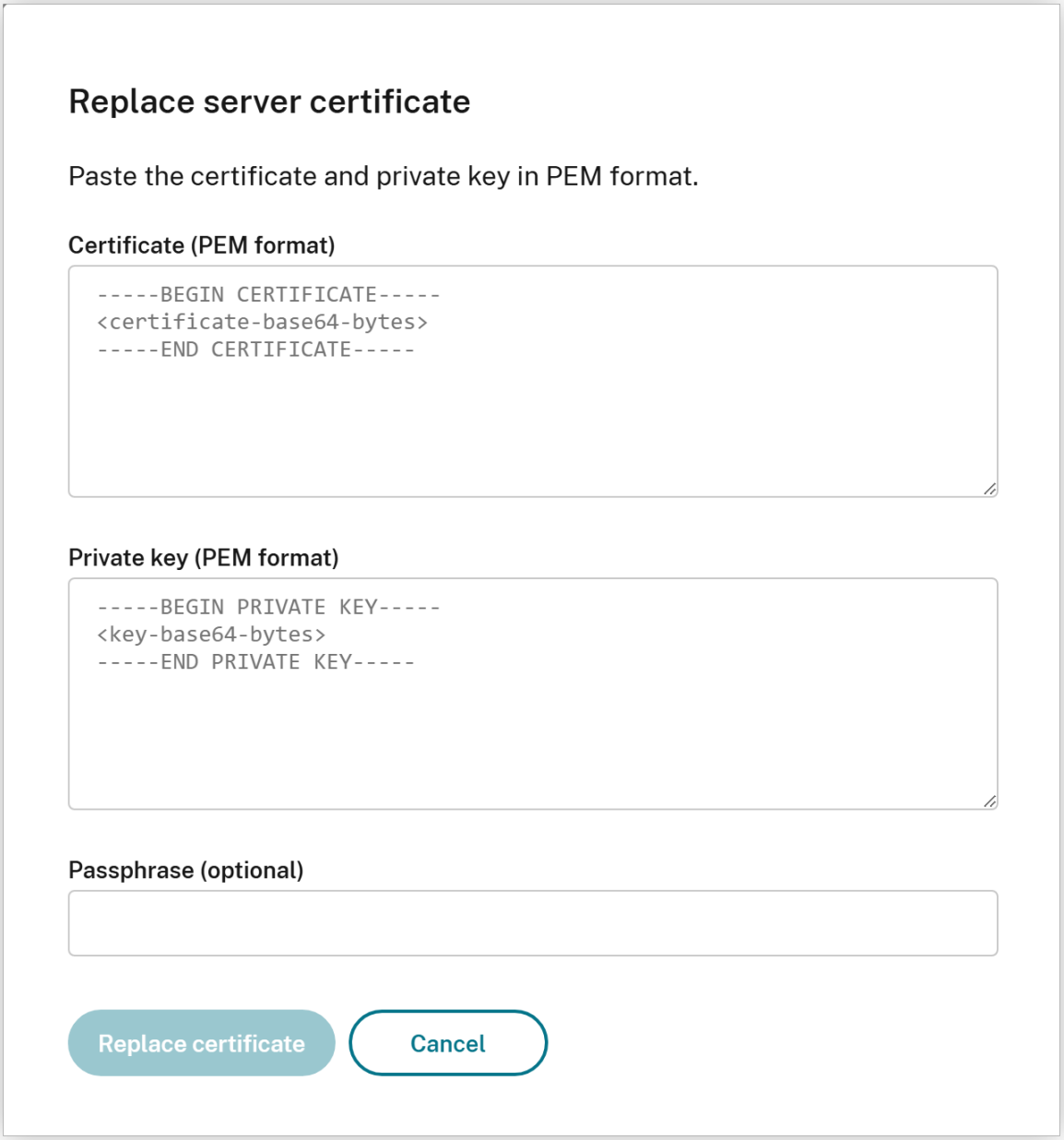
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Steps to replace the certificate

1. From the Connector Appliance console in your hypervisor, copy the IP address and paste it into your browser's address bar.
2. Enter the password that you set when you registered your Connector Appliance.
3. Navigate to **Certificates** in the left-hand menu.
4. Select the **Server certificates** tab.
5. Click the **Replace certificate** button.
6. In the Replace server certificate dialog:
    - Paste the certificate content in PEM format into the **Certificate (PEM format)** field. The certificate should begin with `-----BEGIN CERTIFICATE-----` and end with `-----END CERTIFICATE-----`.
    - Paste the private key in PEM format into the **Private key (PEM format)** field. The key should begin with `-----BEGIN PRIVATE KEY-----` and end with `-----END PRIVATE KEY-----`.
    - (Optional) If the private key is encrypted, enter the passphrase in the **Passphrase (optional)** field.
7. Click **Replace certificate** to submit.

If the replacement is successful, the system displays a success message and updates the certificate card with the new certificate information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Certificate format requirements

- Both the certificate and private key must be in **PEM format**.
- The certificate field supports a full certificate chain. If an intermediate CA signs your certificate, paste the full chain (server certificate followed by intermediate certificates).
- Supported key types are **RSA** and **ECDSA**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

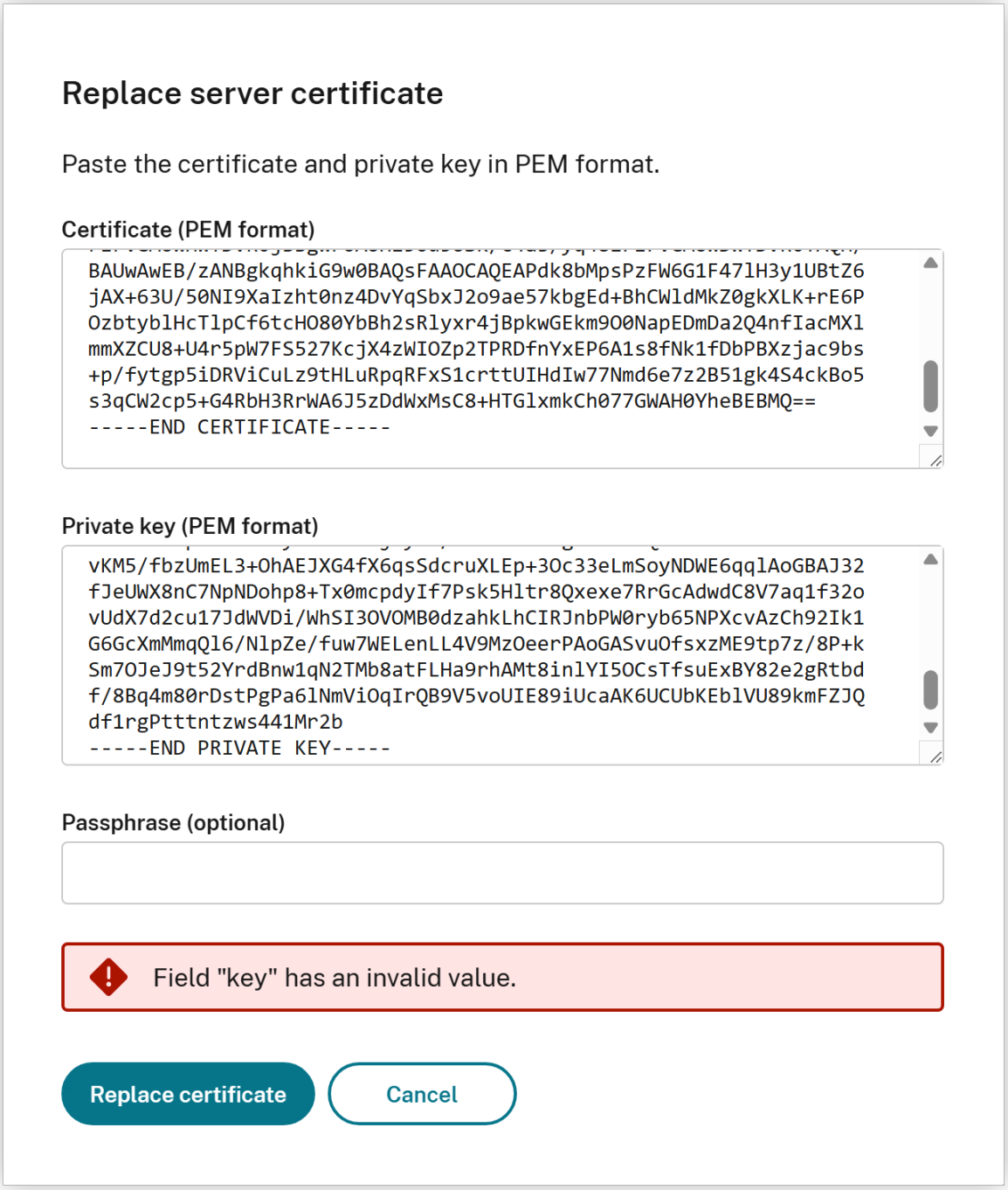
Error handling

If the certificate replacement fails, the dialog displays an error message. Common reasons for failure include:

- The certificate and private key do not match.
- The certificate or private key is not in valid PEM format.
- The private key passphrase is incorrect.

Review the error message, correct the issue, and try again. Click **Cancel** to close the dialog without making changes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Reverting to the self-signed certificate

To revert to the default self-signed certificate, you must re-deploy the Connector Appliance. There is currently no option to revert the certificate independently.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Notes**
>
> - After you replace the certificate, the Connector Appliance administration page uses the new certificate for all subsequent HTTPS connections.
> - The certificate information shown on the **Server certificates** tab is refreshed automatically every 30 seconds.
> - The certificate replacement operation requires you to be logged in with a valid session token.

Active Directory with Connector Appliance

June 22, 2026

You can use Connector Appliance to connect a resource location to forests which do not contain Citrix Virtual Apps and Desktops™ resources. For example, in the case of Citrix Secure Private Access customers or Citrix Virtual Apps and Desktops customers with some forests only used for user authentication.

When using multi-domain Active Directory with Connector Appliance, the following restrictions apply:

- Connector Appliance cannot be used in place of Cloud Connectors in forests that contain VDAs.

Requirements

Active Directory requirements

- Joined to an Active Directory domain that contains the resources and users that you use to create offerings for your users. For more information, see Deployment scenarios for Connector Appliances in Active Directory in this article.
- Each Active Directory forest that you plan to use with Citrix Cloud™ must always be reachable by two Connector Appliances.
- The Connector Appliance must be able to reach domain controllers in both the forest root domain and in the domains that you intend to use with Citrix Cloud. For more information, see the following Microsoft support articles:
  - How to configure domains and trusts
  - "Systems services ports"section in Service overview and network port requirements for Windows

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Use universal security groups instead of global security groups. This configuration ensures that user group membership can be obtained from any domain controller in the forest.

Network requirements

- Connected to a network that can contact the resources you use in your resource location.
- Connected to the Internet. For more information, see System and Connectivity Requirements.

In addition to the ports listed in Connector Appliance communication, the Connector Appliance requires an outbound connection to the Active Directory domain via these ports:

Service	Port	Supported Domain Protocol
Kerberos	88	TCP/UDP
NetBIOS Name Service	137	UDP
NetBIOS Datagram	138	UDP
NetBIOS Session	139	TCP
LDAP	389	TCP/UDP
SMB over TCP	445	TCP
Kerberos kpasswd	464	TCP/UDP
Global Catalog	3268	TCP
Dynamic RPC Ports	49152–65535	TCP

The Connector Appliance uses LDAP signing to secure connections to the domain controller. This means that LDAP over SSL (LDAPS) is not required. For more information on LDAP signing, see How to enable LDAP signing in Windows Server and Microsoft Guidance for Enabling LDAP Channel Binding and LDAP Signing.

Supported Active Directory functional levels

Connector Appliance has been tested and is supported with the following forest and domain functional levels in Active Directory.

Forest Functional Level	Domain Functional Level	Supported Domain Controllers
Windows Server 2016	Windows Server 2016	Windows Server 2019

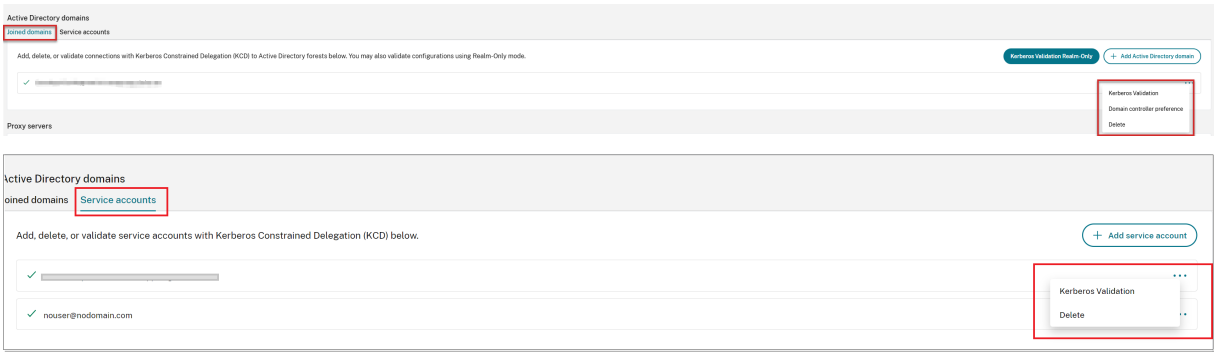
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Other combinations of domain controller, forest functional level, and domain functional level have not been tested with the Connector Appliance. However, these combinations are expected to work and are also supported.

Connect an Active Directory domain to Citrix Cloud by using Connector Appliance

When you connect to the Connector Appliance administration webpage, the **Active Directory domains** section displays two tabs.

- **Joined Domains** –Used for joining the Connector Appliance to AD Domains by creating a machine account for the appliance in the Domain. Kerberos can be validated by clicking the ellipsis menu on the right-hand side of the joined domain. Machine account presence in the domain is required.
- **Service Accounts** –Used as part of a Secure Private access (SPA) solution to achieve Kerberos SSO using a service account instead of the machine account created by joining the domain. Kerberos can be validated by clicking the ellipsis menu on the right-hand side of the service account. Having a specific domain associated with the machine isn't mandatory. However, even if the Connector Appliance isn't connected to the domain, it can still connect to the domain controller.



To configure Active Directory to connect to Citrix Cloud through the Connector Appliance, complete the following steps.

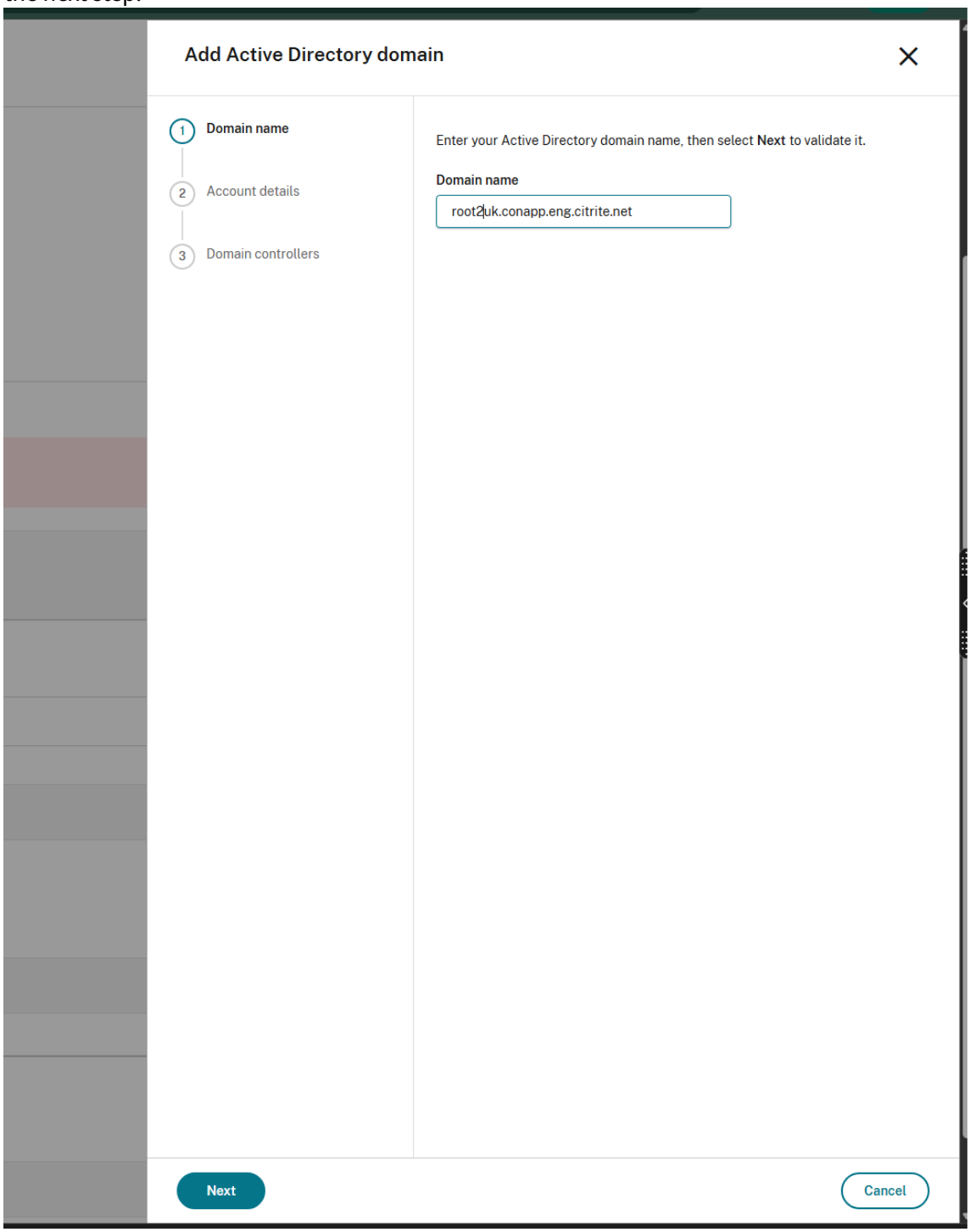
1. Install a **Connector Appliance** in your resource location.

   You can follow the information in the Connector Appliance product documentation.

2. Connect to the **Connector Appliance** administration webpage in your browser by using the IP address provided in the **Connector Appliance** console.
3. In the **Active Directory domains** section, navigate to the **Joined domains** tab.
4. Click **+ Add Active Directory domain**, a new pop-up window displays to enter the domain name.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. On the **Domain name** step, enter the Active Directory domain name and click **Next**. The **Connector Appliance** checks the domain. If the check is successful, the wizard advances to the next step.



6. On the **Account details** step, provide the following information, and then click **Next**:

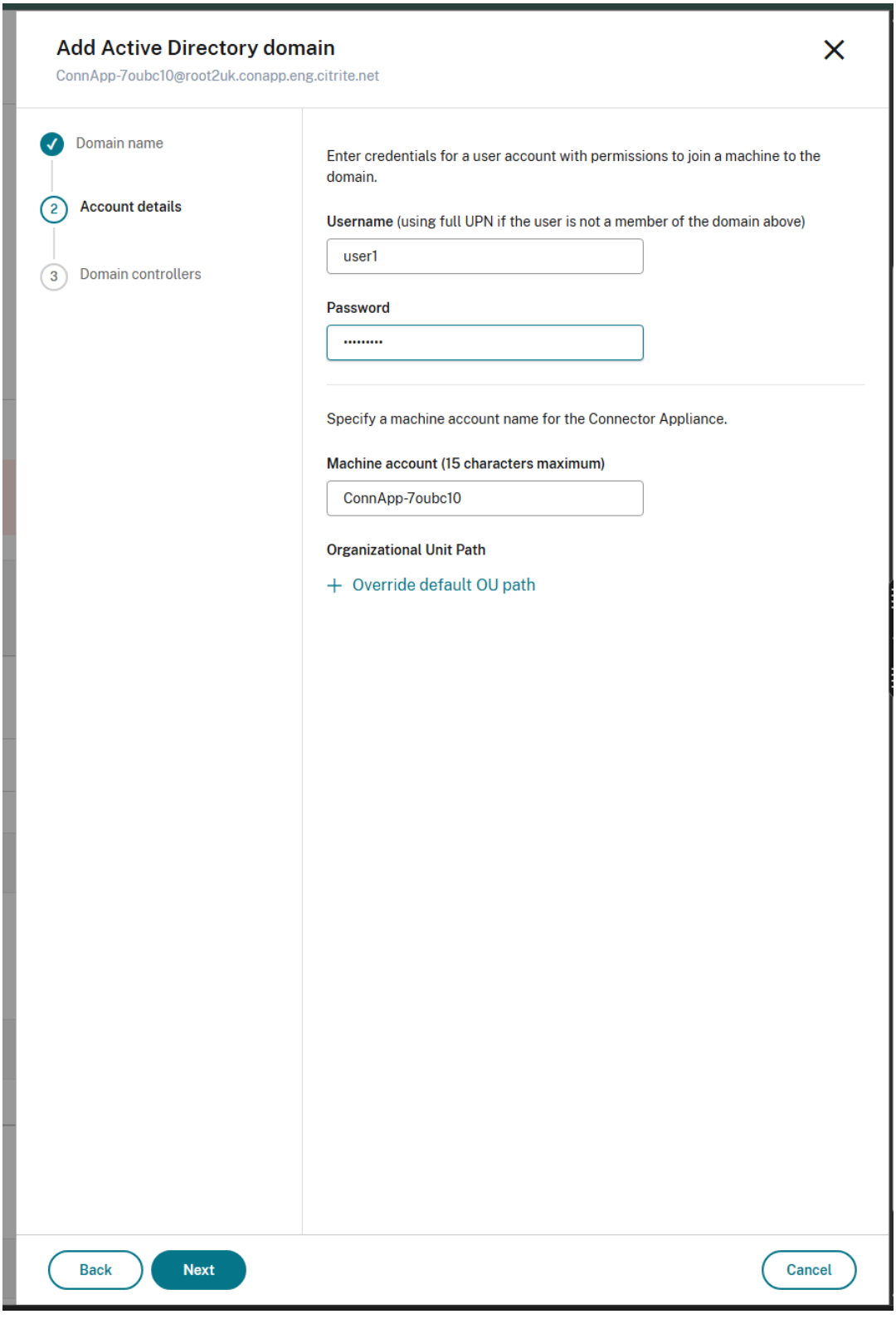
   - The user name and password of an Active Directory user with permission to join the do-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

main.

- A machine name. The **Connector Appliance** suggests a machine name; you can override it with your own machine name of up to 15 characters. This machine name is created in the Active Directory domain when the **Connector Appliance** joins it.

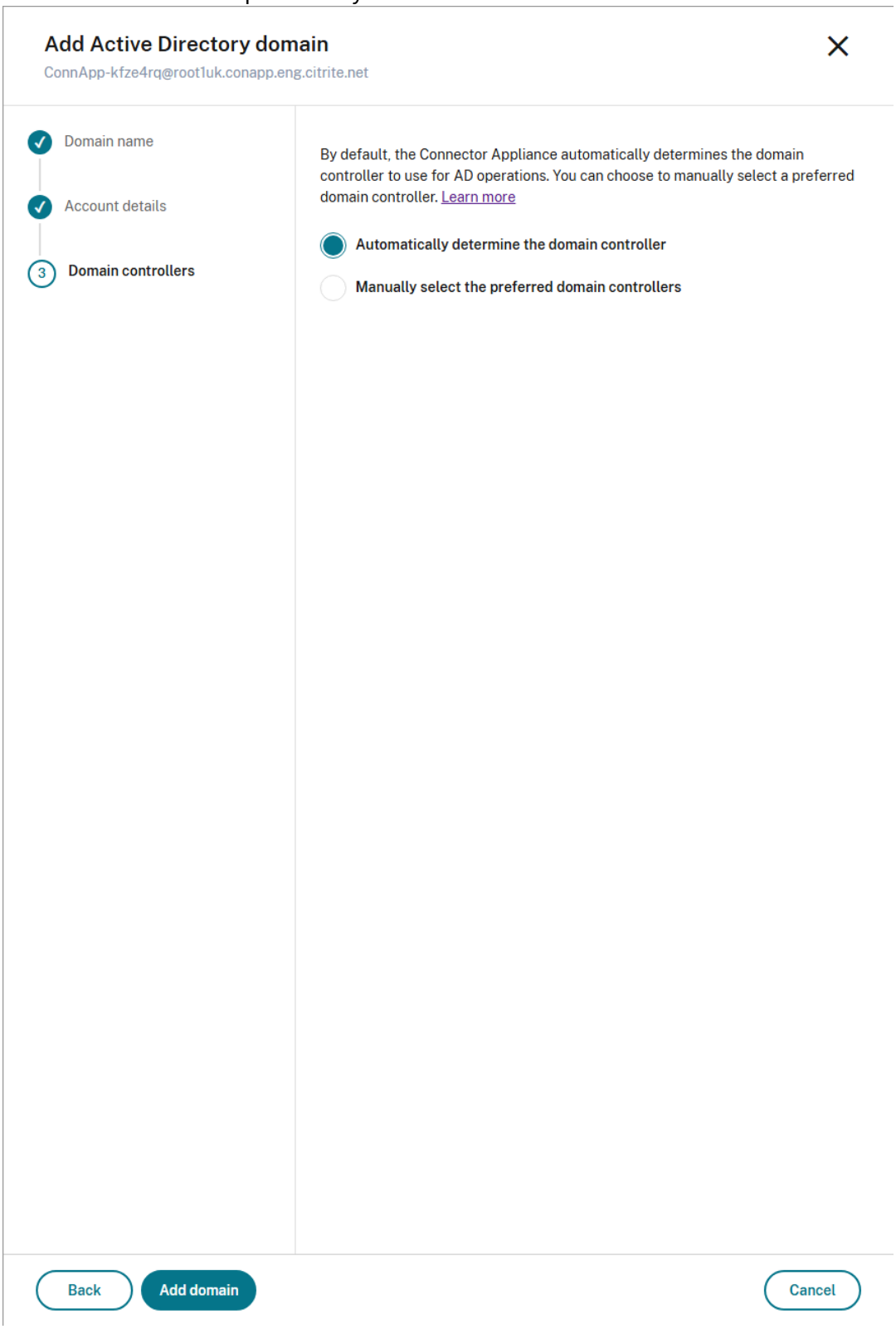
© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. On the **Domain controllers** step, choose one of the following options for how the **Connector Appliance** selects the domain controller for this domain:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

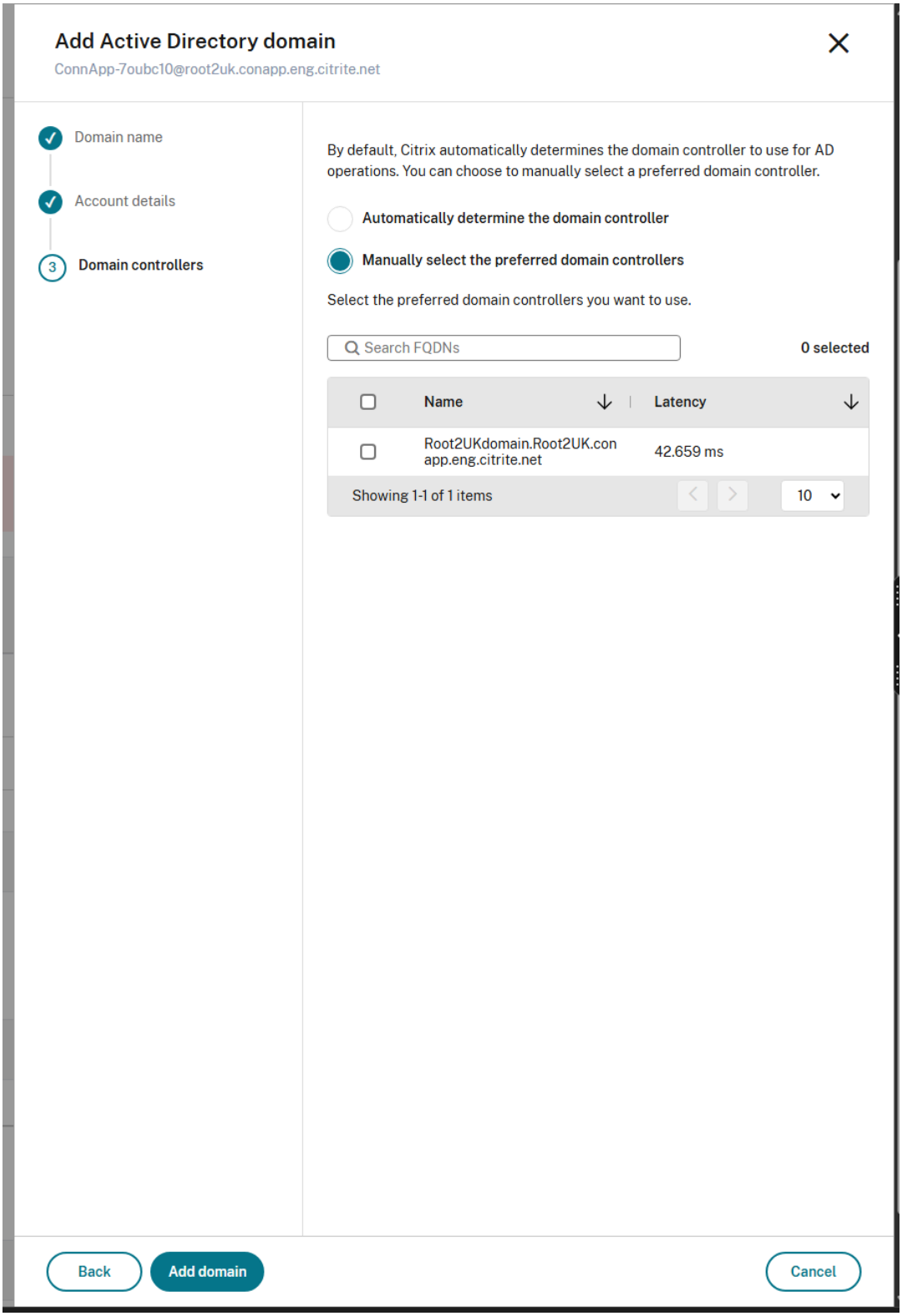
- **Automatically determine the domain controller** (default) –The Connector Appliance automatically determines which domain controller to use for Active Directory operations and re-evaluates this choice periodically.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Manually select the preferred domain controllers** —The **Connector Appliance** uses only the domain controllers you select. A searchable table lists the available domain controllers with their measured **Latency** in milliseconds. Use the search box to filter by name, or sort by **Name** or **Latency**, then select the check boxes for the domain controllers you want to use. If you do not select any domain controllers, the **Connector Appliance** falls back to automatic selection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. Click **Add domain**. The domain is now listed in the **Active Directory domains** section of the **Connector Appliance** UI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's next

- You can add more domains to this Connector Appliance.

  > **Note:**
  >
  > The Connector Appliance is tested with up to 10 forests.

- For resilience, add each domain to more than one Connector Appliance in each resource location.

Viewing your Active Directory configuration

You can view the configuration of the Active Directory domains and Connector Appliances in your resource locations in the following places:

- In Citrix Cloud:

  1. In the menu, go to the **Identity and Access Management** page.
  2. Go to the **Domains** tab.

     Your Active Directory domains are listed with the resource locations that they are part of.

- In the Connector Appliance webpage:

  1. Connect to the Connector Appliance webpage by using the IP address provided in the Connector Appliance console.
  2. Log in with the password you created when you first registered.
  3. In the **Active Directory domains** section of the page, you can see the list of Active Directory domains this Connector Appliance is joined to.

Removing an Active Directory domain from a Connector Appliance

To leave an Active Directory domain, complete the following steps:

1. Connect to the Connector Appliance webpage by using the IP address provided in the Connector Appliance console.
2. Log in with the password you created when you first registered.
3. In the **Active Directory domains** section of the page, find the domain you want to leave in the list of joined Active Directory domains.
4. Note the name of the machine account created by your Connector Appliance.
5. Click the delete icon (trashcan) next to the domain. A confirmation dialog appears.
6. Click **Continue** to confirm the action.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Go to your Active Directory controller.
8. Delete the machine account created by your Connector Appliance from the controller.

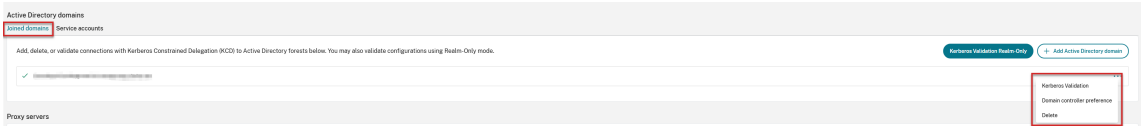
Change the domain controller preference for a joined Active Directory domain

After you join an Active Directory domain, you can change at any time which domain controllers the **Connector Appliance** uses for that domain. By default the **Connector Appliance** automatically determines the domain controller and re-evaluates the choice periodically; you can switch to manually selecting one or more preferred domain controllers if you have observed inconsistent performance in environments with a large number of domain controllers.

To change the domain controller preference for a joined domain, complete the following steps:

1. Connect to the **Connector Appliance** administration webpage by using the IP address provided in the **Connector Appliance** console.
2. Log in with the password you created when you first registered.
3. In the **Active Directory domains** section, on the **Joined domains** tab, find the domain you want to update.
4. Click the ellipsis (**...**) menu next to the domain and select **Domain controller preference**.

   The **Domain controller preference** blade opens.



5. Choose how the **Connector Appliance** selects the domain controller for this domain:

   - **Automatically determine the domain controller** –The **Connector Appliance** automatically determines which domain controller to use for Active Directory operations and re-evaluates this choice periodically.
   - **Manually select the preferred domain controllers** –The **Connector Appliance** uses only the domain controllers you select. A searchable table lists the available domain controllers with their measured **Latency** in milliseconds. Use the search box to filter by name, or sort by **Name** or **Latency**, then select the check boxes for the domain controllers you want to use.

   > **Note:**
   >
   > If you select **Manually select the preferred domain controllers** but do not select any domain controllers, the **Connector Appliance** falls back to automatic selection.

6. Click **Save** to apply your changes.

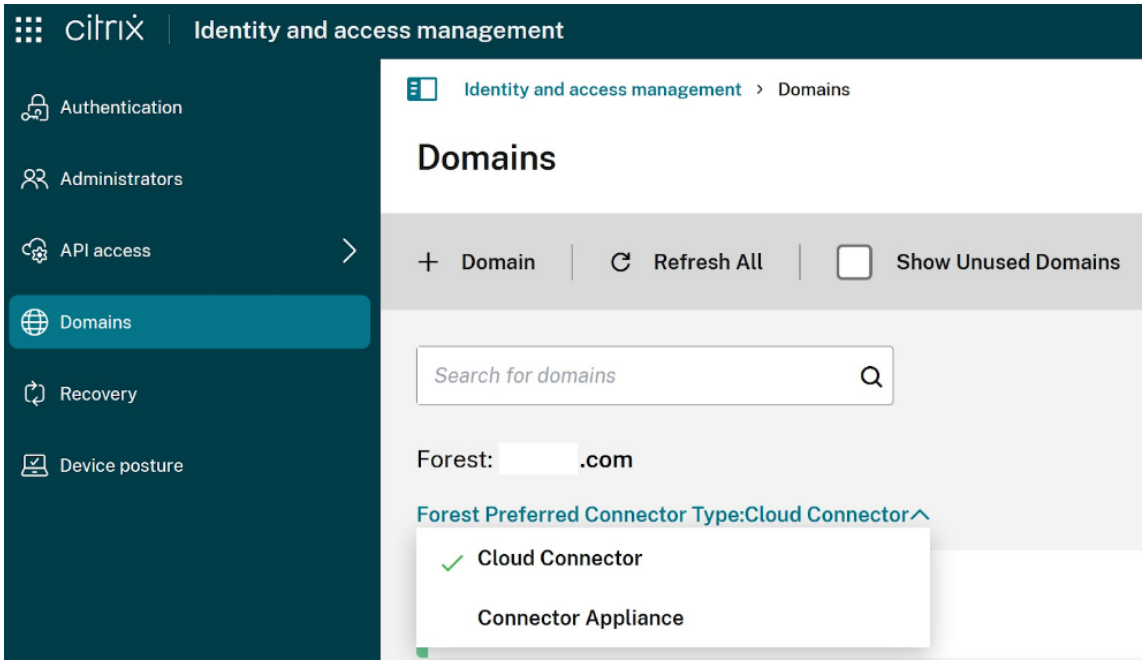
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Set the Forest Preferred Connector Type

When a Citrix Cloud tenant has both Windows connectors and connector appliances joined to the same AD forest it is possible to set the preferred connector type.

To set the preferred connector type for a particular Active Directory forest, complete the following steps:

1. Navigate to **Identity and Access Management > Domains** and Click the down arrow on the AD Forest you want to set the preferred connector type for.
2. Select **Forest Preferred Connector Type**.



Deployment scenarios for using Connector Appliance with Active Directory

You can use both Cloud Connector and Connector Appliance to connect to Active Directory controllers. The type of connector to use depends on your deployment.

For more information about using Cloud Connectors with Active Directory, see Deployment scenarios for Cloud Connectors in Active Directory

Use the Connector Appliance to connect your resource location to the Active Directory forest in the following situations:

- You are setting up Secure Private Access. For more information, see Secure Private Access with Connector Appliance.
- You have one or more forests that are only used for user authentication

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- You want to reduce the number of connectors required to support multiple forests
- You need a Connector Appliance for other use cases

Only users in one or more forests with a single set of Connector Appliances for all forests

This scenario applies to Standard customers or customers using Connector Appliance for Secure Private Access.

In this scenario, there are several forests that contain only user objects (`forest1.local`, `forest2.local`). These forests do not contain resources. One set of Connector Appliances is deployed within a resource location and joined to the domains for each of these forests.

- Trust relationship: None
- Domains listed in **Identity and Access Management**: `forest1.local`, `forest2.local`
- User logons to cloud stores: Supported for all users
- User logons to on-premises stores: Supported for all users

Users and resources in separate forests (with trust) with a single set of Connector Appliances for all forests

This scenario applies to Citrix Virtual Apps and Desktops customers with multiple forests.

In this scenario, some forests (`resourceforest1.local`, `resourceforest2.local`) contain your resources (for example, VDAs) and some forests (`userforest1.local`, `userforest2.local`) contain only your users. A trust exists between these forests that allows users to log on to resources.

One set of Cloud Connectors is deployed within the `resourceforest1.local` forest. A separate set of Cloud Connectors is deployed within the `resourceforest2.local` forest.

One set of Connector Appliances is deployed within the `userforest1.local` forest and the same set is deployed within the `userforest2.local` forest.

- Trust relationship: Bi-directional forest trust, or uni-directional trust from the resource forests to the user forests
- Domains listed in **Identity and Access Management**: `resourceforest1.local`, `resourceforest2.local`, `userforest1.local`, `userforest2.local`
- User logons to Citrix® StoreFront Cloud: Supported for all users
- User logons to an on-premises StoreFront: Supported for all users

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connector Appliance Network Connectivity Probe

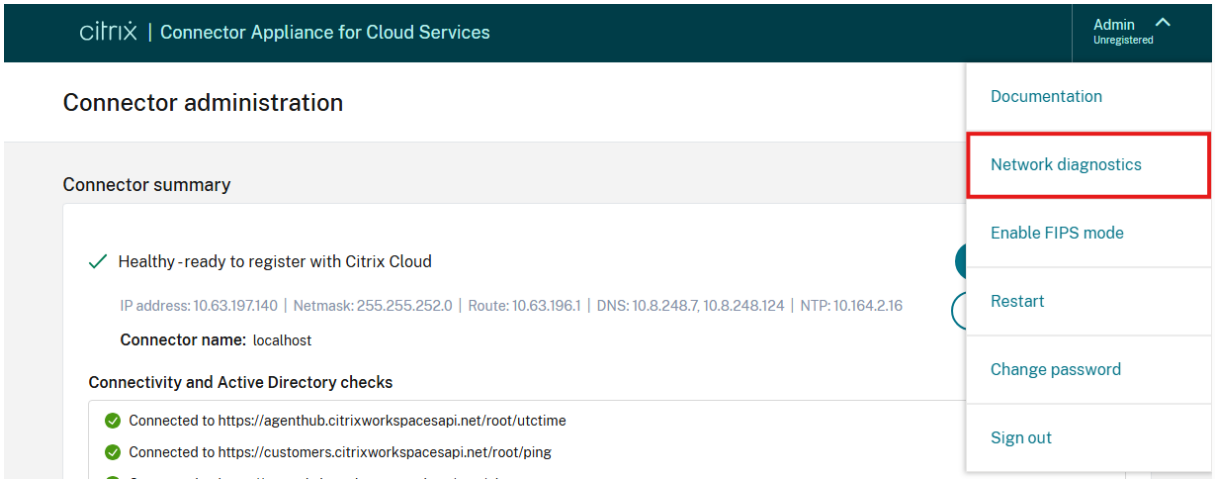
May 7, 2026

The Connector Appliance Network Connectivity Probe allows the user to perform an on-demand connectivity check of a network target.

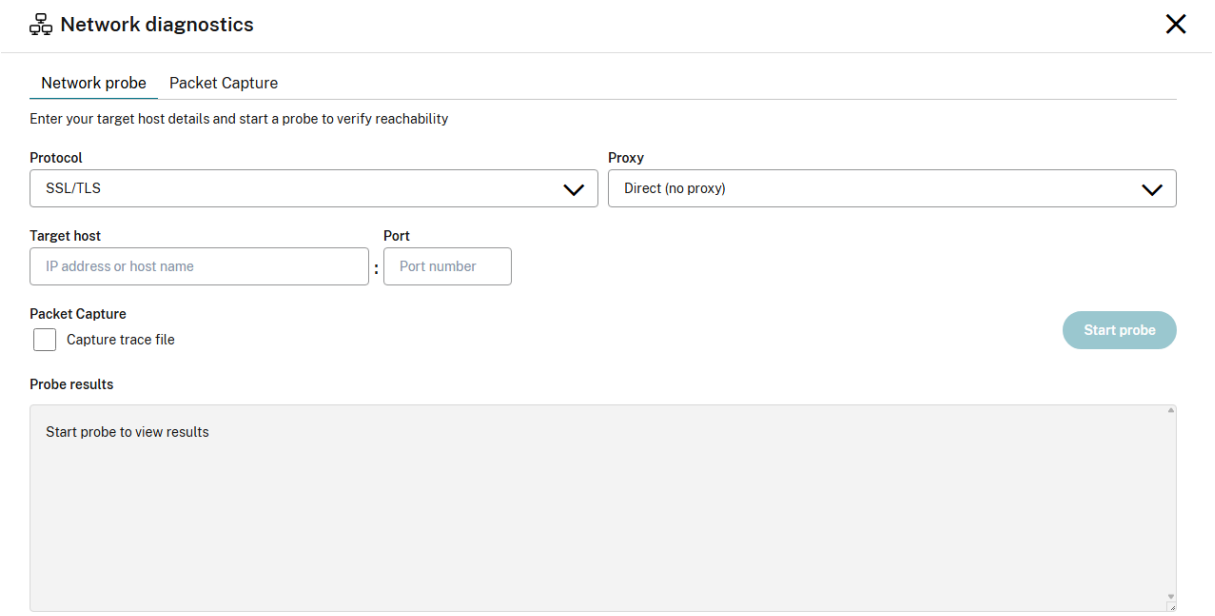
The network probe user interface can be accessed from the Connector Appliance administrator interface by navigating to **Network diagnostics** in the menu in the top-right corner.

The following protocols are supported:

- ICMP (sending a ping request)
- TCP
- TLS
- HTTP
- HTTPS



© 1997–2026 Citrix Systems, Inc. All rights reserved.



Specifying a proxy

By default, the network probe will make a direct connection to the specified target without a proxy.

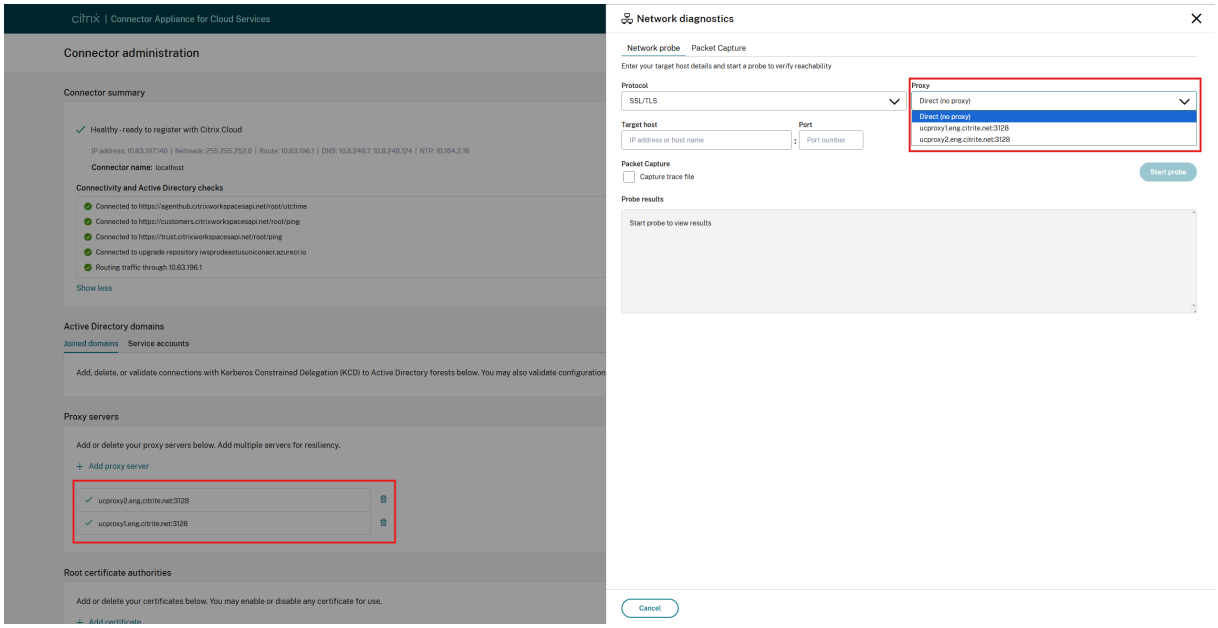
The ICMP network probe never uses a proxy.

For the other protocols, one of the proxies configured on the Connector Appliance can be selected for the network probe using the **Proxy** dropdown. The network probe will then be performed through the selected proxy.

For the TCP, TLS, and HTTPS protocols, the proxy will be used as a HTTPS proxy, and the network probe will send an HTTP CONNECT request to the selected proxy to establish a connection to the specified network target.

If the HTTP protocol is selected, the proxy will be used as a plain HTTP proxy by the network probe.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Allowed network targets

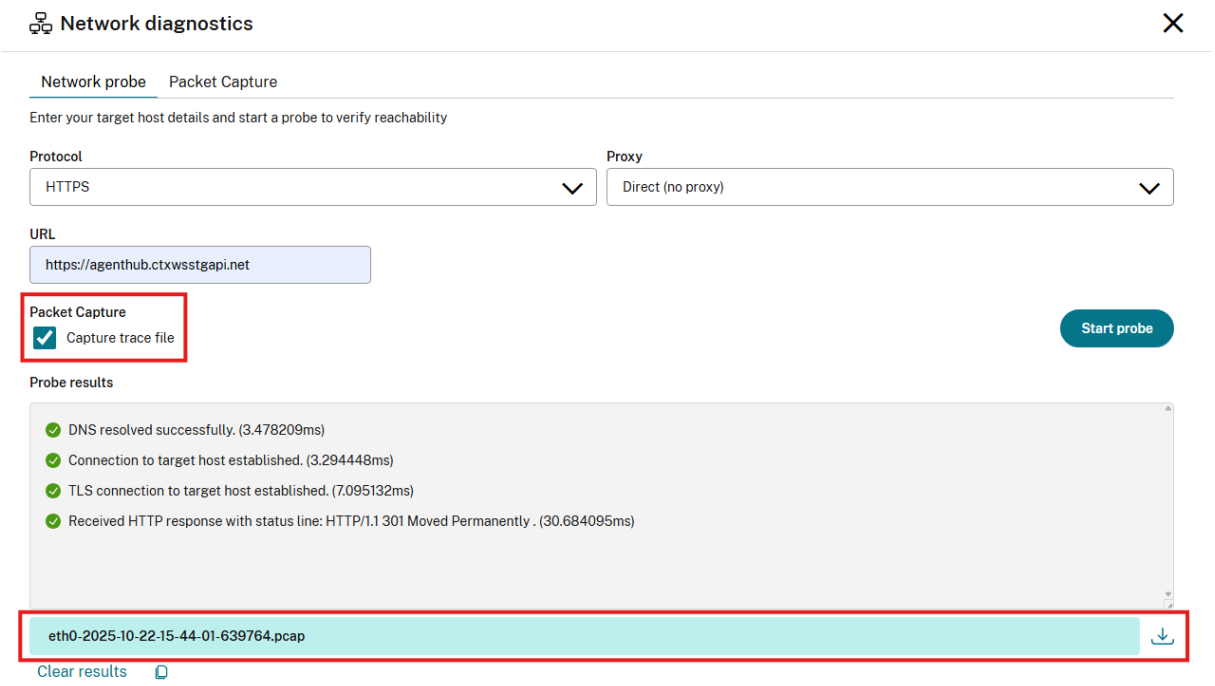
Probing is allowed for all private network targets. For external, public network targets, only the domains listed under the Internet connectivity requirements section are permitted. Each of these domains is either owned by Citrix or belong to a service required for the operation of the Connector Appliance.

Packet capture

Packet tracing can be enabled for the duration of the network probe by ticking the **Capture trace file** checkbox. When the probe has finished, a link to a packet capture will be displayed under the probe **Probe results**. This packet trace file can help further diagnose the network probe result.

> **Note:**
>
> The packet trace captures all traffic on the Connector Appliance during the duration of the network probe, not just the traffic of the network probe itself. This may include sensitive data or credentials.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Network probe result

After clicking the **Start probe** button, the **Probe results** box will display the progress of the network probe. Information will be shown for each step of the network probe, such as DNS resolution, TCP connection, and so on. As the network probe progresses, the icon next to each network probe stage will indicate whether it is in progress, completed, or failed, and timing information and error details will be displayed for each step.



Interpreting the Result of HTTP-based Probes

HTTP and HTTPS network probes are marked as successful, as long as an HTTP response is received from the target URL, regardless of the HTTP status code returned. The HTTP status line of the response, including the HTTP response status code, will be displayed in the **Probe results**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The same is true for a plain HTTP network probe when a proxy is selected. In this case, the selected proxy will be used as a plain HTTP proxy, and the probe will be considered successful as long as the proxy returns an HTTP response. An HTTP status line displayed in the **Probe results** with an error status code could indicate an error from the proxy or an error from the target URL.

Connector updates

June 19, 2026

Periodically, Citrix® releases updates to increase the performance, security, and reliability of the Cloud Connector or Connector Appliance.

When a new connector version is made available to a Citrix Cloud Tenant, the deafault behaviour is for each connector in the tenant to immediately install the update, one at a time, in a random order. Should any connector fail to perform the update it will prevent all subsequent connectors from beginning their update. This is to prevent update failures occuring on all connectors in the tenant. As soon as the connector with failed update either succeeds its update or is removed, subsequent connectors will immediately proceed with their updates. For more information see Troubleshooting Update Failures

To ensure updates are installed timely without unduly affecting your users' Citrix Cloud™ experience, you can control connector updates as follows:

- Schedule the start time for updates for a preferred time of day and a preferred day of the week.
- Perform a one-time delay, so the connectors you specify update two weeks later than scheduled.
- If an update fails due to an issue on the host machine, restart the update after the issue has been addressed.

Also, you can verify your connectors are up-to-date by comparing the current connector version in your resource location with the target version in Citrix Cloud.

> **Note:**
>
> This article describes how to schedule connector updates using the Citrix Cloud management console. For information about configuring preferred time of day and day of week for connector updates using Citrix Cloud APIs, see Citrix Cloud - Maintenance Schedules in the Citrix Developer documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Preferred time of day

When you specify a preferred time of day, Citrix Cloud begins installing updates 24 hours after they become available, at your preferred time. For example, if your preferred time of day is 2:00 AM US Pacific time and an update becomes available on Tuesday, Citrix Cloud waits for 24 hours and then begins installing the update at 2:00 AM the next day.

Preferred day of the week

When you specify a preferred day of the week, Citrix Cloud waits for seven days before beginning to install updates on your preferred day. This seven-day waiting period gives you enough time to choose whether to install the update on demand or wait for Citrix Cloud to begin installing it on your preferred day. Depending on the day of the week you select and the day on which updates become available, Citrix Cloud might wait to begin installing updates for up to 13 days.

Example of an 8-day waiting period

On Monday, you configure Tuesdays at 6:00 PM as your preferred day for updates. Later that day, Citrix Cloud notifies you that there's an update available and displays the **Update** button. If you don't initiate the update, Citrix Cloud waits for seven days and then begins installing the update the next day, on Tuesday at 6:00 PM.

Example of a 13-day waiting period

You configured Mondays at 6:00 PM as your preferred time of day for updates. On Tuesday, Citrix Cloud notifies you that there's an update available and displays the **Update** button. If you don't initiate the update, Citrix Cloud waits for seven days and then begins installing the update six days later, on Monday at 6:00 PM.

> **Note:**
>
> The update schedule indicates the time at which the connector will begin attempting its update. Because updates are installed on each connector, one at a time, the actual update may occur later than the scheduled time. For example, if the first connector to update in a resource location encounters an issue during update which causes the update to take 4 hours to complete, subsequent connectors in the resource location will not begin their updates until at least 4 hours after the scheduled time.
>
> Due to this behavior, before restarting updates on failed connectors or removing from Citrix Cloud a connector which has failed updates, it is important to note that the remaining connec-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> tors may initiate the update immediately, and this update may occur during business hours.

Update notifications and on-demand updates

When updates are available, Citrix Cloud informs you with an alert in your Notifications. Also, each connector displays the date and time when the update will be installed.

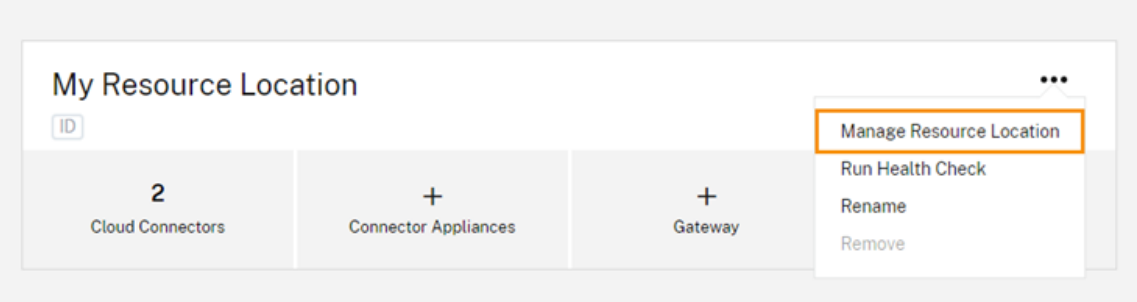
After Citrix Cloud notifies you of an available update, each connector displays an **Update** button so you can install the update sooner than your preferred time or day. After you select **Update** for each connector, Citrix Cloud queues the updates and installs them one at a time. You can't cancel updates after you initiate them.

After the update finishes, Citrix Cloud displays the date of the last update. If some updates cannot be completed, a notification is sent informing you.

Choose an update schedule

Use the steps in this section to schedule connector updates through the Citrix Cloud management console. For information about scheduling updates using Citrix Cloud APIs, see Citrix Cloud - Maintenance Schedules in the Citrix Developer documentation.

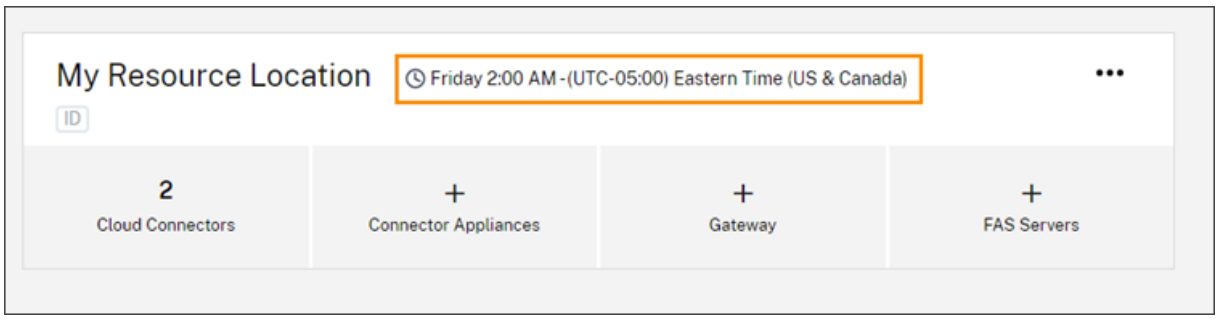
1. From the Citrix Cloud menu, select **Resource Locations**.
2. Locate the resource location you want to modify and, from the ellipsis menu, select **Manage Resource Location**.



3. Under **Choose your update method**, select **Set a maintenance start time** and choose the preferred day, time, and time zone for installing updates.
    - To specify only a preferred time of day, select the hour and time zone that you want updates to be installed. Citrix Cloud installs updates 24 hours after they become available, at your preferred time.
    - To specify a preferred day of the week, select the hour, day, and time zone. Citrix Cloud waits for seven days after updates become available before installing them on your preferred day.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After you configure your update schedule, Citrix Cloud displays it next to the resource location name.



The start time you select is applied to all connectors regardless of the time zone in which they are located. If you have connectors in different time zones, Citrix Cloud installs updates at your selected time and time zone. For example, if you schedule updates for 2:00 AM in the US Pacific time zone, and you have connectors in London, Citrix Cloud starts to install the update on those connectors at 2:00 AM US Pacific time.

> **Note:**
>
> The update schedule indicates the time at which the connector will begin attempting its update. Because updates are installed on each connector, one at a time, the actual update may occur later than the scheduled time. For example, if the first connector to update in a resource location encounters an issue during update which causes the update to take 4 hours to complete, subsequent connectors in the resource location will not begin their updates until at least 4 hours after the scheduled time.
>
> Due to this behavior, before restarting updates on failed connectors or removing from Citrix Cloud a connector which has failed updates, it is important to note that the remaining connectors may initiate the update immediately, and this update may occur during business hours.

Restart updates

If the connector experiences an issue during update installation, the installation pauses until the issue is resolved. Because updates are installed on each connector, one at a time, a paused update on one connector can prevent updates on all remaining Cloud Connectors in your Citrix Cloud account. After the issue is resolved, you can restart the update.

1. From the Citrix Cloud menu, select **Resource Locations**.
2. Locate the resource location you want to manage and select the **Cloud Connectors** or **Connector Appliances** tile.
3. Locate the connector you want to manage and select **Restart updates**.

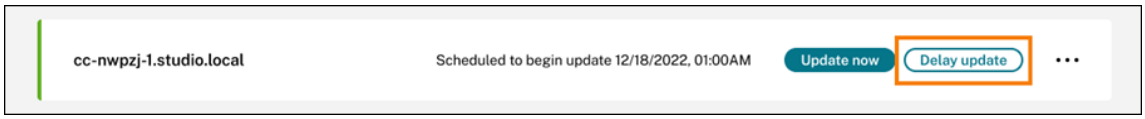
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Delay updates

You can delay a scheduled update so it occurs two weeks later for the connectors you specify. You can delay a scheduled update only once. After you delay the update once, you can't delay it again. Also, you can't change the default two-week period.

1. From the Citrix Cloud menu, select **Resource Locations**.
2. Locate the resource location you want to manage and select the **Cloud Connectors** or **Connector Appliances** tile.
3. Locate the connector you want to manage and select **Delay updates**.



The scheduled date changes to a date two weeks later than the originally scheduled date.

Unscheduled updates

Even if you schedule updates for a later date and time, Citrix Cloud might still install an update as soon as possible after it becomes available. Unscheduled updates occur when:

- The update can't be installed at the preferred time within 48 hours of its availability. For example, if your preferred time is 2:00 AM and the connector is offline for three days following the update release, Citrix Cloud installs the update immediately when the connector is back online.
- The update contains a fix for a critical security or feature issue.

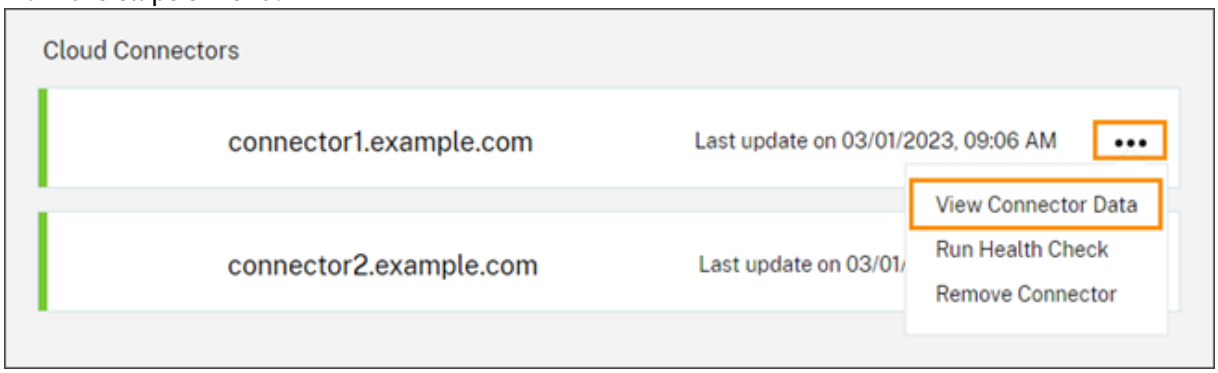
Compare Cloud Connector versions

You can check to see which version of the Cloud Connector is running in your resource location and whether it's the latest version. This information helps you verify that the Cloud Connector is updating successfully.

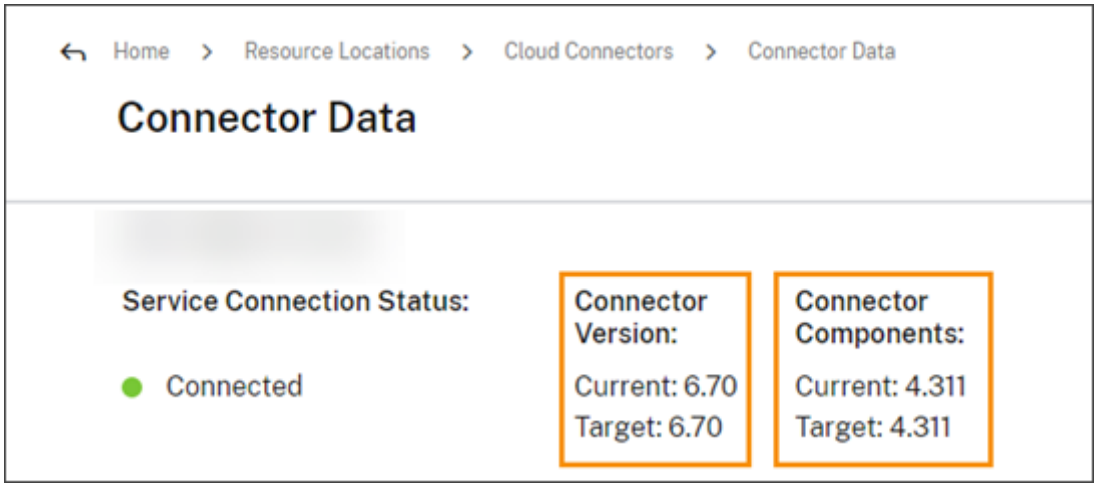
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> This information is not available for Connector Appliances.

From the **Resource Locations** page, select the **Cloud Connectors** tile for the resource location you want to manage. Locate the Cloud Connector you want to examine and select **View Connector Data** from the ellipsis menu.



The **Current** version number is the version of the Cloud Connector software currently running on the Cloud Connector machine. The **Target** version number is the latest version of the Cloud Connector software that Citrix released. If the machine was updated successfully, the Current and Target version numbers match.



Troubleshooting update failures

Conflicting software installed on your Cloud Connector machine or unexpected errors during maintenance can result in the Cloud Connector failing to update and service outages. For information on dealing with a failed update following Cloud Connector maintenance, visit Resolve a Failed Cloud Connector Maintenance.

If the Cloud Connector isn't updating successfully, you can start troubleshooting issues by verifying the following conditions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The Cloud Connector is powered on and connected to Citrix Cloud using the Cloud Connector Advanced Connectivity Checks.
- Proxy and firewalls are configured correctly.
- Required Windows services are in the Started state.
- Advanced logging is enabled on the Cloud Connector.

For instructions for troubleshooting Cloud Connector update failures, see CTX270718 in the Citrix Support Knowledge Center.

For troubleshooting assistance, you can send Citrix Cloud Connector logs to Citrix. For more information, see Log Collection for Citrix Cloud Connector.

Identity and access management

June 22, 2026

Identity and Access Management defines the identity providers and accounts used for Citrix Cloud™ administrators and end users.

Identity providers

Identity providers supported for Citrix Cloud can be used to authenticate Citrix Cloud administrators, end users, or both.

Identity provider	Administrator authentication	End user authentication
Citrix® identity provider	Yes	No
On-premises Active Directory	No	Yes
Active Directory plus token	No	Yes
Microsoft Entra ID	Yes	Yes
Citrix Gateway	No	Yes
Google Cloud Identity	Yes	Yes
Okta	No	Yes
SAML 2.0	Yes	Yes

By default, Citrix Cloud uses the Citrix identity provider to manage your Citrix Cloud account. Citrix identity provider authenticates Citrix Cloud administrators only.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix identity provider

Citrix Cloud includes the built-in Citrix identity provider to authenticate administrators when they sign in. In the Citrix Cloud console, the Citrix identity provider is labeled Citrix Identity.
If you use a different identity provider for administrator authentication, Citrix recommends having at least one full access administrator under the **Citrix identity provider**. This condition ensures that:

- You won't be locked out of your Citrix Cloud account if your primary identity provider becomes unavailable.
- You can access your Citrix Cloud account to perform certain operations that can't be completed when signed in under another identity provider, such as Microsoft Entra ID. For example, If Microsoft Entra ID is your selected identity provider, and you need to reinitiate the connection between your Microsoft Entra ID and Citrix Cloud, you can perform this task after signing in using the Citrix identity provider.

Remove the Citrix identity provider

The Citrix identity provider is connected by default for all new Citrix Cloud accounts. If you choose not to use the Citrix identity provider, you can remove the connection, if needed. For example, you might choose to remove this connection to conform with your organization's policies for security and administrator management.

Removing this connection disables the Citrix identity provider so it can't be used to authenticate Citrix Cloud administrators.

Before you can remove the Citrix identity provider connection, you must have another identity provider configured in Citrix Cloud. Citrix Cloud doesn't allow you to remove this connection without the presence of another configured identity provider.

> **Important**
>
> If you lose access to your chosen identity provider, you must contact Citrix Support to recover your Citrix Cloud account. This process might require several days to complete.

To remove the Citrix identity provider connection:

1. From the Citrix Cloud menu, select **Identity and Access Management**.
2. On the **Authentication** tab, locate the Citrix identity provider.
3. Click the ellipsis menu and select **Delete identity provider**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. When prompted to confirm the removal, select **I understand that deleting this identity provider also deletes the configuration data for this identity provider in Citrix Cloud**.
5. Click **Delete identity provider**.

Citrix Federated Authentication Service

Citrix Cloud also supports using the Citrix Federated Authentication Service to provide single sign-on access for end users. For more information, refer to the following articles:

- Connect FAS to Citrix Cloud: Enable single sign-on for stores with Citrix Federated Authentication Service
- Citrix Tech Zone:
  - Reference Architecture: Federated Authentication Service
  - Tech Insight: Federated Authentication Service

Administrators

Administrators use their identity to access Citrix Cloud, perform management activities, and install the Citrix Cloud Connector.

A Citrix identity mechanism provides authentication for administrators using an email address and password. Administrators can also use their My Citrix credentials to sign in to Citrix Cloud.

Multifactor authentication

Citrix Cloud provides multifactor authentication methods for both administrators and end users.

For administrators, multifactor authentication is required when signing in to Citrix Cloud. Administrators can enroll their device when they onboard their Citrix Cloud account or after accepting an invitation from another administrator. For more information, see the following articles:

- Set up multifactor authentication
- Manage your primary MFA method
- Manage your MFA recovery methods

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For end users, multifactor authentication is enabled when administrators configure the Active Directory plus token authentication method. Active Directory plus token is the default identity provider for Citrix® StoreFront Cloud. After configuration, end users enroll their device for multifactor authentication. For more information, see the following articles:

- Enable Active Directory plus token authentication
- Enroll a device for two-factor authentication
- Re-enroll a device

Alternatively, you can use Microsoft Entra ID multifactor authentication for both Citrix Cloud administrators and end users. For more information about deployment methods, see Microsoft Azure MFA deployment methods.

Add new administrators

During the account onboarding process, an initial administrator is created. As the initial administrator, you can add other administrators to your Citrix Cloud account. These new administrators can use their existing Citrix account credentials or set up a new account if needed. You can also fine-tune the access permissions of the administrators that you add. Setting these permissions allows you to align the level of access with the administrator's role in your organization.

For more information about adding administrators and setting access permissions, see Manage administrator access.

Reset your password

If you forget or want to reset your password, click **Forgot your username or password?** on the Citrix Cloud sign in page. After you enter your email address or username to find your account, Citrix sends you an email with a link to reset your password.

Citrix requires you to reset your password under certain conditions to help you keep your account password safe and secure. For more information about these conditions, see Changing your password.

> **Note:**
>
> Add **customerservice@citrix.com** to your list of allowed email addresses to ensure that Citrix Cloud emails don't land in your spam or trash folders.

Remove administrators

You can remove administrators from your Citrix Cloud account on the **Administrators** tab. When you remove an administrator, they can no longer sign-in to Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

If an administrator is logged in when you remove the account, the administrator remains active for a maximum of one minute. Afterward, access to Citrix Cloud is denied.

> **Note:**
>
> - If there's only one administrator in the account, you can't remove that administrator. Citrix Cloud requires at least one administrator for each customer account.
> - Citrix Cloud Connectors are not linked to administrator accounts. So, Cloud Connectors continue operating even if you remove the administrator who installed them.

End users

An end user's identity defines the services to which they have access in Citrix Cloud. This identity comes from Active Directory domain accounts provided from the domains within the resource location. Assigning an end user to a Library offering authorizes the end user to access that offering.

Administrators can control which domains are used to provide these identities on the **Domains** tab. If you plan to use domains from multiple forests, install at least two Citrix Cloud Connectors in each forest. Citrix recommends at least two Citrix Cloud Connectors to maintain a high availability environment. For more information about deploying Cloud Connectors in Active Directory, see Deployment scenarios for Cloud Connectors in Active Directory.

> **Note:**
>
> - Disabling domains prevents new identities only from being selected. It does not prevent end users from using identities that are already allocated.
> - Each Citrix Cloud Connector can enumerate and use all the domains from the single forest in which it is installed.

Manage end user usage

You can add end users to offerings using individual accounts or Active Directory groups. Using Active Directory groups does not require management through Citrix Cloud after you assign the group to an offering.

When an administrator removes an individual end user or group of end users from an offering, those end users can no longer access the service. For more information about removing end users from specific services, refer to the service's documentation on the Citrix Product Documentation website.

Primary resource locations

A primary resource location is a resource location that you designate as "most preferred"for communications between your domain and Citrix Cloud. For your primary resource locations, select the re-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

source location that has Citrix Cloud Connectors that have the best performance and connectivity to your domain. Making this resource location your primary resource location enables your users to log on quickly to Citrix Cloud.

For more information, see Select a primary resource location.

More information

- Learn more about supported identity providers with the Introduction to Citrix Identity and Authentication education course on the Citrix Training web site.
- Citrix Tech Zone:
  - Tech Brief: Workspace Identity
  - Tech Brief: Workspace Single Sign-On
  - Tech Insight: Mobile SSO

Manage administrator access to Citrix Cloud

September 28, 2026

Administrators are managed from the Citrix Cloud console. Depending on the identity provider you use to authenticate administrators, you can add administrators individually or using groups.

All administrators are required to use tokens as a second factor of authentication when signing in to Citrix Cloud. After you add an administrator, they can enroll their device in multifactor authentication and generate tokens using any app that follows the Time-Based One-Time Password standard, such as Citrix SSO.

Add new administrators

Citrix Cloud supports the following identity providers for authenticating administrators:

- Citrix identity provider: The default identity provider in Citrix Cloud. Supports adding individual administrators only.
- Microsoft Entra ID: Supports adding administrators individually and through ME-ID groups. For more information, see Manage administrator groups.
- SAML 2.0: Supports adding administrators individually and through AD groups. For more information, see Connect SAML as an identity provider to Citrix Cloud
- Google: Supports adding administrators individually and through Google groups. For more information, see Google Cloud Identity

© 1997–2026 Citrix Systems, Inc. All rights reserved.

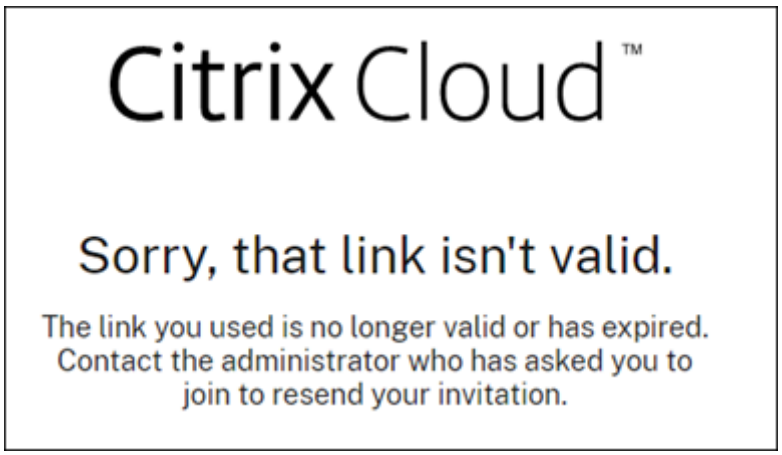
Adding new administrators uses the following workflow:

1. Select the identity provider that you want to use for authenticating administrators.
2. Depending on the identity provider, invite individual administrators or select the groups that the administrators belong to.
3. Specify the access permissions that align with the administrators' roles in your organization. For more information, see Modify administrator permissions in this article.

Invite individual administrators

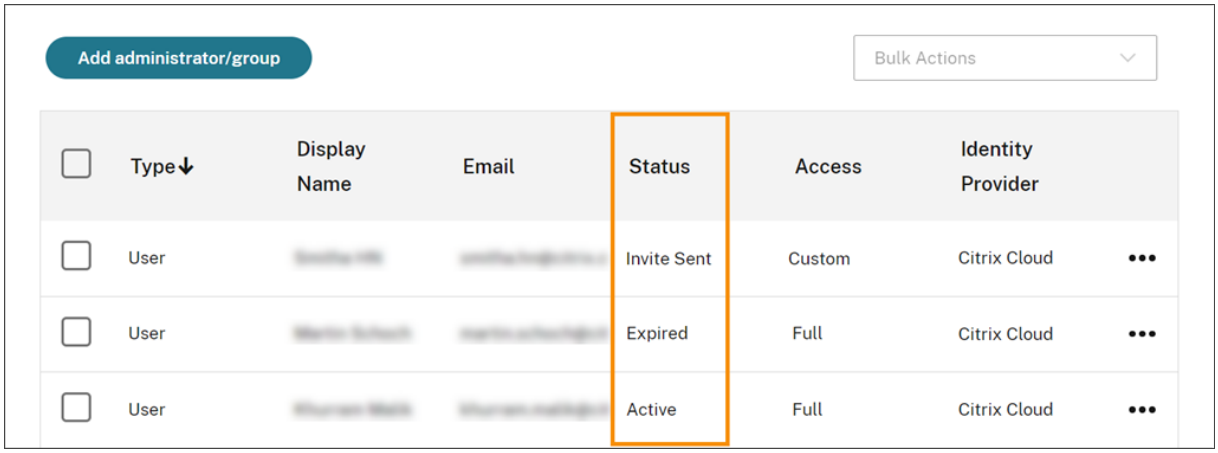
Adding individual administrators involves inviting them to join your Citrix Cloud account. When you add an administrator, Citrix sends them an invitation email. Before the administrator can sign in, they must accept the invitation. Administrators that you add through groups don't receive invitations and can sign in immediately after you add them.

Invitation emails are sent from `cloud@citrix.com` and explain how to access the account. The invitation is valid for five consecutive days from the day that you send it. After five days have elapsed, the invitation link expires. If the invited administrator uses the expired link, Citrix Cloud displays a message indicating the link is not valid.



Citrix Cloud also displays the status of the invitation so you can see whether the administrator accepted it and signed in to Citrix Cloud.

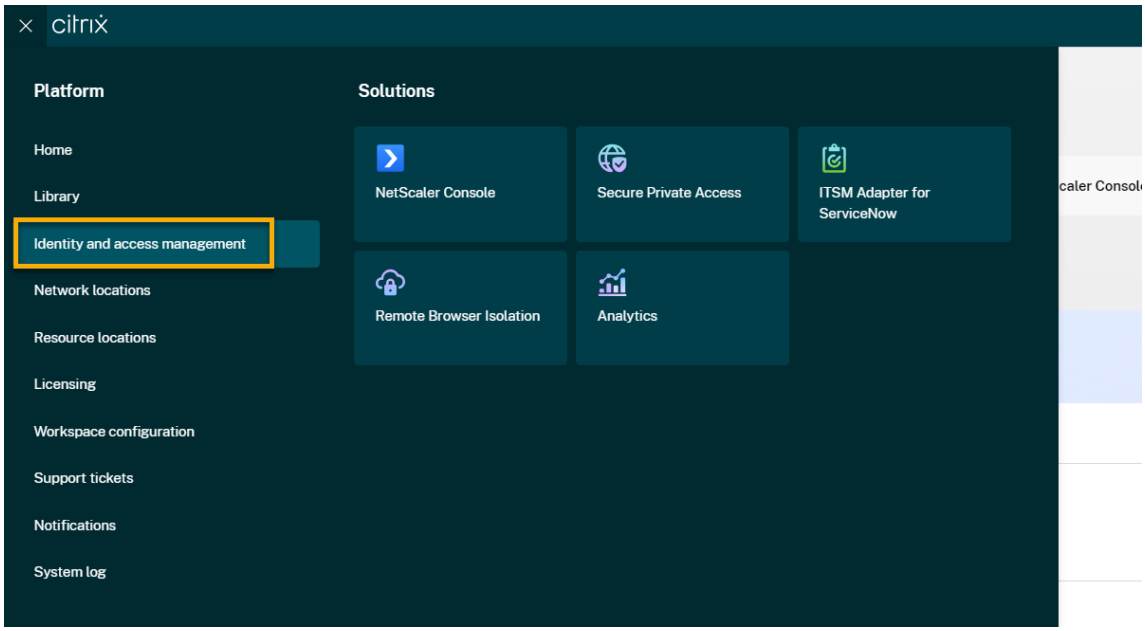
© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Note**
>
> Administrator accounts can be associated with up to 100 customer accounts. If an administrator needs to manage more than 100 customer accounts, they must create a separate administrator account with a different email address to manage the additional customers. Alternatively, you can remove the administrator from customer accounts that they no longer need to manage.

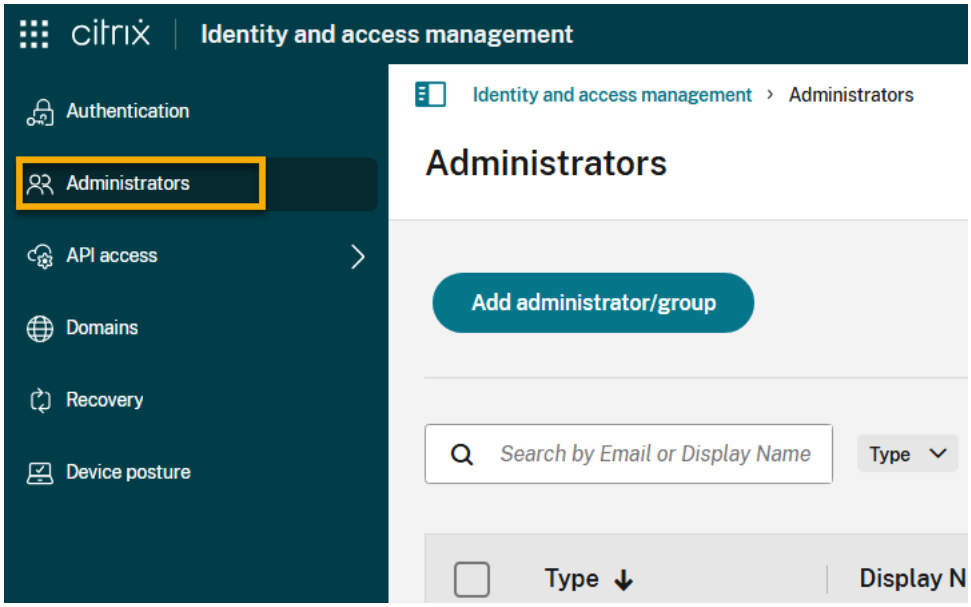
To invite an administrator

1. Sign in to Citrix Cloud and then select **Identity and Access Management** from the menu.



2. On the **Identity and Access Management** page, select **Administrators**. The console shows all the current administrators in the account.

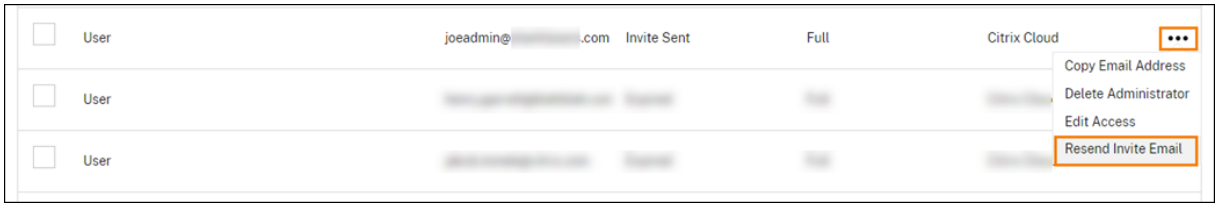
© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Select **Add administrator/group**.
4. In **Administrator details**, select the identity provider you want to use. If using Microsoft Entra ID, Citrix Cloud might prompt you to sign in first.
5. If **Citrix Identity** is selected, enter the user's email address and then select **Next**.
6. If **Microsoft Entra ID** is selected, type the name of the user you want to add and then click **Next**. Inviting ME-ID guest users is not supported.
7. In **Set access**, configure the appropriate permissions for the administrator. **Full access** (selected by default) allows control of all Citrix Cloud functions and subscribed services. **Custom access** allows control of the functions and services that you select.
8. Review the administrator details. Select **Back** to make any changes.
9. Select **Send invitation**. Citrix Cloud sends an invitation to the user you specified and adds the administrator to the list.

Resend an invitation

To resend the invitation, select **Resend Invite Email** from the ellipsis menu at the far-right of the console. Resending an invitation doesn't affect the five-day time limit before the invitation expires.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Resend an invitation with a new sign-in link

If the original invitation email expires, you can send a new one to the administrator. Perform the following steps:

1. Delete the administrator from Citrix Cloud: On the **Administrators** page, locate the administrator in the list and then select **Delete Administrator** from the ellipsis menu.
2. Wait several minutes to ensure Citrix Cloud completes the deletion. In some cases, inviting the administrator again immediately after deletion could result in sending an invitation with a faulty sign-in link.
3. Invite the administrator again as described in To invite an administrator.

Accept an administrator invitation

If you are invited to a Citrix Cloud account, Citrix sends you an email that includes the organization ID and the customer name of the account.

To accept the invitation, click **Sign In**. Afterwards, a browser window opens. If you don't already have a Citrix Cloud account, the browser displays a page where you can create your password. If you already have an account, Citrix Cloud prompts you to use your existing password to sign in.

During sign-in, you might be prompted to enroll in multifactor authentication. For enrollment instructions, see Set up multifactor authentication.

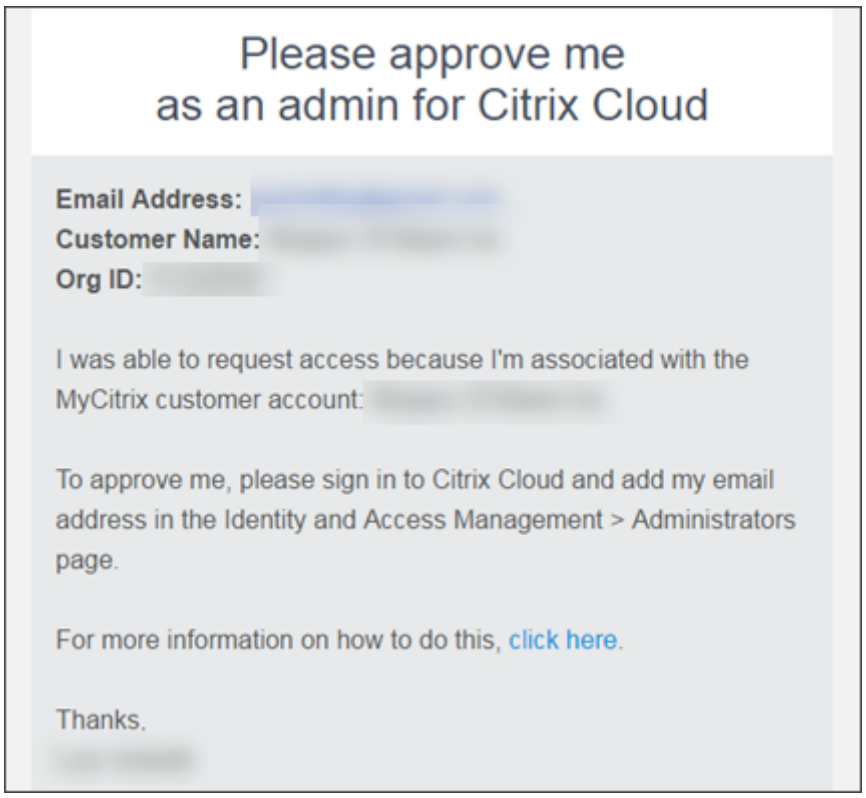
Add administrator groups

You can add administrators using AD groups (for SAML authentication), Microsoft Entra ID groups (for Microsoft Entra ID authentication) or Google groups (for Google Authentication). For more information, see Manage administrator groups.

Approve requests to join Citrix Cloud

From time to time, you might receive an approval request from Citrix Cloud on behalf of someone in your organization who would like to join your Citrix Cloud account as an administrator.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To approve these requests, you invite the person requesting access to be an administrator, as described in Invite individual administrators in this article. You must use the same email address that appears in the approval request email.

After receiving the invitation, the person requesting access clicks the **Sign in** link to accept the invitation. The person can then create a password for Citrix Cloud and sign in to your account.

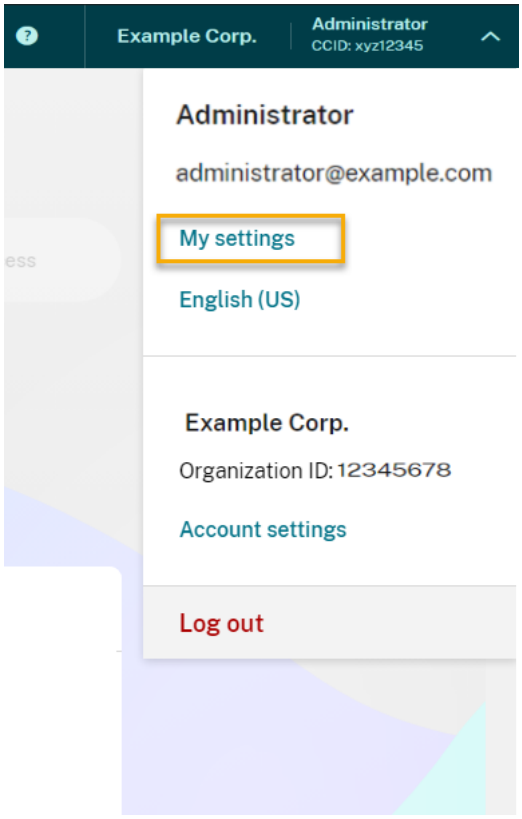
For more information about how approval requests are generated, see What happens if the account is already in use?.

Change your email address

You can change your own email address in Citrix Cloud. Your new address must be different from your recovery email address for multifactor authentication (MFA). When changing your email address, Citrix Cloud sends you a verification email to the new address. After verification, Citrix Cloud signs you out so the change can be completed. After a few minutes, you can sign in again with your new email address.

1. From the top-right menu, select **My settings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. In **Email address**, select **Change email**.
3. Enter the new email address and then select **Send verification email**.
4. Enter the 6-digit verification code from the email and then select **Verify and complete**.
5. Select **Yes, change my email address** to confirm the change.

After confirming your changes, Citrix Cloud signs you out. After a few minutes you can sign in again with your new email address.

Modify administrator permissions

When you add administrators to your Citrix Cloud account, you define the administrator permissions that are appropriate for their role in your organization. By default, new administrators are assigned *full access permissions* to all Citrix Cloud account functions and available services. If you want to limit access to certain areas of the management console or specific services, you can define *custom access permissions*.

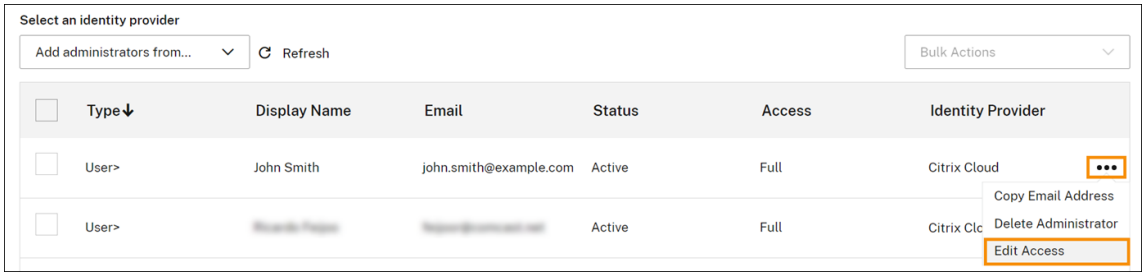
Only Citrix Cloud administrators with full access can define permissions for other administrators.

To change existing administrator permissions:

1. Sign in to Citrix Cloud at https://citrix.cloud.com.

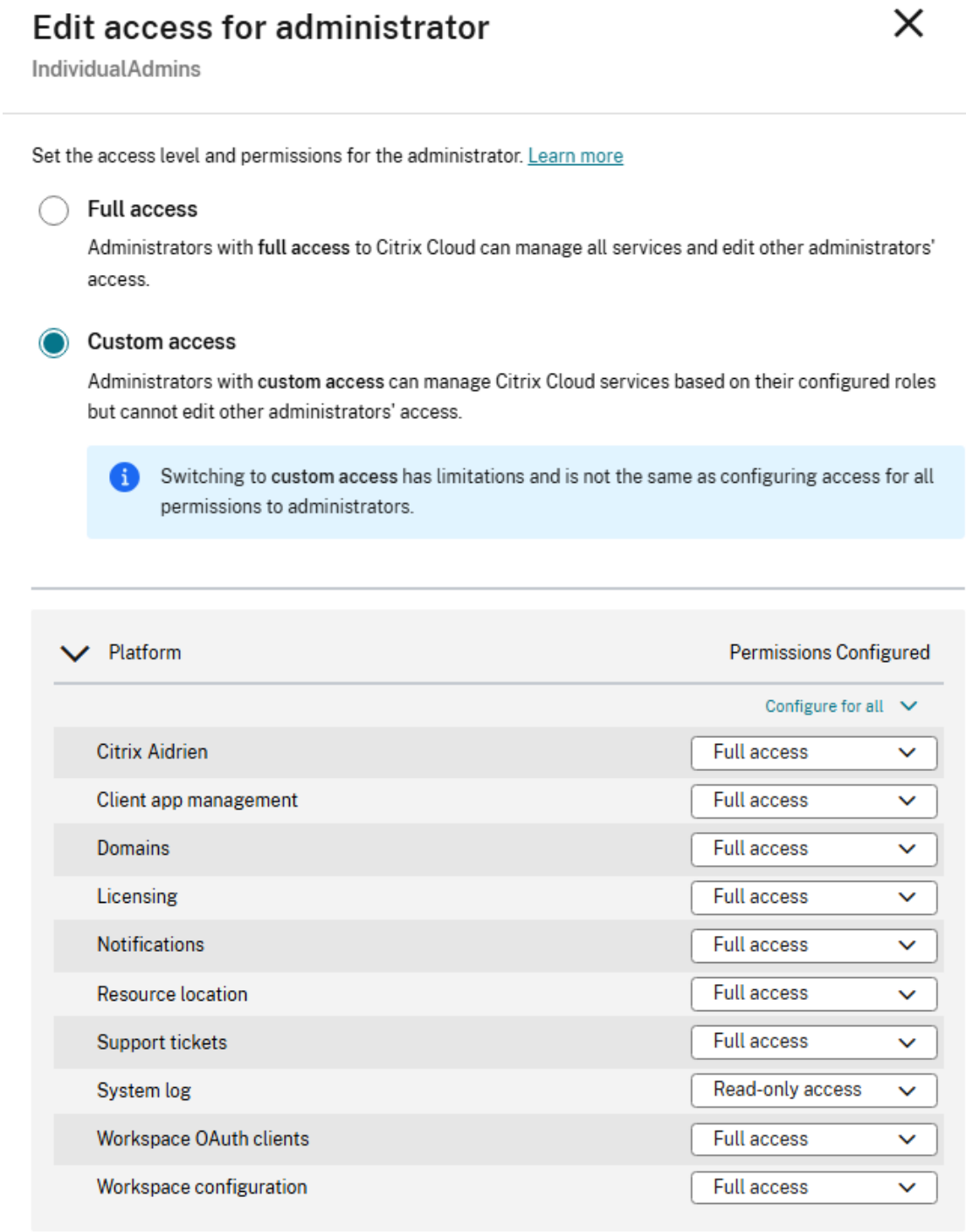
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. From the Citrix Cloud menu, select **Identity and Access Management** and then select **Administrators**.
3. Select the identity provider you want to manage: Citrix Identity (default), Active Directory (if using SAML as your identity provider) or Microsoft Entra ID (if connected).
4. Locate the administrator or group you want to manage, click the ellipsis button, and select **Edit access**.



5. To allow or disallow specific permissions, select **Custom access**. To allow access to all Citrix Cloud functions, select **Full access**.
6. To locate service permissions quickly, start typing in the search box. Citrix Cloud displays matching permissions as you type. For example, if you start typing "read only," permissions with "read only" in the title are displayed. Searching permissions is case-insensitive.
7. To define custom access permissions for the Citrix Cloud management console, expand **General**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. To define custom access permissions for a specific service, expand the service.
9. For each permission, select or clear the check mark as needed.
10. Select **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Console permissions

This section describes the custom access permissions that are available for the Citrix Cloud management console. For more information about the custom access permissions for a specific service, consult the service's documentation. Most platform roles support **Read-Only** access, but some roles are limited to either **Read-only** or **Full Access** only (see below):

- **Customer Dashboard:** For Citrix Service Providers (CSPs) only. Grants view access to the Customer Dashboard. (Read-Only only)
- **Domains:** Grants access to the **Identity and Access Management > Domains** tab. Administrators can add an Active Directory domain by downloading the Citrix Cloud Connector™ software from this tab and installing it on a server in the domain.
- **Licensing:** Grants access to the **Cloud Services** and **Licensed Deployments** tabs of the **Licensing** console page. (Read-Only only)
- **Notifications:** Grants access to the **Notifications** console page. Administrators can view and dismiss Citrix Cloud notifications.
- **Resource Locations:** Grants access to the **Resource Locations** console page. Administrators can add new resource locations and add FAS servers for single sign-on. They can also manage connector updates.
- **Support Tickets:** Grants access to the **Support Tickets** console menu option and the **Open a Ticket** Help menu option. Selecting either of these options sends the administrator to the My Support portal. For more information, see Technical Support. (Full-Access only)
- **System Log:** Grants access to the **System Log** console page. Administrators can view system log events and export events to a CSV file.(Read-Only only)
- **StoreFront Cloud:** Grants access to the **StoreFront Cloud** console page. Administrators can change authentication methods, customize store appearance and behavior, enable and disable services, and configure site aggregation. For more information, see the Citrix® StoreFront Cloud product documentation. (Full-Access only)
- **Store OAuth Clients (preview):** Grants access to the **Identity and Access Management > API Access > store API** tab. Administrators can create and manage their own OAuth client to interact with StoreFront Cloud platform APIs. OAuth clients are used exclusively for store APIs and include the option to create private clients that expire automatically.

> **Note:**
>
> It is recommended to assign the **Store OAuth clients** custom role with caution. The access privileges associated with this role might enable administrators to access end users' resources (VDAs or applications) on the store platform. It is also important to note that administrators with **Full access** will automatically have access permissions equivalent to that of an administrator with the **Store OAuth clients** permission.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage your primary MFA method

To sign in to Citrix Cloud with multifactor authentication (MFA), you can use an authenticator app or you can use your email address. This section describes how to change your device enrollment for MFA or switch to a different MFA method.

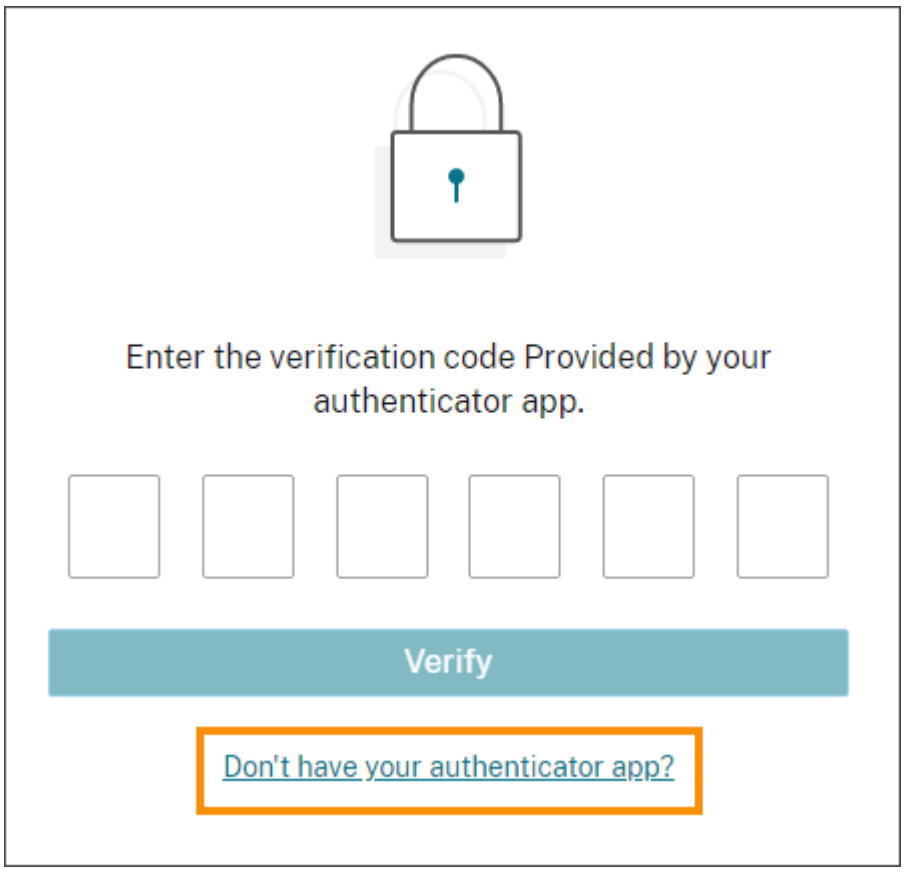
Change your device for MFA

If you lose your enrolled device, want to use a different device with Citrix Cloud, or reset your authenticator app, you can re-enroll in Citrix Cloud MFA.

> **Notes**
>
> - Changing your device deletes the current device enrollment and generates a new authenticator app key.
> - If you are re-enrolling with the same authenticator app from your original enrollment, delete the Citrix Cloud entry from your authenticator app before you re-enroll. The codes displayed in this entry will no longer work after you complete re-enrollment. If you don't delete this entry before or after re-enrollment, your authenticator app displays two Citrix Cloud entries with differing codes which can cause confusion when signing in to Citrix Cloud.
> - If you are re-enrolling with a new device and don't have an authenticator app, download and install one from your device's app store. For a smoother experience, Citrix recommends installing an authenticator app before you re-enroll your device.

1. Sign in to Citrix Cloud and enter the code from your authenticator app.

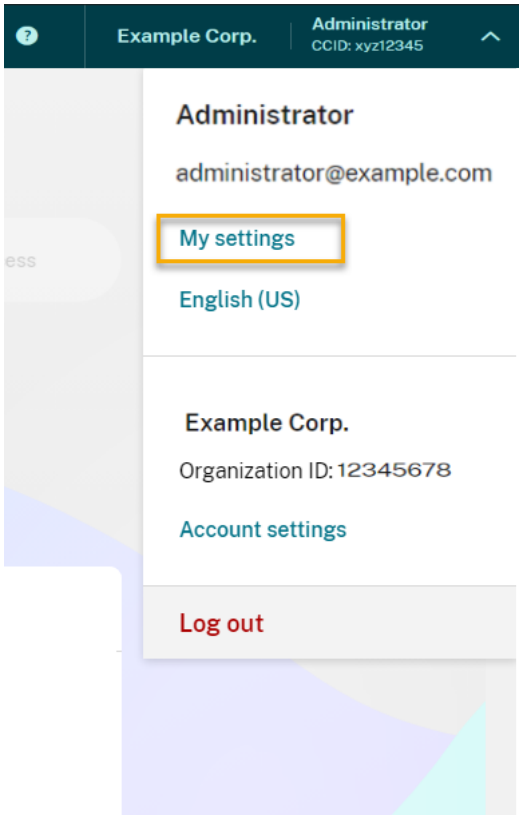
© 1997–2026 Citrix Systems, Inc. All rights reserved.



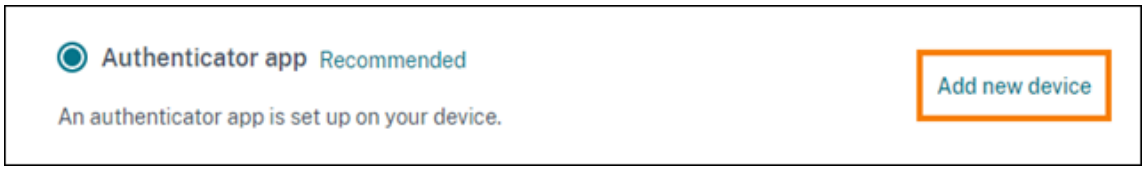
If you don't have your authenticator app, click **Don't have your authenticator app?** and select a recovery method to help you sign in. Depending on the recovery method selected, enter the recovery code you received or an unused backup code and select **Verify**.

2. If you are an administrator for multiple customer organizations, select any customer organization.
3. From the top-right menu, select **My settings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. In **Authenticator app**, select **Add new device**.



5. When prompted to confirm changing your device, select **Yes, change my device**.
6. Verify your identity by entering a verification code from your authenticator app. If you don't have an authenticator app, select **Use a recovery method** to verify your identity with the recovery method of your choice. Depending on the recovery method you select, enter the verification code or recovery code you receive or an unused backup code. Select **Verify and continue**.
7. If you are using the device you originally enrolled and your original authenticator app, delete the existing Citrix Cloud entry from your authenticator app.
8. If you are enrolling a new device and don't have an authenticator app, download one from your device's app store.
9. From your authenticator app, scan the QR code with your device or enter the key manually.
10. Enter the 6-digit verification code from your authenticator app and select **Verify code**.

After you change your device, Citrix strongly recommends checking that the verification methods in your My Profile page are up-to-date.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Change your MFA method

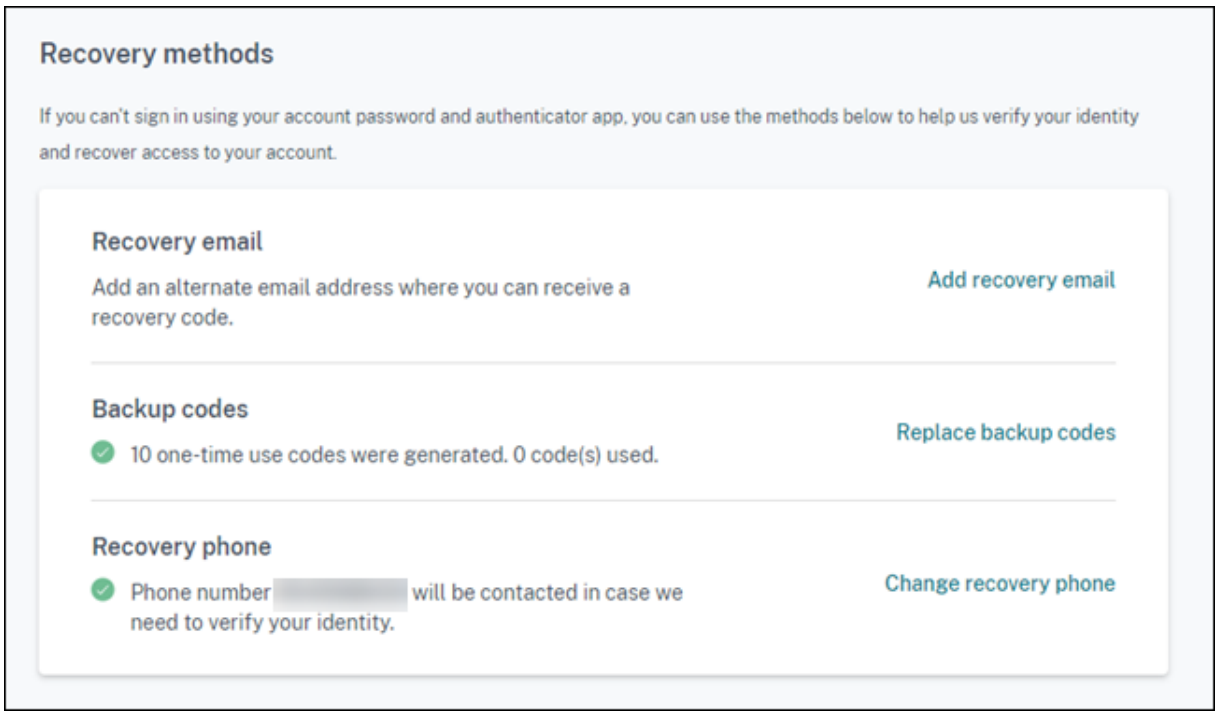
If you enrolled in MFA using an authenticator app and you want to switch to using your email address, be aware that changing your authentication method deletes your device enrollment. If you want to go back to using an authenticator app for MFA, you'll need to re-enroll your device.

1. From the top-right menu of the Citrix Cloud console, select **My settings**.
2. Under **Multifactor Authentication (MFA)**, select the authentication method you want to switch to.
3. If switching to email MFA:
    a) Select **Yes, change to email** to confirm you want to change your MFA method.
    b) Enter the code from your authenticator app or use a recovery method to confirm your identity.
    c) Select **Verify and continue** to complete the change.
4. If switching to an authenticator app:
    a) When prompted, enter the verification code that Citrix Cloud sends to your email address and select **Verify and continue**. Alternatively, use a recovery method to confirm your identity.
    b) Using your authenticator app, scan the QR code with your device's camera or enter the alphanumeric key.
    c) Under **Verify your authenticator app**, enter the 6-digit code from your authenticator app.
    d) Click **Verify code** to complete the device enrollment.

Manage your MFA recovery methods

> **Important:**
>
> To ensure your Citrix Cloud account remains secure, keep your verification methods up-to-date with accurate information. If you lose access to your authenticator app or MFA email address, these verification methods are the only way you can recover access to your account.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Add or change your recovery email

1. From the top-right menu, select **My settings**.
2. Under **Recovery methods**, in **Recovery email**, select **Add recovery email** if you haven't yet added a recovery email address. If you've already added a recovery email address, select **Change recovery email**.
3. When prompted, enter the verification code from your authenticator app or the code sent to your email address.
4. Enter the new email address you want to use and then select **Send verification email**. This email address must be different from the email address you use for your Citrix Cloud account. Citrix Cloud sends you a verification email to the email address you entered.
5. Enter the code from the verification email and then click **Verify code and complete**.

Generate new backup codes

You can generate a new set of backup codes at any time. When you use backup codes, Citrix Cloud records the number that have been used in your My Profile page.

After you generate new backup codes, be sure to store them in a safe place.

1. From the top-right menu, select **My settings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Under **Recovery methods**, in **Backup codes**, select **Generate new backup codes** if you haven't generated backup codes before. If you previously generated backup codes, select **Replace backup codes**.
3. When prompted to replace your backup codes, select **Yes, replace my codes**.
4. Verify your identity by entering a verification code from your authenticator app or the code sent to your email address.
5. Select **Verify and continue**. Citrix Cloud generates and displays a new set of backup codes.
6. Select **Download codes** to download your new codes as a text file. Then, select **I've stored my backup codes**.
7. Select **I've stored my backup codes** to finish replacing your backup codes.

Change your recovery phone number

1. From the top-right menu, select **My settings**.
2. Under **Recovery methods**, in **Recovery phone**, select **Change recovery phone**.
3. Enter the verification code from your authenticator app or the code sent to your email address. Select **Verify and continue**.
4. Enter the new phone number you want to use. Then, re-enter the phone number to confirm.
5. Select **Save recovery phone number**.

> **Note:**
>
> You can modify the permissions of Citrix Endpoint Management™ (CEM) administrators only after the administrator has accepted an administrator invitation and clicked **Manage** on the CEM tile. Like all Citrix Cloud administrators, CEM administrators have Full access by default.

Manage administrator groups

September 28, 2026

You can add administrators to your Citrix Cloud™ account using groups in your Active Directory, Microsoft Entra ID (ME-ID), or Google Cloud Identity. You can then manage service access permissions for all administrators in the group.

AD prerequisites

Citrix Cloud supports AD group authentication through SAML 2.0. Before adding members of your AD administrator groups to Citrix Cloud, you need to configure a connection between Citrix Cloud

© 1997–2026 Citrix Systems, Inc. All rights reserved.

and your SAML provider. For more information, see Connect SAML as an identity provider to Citrix Cloud.

If you already have a SAML connection in Citrix Cloud, you must reconnect your SAML provider to Citrix Cloud before adding AD administrator groups. If you don't reconnect SAML, adding AD administrator groups might fail. For more information, see Using an existing SAML connection for administrator authentication.

Microsoft Entra ID prerequisites

Using Microsoft Entra ID group authentication requires the latest version of the Microsoft Entra ID application for connecting your Microsoft Entra ID to Citrix Cloud. Citrix Cloud acquired this application when you connected your Microsoft Entra ID for the first time. If you connected your Microsoft Entra ID to Citrix Cloud before May 2019, Citrix Cloud might not be using the most current application to connect with Microsoft Entra ID. Citrix Cloud can't display your Microsoft Entra ID groups if your account isn't using the most current application.

Before using Microsoft Entra ID groups in Citrix Cloud, perform the following tasks:

1. Verify that you're using the latest application for your Microsoft Entra ID connection. Citrix Cloud displays a notification if you're not using the most current application.
2. If the application must be updated, reconnect your Microsoft Entra ID to Citrix Cloud. By reconnecting to your Microsoft Entra ID, you grant application-level read-only permissions to Citrix Cloud and allow Citrix Cloud to reconnect to your Microsoft Entra ID on your behalf. During reconnection, a list of these permissions is displayed for your review. For more information about the permissions Citrix Cloud requests, see Microsoft Entra ID Permissions for Citrix Cloud.

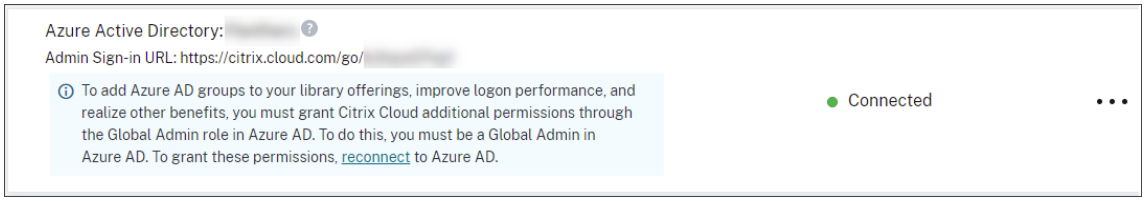
   > **Important:**
   >
   > To complete this task, you must be a Global Admin in Microsoft Entra ID. Also, you must be signed in to Citrix Cloud using a Full Access administrator account under the Citrix identity provider. If you sign in with your Microsoft Entra ID credentials, the reconnection fails. If you don't have any administrators using the Citrix identity provider, you can add one temporarily to perform this task and then delete it afterward.

To verify your connection to Microsoft Entra ID

1. Sign in to Citrix Cloud using a Full Access administrator account under the Citrix identity provider.
2. From the Citrix Cloud menu, select **Identity and Access Management** and then select **Authentication**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Locate **Microsoft Entra ID**. A notification appears if Citrix Cloud must update the application for your Microsoft Entra ID connection.



   If Citrix Cloud is already using the most current application, no notification appears.

To reconnect to Microsoft Entra ID

1. From the Microsoft Entra ID notification in the Citrix Cloud console, click the **reconnect** link. A list of the requested Azure permissions appears.
2. Review the permissions and then select **Accept**.

Google Cloud Identity

Citrix Cloud supports administrator group authentication through Google Cloud Identity. Before adding your administrator groups to Citrix Cloud, you must configure a connection between Citrix Cloud and Google Cloud Identity. For more information, see Connect Google Cloud Identity as an identity provider to Citrix Cloud.

Supported permissions

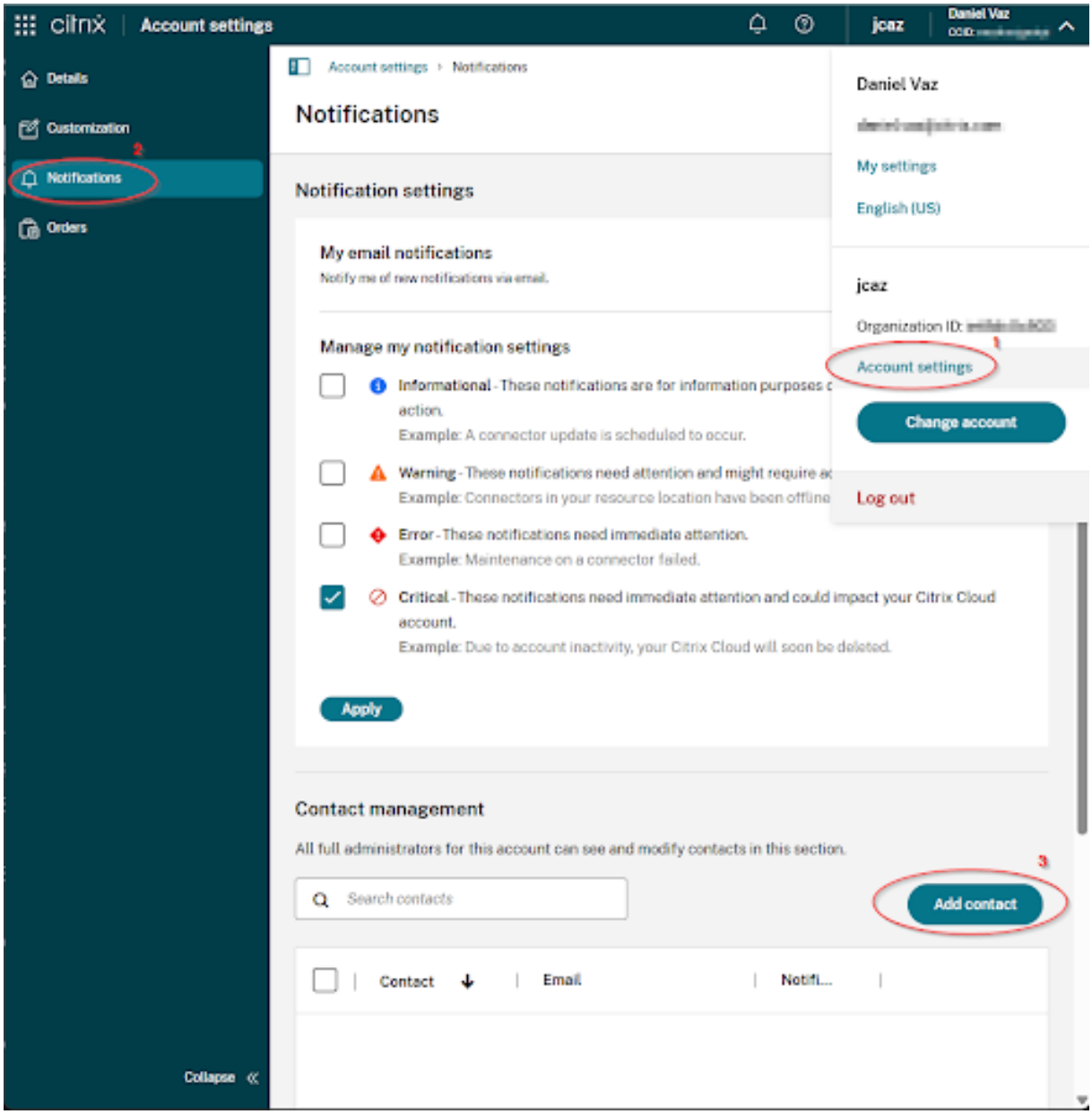
See supported permissions descriptions here, Console permissions.

Limitations

Custom access permissions for the Notifications feature are not available to members of administrator groups.

You can add notifications contacts for members of groups under Notifications Contact Management, as shown in the following image:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Citrix DaaS™ features that rely on Citrix Cloud platform capabilities such as Quick Deploy user assignment are not available.

Permission changes for an administrator group member who's already signed in will take effect only after they sign out and sign in again.

Resultant permissions for administrators with Citrix®, AD, Microsoft Entra ID, and Google Cloud identities

When an administrator signs in to Citrix Cloud, only certain permissions might be available if the administrator has both a Citrix identity (the default identity provider in Citrix Cloud) and a single-user

© 1997–2026 Citrix Systems, Inc. All rights reserved.

or group-based identity through AD, Microsoft Entra ID, or Google Cloud Identity. The table in this section describes the permissions that are available for each combination of these identities.

Single-user identity refers to AD, Microsoft Entra ID, or Google Cloud Identity permissions that are granted to the administrator through an individual account. *Group-based identity* refers to AD, Microsoft Entra ID, or Google Cloud Identity permissions that are granted as a member of a group.

Citrix identity	Single-user AD or Microsoft Entra ID identity	Group-based AD or Microsoft Entra ID identity	Single-user or group-based Google Cloud Identity	Permissions available after authentication
X	X			Administrator has cumulative permissions of both identities after successful authentication with either the Citrix identity, the AD identity, or the Microsoft Entra ID identity.
X		X		Each identity is treated as an independent entity. Available permissions depends on whether the administrator authenticates using the Citrix identity or the Microsoft Entra ID identity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix identity	Single-user AD or Microsoft Entra ID identity	Group-based AD or Microsoft Entra ID identity	Single-user or group-based Google Cloud Identity	Permissions available after authentication
X			X	Each identity is treated as an independent entity. Available permissions depends on whether the administrator authenticates using the Citrix identity or Google Cloud Identity.
	X	X		Administrator has cumulative permissions of both identities when authenticating to Citrix Cloud with AD or Microsoft Entra ID.
	X		X	Each identity is treated as an independent entity. Available permissions depends on whether the administrator authenticates using the Citrix identity or Google Cloud Identity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

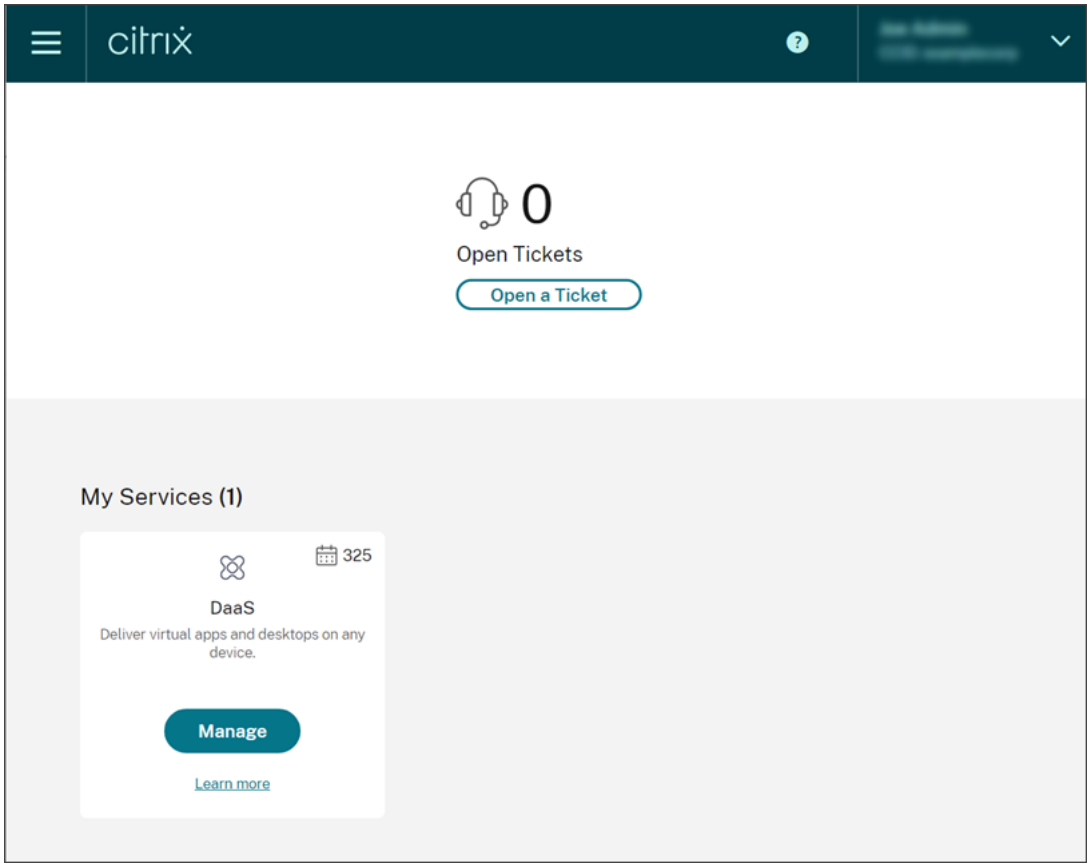
Citrix identity	Single-user AD or Microsoft Entra ID identity	Group-based AD or Microsoft Entra ID identity	Single-user or group-based Google Cloud Identity	Permissions available after authentication
		X	X	Each identity is treated as an independent entity. Available permissions depends on whether the administrator authenticates using the Citrix identity or Google Cloud Identity.
X	X	X		When authenticating with their Citrix identity, the administrator has cumulative permissions of both the Citrix identity and the single-user Microsoft Entra ID identity. When authenticating with Microsoft Entra ID, the administrator has cumulative permissions of all three identities.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sign-in experience for administrators

After you add a group to Citrix Cloud and define the service permissions, administrators in the group simply sign in by selecting **Sign in with my company credentials** on the Citrix Cloud sign-in page and entering their sign-in URL for the account (for example, `https://citrix.cloud.com/go/mycompany`). Unlike adding individual administrators, administrators in the group aren't explicitly invited, so they won't receive any emails to accept an invitation to be Citrix Cloud administrators.

After signing in, administrators select **Manage** from the service tile to access the service's management console.



Administrators who are granted permissions only as members of groups can access the Citrix Cloud account using the sign-in URL for the Citrix Cloud account.

Administrators who are granted permissions through an individual account and as a member of a group can choose the Citrix Cloud account they want to access. If the administrator is a member of multiple Citrix Cloud accounts, they can select a Citrix Cloud account from the customer picker after authenticating successfully.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Known issue

After renaming a group in Active Directory, the new name might not be displayed. As a workaround, delete the old group in **Citrix Identity and Access Management** and add the renamed group.

Limitations

Impact of multiple groups on application performance

Citrix recommends that a single administrator belongs to no more than 20 groups that have been added to Citrix Cloud. Membership in a larger number of groups might result in reduced application performance.

Impact of multiple groups on authentication

If a group-based administrator is assigned to multiple groups in AD or Microsoft Entra ID, authentication might fail because the number of groups is too large. This issue occurs due to a limitation in Citrix Cloud's integration with AD and Microsoft Entra ID. When the administrator attempts to sign in, Citrix Cloud attempts to compress the number of groups that are retrieved. If Citrix Cloud can't apply the compression successfully, all groups can't be retrieved and the authentication fails.

This issue might also affect users who authenticate to cloud stores through AD or Microsoft Entra ID. If a user belongs to multiple groups, authentication might fail because the number of groups is too large.

To resolve this issue, review the administrator or user account and verify that they belong only to the groups that are required for their role in the organization.

Adding groups fails due to too many assigned role/scope pairs

When adding a group with multiple role/scope pairs, an error might occur that indicates the group can't be created. This error occurs because the number of role/scope pairs that are assigned to the group is too large. To resolve this error, divide the role/scope pairs among two or more groups and assign the administrators to those groups.

Add an administrator group to Citrix Cloud

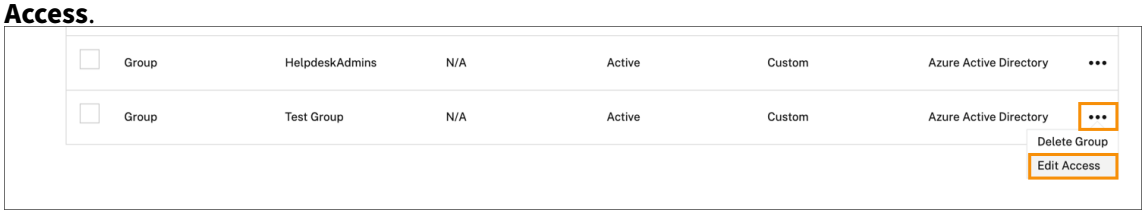
1. From the Citrix Cloud menu, select **Identity and Access Management** and then select **Administrators**.
2. Select **Add administrator/group**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In **Administrator details**, select the identity provider you want to use. If Microsoft Entra ID is selected, sign in to your Azure, if needed. Select **Next**.
4. If needed, select the domain you want to use.
5. Search for the group you want to add and select the group.
6. In **Set access**, select the roles you want to assign to the group. You must select at least one role.
7. When you're finished, select **Save**.

Modify service permissions for an administrator group

1. From the Citrix Cloud menu, select **Identity and Access Management** and then select **Administrators**.
2. Locate the administrator group you want to manage and, from the ellipsis menu, select **Edit Access**.



3. Select or clear the check marks next to one or more role and scope pairs as needed.
4. When you're finished, select **Save.**

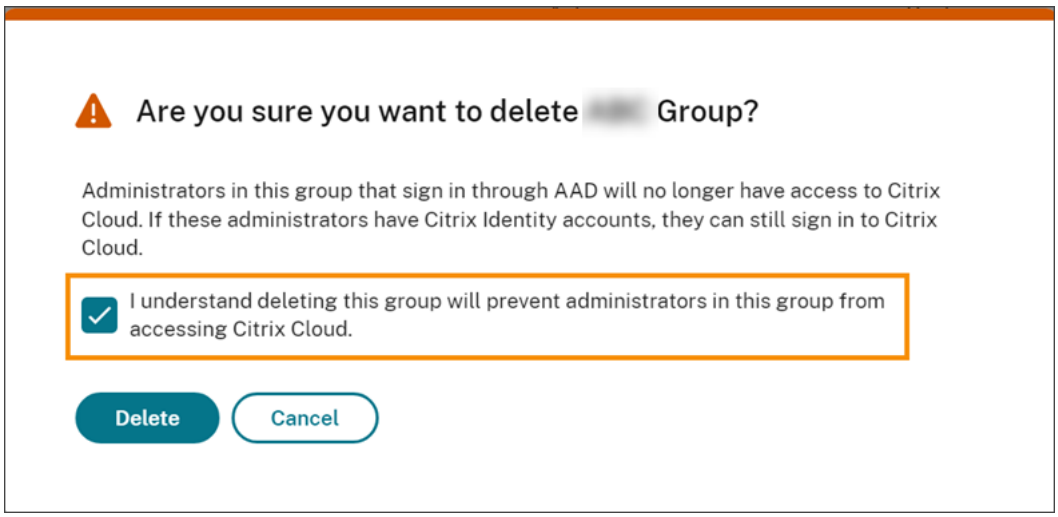
Delete an administrator group

1. From the Citrix Cloud menu, select **Identity and Access Management** and then select **Administrators**.
2. Locate the administrator group you want to manage and, from the ellipsis menu, select **Delete Group**.



A confirmation message appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



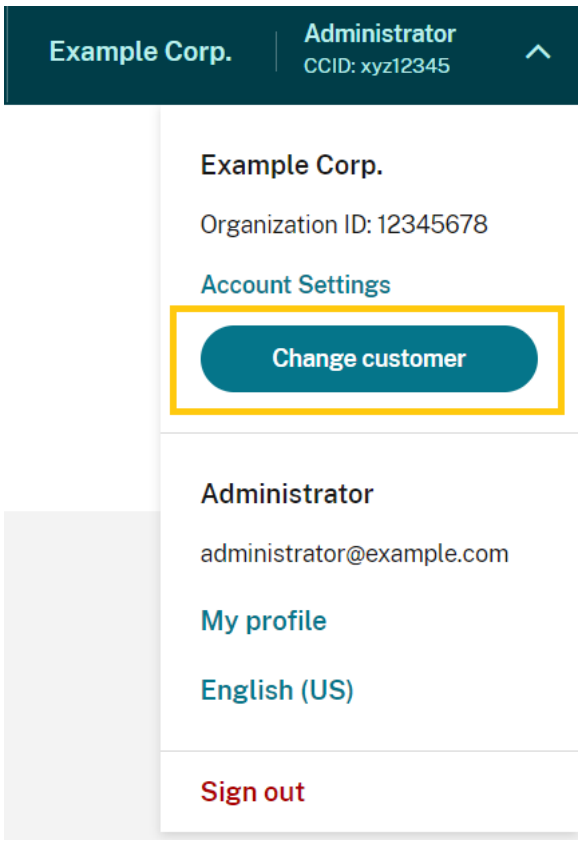
3. Choose **I understand deleting this group will prevent administrators in the group from accessing Citrix Cloud.** to confirm you're aware of the effects of deleting the group.
4. Select **Delete**.

Switch between multiple Citrix Cloud accounts

> **Note:**
>
> This section describes a scenario that affects members of Microsoft Entra ID administrator groups only.

By default, members of Microsoft Entra ID administrator groups can't switch between other Citrix Cloud accounts that they can access. For these administrators, the **Change Customer** option, shown in the image below, doesn't appear in the Citrix Cloud user menu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



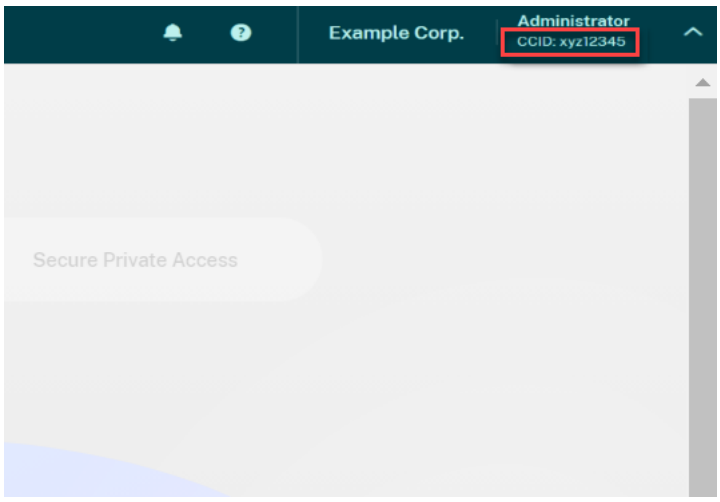
To enable this menu option and allow Microsoft Entra ID group members to switch between other Citrix Cloud accounts, you must link the accounts that you want to change between.

Linking Citrix Cloud accounts involves a hub-and-spoke-approach. Before linking accounts, decide which Citrix Cloud account will act as the account from which the other accounts are accessed (the "hub") and which accounts you want to have listed in the customer picker (the "spokes").

Before linking accounts, ensure you meet the following requirements:

- You have full access permissions in Citrix Cloud.
- You have access to the Windows PowerShell Integrated Scripting Environment (ISE).
- You have the customer IDs for the Citrix Cloud accounts you want to link. The customer ID appears in the top-right corner of the management console for each account.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- You have the Citrix CWSAuth bearer token for the Citrix Cloud account you want to link as the hub account. To retrieve this bearer token, follow the instructions in CTX330675. You need to supply this information when linking your Citrix Cloud accounts.

To link Citrix Cloud accounts

1. Open the PowerShell ISE and paste the following script into the working pane:

```
1  $headers = @{
2    }
3
4  $headers.Add("Accept","application/json")
5  $headers.Add("Content-Type","application/json")
6  $headers.Add("Authorization","CWSAuth bearer=XXXXXXX")
7
8  $uri = "https://trust.citrixworkspacesapi.net/HubCustomerID/links"
9
10 $resp = Invoke-RestMethod -Method Get -Uri $uri -Headers $headers
11 $allLinks = $resp.linkedCustomers + @("SpokeCustomerID")
12
13 $body = @{
14  "customers"=$allLinks }
15
16 $bodyjson = $body | ConvertTo-Json
17
18 $resp = Invoke-WebRequest -Method Post -Uri $uri -Headers $headers
       -Body $bodyjson -ContentType 'application/json'
19 Write-Host "Citrix Cloud Status Code: $($resp.RawContent)"
```

2. On Line 4, replace `CWSAuth bearer=XXXXXXX` with your CWSAuth value (for example, `CWSAuth bearer=AbCdef123Ghik...`). This value is a long hash that resembles a certificate key.
3. On Line 6, replace `HubCustomerID` with the customer ID of the hub account.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. On Line 9, replace `SpokeCustomerID` with the customer ID of the spoke account.
5. Run the script.
6. Repeat Steps 3-5 to link additional accounts as spokes.

To unlink Citrix Cloud accounts

1. Open the PowerShell ISE. If the PowerShell ISE is already open, clear the working pane.
2. Paste the following script into the working pane:

```
1  $headers = @{
2    }
3
4  $headers.Add("Accept","application/json")
5  $headers.Add("Content-Type","application/json")
6  $headers.Add("Authorization","CWSAuth bearer=XXXXXXX")
7
8  $uri = "https://trust.citrixworkspacesapi.net/HubCustomerID/links/
       SpokeCustomerID"
9
10 $resp = Invoke-WebRequest -Method Delete -Uri $uri -Headers
       $headers
11 Write-Host "Response: $($resp.RawContent)"
```

3. On Line 4, replace `CWSAuth bearer=xxxxxxx1` with your CWSAuth value (for example, `CWSAuth bearer=AbCdef123Ghik...`). This value is a long hash that resembles a certificate key.
4. On Line 6, replace `HubCustomerID` with the customer ID of the hub account.
5. On Line 6, replace `SpokeCustomerID` with the customer ID of the spoke account.
6. Run the script.
7. Repeat Steps 4-6 to unlink additional accounts.

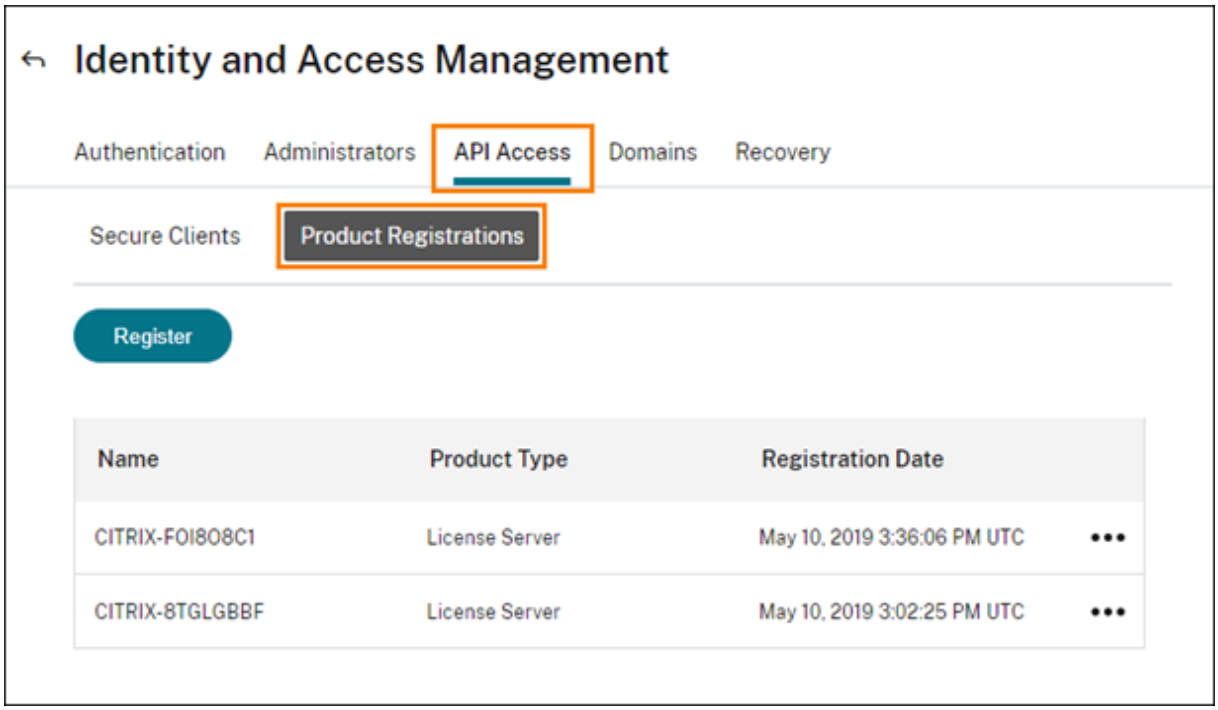
Register on-premises products with Citrix Cloud™

September 6, 2025

You can easily register your on-premises Citrix product using short-code activation through Citrix Cloud. Depending on your product, this 8-digit code might be generated during the product installation process or when you run the product's management console. When the product prompts you to register, the product requests the code from Citrix Cloud and displays it. You can then copy and paste this code or enter it manually in Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After registration, the Product Registrations page (**Identity and Access Management > API Access > Product Registrations**) displays the servers where your registered products reside.



On-premises products that you can register with Citrix Cloud include:

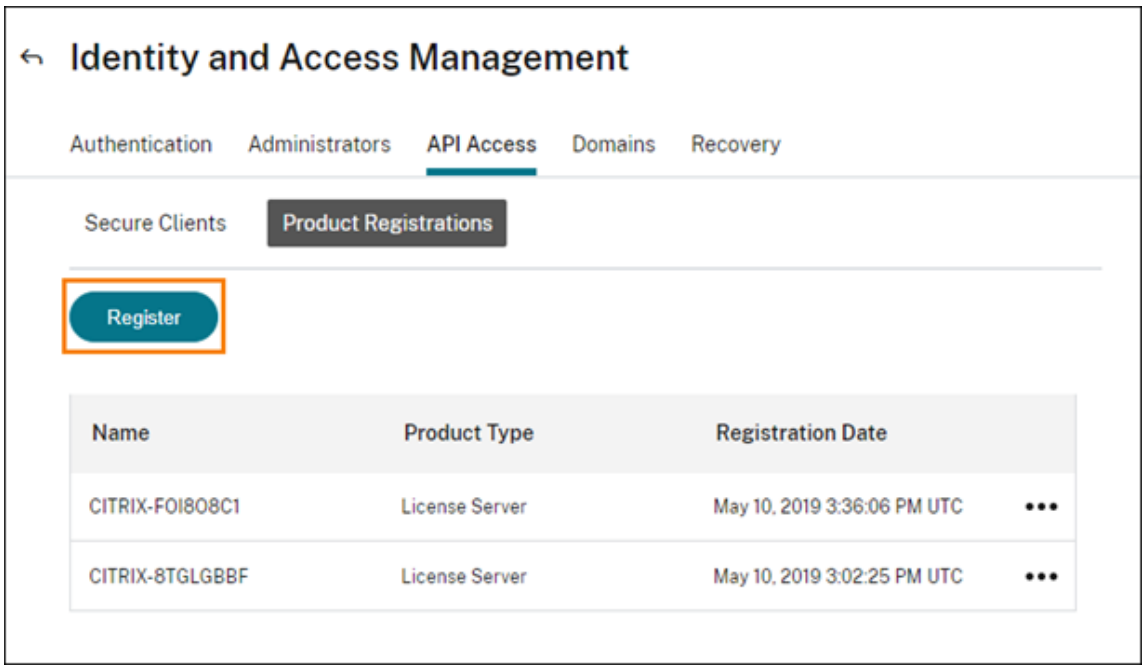
- Citrix Connector™ Appliance for Cloud Services
- Citrix Federated Authentication Service
- Citrix License Server
- Citrix Virtual Apps and Desktops, when registering a site with Citrix Analytics for Performance™

> **Note:**
>
> This article describes the steps for registering an on-premises product with Citrix Cloud. For product-specific requirements, refer to the documentation for that product.

Register a product

1. From the Citrix Cloud menu, select **Identity and Access Management**.
2. Select **API Access > Product Registrations** and then select **Register**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

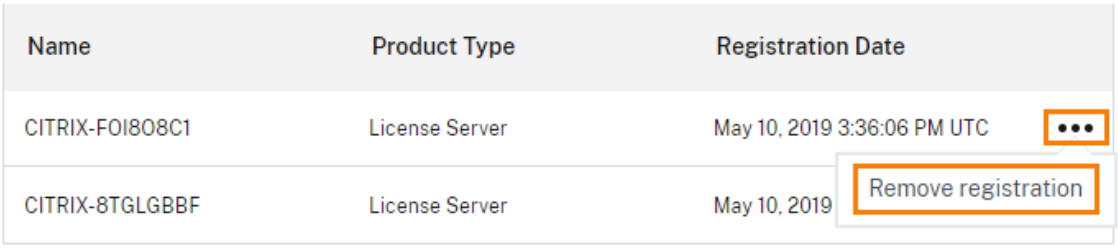


3. Enter the 8-character alphanumeric code for your Citrix product and click **Continue**.
4. Review the registration details and then click **Register**.

Remove a product registration

If you remove servers running a registered Citrix product from your environment, the Product Registrations page still displays the servers. Use the following steps to remove the servers from Citrix Cloud. If needed, you can register the product again later to display the servers on the Product Registrations page.

1. From the Product Registrations page, locate the server you want to remove.
2. Click the ellipsis button and select **Remove registration**.



3. When prompted, select **Remove**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

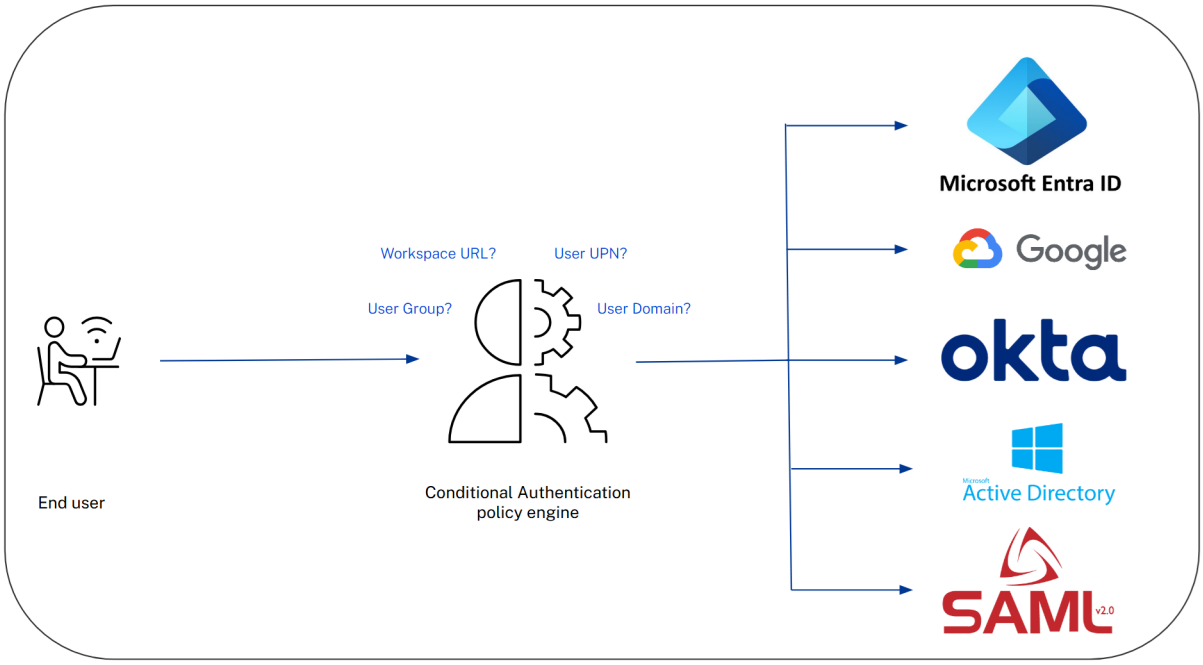
Conditional Authentication

June 22, 2026

Author:
Daniel Vaz, Mark Dear, Javier Lopez Santacruz

Conditional Authentication is a new security feature to help further enhance your Zero Trust framework. Conditional authentication allows Citrix Cloud™ admins to direct end users to different IdPs during the store login flow based on policy conditions you set. As such, different end users will have different levels of access verification based on risk factors established by the Administrator.

At the time of writing, five different switching conditions are supported that will direct your end users to different IdP instances based on the policies you define.



Common use cases

- Mergers and Acquisitions, where a large parent organization contains multiple smaller companies in the process of merging.
- Granting store access to third party users and contractors by directing them to a dedicated IdP, OIDC application or SAML application, which is different from what full time employees within your organization are normally authorized to use.
- Large Organizations with multiple branches or departments that require different authentication mechanisms.

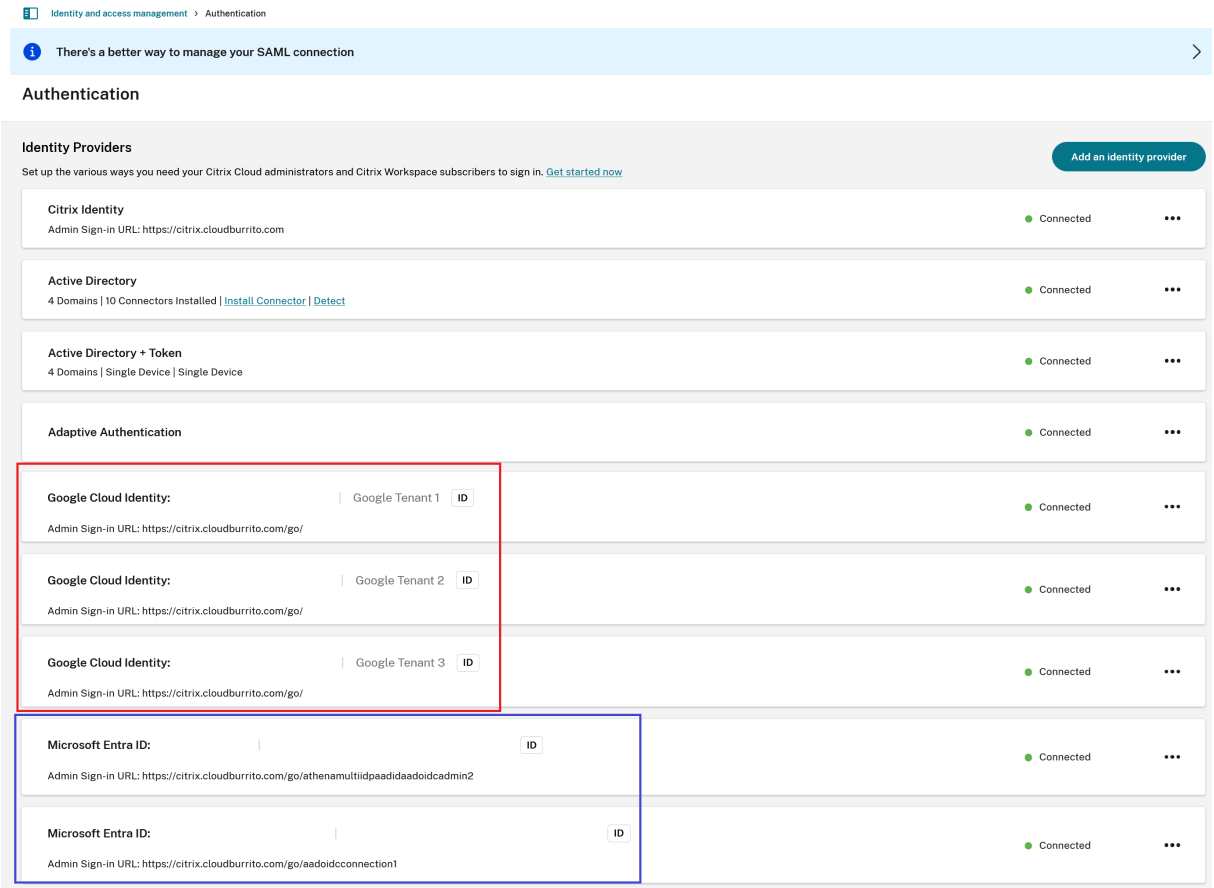
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

- Two or more Identity providers created in Citrix Cloud Identity and Access Management page

Multi-IdP

Historically, only a single instance of an Identity type was allowed. Citrix Cloud® now supports adding multiple instances of the same Identity provider type. For example, multiple EntraID IdP, Google IdP or Okta IdP connections which each point at **different** IdP tenants can now be added under the Identity and Access Management tab.

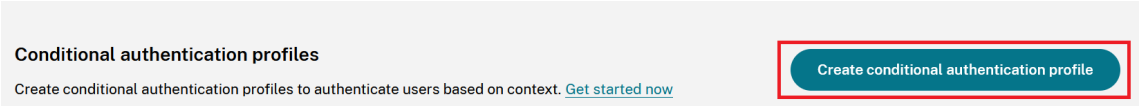


> **Important:**
>
> While DaaS and SPA currently support multiple IdPs, some services are still working on implementing this functionality and will be available shortly.

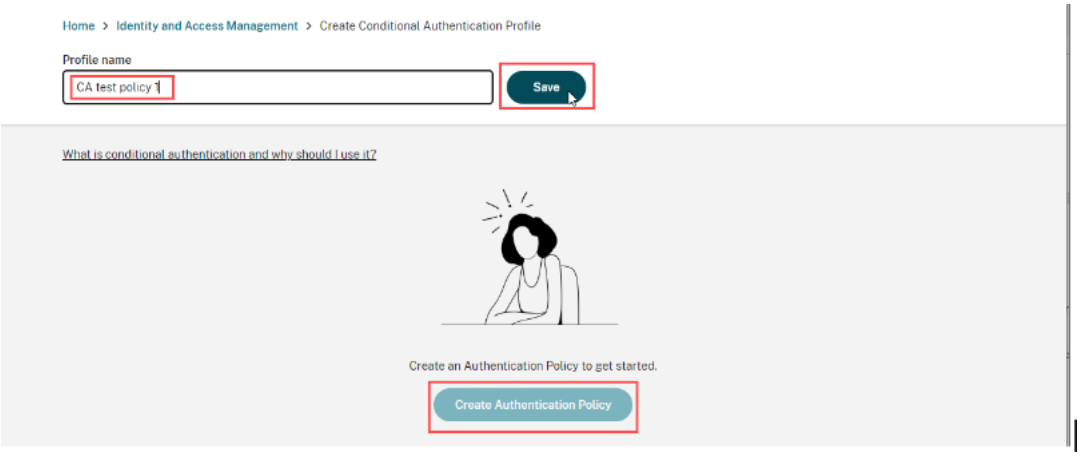
Configuring Conditional Authentication

1. Click **Create conditional authentication profile**.

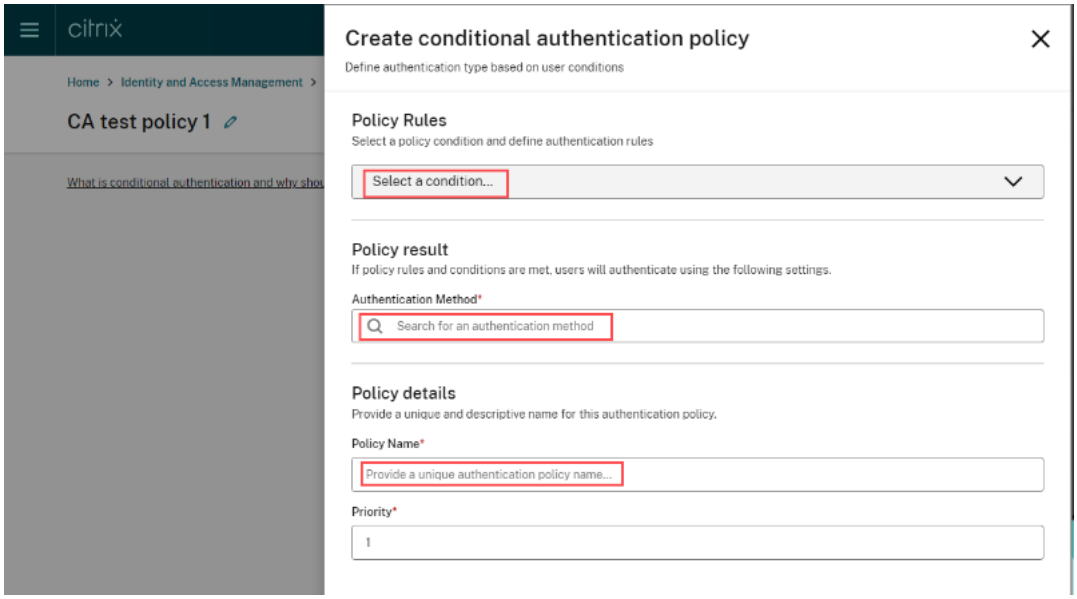
© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Enter a name for your profile and then click **Create authentication policy**.

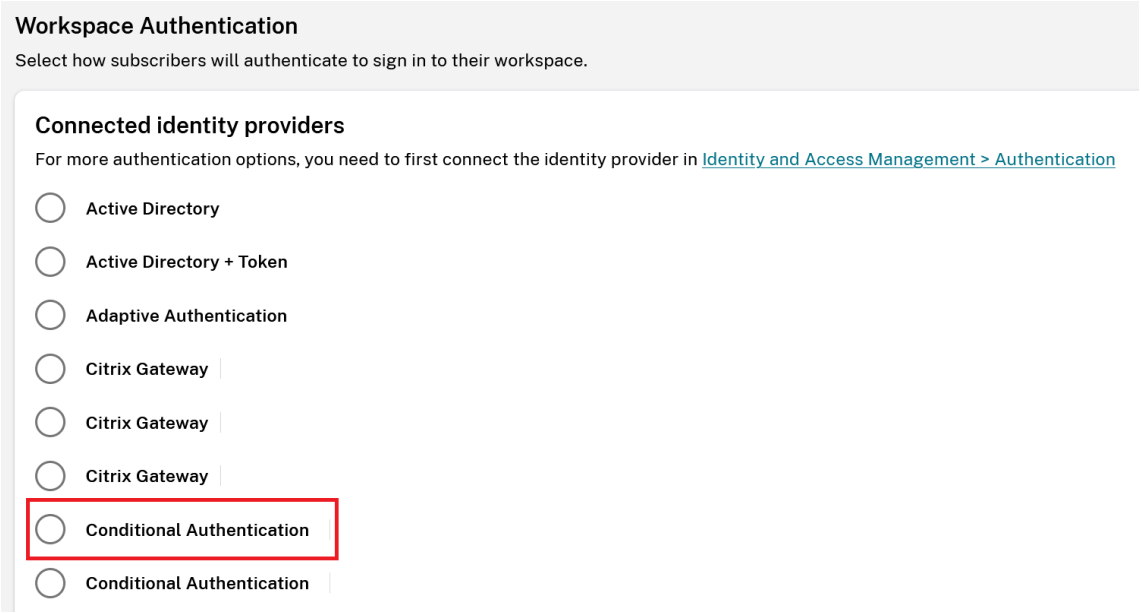


3. Select the conditions to apply to the policy as needed then click **Save**.



4. Navigate to **StoreFront Cloud** and click **Authentication** to select your identity provider or conditional authentication profile.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Conditional Authentication concepts

Conditional Authentication Profile

A Conditional Authentication Profile consists of several Conditional Authentication Policies that controls how your end users authenticate to store depending on the conditions you define. This profile allows for policy prioritization and reordering, enabling you to specify the sequence in which policies should be evaluated.

Conditional Authentication Policy

A Conditional Authentication Policy is a policy comprising one or more conditions. These conditions, when met using AND logic, guide the end user's login process to a specific target IdP instance, such as Okta OIDC, SAML, or Gateway IDP connection. Individual policies can be cloned, allowing for modification and renaming as needed.

Each conditional authentication policy consists of the following data:

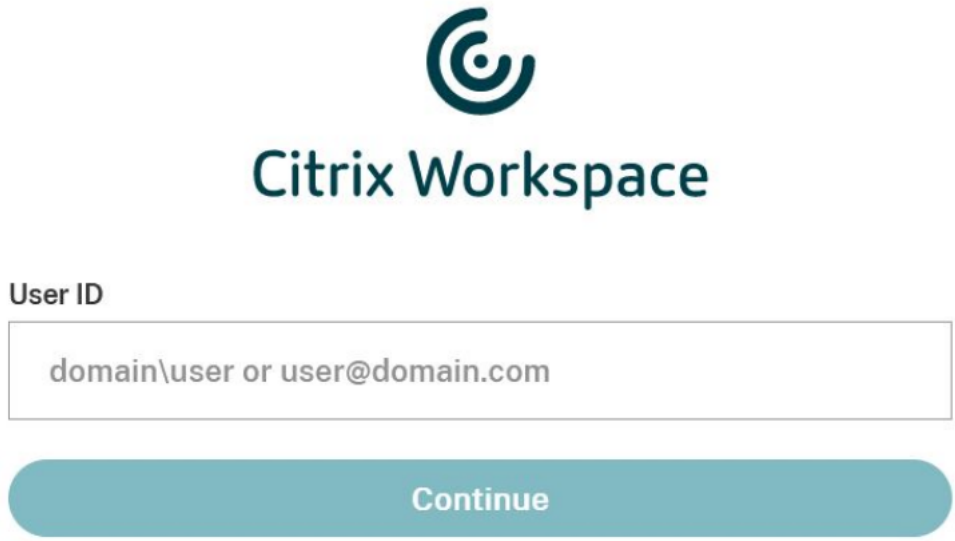
- **Policy Rules** which are one or more conditions that must be met to direct the end user to a particular IdP instance. For example, store URL 1 is used AND user is a member of AD Group1.
- **Policy Resultant IdP** which is the target IdP instance the user is directed to during the logon process. For example, `store URL 1 is used AND user is a member of AD Group1 → EntraID SAML IDP Instance`.
- **Policy Name** which is an admin friendly name used to identify and describe the policy. For example, `store URL 1 AND Group1 - EntraID SAML`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Policy Priority** which determines the order in which the policy is evaluated. Priorities are evaluated in descending order. For example: Priority 1 is higher than Priority 2.

Conditional Authentication Pre-Authentication Page

Depending on how your store is configured and the conditions set in your conditional authentication profile, your store users might encounter a pre-authentication page during their login process. This page is essential for capturing the store user's username format, which is crucial for making decisions based on conditional authentication policies. It ensures that the user's login flow is directed to the appropriate IdP instance.

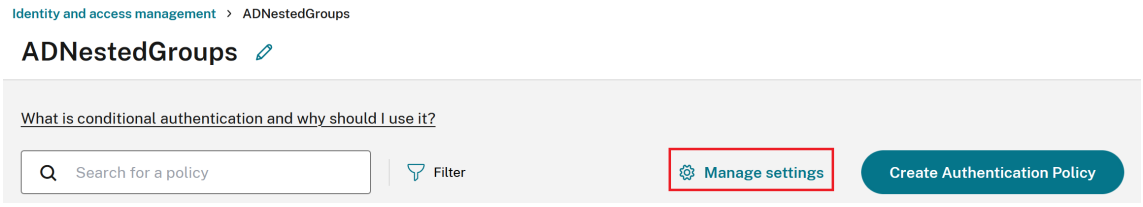


Login Auto-Fill

When a pre-authentication page is necessary, we've introduced a login auto-fill feature that automatically populates the username field on the login page with the user's input from the pre-authentication page. This eliminates the need for users to enter their username twice.

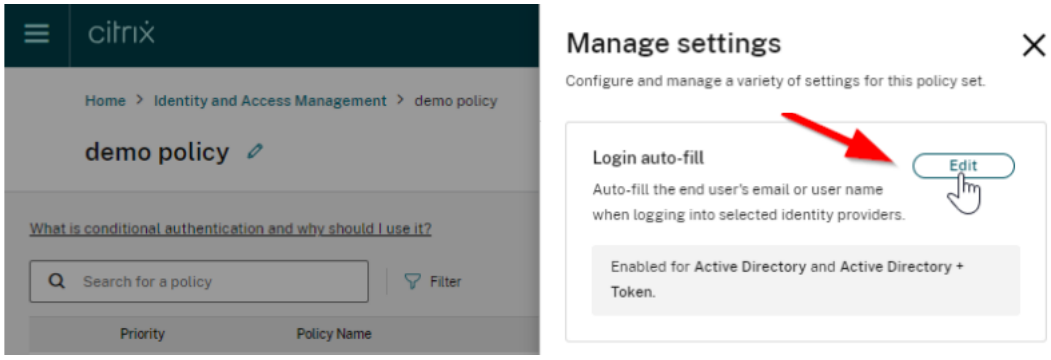
The login auto-fill feature is administered and configured by the administrator in the Conditional Authentication Profile settings, as illustrated below:

1. Click **Manage settings** in the Conditional Authentication profile page.

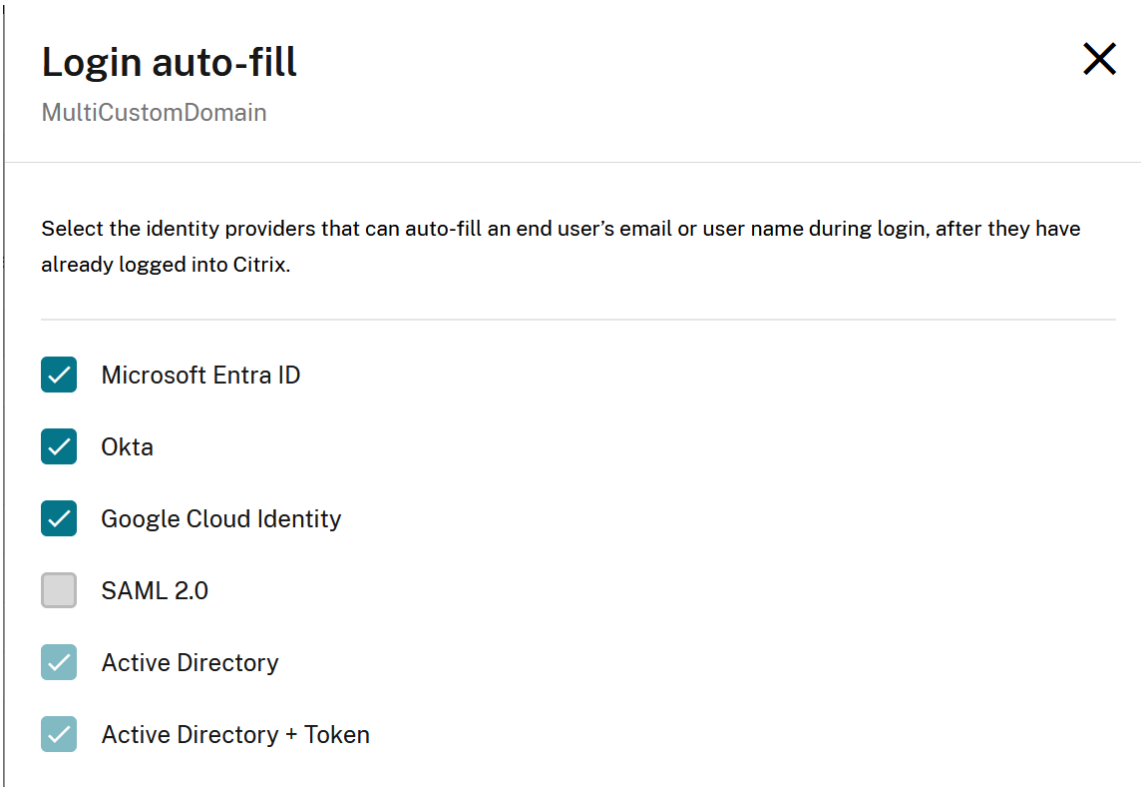


© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click **Edit**



3. Select the IdPs you would like to enable Login auto-fill for.



> **Important:**
>
> Login auto-fill is only available for IdPs that support it and will be enabled and enforced by default for AD & AD+TOTP (see screenshot above for the default settings).
>
> Certain IdPs expect a specific login format and some can support more than one type of username format. For example, Google Cloud Identity requires users to login with their email address (`user.name@domain.com`), which may sometimes be different from their UPN (`username@domain.com`). If the store end user enters a down-level logon name (domain\username) in the pre-authentication page, the down-level logon name will be pre-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

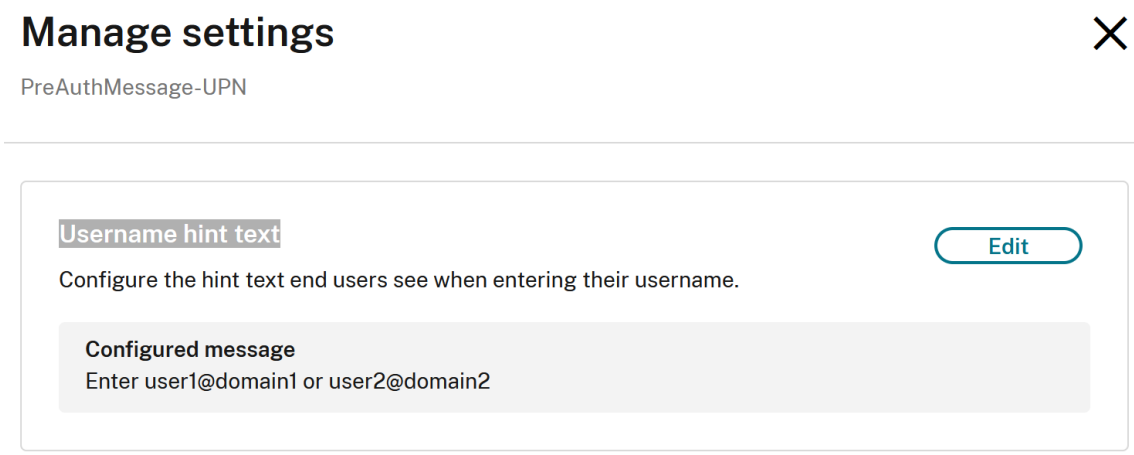
> populated within the IdP login page username field and cause an error when the user attempts to logon. Administrators should consider the IdP switching policy condition that is most appropriate and which username formats a particular IdP is expecting to receive during the logon process before configuring the login auto-fill feature.

Username hint text

When Conditional Authentication requires additional AD domain or AD group user context to make IDP switching decisions, a pre-authentication page is shown to the end user during the logon flow. Entering the user's username in an unexpected or incorrect format that does not match any of the configured CA policies will prevent the user from logging in. It is possible to customize the username hint text that appears inside the pre authentication dialogue to provide guidance to your end users, so they enter their username in the correct and expected format.

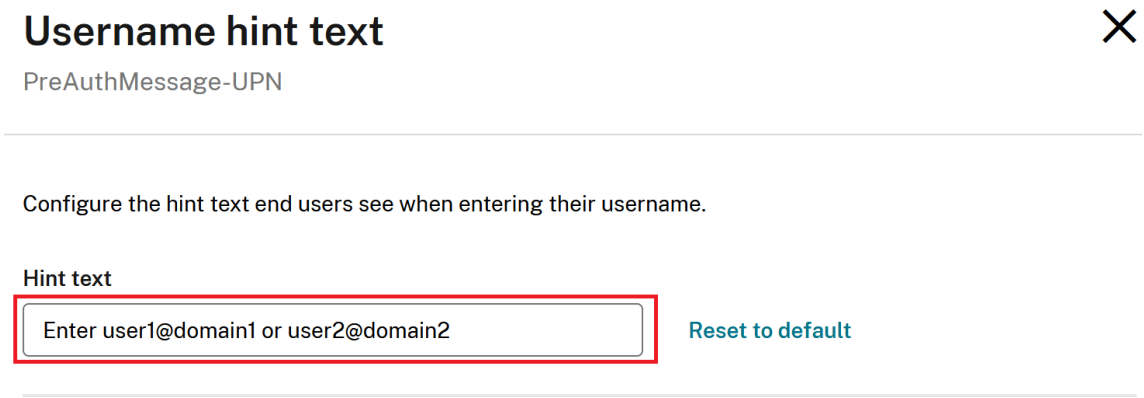
> **Important:**
>
> Use the username hint text feature with appropriate care to avoid divulging sensitive information regarding your Citrix environment, AD domains and user details. The use of generic username examples is recommended.

1. Click **Manage settings** in the Conditional Authentication profile page.
2. Click **Edit** on **Username hint text**.

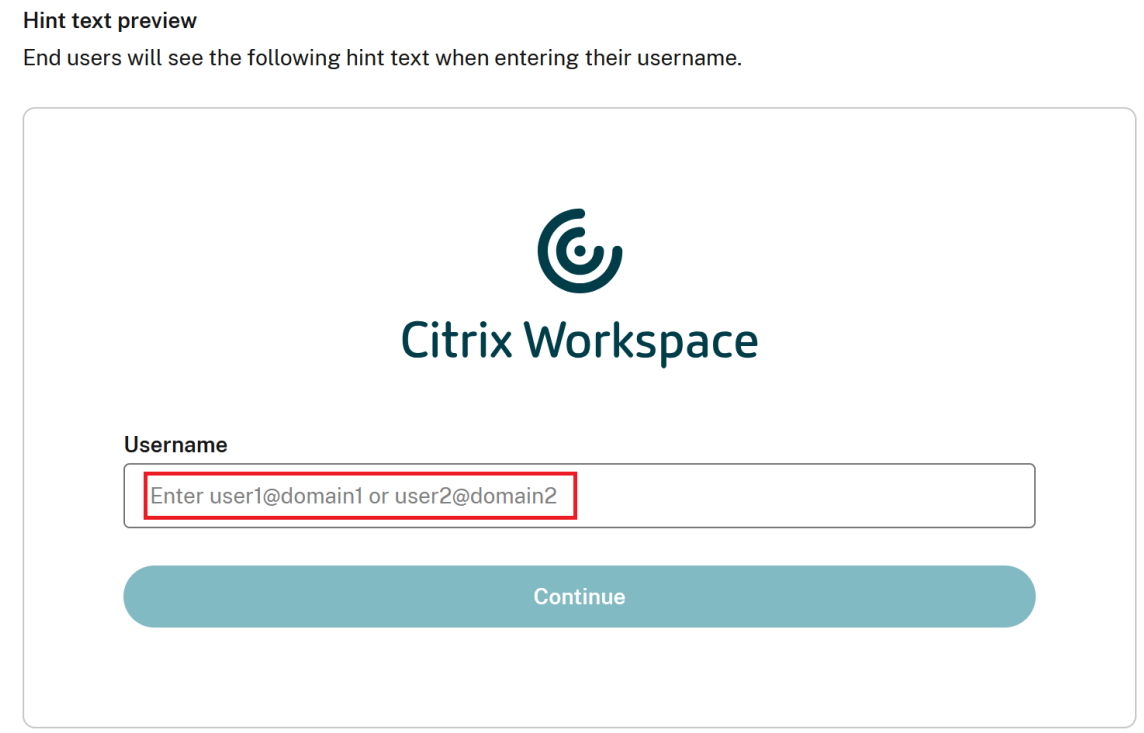


3. Set the **logon hint text** you wish to appear inside the pre-authentication dialogue during a Conditional Authentication logon flow.

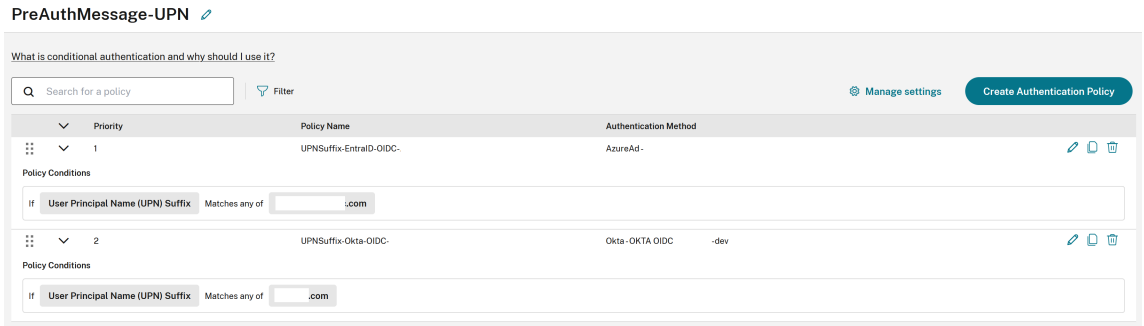
© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. View the preview image to see how the logon hint text will appear to your end users.



The example shown above is suitable for UPN-based switching between different IdPs.



5. Click **Save**.

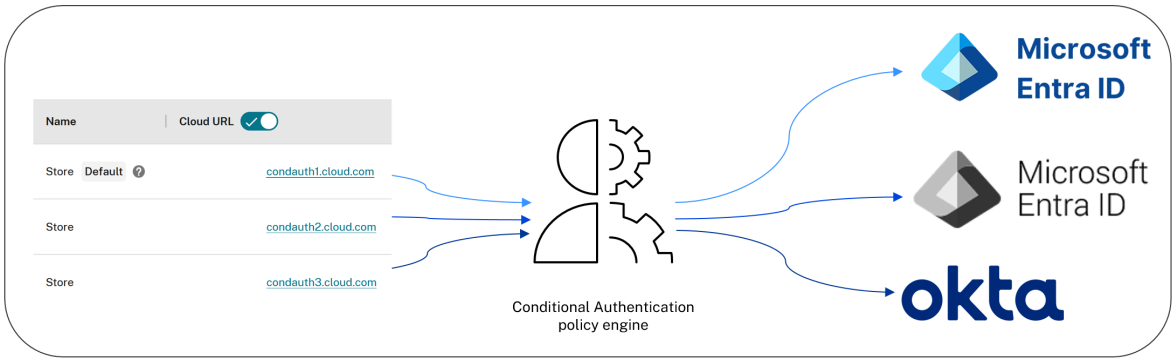
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Policy Condition Types

> **Note:**
>
> If a Conditional Authentication profile only contains policies of just store URL condition type or Network Location Name condition type, then no pre-authentication page will be displayed and users will be redirected straight to the IdP. If the profile contains any other policy condition types, the pre-authentication page will be displayed to the end user. This is true even if the matching policy is of store URL or Network Location Name type.

Store URL

Within **StoreFront Cloud** > **Access**, each store URL can be linked to a distinct IdP instance. Furthermore, multiple store URLs can be associated with the same policy, directing your end users to the same IdP instance.



Accessing store using either the Store URL or Custom URL

Your end users can switch to different resultant IdPs based on either the Store URL or custom URL they enter into a browser, or the store they configure inside Citrix Workspace app.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Name	Cloud URL	Custom URL
Store Default	1.cloud.com	1. .com
Store	2.cloud.com	2. .com
Store	3.cloud.com	3. .com
Store	4.cloud.com	4. .com
Store	5.cloud.com	5. .com
Store	6.cloud.com	6. .com
Store	7.cloud.com	7. .com
Store	8.cloud.com	8. .com
Store	9.cloud.com	9. .com
Store	10.cloud.com	10. .com

End users can reach a particular Conditional Authentication policy resultant IdP instance using either of these URLs. Citrix Cloud admins must provide the correct store URL to their end users.

`https://workspaces1.cloud.com` URL

OR,

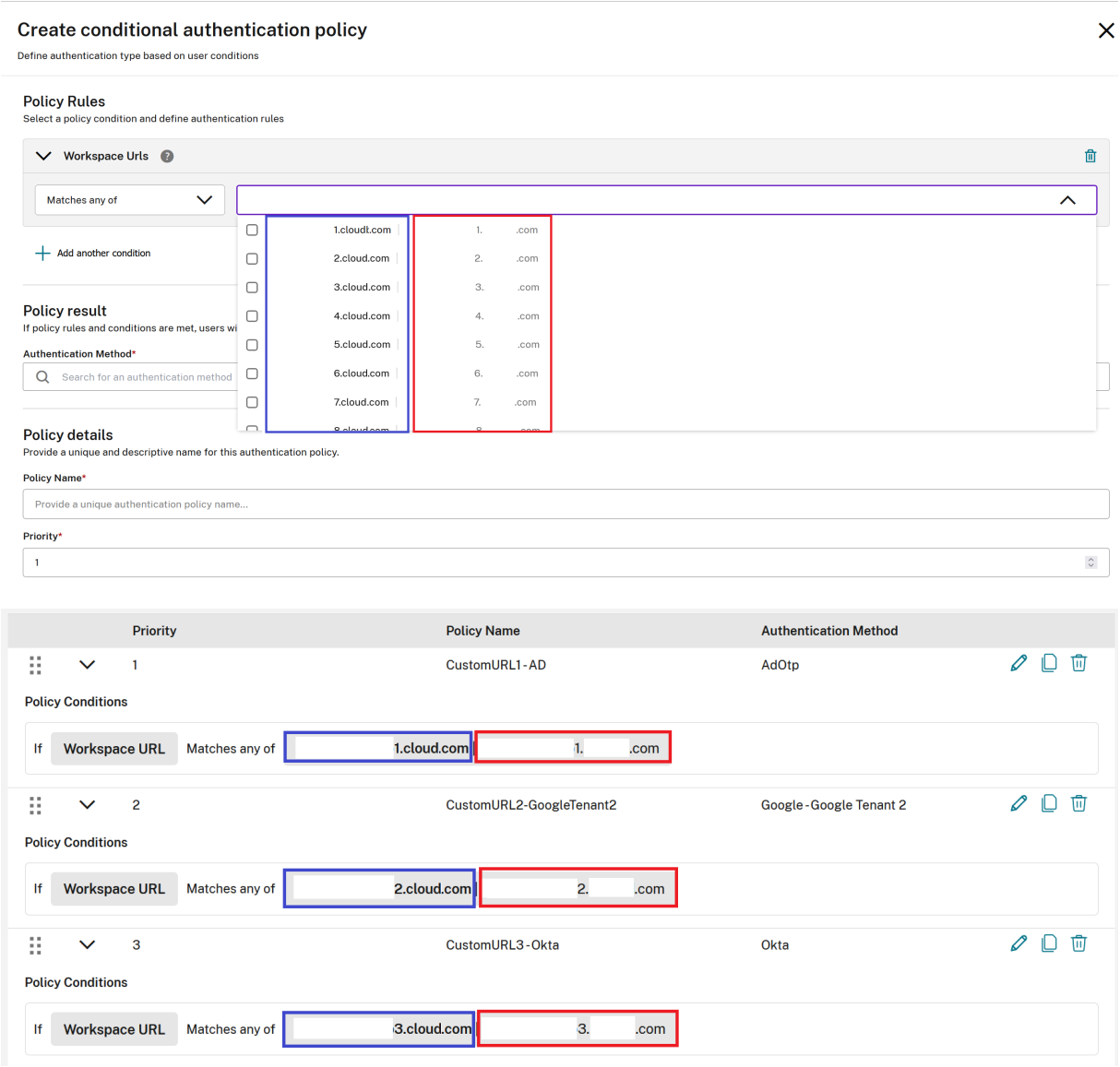
`https://workspaces1.mycompany.com` custom URL

Configure the Conditional Authentication policy by selecting a pair of URLs using the dropdown list.

- Store URLs shown in **Blue** such as `https://workspaces1.cloud.com`
- Custom URLs shown in **Red** such as `https://workspaces1.mycompany.com`

Configure a Conditional Authentication Policy using a URL pair:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Important:**
>
> Unmigrated legacy custom domains cannot be used to access store using Conditional Authentication. Migrate these legacy custom URLs first before providing your end users with the custom URL. There are also additional considerations if your Conditional Authentication policies resolve to SAML IdP instances.

For in depth instructions on how to configure Conditional Authentication with SAML and custom URLs, refer to Sign in to stores with SAML using custom domains.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

AD user group membership

AD user group membership allows you to designate an IdP instance for a specific group of Active Directory users based on their group membership.

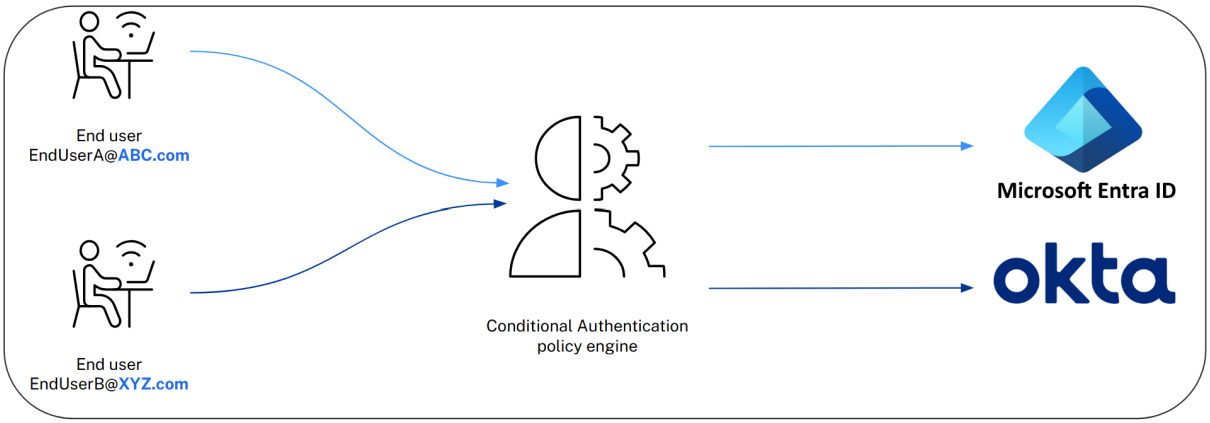
UPN Suffix or Domain Down-Level Logon Name are two mutually exclusive policy conditions. These determine the required username format that your end users must enter into the pre authentication page. You cannot use both of these conditions within the same policy.

Both Direct AD group membership (recommended) and nested AD group membership are supported.

Requirements:

- Only **universal** AD groups are supported.
- Citrix Cloud connectors domain joined within the required AD forest to check which AD groups the user is a member of.
- For AD group conditions, where a user enters their UPN, the user's UPN suffix determines the domain context that is used to perform the AD group membership lookup.

> **Important:**
>
> The unique UPN suffix must be defined in only one connected AD forest. Ambiguous UPN suffixes that occur in two or more AD forests connected to the same Citrix Cloud tenant are not supported.



UPN Suffix

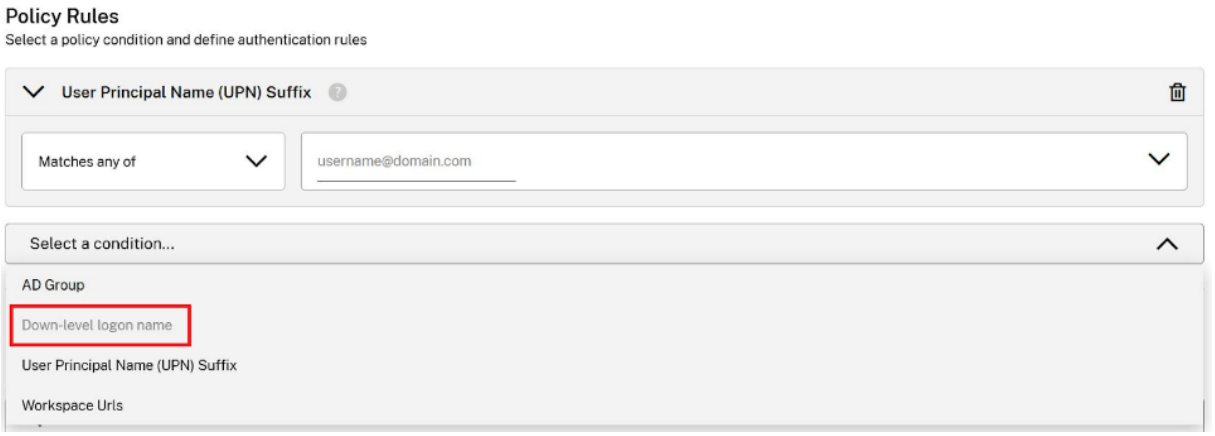
Configure an IdP instance for one or more UPN suffixes, such as `username1@domain.com` or `username2@domain.net`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Domain Down-Level Logon Name

Assign an IdP instance to one or more domain names, like `DOMAIN1\username1` or `DOMAIN1.COM\username1`.

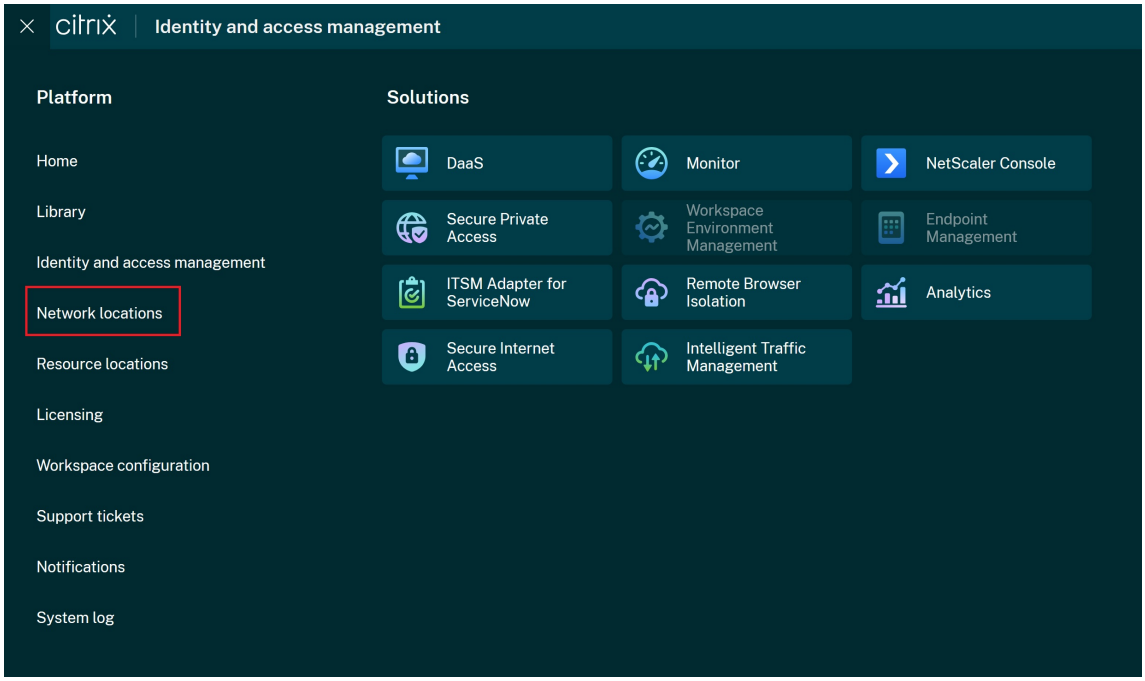
When one of the two mutually exclusive conditions is selected, the dropdown menu option for the other condition is disabled to prevent it from being added to the same policy.



Network Location Name

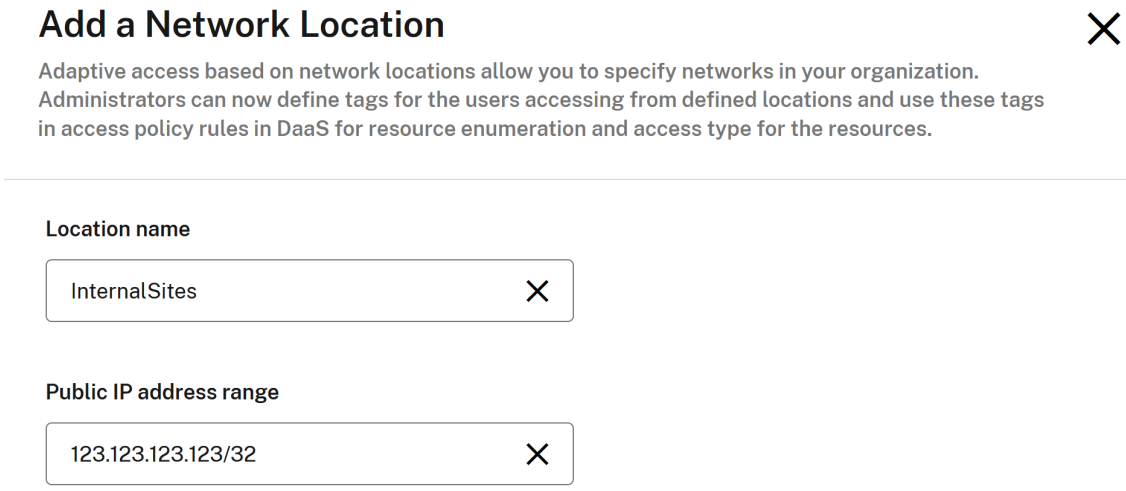
Assign an IdP instance based on client public egress IP and network location name.

1. Create your public IP address range(s) under Network Locations.

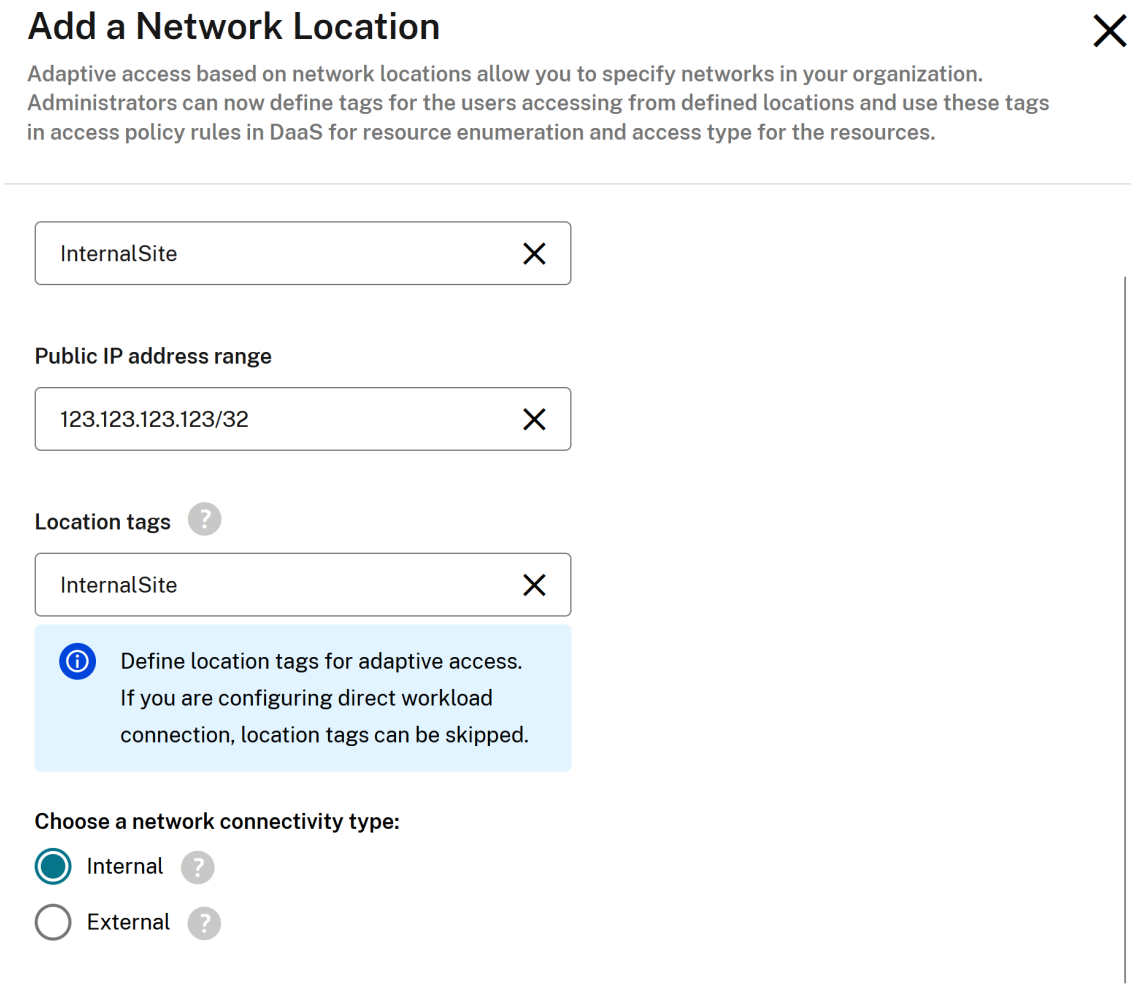


2. Click 'Add network location', input a name and a public IP address range (CIDR notation)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

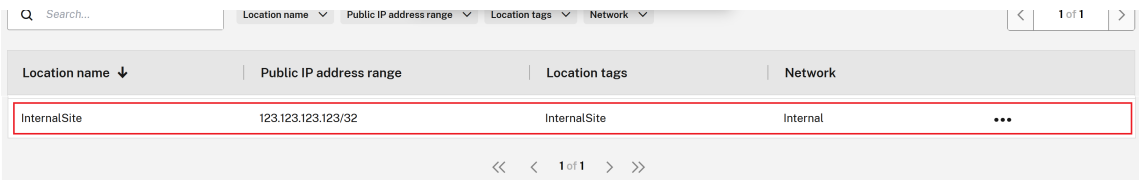


OR, when Smart Access Tagging is enable on the Citrix Cloud tenant

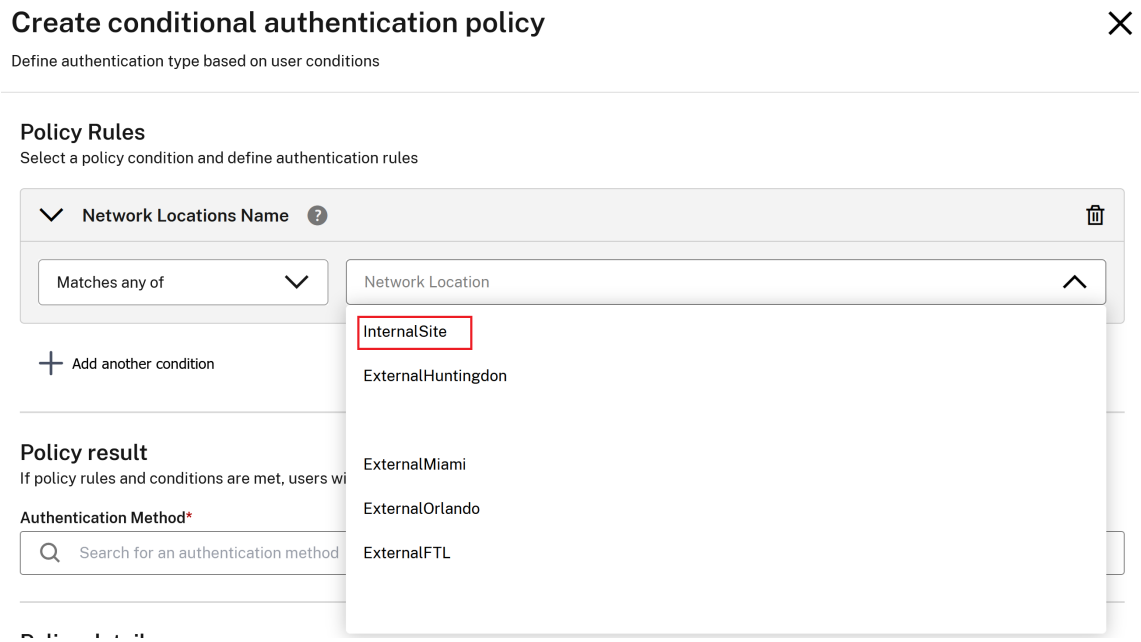


3. Confirm the network location is added properly.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Within your Conditional authentication profile, the location names will be pre-populated. Select the desired location name and assign a target IdP.

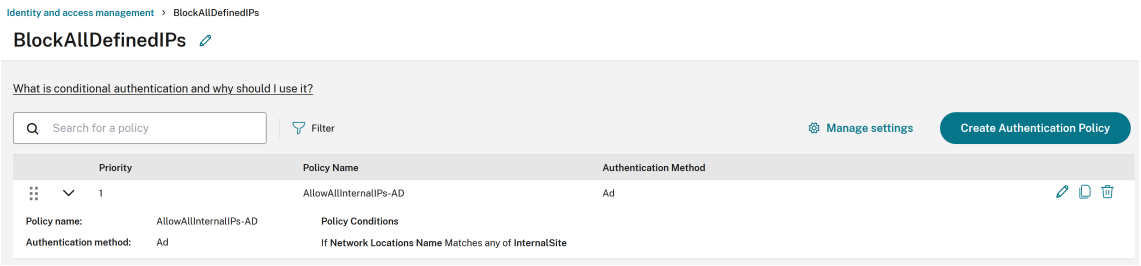


> **Important:**
>
> Any client egress IP not explicitly defined inside a Network Location Site AND NOT referenced by a Network Location Name policy is classified as “undefined”.

Common NLS use cases / configuration:

1. **NLS Scenario 1**: Block external (undefined) IPs from authenticating and accessing store.

   Policy1: Only internal clients with egress IPs defined inside the AllInternalIPs NLS site can log into store using AD.



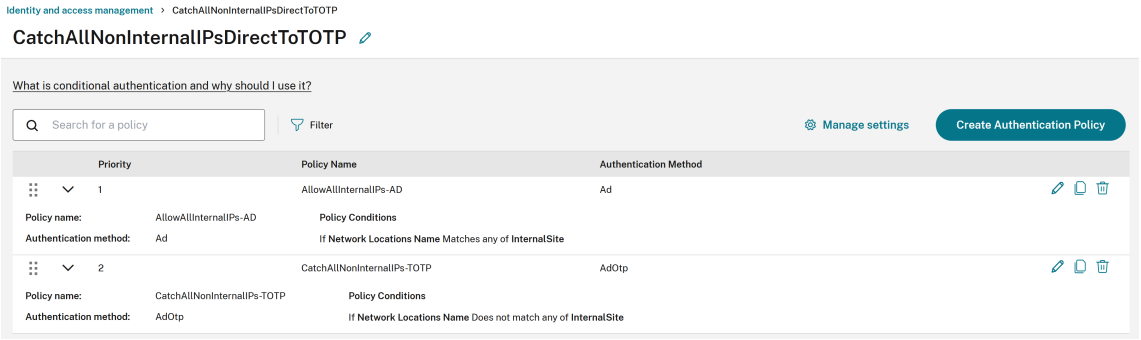
2. **NLS Scenario 2**: Direct all “undefined”egress IPs to the “catch all Idp instance”with extra authentication factors and/or increased security. Define a “catch all undefined egress IPs”policy

© 1997–2026 Citrix Systems, Inc. All rights reserved.

using “Does not match any of”and a list of all your internal NLS sites.

Policy1: Only internal clients with egress IPs defined inside the AllInternalIPs NLS site can log into store using AD.

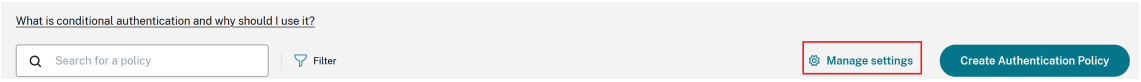
Policy2: Any external egress IPs NOT defined inside the AllInternalIPs NLS site must log into store using TOTP.



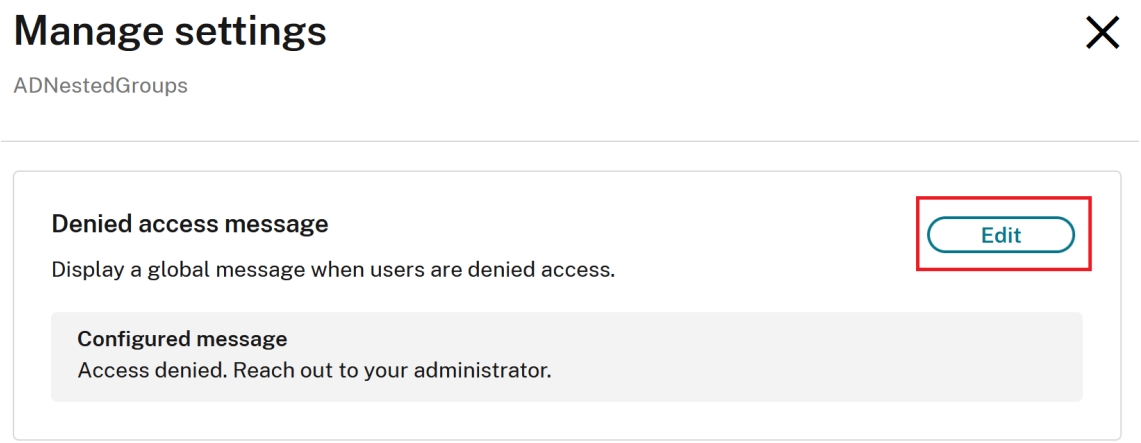
Setting a Custom Error Message for a Conditional Authentication Profile

It is possible to configure user friendly error messages which are shown to the store end user when none of your policy conditions match what the user has entered.

1. Within your Conditional Authentication profile, select **Manage settings**.



2. Edit the default error message to be displayed to your end users.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage settings

This message will be displayed when users are denied access.

*All fields required unless marked optional.

Message

Reset to default

Enter your username in the format of username@domain.com

56/50000

Message preview

End users will see the following message when access is denied.



Oops! No policies matched.

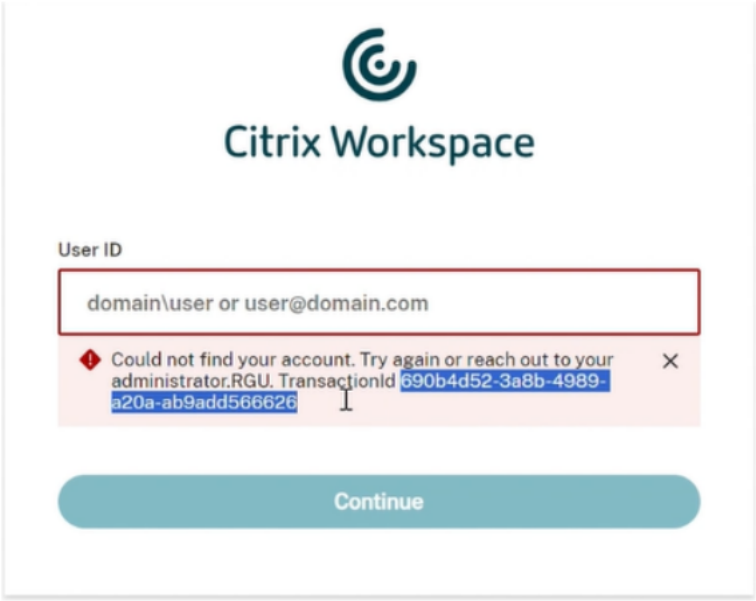
Enter your username in the format of username@domain.com

Transaction ID: 00000000000000000

© 1997–2026 Citrix Systems, Inc. All rights reserved.

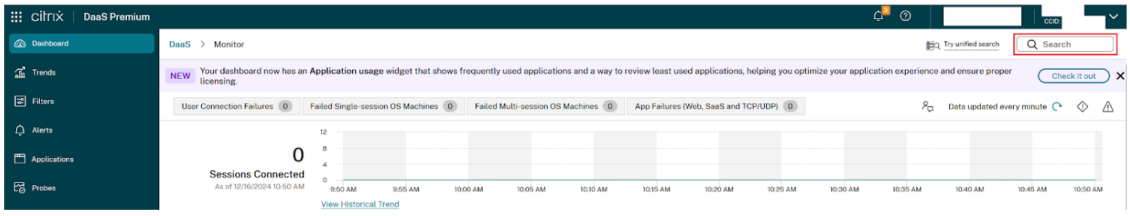
Troubleshooting with the Citrix monitor integration

If a user's login attempt fails due to a lack of matching policy, an error page is displayed, showing a transaction ID. The user can then provide this transaction ID to their Citrix Cloud administrator for further assistance.

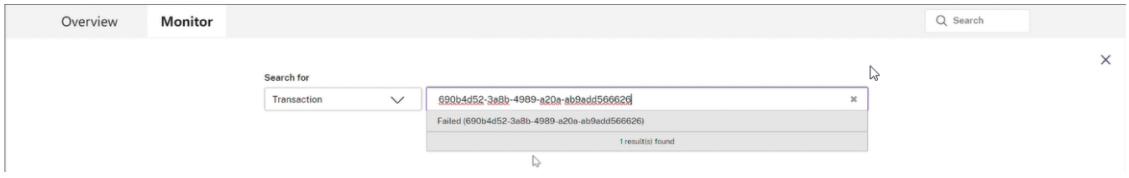


The Citrix Cloud administrator can paste the transaction ID provided by the store end user into Citrix Monitor to access details about the policy, the entered username, and the associated Conditional Authentication policies. This information helps the administrator troubleshoot and resolve the Conditional Authentication issue more efficiently.

1. Select **Monitor** and then click the Search box in the top-right hand corner.



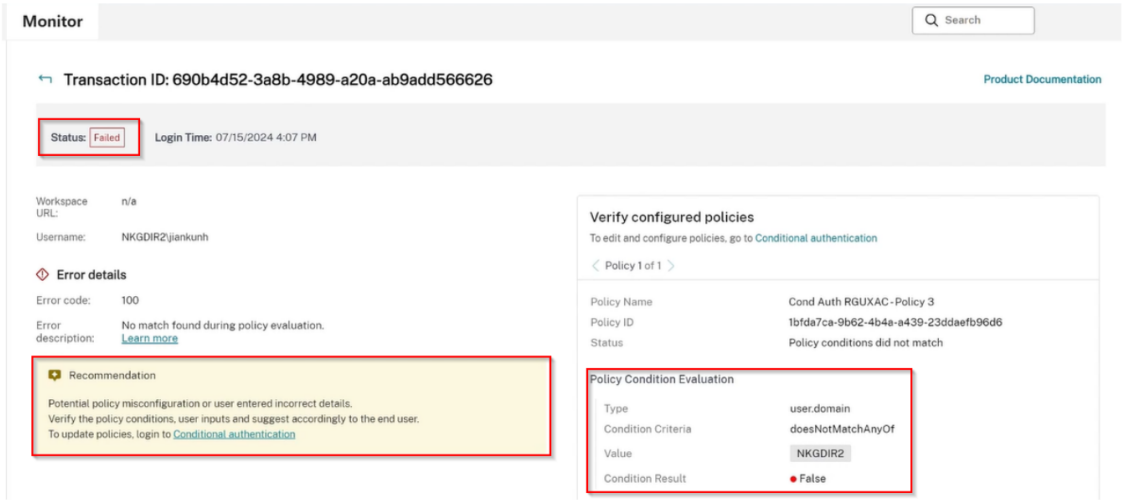
2. Select the Transaction ID from the dropdown list. Only transactions from the past 3 days are available.



3. View the failed transaction for the end user, along with the details of the Conditional Authentication policies that were evaluated. You can click the chevron buttons to navigate through all

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the evaluated policies such as <Policy 1 of 3> for the end user.

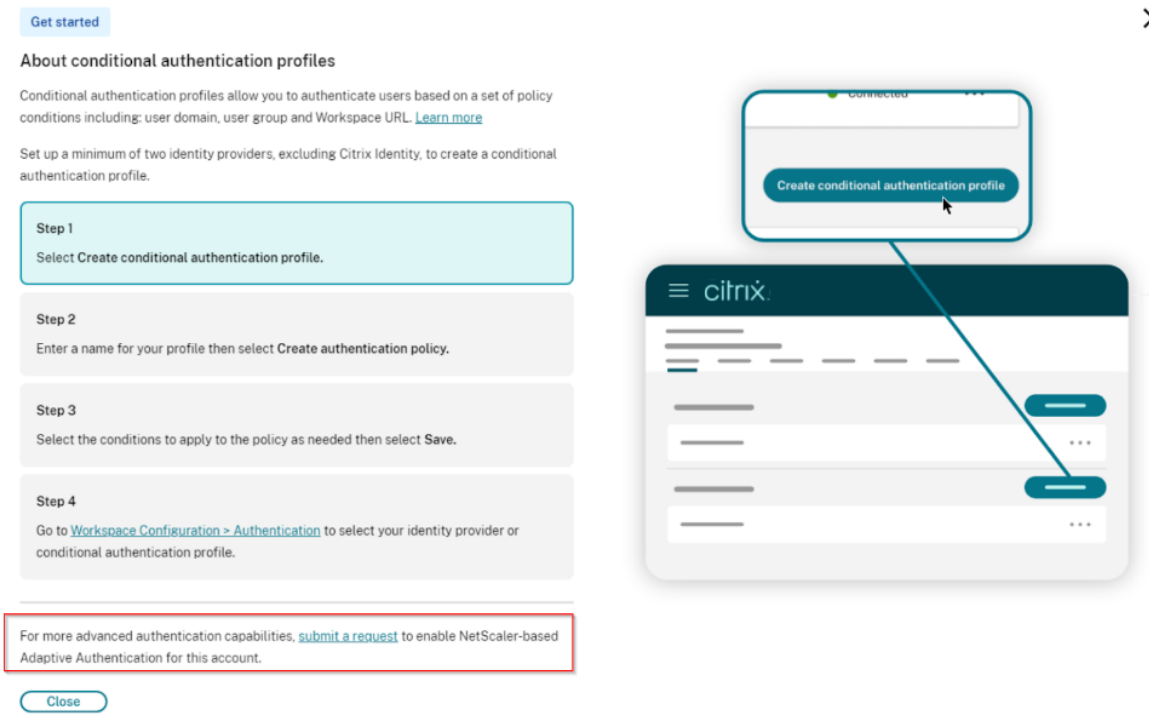


Comparison between Cloud-native Conditional Authentication and Netscaler-based Adaptive Authentication

The Cloud-native Conditional Authentication feature is designed to cover most conditional authentication use cases. However, for more advanced authentication capabilities, NetScaler-based Adaptive Authentication is available.

To use NetScaler-based Adaptive Authentication, submit a request through the Citrix Cloud **Identity and Access Management** page > **Conditional Authentication profiles** section.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Known issues and limitations

- Setting a negative priority to a policy does not behave as expected. Will be addressed in future updates.
- Currently, groups conditions are only supported for Active Directory. The native Entra Id group conditions will be added in the future.

Connect Active Directory to Citrix Cloud™

July 21, 2026

Citrix Cloud supports using your on-premises Active Directory (AD) to authenticate end users. Also, some store authentication methods require a connection between your AD and Citrix Cloud. For more information, see Choose or change authentication methods.

Citrix Cloud also supports using tokens as a second factor of authentication for end users signing in to their stores through Active Directory. End users can generate tokens using any app that follows the Time-Based One-Time Password standard, such as Citrix SSO.

For more information about authenticating end users with Active Directory plus tokens, see Active Directory plus token.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Tip:**
>
> Learn more about supported identity providers with the Introduction to Citrix Identity and Authentication education course. The "Planning Citrix Identity and Access Management"module includes short videos that walk you through connecting this identity provider to Citrix Cloud and enabling authentication for Citrix® StoreFront Cloud.

Connecting Active Directory

Connecting your Active Directory to Citrix Cloud involves installing connectors in your domain. You can choose to use either Cloud Connectors or Connector Appliances as your connectors for Active Directory. To choose which type of connector to use for your environment, see the following articles:

- Deployment scenarios for Cloud Connectors in Active Directory
- Deployment scenarios for Connector Appliances in Active Directory

Connecting Active Directory through Connector Appliances

You can use Connector Appliance to connect a resource location to forests which do not contain Citrix Virtual Apps and Desktops™ resources. For example, in the case of Citrix Secure Private Access customers or Citrix Virtual Apps and Desktops customers with some forests only used for user authentication.

For more information, see Active Directory with Connector Appliance

Connecting Active Directory through Cloud Connectors

At least two Cloud Connectors are required to ensure a highly available connection to Citrix Cloud. For more information, see the following articles:

- Cloud Connector system requirements.
- Cloud Connector Technical Details: For deployment recommendations.
- Cloud Connector Installation: For installation instructions using either the graphical interface or the command line.

Connecting your Active Directory to Citrix Cloud involves the following tasks:

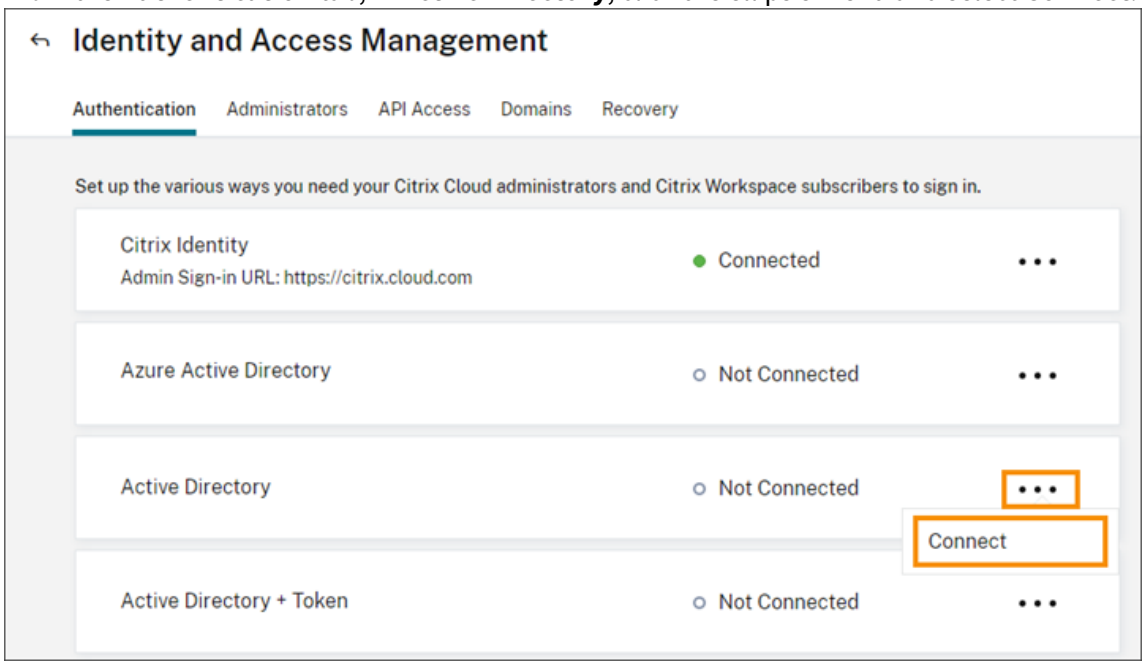
1. Install Cloud Connectors in your domain. Citrix recommends installing two Cloud Connectors for high availability.
2. If applicable, enable tokens for user devices. End users can enroll only one device at a time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> If you are deploying Cloud Connectors for use with Citrix DaaS, additional steps might be required to ensure your AD domains are registered and active after Cloud Connector deployment. Verifying that your AD domains are active in Citrix Cloud ensures that machine catalog setup occurs smoothly. For more information about post-deployment steps for Citrix DaaS, see Add a resource type or activate an unused domain in Citrix Cloud in the Citrix DaaS product documentation.

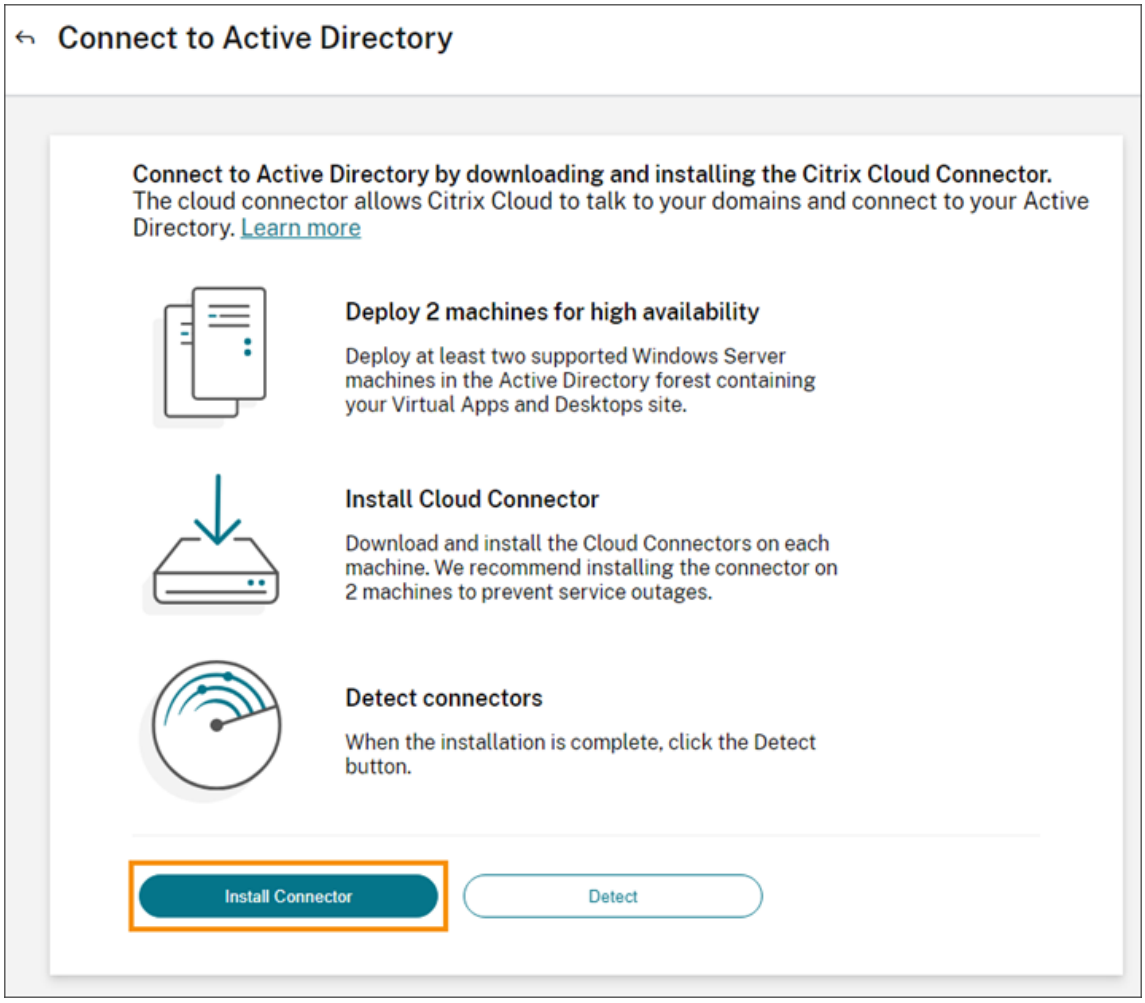
To connect your Active Directory to Citrix Cloud

1. From the Citrix Cloud menu, select **Identity and Access Management**.
2. From the **Authentication** tab, in **Active Directory**, click the ellipsis menu and select **Connect**.



3. Click **Install Connector** to download the Cloud Connector software.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Launch the Cloud Connector installer and follow the installation wizard.
5. From the **Connect to Active Directory** page, click **Detect**. After verification, Citrix Cloud displays a message that your Active Directory is connected.
6. Click **Return to Authentication**. The **Active Directory** entry is marked **Enabled** on the **Authentication** tab.

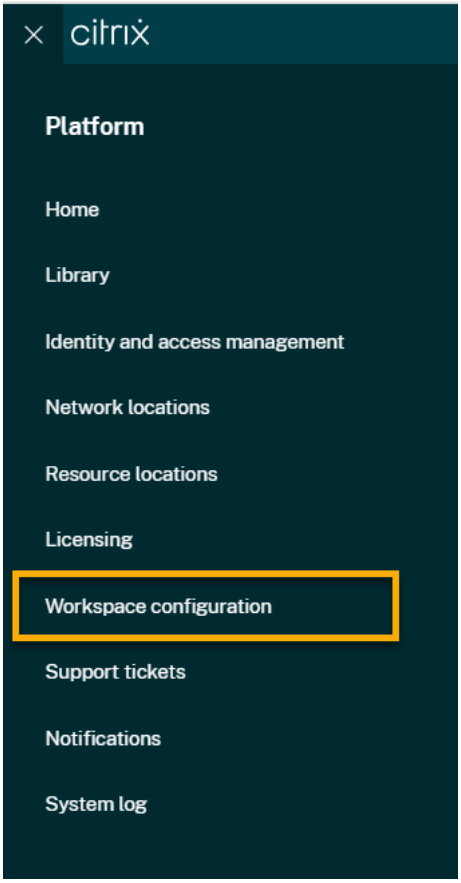
To enable Active Directory plus token authentication

1. Connect Active Directory to Citrix Cloud by using either Connector Appliances or Cloud Connectors.
2. In the Citrix Cloud **Identity and Access Management** section, on the **Authentication** tab, check that the **Active Directory** entry is marked **Enabled**.
3. Click **Next**. The **Configure Token** page appears and the **Single device** option is selected by default.
4. Click **Save and Finish** to complete the configuration. On the **Authentication** tab, the **Active Directory + Token** entry is marked as **Enabled**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Enable token authentication for stores:

   a) From the Citrix Cloud menu, select **StoreFront Cloud**.



   b) From the **Authentication** tab, select **Active Directory + Token**.

After enabling Active Directory plus token authentication, end users can register their device and use an authenticator app to generate tokens. End users can register only one device at a time. For instructions to register end users' devices, see Two-factor authentication (optional).

For options to re-enroll end users' devices, see Re-enroll a device.

More information

Citrix Tech Zone:

- Tech Insight: Authentication - TOTP
- Tech Insight: Authentication - Push

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connect Microsoft Entra ID to Citrix Cloud™

July 17, 2026

Citrix Cloud supports using Microsoft Entra ID (ME-ID) to authenticate Citrix Cloud administrators and end users.

By using Microsoft Entra ID with Citrix Cloud, you can:

- Leverage your own Active Directory, so you can control auditing, password policies, and easily disable accounts when needed.
- Configure multifactor authentication for a higher level of security against the possibility of stolen sign-in credentials.
- Use a branded sign-in page, so your users know they're signing in at the right place.
- Use federation to an identity provider of your choice including ADFS, Okta, and Ping, among others.

Microsoft Entra ID app and permissions

Citrix Cloud includes an Microsoft Entra ID app that allows Citrix Cloud to connect with Microsoft Entra ID without the need for you to be logged in to an active Microsoft Entra ID session. Since the introduction of this app, Citrix released updates that improve performance and support new features and permissions.

If you have an existing Microsoft Entra ID connection to Citrix Cloud and want to use the latest updated app, you need to update your Microsoft Entra ID connection in Citrix Cloud. For more information, see Reconnect to Microsoft Entra ID for the updated app in this article. If you choose not to update the app, your existing connection continues to function normally.

For more information about the Microsoft Entra ID apps and permissions that Citrix Cloud uses to connect with your Microsoft Entra ID, see Microsoft Entra ID permissions for Citrix Cloud.

> **Tip:**
>
> Learn more about supported identity providers with the Introduction to Citrix Identity and Authentication education course. The "Planning Citrix Identity and Access Management"module includes short videos that walk you through connecting this identity provider to Citrix Cloud and enabling authentication for Citrix® StoreFront Cloud.

Authentication with multiple Citrix Cloud accounts

This article describes how to connect your Microsoft Entra ID as an identity provider to a single Citrix Cloud account. If you have multiple Citrix Cloud accounts, you can connect each one to the same

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Entra ID tenant. Perform the following tasks:

1. Sign in to your Citrix Cloud account and select the appropriate customer ID from the customer picker.
2. If the selected customer is the first one that you're connecting to your Microsoft Entra ID, follow all the steps in this article for syncing your AD and Microsoft Entra ID, connecting the customer to Citrix Cloud, and adding administrators.
3. To connect another customer, click the user menu in the top-right corner of the Citrix Cloud console, select **Change customer**, and select the next customer ID you want to connect.
4. Connect the customer to your Microsoft Entra ID as described in Connect Citrix Cloud to Microsoft Entra ID in this article.
5. Repeat Steps 3 and 4 for each customer ID.

Prepare your Active Directory and Microsoft Entra ID

Before you can use Microsoft Entra ID, be sure you meet the following requirements:

- You have a Microsoft Azure account. Every Azure account comes with Microsoft Entra ID free of charge. If you don't have an Azure account, sign up at https://azure.microsoft.com/en-us/free/?v=17.36.
- You have the Global admin role in Microsoft Entra ID. This role is required to give Citrix Cloud your consent to connect with Microsoft Entra ID.
- Administrator accounts have their "mail"property configured in Microsoft Entra ID. To do this, you can sync accounts from your on-premises Active Directory into Microsoft Entra ID using Microsoft's Microsoft Entra ID Connect tool. Alternatively, you can configure non-synced Microsoft Entra ID accounts with Office 365 email.

Sync accounts with Microsoft Entra ID Connect

1. Ensure that the Active Directory accounts have the Email user property configured:
   a) Open Active Directory Users and Computers.
   b) In the **Users** folder, locate the account you want to check, right-click and select **Properties**. On the **General** tab, verify the **Email** field has a valid entry. Citrix Cloud requires that administrators added from Microsoft Entra ID have different email addresses than administrators who sign in using a Citrix-hosted identity.
2. Install and configure Microsoft Entra ID Connect. For complete instructions, see Getting started with Microsoft Entra ID Connect using express settings on the Microsoft Azure website.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connect Citrix Cloud to Microsoft Entra ID

When connecting your Citrix Cloud account to your Microsoft Entra ID, Citrix Cloud needs permission to access your user profile (or the profile of the signed-in user) in addition to the basic profiles of the users in your Microsoft Entra ID. Citrix requests this permission so it can acquire your name and email address (as the administrator) and enable you to browse for other users and add them as administrators later. For more information about the app permissions that Citrix Cloud requests, see Microsoft Entra ID permissions for Citrix Cloud.

> **Important:**
>
> You must be a Global admin in Microsoft Entra ID to complete this task or ask any Global admin to perform the prerequisites before signing in to Citrix Cloud.

1. Click **Menu** on the top-left corner of the page and select **Identity and Access Management**.
2. Locate Microsoft Entra ID and select **Connect** from the ellipsis menu.
3. When prompted, enter a short, URL-friendly identifier for your company and click **Connect**. The identifier you choose must be globally unique within Citrix Cloud.
4. When prompted, sign in to the Azure account with which you want to connect. Azure shows you the permissions that Citrix Cloud needs to access the account and acquire the information required for connection. Most of these permissions are read-only and allow Citrix Cloud to gather basic information from your Microsoft Graph such as groups and user profiles. If you integrated Citrix Endpoint Management or XenMobile Server with Microsoft Intune, you must grant Microsoft Intune-related read-write permissions. For more information, see Microsoft Entra ID Permissions for Citrix Cloud.
5. Click **Accept** to accept the permissions request.

Alternative connection method

You can separate connection flow in the following two phases:

1. Microsoft Entra ID app creation in Azure.
2. Citrix Cloud connection to the Microsoft Entra ID app in Citrix Cloud.

First, you need to construct a URL that the Global admin can use to add the enterprise apps into the tenant. For more information, see Construct the URL for granting tenant-wide admin consent.

Here is the explanation of the constructed URL.

```
https://login.microsoftonline.com/<tenant url>/adminconsent?client_id
=f9c0e999-22e7-409f-bb5e-956986abdf02&redirect_uri=https://portal.
azure.com
```

where:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

`tenant url` is your tenant URL or ID.
`f9c0e999-22e7-409f-bb5e-956986abdf02` is the client ID for Citrix Cloud.

Add administrators to Citrix Cloud from Microsoft Entra ID

Citrix Cloud supports adding administrators either individually or as Microsoft Entra ID groups.

To add individual administrators from Microsoft Entra ID, see Manage administrator access.

To add Microsoft Entra ID administrator groups to Citrix Cloud, see Manage administrator groups.

Sign in to Citrix Cloud using Microsoft Entra ID

After the Microsoft Entra ID user accounts are connected, users can sign in to Citrix Cloud using one of the following methods:

- Navigate to the administrator sign-in URL that you configured when you initially connected the Microsoft Entra ID identity provider for your company. Example: `https://citrix.cloud.com/go/mycompany`
- From the Citrix Cloud sign-in page, click **Sign in with my company credentials**., type the identifier you created when you initially connected Microsoft Entra ID (for example, "mycompany"), and click **Continue**.

Enable Microsoft Entra ID authentication for stores

After you connect Microsoft Entra ID to Citrix Cloud, you can allow your end users to authenticate to their stores through Microsoft Entra ID.

> **Important:**
>
> Before enabling Microsoft Entra ID store authentication, review the Microsoft Entra ID section for considerations for using Microsoft Entra ID with stores.

1. In Citrix Cloud, click the menu button in the top-left corner and select **StoreFront Cloud**.
2. From the **Authentication** tab, select **Microsoft Entra ID**.
3. Click **Confirm** to accept the store experience changes that will occur when Microsoft Entra ID authentication is enabled.

Enable advanced Microsoft Entra ID capabilities

Microsoft Entra ID provides advanced multifactor authentication, world-class security features, federation to 20 different identity providers, and self-service password change and reset, among many

© 1997–2026 Citrix Systems, Inc. All rights reserved.

other features. Turning these features on for your Microsoft Entra ID users enables Citrix Cloud to leverage those capabilities automatically.

To compare Microsoft Entra ID service level capabilities and pricing, see https://azure.microsoft.com/en-us/pricing/details/active-directory/.

Reconnect to Microsoft Entra ID for the updated app

Citrix Cloud includes an Microsoft Entra ID app that allows Citrix Cloud to connect with Microsoft Entra ID without the need for you to be logged in to an active Microsoft Entra ID session. Since the introduction of this app, Citrix has updated the app as follows:

- In August 2018, the app was updated to improve performance and allow you to be ready for future releases.
- In May 2019, the app was updated to support adding Microsoft Entra ID administrator groups to Citrix Cloud.
- In April 2022, the app was updated to use the GroupMember.Read.All permission, which replaces the Group.Read.All permission.

If you connected your Microsoft Entra ID to Citrix Cloud before these updates were released and you want to use the latest updated app, you need to disconnect your Microsoft Entra ID from Citrix Cloud and then reconnect it. Using the latest app is optional. If you choose not to update the app, your existing connection still functions normally.

Requirements

Before you reconnect your Microsoft Entra ID, verify that you meet the following requirements:

- You must be an administrator with full access permissions under the default Citrix identity provider. If you are signed in to Citrix Cloud with your Microsoft Entra ID credentials, the reconnection fails. If you don't have any administrators using the Citrix identity provider in your account, you can temporarily add one and delete it after reconnecting your Microsoft Entra ID. For instructions, see Invite individual administrators.
- If you are using Microsoft Entra ID to authenticate end users, select a different identity provider temporarily. Citrix Cloud doesn't allow you to disconnect your Microsoft Entra ID if it's also used as an authentication method for StoreFront Cloud. For more information, see Choose or change authentication methods in the StoreFront Cloud documentation.

To reconnect Microsoft Entra ID

1. Sign in to Citrix Cloud as an administrator with full access permissions under the Citrix identity provider.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. From the Citrix Cloud menu, select **Identity and Access Management** and then select **Authentication**.
3. Locate **Microsoft Entra ID** and select **Disconnect** from the ellipsis menu at the far right of the page.
4. From the ellipsis menu, select **Connect**.

> **Note:**
>
> If you are disconnecting the Microsoft Entra ID as mentioned in step 3, Citrix Cloud requests the admin to delete all the admin profiles under this Identity Provider.
> To bypass this effort, the admin can follow the steps below to reconnect the Microsoft Entra ID Identity provider.
>
> 1. As a Global admin, navigate to Azure and delete the App.
> 2. Login to Citrix Cloud and navigate to **Identity and Access Management** and click **Authentication**. From the **Authentication** tab, you can notice that Microsoft Entra ID is still connected.
> 3. Add a new Administrator in Citrix Cloud for Microsoft Entra ID.
>
> This will trigger the recreation of the app and the reconnection without deleting the administrators.

Microsoft Entra ID Permissions for Citrix Cloud™

June 22, 2026

This article describes the permissions that Citrix Cloud requests when connecting and using Microsoft Entra ID (ME-ID). Depending on how Microsoft Entra ID is used with the Citrix Cloud account, one or more enterprise applications might be created in the target Microsoft Entra ID tenant. You can connect multiple Citrix Cloud accounts to one Microsoft Entra ID tenant and use the same enterprise applications, without creating a set of applications for each account.

> **Note:**
>
> As of April 2022, the Microsoft Entra ID app that Citrix Cloud uses to connect your Microsoft Entra ID was updated to use the GroupMember.Read.All permission instead of the Group.Read.All permission. If you have an existing Microsoft Entra ID connection (before April 2022) and you want the app to use the new permission, you must disconnect and then reconnect your Microsoft Entra ID to Citrix Cloud. This action ensures your account is using the latest Microsoft Entra ID app in Citrix Cloud. For more information, see Reconnect to Microsoft Entra ID for the upgraded app.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> If you choose not to update the app, your existing connection still functions normally.

Enterprise applications

The following table lists the Microsoft Entra ID enterprise applications that Citrix Cloud uses when connecting and using Microsoft Entra ID and the purpose for which each application is used.

Name	Application ID	Usage
Citrix Cloud	e95c4605-aeab-48d9-9c36-1a262ef8048e	Store end user login
Citrix Cloud	f9c0e999-22e7-409f-bb5e-956986abdf02	Default connection between Microsoft Entra ID and Citrix Cloud
Citrix Cloud	1b32f261-b20c-4399-8368-c8f0092b4470	Administrator invitations and logins
Citrix Cloud	5c913119-2257-4316-9994-5e8f3832265b	Default connection between Microsoft Entra ID and Citrix Cloud with Citrix Endpoint Management™
Citrix Cloud	e067934c-b52d-4e92-b1ca-70700bd1124e	Legacy connection between Microsoft Entra ID and Citrix Cloud with Citrix Endpoint Management

Permissions

The permissions in Citrix Cloud's enterprise applications allow Citrix Cloud to access certain data in your Microsoft Entra ID tenant. Citrix Cloud uses these data to perform specific functions such as connecting to your Microsoft Entra ID tenant, enabling administrators to sign in to Citrix Cloud using a dedicated sign-in URL, and connecting your Microsoft Entra ID tenant with Endpoint Management. Citrix Cloud can only access these data with your consent. These permissions represent the least amount of privilege that Citrix Cloud needs to function with your Microsoft Entra ID. For more information about Microsoft Entra ID permissions and consent, see Permissions and consent in the Microsoft identity platform on the Microsoft Azure documentation web site.

In this article, each set of Microsoft Entra ID application permissions includes the following information:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **API Name:** The resource applications from which Citrix Cloud requests permissions. These applications are Microsoft Graph and Windows Microsoft Entra ID. Citrix Cloud requests the same permissions from both of these resource applications.
- **Type:** The levels of access that Citrix Cloud requests for a given permission. Permissions in a given enterprise application can have one of the following access levels:
  - **Delegated permissions** are used to act on behalf of a signed-in user, such as when querying the profile of the user.
  - **Application permissions** are used when the application performs an action without the user's presence, such as querying users within a particular group. This permission type requires consent of a Global Administrator in Microsoft Entra ID.
- **Claim Value:** The string of information that Microsoft Entra ID assigns to a given permission. Permissions in a given enterprise application can have one of the following claim values:
  - **User.Read:** Allows Citrix Cloud administrators to add users from the connected Microsoft Entra ID as administrators on the Citrix Cloud account.
  - **User.ReadBasic.All:** Gathers basic info from the user's profile. It's a subset from User.Read.All but the permission itself remains for backwards compatibility.
  - **User.Read.All:** Citrix Cloud calls List users in Microsoft Graph to enable browsing and selection of users from the customer's connected Microsoft Entra ID. For example, users from Microsoft Entra ID can be given access to a Citrix DaaS resource with the store. Citrix Cloud can't use `User.ReadBasic.All` as Citrix Cloud needs to access properties outside of the basic profile such as `onPremisesSecurityIdentifier`.
  - **GroupMember.Read.All:** Citrix Cloud calls List groups in Microsoft Graph to allow browsing and selection of groups from the customer's connected Microsoft Entra ID. For example, groups from Microsoft Entra ID can also be granted access to Citrix DaaS applications.
  - **Directory.Read.All:** Citrix Cloud calls List memberOf in Microsoft Graph to get the user's group membership as `Groups.Read.All` is not sufficient.
  - **DeviceManagementApps.ReadWrite.All:** Allows Citrix Cloud to read and write the properties, group assignments, status of apps, app configurations, and app protection policies managed by Microsoft Intune.
  - **Directory.AccessAsUser.All:** Allows Citrix Cloud to have the same access to information in the directory as the signed-in user.

> **Note:**
>
> The **Directory.Read.All** is applicable only for **Default connection between Microsoft Entra ID and Citrix Cloud with Endpoint Management**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Store end user login

This Citrix Cloud application (ID: e95c4605-aeab-48d9-9c36-1a262ef8048e) uses the following permissions:

API Name	Claim Value	Permission Name	Type
Microsoft Graph	User.Read	Sign in and read user profile	Delegated

Default connection between Microsoft Entra ID and Citrix Cloud

This Citrix Cloud application (ID: f9c0e999-22e7-409f-bb5e-956986abdf02) uses the following permissions:

API Name	Claim Value	Permission	Type
Microsoft Graph	GroupMember.Read.All	Read all groups	Delegated
Microsoft Graph	User.ReadBasic.All	Read all users' basic profiles	Delegated
Microsoft Graph	User.Read.All	Read all users' full profiles	Delegated
Microsoft Graph	User.Read	Sign in and read user profile	Delegated
Microsoft Graph	GroupMember.Read.All	Read all groups	Application
Microsoft Graph	User.Read.All	Read all users' full profile	Application

Administrator invitations and logins

This Citrix Cloud application (ID: 1b32f261-b20c-4399-8368-c8f0092b4470) uses the following permissions:

API Name	Claim Value	Permission Name	Type
Microsoft Graph	User.Read	Sign in and read user profile	Delegated
Microsoft Graph	User.ReadBasic.All	Read all users' basic profiles	Delegated

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Default connection between Microsoft Entra ID and Citrix Cloud with Endpoint Management

This Citrix Cloud application (ID: 5c913119-2257-4316-9994-5e8f3832265b) uses the following permissions:

API Name	Claim Value	Permission Name	Type
Microsoft Graph	GroupMember.Read.All	Read all groups	Delegated
Microsoft Graph	User.ReadBasic.All	Read all users' basic profiles	Delegated
Microsoft Graph	User.Read	Sign in and read user profile	Delegated
Microsoft Graph	Directory.Read.All	Read directory data	Application
Microsoft Graph	Directory.Read.All	Read directory data	Delegated
Microsoft Graph	DeviceManagementApps.ReadWrite.All	Read and write Microsoft Intune apps	Delegated
Microsoft Graph	Directory.AccessAsUser.All	Access directory as the signed-in user	Delegated

Legacy connection between Microsoft Entra ID and Citrix Cloud with Endpoint Management

This Citrix Cloud application (ID: e067934c-b52d-4e92-b1ca-70700bd1124e) uses the following permissions:

API Name	Claim Value	Permission Name	Type
Microsoft Graph	GroupMember.Read.All	Read all groups	Delegated
Microsoft Graph	User.ReadBasic.All	Read all users' basic profiles	Delegated
Microsoft Graph	User.Read	Sign in and read user profile	Delegated
Microsoft Graph	DeviceManagementApps.ReadWrite.All	Read and write Microsoft Intune apps	Delegated
Microsoft Graph	Directory.AccessAsUser.All	Access directory as the signed-in user	Delegated

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connect an on-premises Citrix Gateway as an identity provider to Citrix Cloud™

July 21, 2026

Citrix Cloud supports using an on-premises Citrix Gateway as an identity provider to authenticate end users signing in to their stores.

By using Citrix Gateway authentication, you can:

- Continue authenticating users through your existing Citrix Gateway so they can access the resources in your on-premises Virtual Apps and Desktops deployment through Citrix® StoreFront Cloud.
- Use the Citrix Gateway authentication, authorization, and auditing (AAA) functions with StoreFront Cloud.
- Use features such as pass-through authentication, smart cards, secure tokens, conditional access policies, federation, and many others while providing your users access to the resources they need through StoreFront Cloud.

> **Tip:**
>
> Learn more about supported identity providers with the Introduction to Citrix Identity and Authentication education course. The "Planning Citrix Identity and Access Management" module includes short videos that walk you through connecting this identity provider to Citrix Cloud and enabling authentication for StoreFront Cloud.

Supported versions

Citrix Gateway authentication is supported for use with the following on-premises product versions:

- Citrix Gateway 12.1 54.13 Advanced edition or later
- Citrix Gateway 13.0 41.20 Advanced edition or later

Prerequisites

Cloud Connectors

You need at least two (2) servers on which to install the Citrix Cloud Connector™ software. These servers must meet the following requirements:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Meets the system requirements described in Cloud Connector system requirements.
- Does not have any other Citrix components installed, is not an Active Directory domain controller, and is not a machine critical to your resource location infrastructure.
- Joined to the domain where your Site resides. If users access your Site's applications in multiple domains, you must install at least two Cloud Connectors in each domain.
- Connected to a network that can contact your Site.
- Connected to the Internet. For more information, see System and Connectivity Requirements.
- At least two Cloud Connectors are required to ensure a highly available connection with Citrix Cloud. After installation, the Cloud Connectors allow Citrix Cloud to locate and communicate with your Site.

For more information about installing the Cloud Connector, see Cloud Connector Installation.

Active Directory

Before enabling Citrix Gateway authentication, perform the following tasks:

- Verify that your end users have user accounts in Active Directory (AD). End users without AD accounts can't sign in to their stores successfully.
- Ensure that the user properties in your end users' AD accounts are populated. Citrix Cloud requires these properties to establish the user context when end users sign in. If these properties aren't populated, end users can't sign in to their store. These properties include:
  - Email address
  - Display name
  - Common name
  - SAM account name
  - User Principal Name
  - OID
  - SID
- Connect your Active Directory (AD) to your Citrix Cloud account. In this task, you install the Cloud Connector software on the servers you prepared, as described in the Cloud Connectors section. The Cloud Connectors enable Citrix Cloud to communicate with your on-premises environment. For instructions, see Connect Active Directory to Citrix Cloud.
- If you are performing federation with Citrix Gateway authentication, synchronize your AD users to the federation provider. Citrix Cloud requires the AD user attributes for your end users so they can sign in successfully.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requirements

Citrix Gateway advanced policies

Citrix Gateway authentication requires the use of advanced policies on the on-premises Gateway due to deprecation of classic policies. Advanced policies support multifactor authentication (MFA) for Citrix Cloud, including options such as Identity Provider Chaining. If you currently use classic policies, you must create new advanced policies to use Citrix Gateway authentication in Citrix Cloud. You can reuse the Action portion of the classic policy when you create the advanced policy.

Certificates for signature

When configuring the Gateway for authenticating end users to StoreFront Cloud, the Gateway acts as an OpenID Connect provider. Messages between Citrix Cloud and Gateway conform to the OIDC protocol, which involves digitally signing tokens. Therefore, you must configure a certificate for signing these tokens. This certificate must be issued from a public Certificate Authority (CA). Using a certificate issued by a private CA is not supported as there is no way to provide Citrix Cloud with the private root CA certificate. So, the certificate chain of trust cannot be established. If you configure multiple certificates for signature, these keys are rotated for each message.

Keys must be bound to **vpn global**. Without these keys, end users can't access their store successfully after signing in.

Clock synchronization

Because digitally signed messages in OIDC carry a timestamp, the Gateway must be synchronized to NTP time. If the clock isn't synchronized, Citrix Cloud assumes that tokens are stale when checking their validity.

Task overview

To set up Citrix Gateway authentication, you perform the following tasks:

1. In **Identity and Access Management**, start configuring the connection to your Gateway. In this step, you generate the client ID, secret, and redirect URL for the Gateway.
2. On the Gateway, create an OAuth IdP advanced policy using the generated information from Citrix Cloud. This enables Citrix Cloud to connect with your on-premises Gateway. For instructions, see the following articles:
    - Citrix Gateway 12.1: Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud

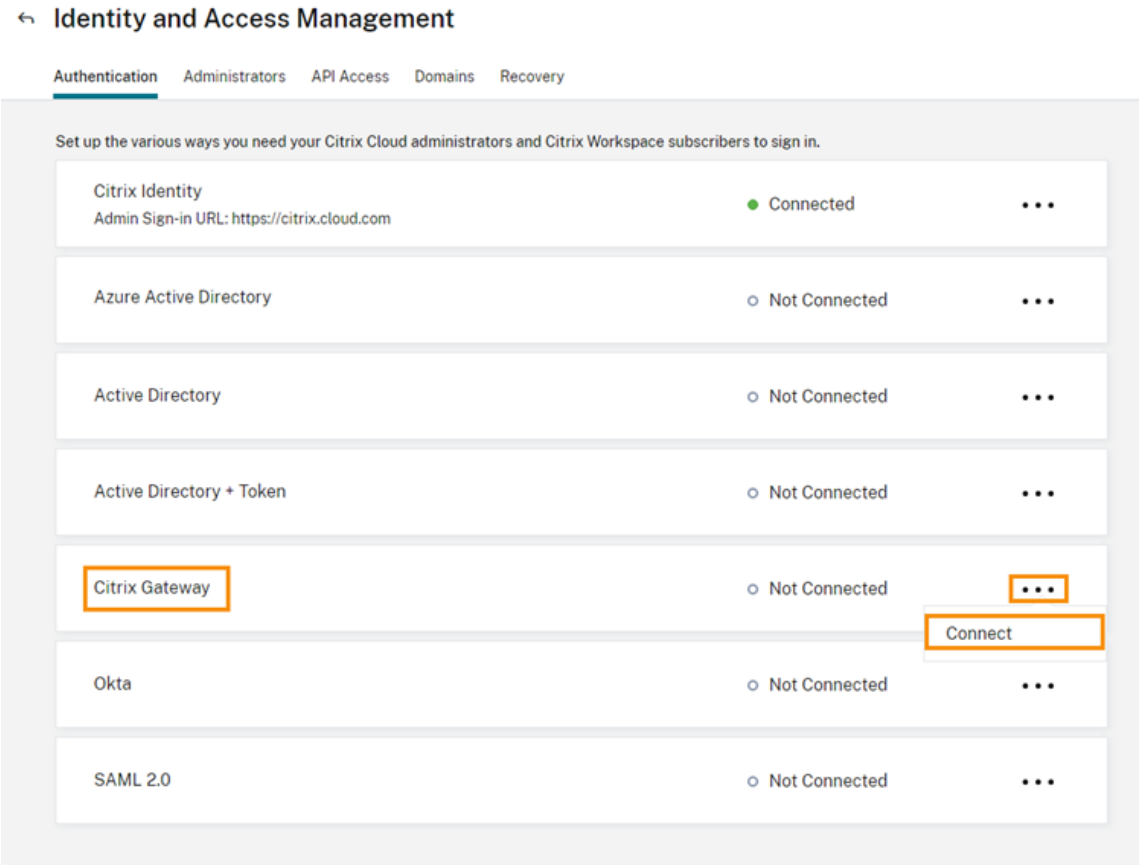
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Gateway 13.0: Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud

3. In **StoreFront Cloud**, enable Citrix Gateway authentication for end users.

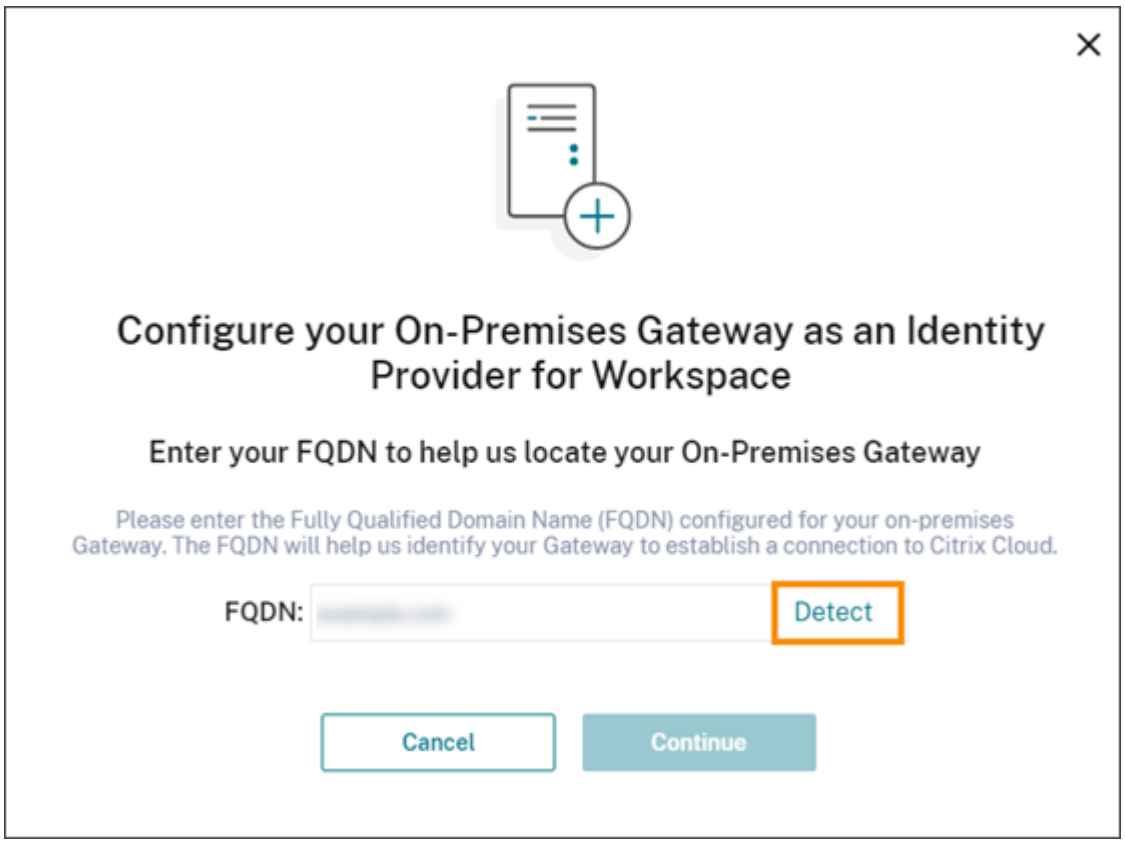
To enable Citrix Gateway authentication for end users

1. From the Citrix Cloud menu, select **Identity and Access Management**.
2. From the **Authentication** tab, in **Citrix Gateway**, click the ellipsis menu and select **Connect**.



3. Enter the FQDN of your on-premises Gateway and click **Detect**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

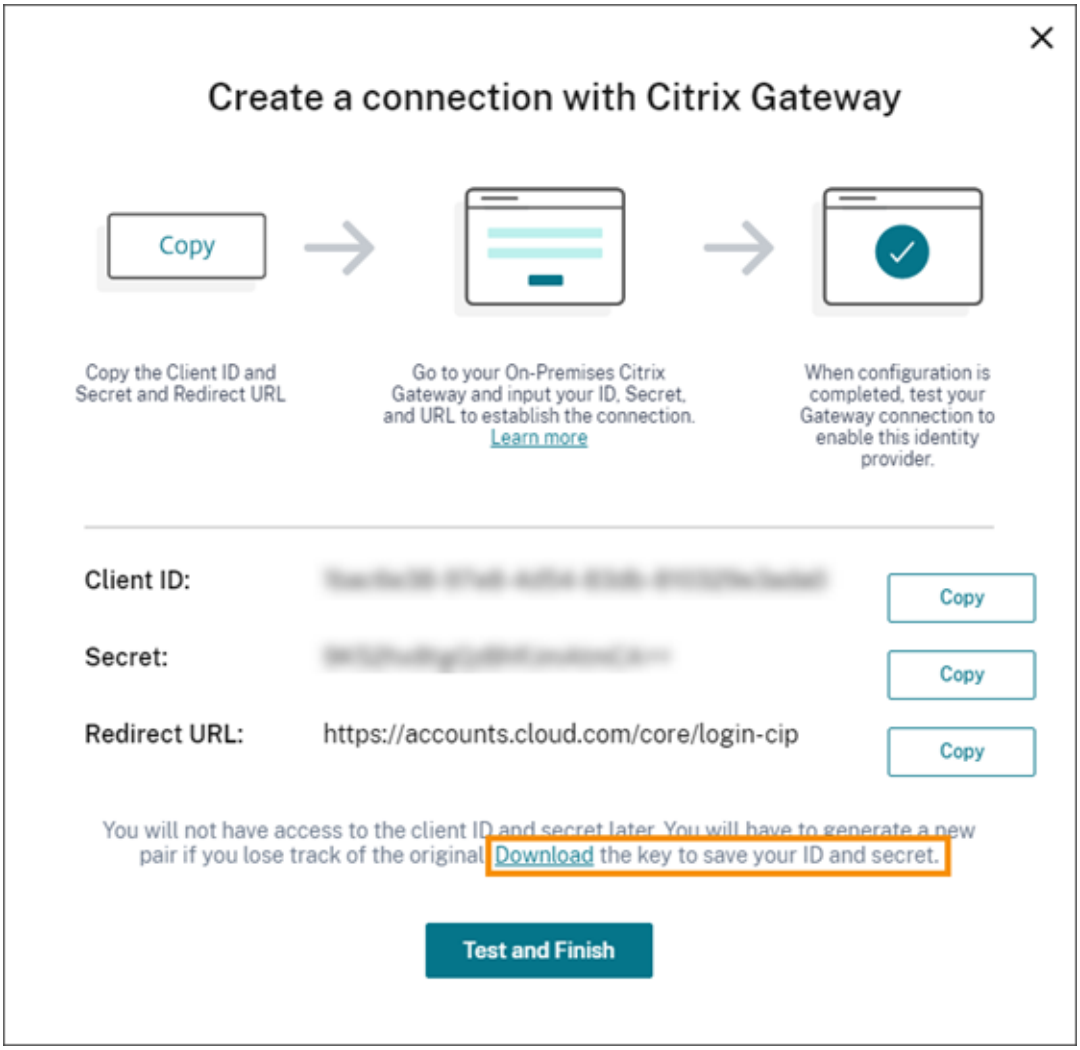


After Citrix Cloud detects it successfully, click **Continue**.

4. Create a connection with your on-premises Gateway:

   a) Copy the Client ID, Secret, and Redirect URL that Citrix Cloud displays.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Also, download a copy of this information and save it securely offline for your reference. This information is not available in Citrix Cloud after it's generated.

b) On the Gateway, create an OAuth IdP advanced policy using the client ID, Secret, and Redirect URL from Citrix Cloud. For instructions, see the following articles:

- For Citrix Gateway 12.1: Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud
- For Citrix Gateway 13.0: Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud

c) Click **Test and Finish**. Citrix Cloud verifies that your Gateway is reachable and configured correctly.

5. Enable Citrix Gateway authentication for stores:

a) From the Citrix Cloud menu, select **StoreFront Cloud**.
b) From the **Authentication** tab, select **Citrix Gateway**.
c) Select **I understand the impact on end user experience** and then click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

As a first step, review the Prerequisites and Requirements sections in this article. Verify you have all the required components in your on-premises environment and that you have made all required configurations. If any of these items are missing or misconfigured, store authentication with Citrix Gateway does not work.

If you experience an issue establishing a connection between Citrix Cloud and your on-premises Gateway, verify the following items:

- The Gateway FQDN is reachable from the Internet.
- You have entered the Gateway FQDN correctly in Citrix Cloud.
- You have entered the Gateway URL correctly in the `-issuer` parameter of the OAuth IdP policy. Example: `-issuer https://GatewayFQDN.com`. The `issuer` parameter is case sensitive.
- The client ID, secret, and redirect URL values from Citrix Cloud are entered correctly in the Client ID, Client Secret, Redirect URL, and Audience fields of the OAuth IdP policy. Verify that the correct client ID has been entered in the Audience field of the policy.
- The OAuth IdP authentication policy is configured correctly. For instructions, see the following articles:
  - Citrix Gateway 12.1: Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud
  - Citrix Gateway 13.0: Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud
- Verify the policy is bound correctly to the AAA authentication server as described in Binding Authentication Policies.

Global catalog servers

In addition to retrieving user account details, Gateway retrieves users'domain name, AD NETBIOS name, and the root AD domain name. To retrieve the AD NETBIOS name, Gateway searches the AD where the user accounts reside. NETBIOS names are not replicated on global catalog servers.

If you use global catalog servers in your AD environment, LDAP actions configured on these servers do not work with Citrix Cloud. Instead, you must configure the individual ADs in the LDAP action. If you have multiple domains or forests, you can configure multiple LDAP policies.

AD search for single sign-on with Kerberos or IdP chaining

If you use Kerberos or an external identity provider that uses SAML or OIDC protocols for end user sign-in, verify that AD lookup is configured. Gateway requires AD lookups to retrieve end users'AD

© 1997–2026 Citrix Systems, Inc. All rights reserved.

user properties and AD configuration properties.

Ensure that you have LDAP policies configured, even if authentication is handled by third party servers. To configure these policies, you add a second authentication factor to your existing login schema profile by performing the following tasks:

1. Create an LDAP authentication server that performs only attribute and group extraction from Active Directory.
2. Create an LDAP advanced authentication policy.
3. Create an Authentication Policy Label.
4. Define the Authentication Policy Label as the next factor, after the primary identity provider.

To add LDAP as a second authentication factor

1. Create the LDAP authentication server:
    a) Select **System > Authentication > Basic Policies > LDAP > Servers > Add**.
    b) On the **Create Authentication LDAP Server** page, enter the following information:
        - In **Choose Server Type**, select **LDAP**.
        - In **Name**, enter a friendly name for the server.
        - Select **Server IP** and then enter LDAP server's IP address.
        - In **Security Type**, select your required LDAP security type.
        - In **Server Type**, select **AD**.
        - In **Authentication**, do not select the check box. This check box must be cleared because this authentication server is only for extracting user attributes and groups from Active Directory, not authentication.
    c) Under **Other Settings**, enter the following information:
        - In **Server Logon Name Attribute**, enter **UserPrincipalName**.
        - In **Group Attribute**, select **memberOf**.
        - In **Sub Attribute Name**, select **cn**.
2. Create the LDAP advanced authentication policy:
    a) Select **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Policy > Add**.
    b) On the **Create Authentication Policy** page, enter the following information:
        - In **Name**, enter a friendly name for the policy.
        - In **Action Type**, select **LDAP**.
        - In **Action**, select the LDAP authentication server you created earlier.
        - In **Expression**, enter **TRUE**.
    c) Click **Create** to save the configuration.
3. Create the Authentication Policy Label:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

a) Select **Security > AAA –Application Traffic > Policies > Authentication > Advanced Policies > Policy Label > Add**.
b) In **Name**, enter a friendly name for the authentication policy label.
c) In Login Schema, select **LSCHEMA_INT**.
d) Under **Policy Binding**, in **Select Policy**, select the LDAP advanced authentication policy you created earlier.
e) In **GoTo Expression**, select **END**.
f) Click **Bind** to finish the configuration.

4. Define the LDAP Authentication Policy Label as the next factor, after the primary identity provider:

a) Select **System > Security > AAA - Application Traffic > Virtual Servers**.
b) Select the virtual server that contains the binding for your primary identity provider and select **Edit**.
c) Under **Advanced Authentication Policies**, select the existing **Authentication Policy** bindings.
d) Select the binding for your primary identity provider and then select **Edit Binding**.
e) On the **Policy Binding** page, in **Select Next Factor**, select the LDAP Authentication Policy Label you created earlier.
f) Click **Bind** to save the configuration.

Default password for multifactor authentication

If you use multifactor authentication (MFA) for end users, Gateway uses the last factor's password as the default password for single sign-on. This password is sent to Citrix Cloud when end users sign in to their store. If LDAP authentication is followed by another factor in your environment, you must configure the LDAP password as the default password that is sent to Citrix Cloud. Enable **SSOCredentials** on the login schema corresponding to the LDAP factor.

More information

Citrix Tech Zone: Tech Insight: Authentication - Gateway

Connect Google Cloud Identity as an identity provider to Citrix Cloud™

July 21, 2026

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Cloud supports using Google Cloud Identity as an identity provider to authenticate end users signing in to their stores. By connecting your organization's Google account to Citrix Cloud, you can provide a unified sign-in experience for accessing Citrix® StoreFront Cloud and Google resources.

Requirements for domain-joined and non-domain-joined configuration

You can configure Google Cloud Identity as an identity provider in Citrix Cloud using a machine that's domain-joined or non-domain-joined.

- Domain-joined means machines are joined to a domain in your on-premises Active Directory (AD) and authentication uses the user profiles that are stored there.
- Non-domain-joined means machines aren't joined to an AD domain and authentication uses the user profiles that are stored in your Google Workspace directory (also known as Google-native users).

The following table lists the requirements for each configuration type.

Requirement	Domain-joined	Non-domain-joined	More information
On-premises AD	Yes	No	See Prepare Active Directory and Citrix Cloud Connectors in this article.
Citrix Cloud Connectors deployed in your resource location	Yes	No; Cloud Connectors aren't needed to access non-domain-joined machines.	Prepare Active Directory and Citrix Cloud Connectors in this article.
AD synchronization with Google Cloud	Optional only if using Gateway service and no other services. Otherwise, this task is required.	No	See Sync Active Directory with Google Cloud Identity in this article.
Developer account with access to the Google Cloud Platform console. Used for creating a service account and key, and enabling the Admin SDK API.	Yes	Yes	See Create a service account, Create a service account key, and Configure domain-wide delegation in this article.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requirement	Domain-joined	Non-domain-joined	More information
An administrator account with access to the Google Workspace Admin console. Used for configuring domain-wide delegation and a read-only API user account.	Yes	Yes	See Configure domain-wide-delegation and Add a read-only API user account in this article.

Authentication with multiple Citrix Cloud accounts

This article describes how to connect Google Cloud Identity as an identity provider to a single Citrix Cloud account. If you have multiple Citrix Cloud accounts, you can connect each one to the same Google Cloud account using the same service account and read-only API user account. Simply sign in to Citrix Cloud and select the appropriate customer ID from the customer picker.

Prepare Active Directory and Citrix Cloud Connectors

If you are using a **domain-joined** machine with Google Cloud Identity, use this section to prepare your on-premises AD. If you are using a non-domain-joined machine, skip this task and continue to Create a service account in this article.

You need at least two (2) servers in your Active Directory domain on which to install the Citrix Cloud Connector software. Cloud Connectors are required for enabling communication between Citrix Cloud and your resource location. At least two Cloud Connectors are required to ensure a highly available connection with Citrix Cloud. These servers must meet the following requirements:

- Meets the requirements described in Cloud Connector system requirements.
- Does not have any other Citrix® components installed, is not an Active Directory domain controller, and is not a machine critical to your resource location infrastructure.
- Joined to your Active Directory (AD) domain. If your store resources and users reside in multiple domains, you must install at least two Cloud Connectors in each domain. For more information, see Deployment scenarios for Cloud Connectors in Active Directory.
- Connected to a network that can contact the resources that users access through cloud stores.
- Connected to the Internet. For more information, see System and Connectivity Requirements.

For more information about installing Cloud Connectors, see Cloud Connector Installation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sync Active Directory with Google Cloud Identity

If you are using a **domain-joined** machine with Google Cloud Identity, use this section to prepare your on-premises AD. If you are using a non-domain-joined machine, skip this task and continue to Create a service account in this article.

Synchronizing your AD with Google Cloud Identity is optional if you are using only Citrix Gateway service, with no other services enabled. For these services alone, you can use Google-native users without needing to synchronize with your AD.

If you are using other Citrix Cloud services, synchronizing your AD with Google Cloud Identity is required. Google Cloud must pass the following AD user attributes to Citrix Cloud:

- SecurityIDentifier (SID)
- objectGUID
- userPrincipalName (UPN)

To sync your AD with Google Cloud

1. Download and install the Google Cloud Directory Sync utility from the Google web site. For more information about this utility, see the Google Cloud Directory Sync documentation on the Google web site.
2. After installing the utility, launch the Configuration Manager (**Start > Configuration Manager**).
3. Specify the Google domain settings, and LDAP settings as described in Set up your sync with Configuration Manager of the utility documentation.
4. In **General Settings**, select **Custom Schemas**. Leave the default selections unchanged.
5. Configure a custom schema to apply to all user accounts. Enter the required information using the exact casing and spelling specified in this section.
    a) Select the **Custom Schemas** tab and then select **Add Schema**.
    b) Select **Use rules defined in "User Accounts"**.
    c) In **Schema Name**, enter **citrix-schema**.
    d) Select **Add Field** and then enter the following information:
        - Under **Schema field template**, in **Schema Field**, select **userPrincipalName**.
        - Under **Google field details**, in **Field Name**, enter **UPN**.
    e) Repeat Step 4 to create the following fields:
        - objectGUID: Under **Schema field template**, select **objectGUID**. Under **Google field details**, enter **objectGUID**.
        - SID: Under **Schema field template**, select **Custom**. Under **Google field details**, enter **SID**.
        - objectSID: Under **Schema field template**, select **Custom**. Under **Google field details**, enter **objectSID**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

f) Select **OK** to save your entries.

6. Finish configuring any remaining settings for your organization and verify synchronization settings as described in Set up your sync with Configuration Manager of the utility documentation.
7. Select **Sync & apply changes** to synchronize your Active Directory with your Google account.

After the sync finishes, the User Information section in Google Cloud displays users' Active Directory information.

Create a service account

To complete this task, you need a Google Cloud Platform developer account.

1. Sign in to https://console.cloud.google.com.
2. From the Dashboard sidebar, select **IAM & Admin** and then select **Service Accounts**.
3. Select **Create service account**.
4. Under **Service account details**, enter the service account name and service account ID.
5. Select **Done**.

Create a service account key

1. On the **Service Accounts** page, select the service account you just created.
2. Select the **Keys** tab and then select **Add key > Create new key**.
3. Leave the default JSON key type option selected.
4. Select **Create**. Save the key to a secure location that you can access later. You enter the private key in the Citrix Cloud console when you connect Google Cloud Identity as an identity provider.

Configure domain-wide delegation

1. Enable the Admin SDK API:

   a) From the Google Cloud Platform menu, select **APIs & Services > Enabled APIs & services**.
   b) Select **Enable APIs and services** near the top of the console. The API Library home page appears.
   c) Search for **Admin SDK API** and select it from the results list.
   d) Select **Enable**.

2. Create an API client for the service account:

   a) From the Google Cloud Platform menu, select **IAM & Admin > Service Accounts** and then select the service account you created earlier.
   b) From the service account's **Details** tab, expand **Advanced settings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

c) Under **Domain-wide Delegation**, copy the Client ID and then select **View Google Workspace Admin Console**.

d) If applicable, select the Google Workspace administrator account you want to use. The Google Admin console appears.

e) From the Google Admin sidebar, select **Security > Access and data control > API controls**.

f) Under **Domain wide delegation**, click **Manage Domain Wide Delegation**.

g) Select **Add new**.

h) In **Client ID** paste the client ID for the service account that you copied in Step C.

i) In **OAuth scopes**, enter the following scopes in a single comma-delimited line:

```
https://www.googleapis.com/auth/admin.directory.user.readonly,
    https://www.googleapis.com/auth/admin.directory.group.
    readonly,https://www.googleapis.com/auth/admin.directory.
    domain.readonly
```

j) Select **Authorize**.

Add a read-only API user account

In this task, you create a Google Workspace user account that has read-only API access for Citrix Cloud. This account is not used for any other purpose and has no other privileges.

1. From the Google Admin menu, select **Directory > Users**.
2. Select **Add new user** and enter the appropriate user information.
3. Select **Add new user** to save the account information.
4. Create a custom role for the read-only user account:

   a) From the Google Admin menu, select **Account > Admin roles**.
   b) Select **Create new role**.
   c) Enter a name for the new role. Example: API-ReadOnly
   d) Select **Continue**.
   e) Under **Admin API privileges**, select the following privileges:
      - Users > Read
      - Groups > Read
      - Domain Management
   f) Select **Continue** and then select **Create role**.

5. Assign the custom role to the read-only user account you created earlier:

   a) From the custom role details page, in the **Admins** pane, select **Assign users**.
   b) Start typing the name of the read-only user account and select it from the user list.
   c) Select **Assign role**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d) To verify the role assignment, return to the Users page (**Directory > Users**) and select the read-only user account. The custom role assignment is displayed under **Admin roles and privileges**.

Connect Google Cloud Identity to Citrix Cloud

1. Sign in to Citrix Cloud at https://citrix.cloud.com.
2. From the Citrix Cloud menu, select **Identity and Access Management**.
3. Locate **Google Cloud Identity** and then select **Connect** from the ellipsis menu.
4. When prompted, enter a short, URL-friendly identifier for your company and select **Save and Continue**. The identifier you choose must be globally unique within Citrix Cloud.
5. Select **Import File** and then select the JSON file you saved when you created the key for the service account. This action imports your private key and the email address for the Google Cloud service account that you created.
6. In **Impersonated User**, enter the name of the read-only API user account.
7. Select **Next**. Citrix Cloud verifies your Google account details and tests the connection.
8. Review the associated domains that are listed. If they're correct, select **Confirm** to save your configuration.

Add administrators to Citrix Cloud

You can add individual Citrix Cloud administrators and administrator groups through Google Cloud. For more information, see the following articles:

- For individual administrators: Manage administrator access to Citrix Cloud
- For administrator groups: Manage administrator groups

After you add administrators to Citrix Cloud, they can sign in using one of the following methods:

- Navigate to the administrator sign-in URL that you configured when you initially configured Google Cloud as an identity provider. Example: `https://citrix.cloud.com/go/mycompany`
- From the Citrix Cloud sign-in page, select **Sign in with my company credentials**, enter the unique identifier for your company (for example, "mycompany"), and click **Continue**.

Enable Google Cloud Identity for store authentication

1. From the Citrix Cloud menu, select **StoreFront Cloud > Authentication**.
2. Select **Google Cloud Identity**. When prompted, select **I understand the impact on the end user experience** and then click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connect Okta as an identity provider to Citrix Cloud™

July 21, 2026

Author:
Mark Dear

Citrix Cloud supports using Okta as an identity provider to authenticate end users signing in to their stores. By connecting your Okta organization to Citrix Cloud, you can provide a common sign-in experience for your end users to access resources in Citrix® StoreFront Cloud.

After enabling Okta authentication in StoreFront Cloud, end users have a different sign-in experience. Selecting Okta authentication provides federated sign-in, not single sign-on. End users sign in to stores from an Okta sign-in page, but they may have to authenticate a second time when opening an app or desktop from Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). To enable single sign-on and prevent a second logon prompt, you need to use the Citrix Federated Authentication Service with Citrix Cloud. For more information, see Connect Citrix Federated Authentication Service to Citrix Cloud.

Prerequisites

Cloud Connectors or Connector Appliances

Either Cloud Connectors or Connector Appliances are required for enabling communication between Citrix Cloud and your resource location. At least two Cloud Connectors or Connector Appliances are required to ensure a highly available connection with Citrix Cloud. You need at least two Connectors joined to your Active Directory domain. These can be either Cloud Connectors or Connector Appliances.

The connectors must meet the following requirements:

- Meet the requirements described in their respective documentation
- Joined to your Active Directory (AD) domain. If your store users reside in multiple domains, the Connector Appliance multi-domain feature can be used to join multiple domains.
- Connected to a network that can contact the resources that users access through cloud stores.
- Connected to the Internet. For more information, see System and Connectivity Requirements.

For more information about installing Cloud Connectors, see Cloud Connector Installation.
For more information about installing Connector Appliances, see Connector Appliance Installation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Okta domain

When connecting Okta to Citrix Cloud, you must supply the Okta domain for your organization. Citrix supports the following Okta domains:

- okta.com
- okta-eu.com
- oktapreview.com

You can also use Okta custom domains with Citrix Cloud. Review the important considerations for using custom domains in Customize the Okta URL domain on the Okta web site.

For more information about locating the custom domain for your organization, see Finding Your Okta Domain on the Okta web site.

Okta OIDC web application

To use Okta as an identity provider, you must first create an Okta OIDC web application with client credentials you can use with Citrix Cloud. After you create and configure the application, note the Client ID and Client Secret. You supply these values to Citrix Cloud when you connect your Okta organization.

To create and configure this application, see the following sections in this article:

- Create an Okta OIDC web app integration
- Configure the Okta OIDC web application

Store URL

When creating the Okta application, you must supply your store URL from Citrix Cloud. To locate the store URL, select **StoreFront Cloud** from the Citrix Cloud menu. The store URL is shown on the **Access** tab.

> **Important:**
>
> If you modify the store URL later on, you must update the Okta application configuration with the new URL. Otherwise, your end users might experience issues with logging off from their store.

Okta API token

Using Okta as an identity provider with Citrix Cloud requires an API token for your Okta organization. Create this token using a Read-Only Administrator account in your Okta organization. This token must be able to read the users and groups in your Okta organization.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To create the API token, see Create an Okta API token in this article. For more information about API tokens, see Create an API Token on the Okta website.

> **Important:**
>
> When you create the API token, make a note of the token value (for example, copy the value temporarily to a plain text document). Okta displays this value only once, so you might create the token just before you perform the steps in Connect Citrix Cloud to your Okta organization.

Sync Active Directory accounts to Okta using the Okta AD agent

To use Okta as an identity provider, you must first integrate your on-premises AD with Okta. To do this, you install the Okta AD agent in your domain and add your AD to your Okta organization. For guidance for deploying the Okta AD agent, see Get started with Active Directory integration on the Okta web site.

Afterward, you import your AD users and groups to Okta. When importing, include the following values associated with your AD accounts:

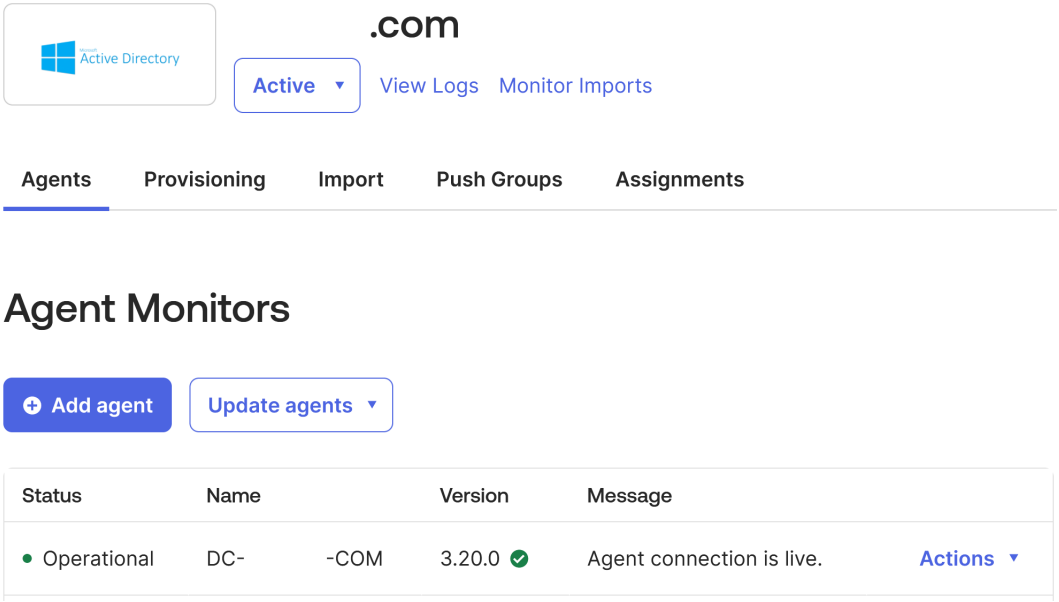
- Email
- SID
- UPN
- OID

> Note:
>
> If you are using Citrix Gateway service with store, you don't need to synchronize your AD accounts with your Okta organization.

To synchronize your AD users and groups with your Okta organization:

1. Install and configure the Okta AD agent. For complete instructions, refer to the following articles on the Okta website:
    - Install the Okta Active Directory agent
    - Configure Active Directory import and account settings
    - Configure Active Directory provisioning settings

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Add your AD users and groups to Okta by performing a manual import or an automated import. For more information about Okta import methods and instructions, refer to Manage Active Directory users and groups on the Okta website.

Create an Okta OIDC web app integration

1. From the Okta management console, under **Applications**, select **Applications**.
2. Select **Create App Integration**.
3. In **Sign in method**, select **OIDC - OpenID Connect**.
4. In **Application type**, select **Web Application**. Select **Next**.
5. In **App Integration Name**, enter a friendly name for the app integration.
6. In **Grant type**, select **Authorization Code** (selected by default).
7. In **Sign-in redirect URIs**, enter `https://accounts.cloud.com/core/login-okta`.
    - If your Citrix Cloud customer is in the European Union, United States, or Asia Pacific-South regions, enter `https://accounts.cloud.com/core/login-okta`.
    - If your Citrix Cloud customer is in the Japan region, enter `https://accounts.citrixcloud.jp/core/login-okta`.
    - If your Citrix Cloud customer is in the Citrix Cloud Government region, enter `https://accounts.cloud.us/core/login-okta`.
8. In **Sign-out redirect URIs**, enter your store URL from Citrix Cloud.
9. If you are also using a store custom domain you will also need to enter this too. For example
    - `https://workspaceurl1.cloud.com`
    - `https://workspaceurl2.cloud.com`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

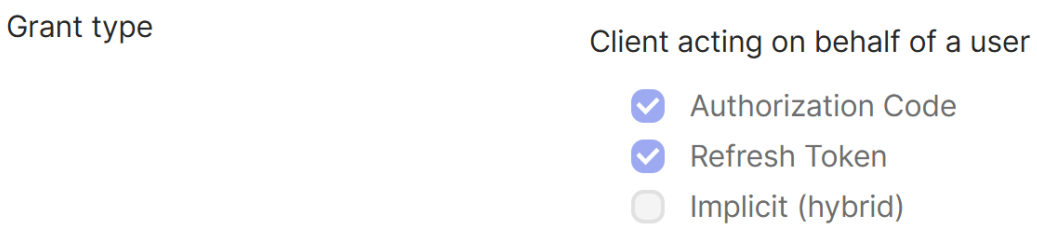
- `https://workspaceurl1.mycustomdomain.com`

10. Under **Assignments**, in **Controlled access**, select whether to assign the app integration to everyone in your organization, only groups that you specify, or to assign access later.
11. Select **Save**. After you save the app integration, the console displays the application configuration page.
12. In the **Client Credentials** section, copy the **Client ID** and **Client Secret** values. You use these values when you connect Citrix Cloud to your Okta organization.

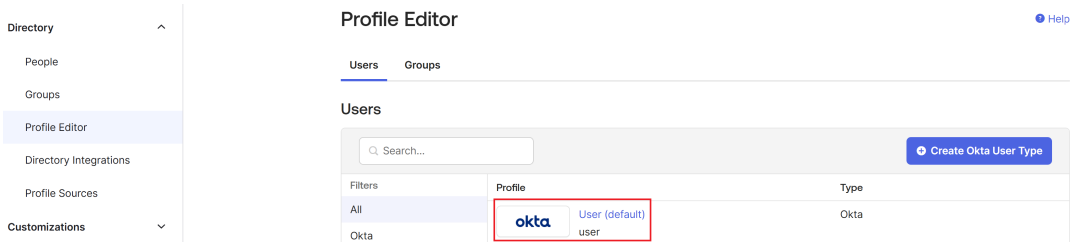
Configure the Okta OIDC web application

In this step, you configure your Okta OIDC web application with the settings required for Citrix Cloud. Citrix Cloud requires these settings to authenticate your end users through Okta when they sign in to their stores.

1. (Optional) Update client permissions for the implicit grant type. You might choose to perform this step if you prefer to allow the least amount of privilege for this grant type.
   a) From the Okta application configuration page, on the **General** tab, scroll to the **General Settings** section and select **Edit**.
   b) In the **Application** section, in **Grant type**, under **Client acting on behalf of a user**, clear the **Allow Access Token with implicit grant type** setting.

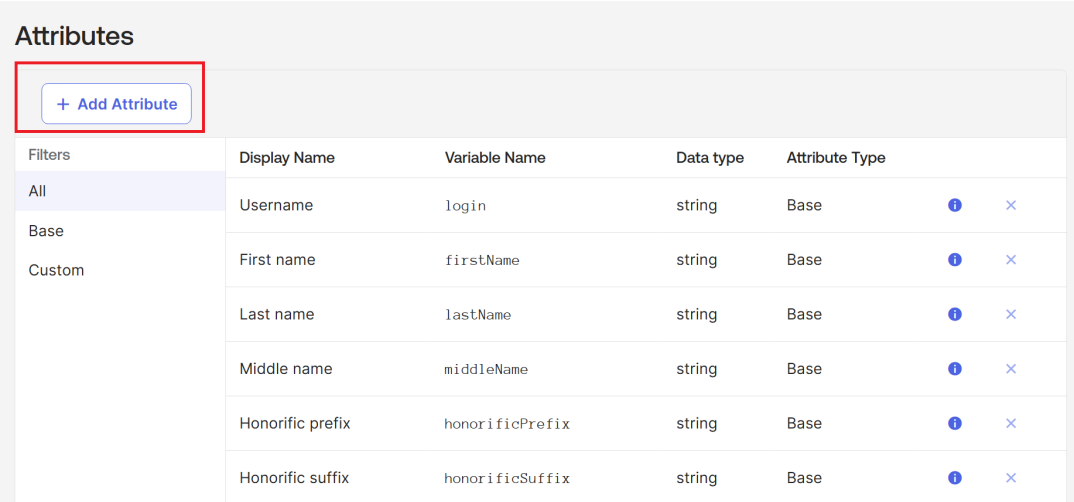


   c) Select **Save**.
2. Add application attributes. These attributes are case-sensitive.
   a) From the Okta console menu, select **Directory > Profile Editor**.
   b) Select the Okta **User (default)** profile. Okta displays the **User** profile page.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

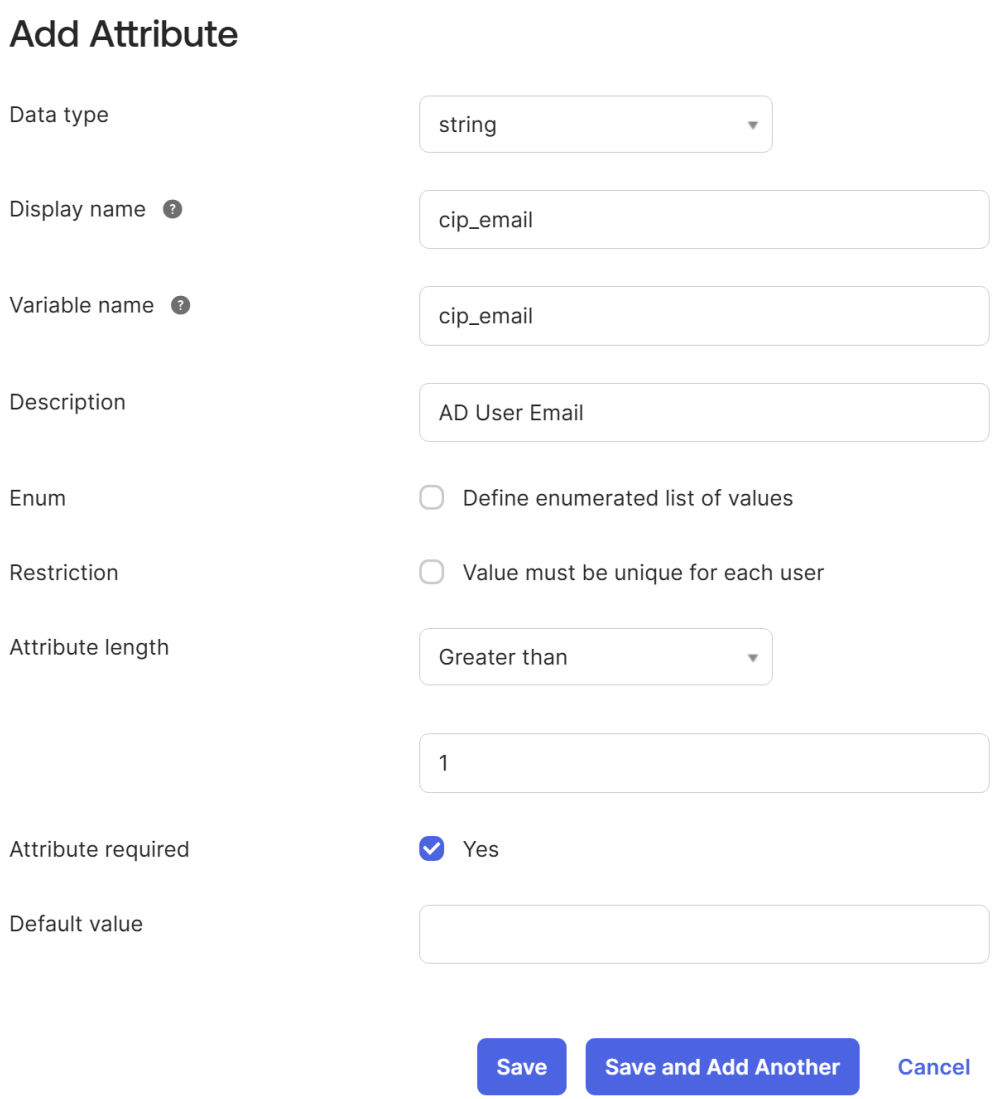
c) Under **Attributes**, select **Add attribute**.



d) Enter the following information:

- Display Name: cip_email
- Variable Name: cip_email
- Description: AD User Email
- Attribute Length: Select **Greater than** and then enter **1**.
- Attribute Required: Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.



e) Select **Save and Add Another**.

f) Enter the following information:

- Display Name: cip_sid
- Variable Name: cip_sid
- Description: AD User Security Identifier
- Attribute Length: Select **Greater than** and then enter **1**.
- Attribute Required: Yes

g) Select **Save and Add Another**.

h) Enter the following information:

- Display Name: cip_upn
- Variable Name: cip_upn
- Description: AD User Principal Name
- Attribute Length: Select **Greater than** and then enter **1**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Attribute Required: Yes

i) Select **Save and Add Another**.

j) Enter the following information:

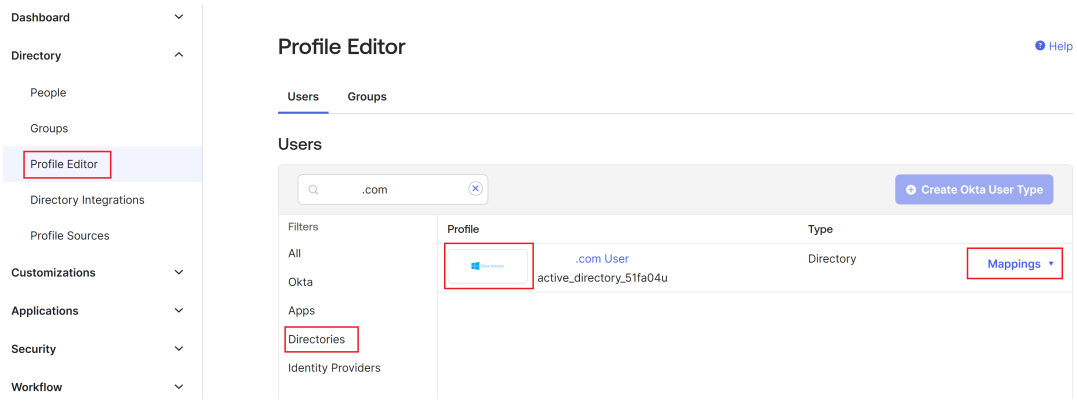
- Display Name: cip_oid
- Variable Name: cip_oid
- Description: AD User GUID
- Attribute Length: Select **Greater than** and then enter **1**.
- Attribute Required: Yes

k) Select **Save**.

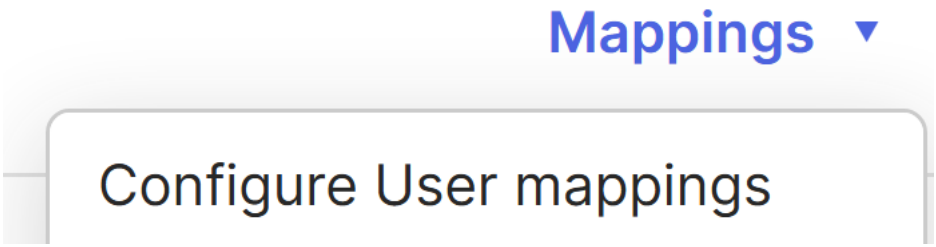
3. Edit attribute mappings for the application:

a) From the Okta console, select **Directory > Profile Editor > Directories**.

b) Locate the **active_directory** profile for your AD. This profile might be labelled using the format `myDomain User`, where `myDomain` is the name of your integrated AD domain.

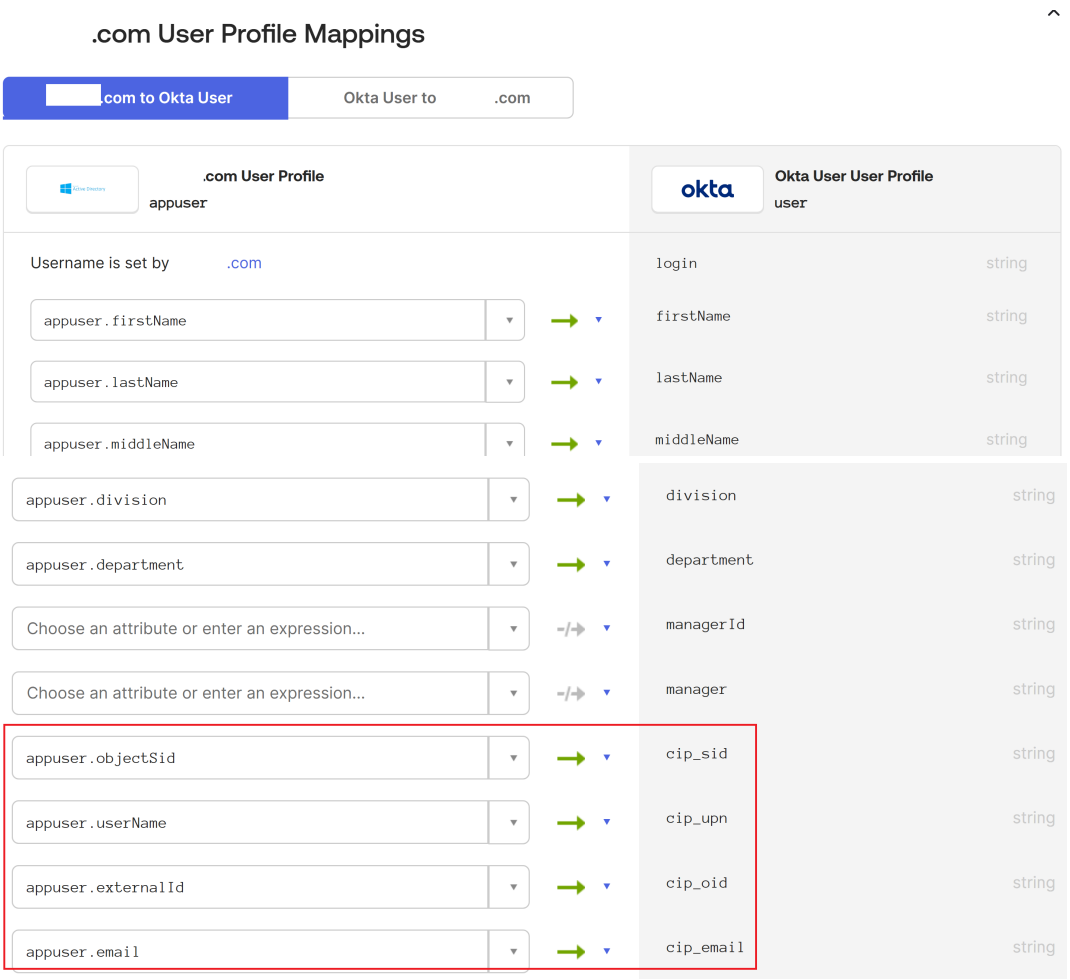


c) Select **Mappings**. The User Profile Mappings page for your AD domain appears and the tab for mapping your AD to Okta User is selected.



d) In the **Okta User User Profile** column, locate the attributes you created in Step 2 and map as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- For `cip_email`, select `email` from the User Profile column for your domain. When selected, the mapping appears as `appuser.email`.
- For `cip_sid`, select `objectSid` from the User Profile column for your domain. When selected, the mapping appears as `appuser.objectSid`.
- For `cip_upn`, select `userName` from the User Profile column for your domain. When selected, the mapping appears as `appuser.userName`.
- For `cip_oid`, select `externalId` from the User Profile column for your domain. When selected, the mapping appears as `appuser.externalId`.

e) Select **Save Mappings**.

f) Select **Apply updates now**. Okta starts a job to apply the mappings.

g) Sync Okta with your AD.

i. From the Okta console, select **Directory > Directory Integrations**.
ii. Select your integrated AD.
iii. Select the **Provisioning** tab.
iv. Under **Settings**, select **To Okta**.
v. Scroll to the **Okta Attribute Mappings** section and then select **Force Sync**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create an Okta API token

1. Sign in to the Okta console using a Read-Only Administrator account.
2. From the Okta console menu, select **Security > API**.
3. Select the **Tokens** tab and then select **Create Token**.
4. Enter a name for the token.
5. Select **Create Token**.
6. Copy the token value. You supply this value when you connect your Okta organization to Citrix Cloud.

Connect Citrix Cloud to your Okta organization

1. Sign in to Citrix Cloud at https://citrix.cloud.com.
2. From the Citrix Cloud menu, select **Identity and Access Management**.
3. Locate **Okta** and select **Connect** from the ellipsis menu.
4. In **Okta URL**, enter your Okta domain.
5. In **Okta API Token**, enter the API token for your Okta organization.
6. In **Client ID** and **Client Secret**, enter the client ID and secret from the OIDC web app integration you created earlier. To copy these values from the Okta console, select **Applications** and locate your Okta application. Under **Client Credentials**, use the **Copy to Clipboard** button for each value.
7. Click **Test and Finish**. Citrix Cloud verifies your Okta details and tests the connection.

After the connection is verified successfully, you can enable Okta authentication for end users.

Enable Okta authentication for stores

1. From the Citrix Cloud menu, select **StoreFront Cloud > Authentication**.
2. Select **Okta**.
3. When prompted, select **I understand the impact on the end user experience**.
4. Select **Save**.

After switching to Okta authentication, Citrix Cloud temporarily disables stores for a few minutes. When stores are re-enabled, your end users can sign in using Okta.

More information

- Citrix Tech Zone:
  - Tech Insight: Authentication - Okta

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Tech Brief: Workspace Identity
- Tech Brief: Workspace SSO

Troubleshooting

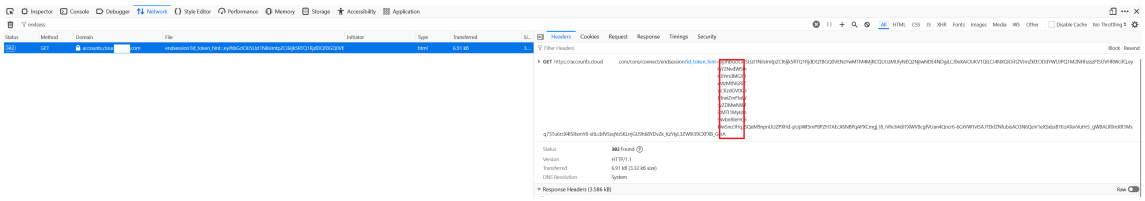
Problem 1 Okta OIDC authentication to store succeeds but DaaS resources cannot be seen for the end user inside store. This can be caused by missing claims like "ctx_user.sid"not being sent to DaaS.

Debugging Steps 1

1. Capture a HAR file using your browser and perform a log into store using Okta OIDC authentication and then logout of store.
2. Locate the following call within your browser developer tools when the user performs an explicit logout action from store

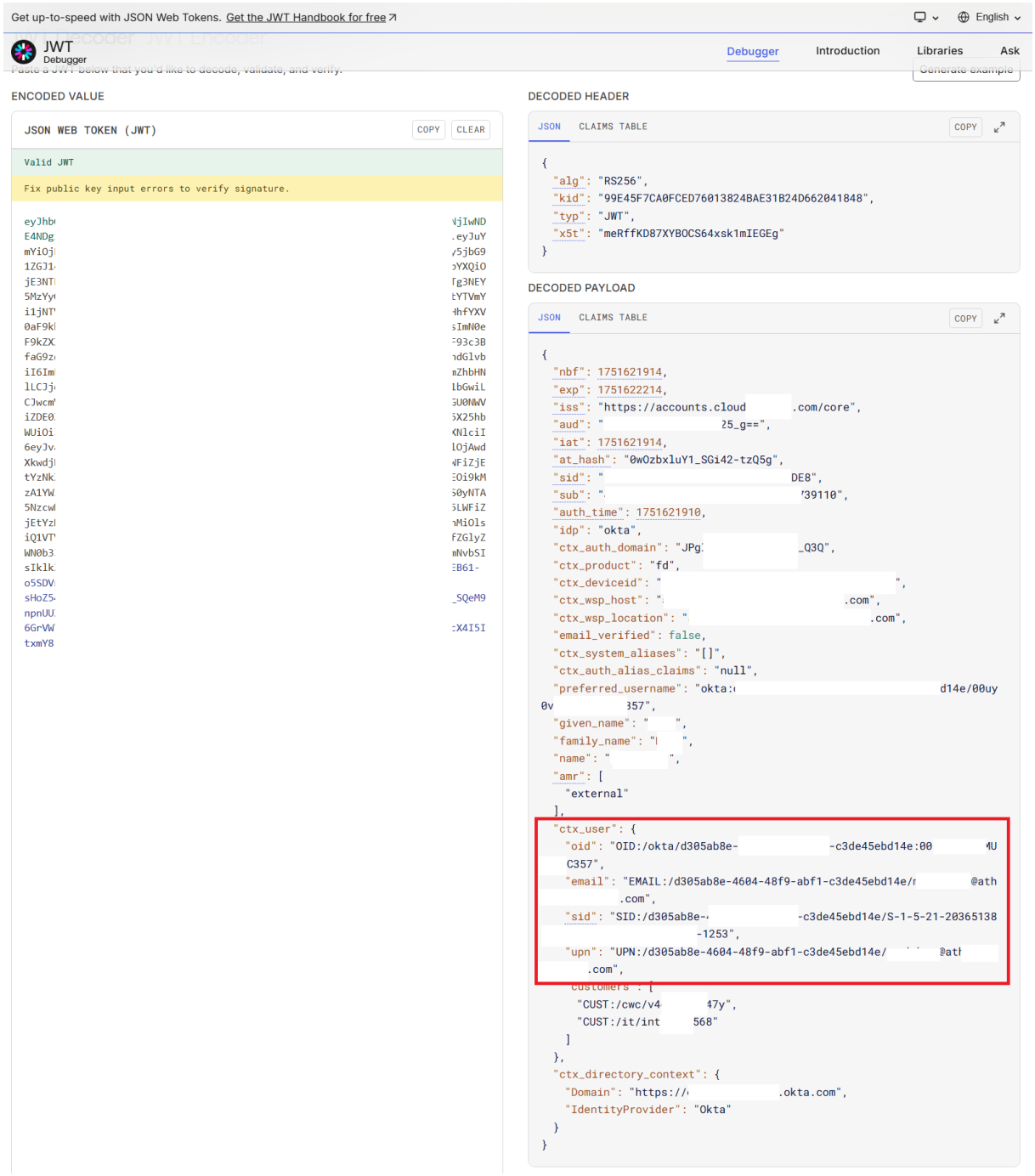
   GET `https://accounts.cloud.com/core/connect/endsession?id_token_hint=<base64string>`

3. Copy the base64 string after ?`id_token_hint`=, which contains a JWT. Example taken from FireFox dev tools.



Paste this base64 string into the Encoded Value JSON WEB TOKEN (JWT) field within `https://jwt.io` to examine the claims Citrix Cloud received from your Okta OIDC application.
Verify that all required claims are present inside `"ctx_user": { }` and that each claim contains the correct user data for the user who logged into store. Ensure that there are four claims inside `"ctx_user": { }` called `"oid"`, `"email"`, `"sid"`, and `"upn"`. Example of decoded JWT.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



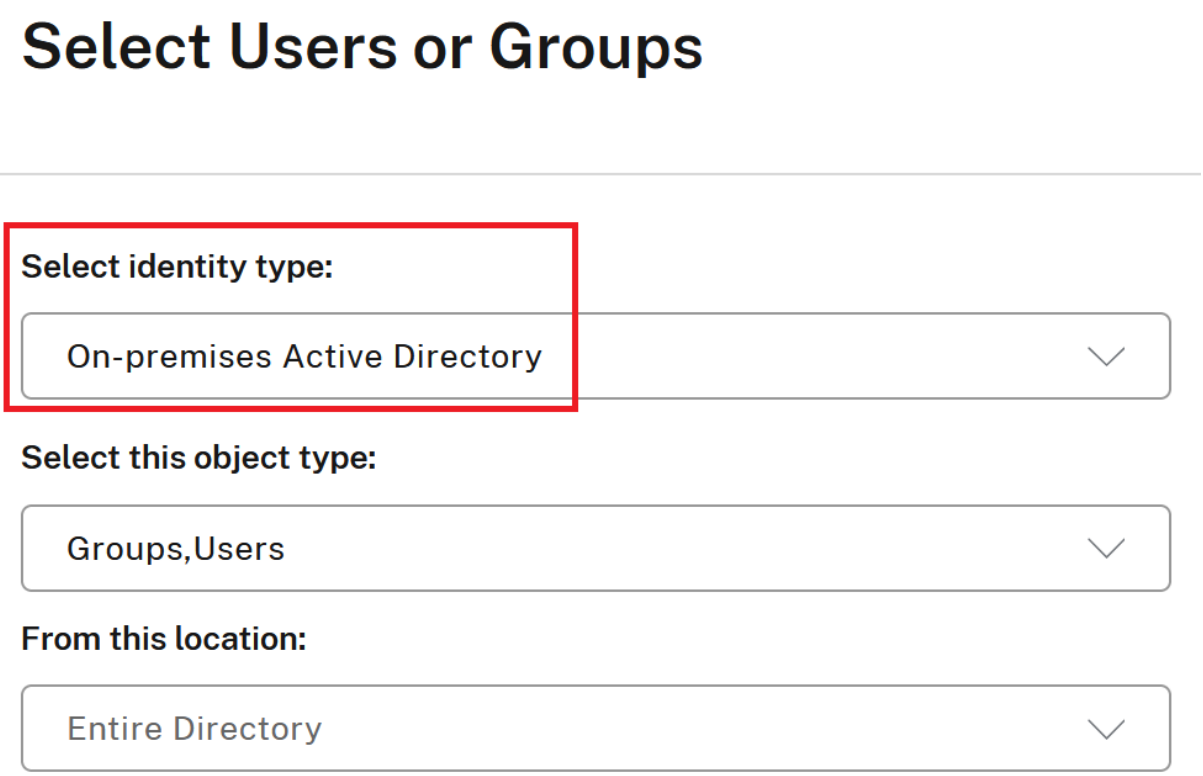
Cause 1 Your Okta OIDC application is not sending all four of the required cip_* claims or your Okta user profile does not include the required attributes.

Solution 1 Review your Okta OIDC application configuration and Okta user profile attribute mapping. Make sure your Okta OIDC app is sending the correct claims. Use the claim names `cip_upn`, `cip_email`, `cip_sid`, and `cip_oid`. All claim names must be lowercase.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

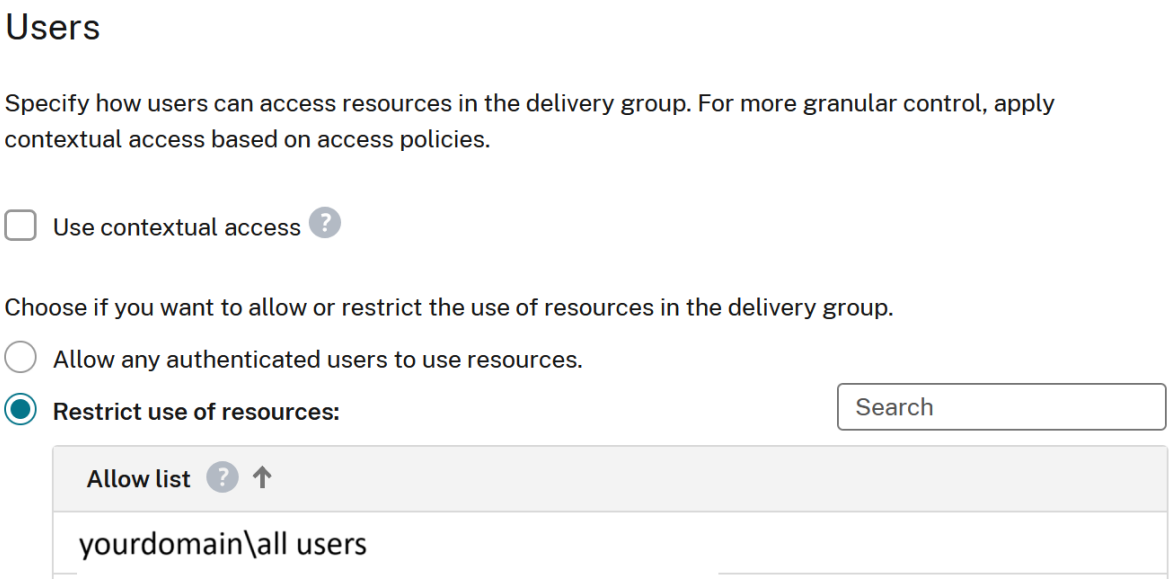
Cause 2 You have configured your DaaS delivery group incorrectly and mapped your resources to **Okta** identities instead of **Active Directory** identities.

Solution 2 Map AD domain joined delivery groups and VDAs to **Active Directory** identities, not **Okta** identities. Use **Okta** identities only for launching **non domain joined** resources.



Configure your delivery groups to **Restrict use of resources** based on AD users and groups.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Cause 3 You have not used **AD Universal Groups** as per Citrix Cloud's requirements or your Citrix Cloud Connectors are not joined at the correct AD domain level. See this article for details Citrix Cloud Connector system requirements

Solution 3 Use Universal Groups when assigning your users to DaaS resources

Or,

Assign the store user directly to the delivery group.

Connect SAML as an identity provider to Citrix Cloud™

July 17, 2026

Author:
Mark Dear

Citrix Cloud supports using SAML (Security Assertion Markup Language) as an identity provider to authenticate Citrix Cloud administrators and end users signing in to their stores. You can use the SAML 2.0 provider of your choice with your on-premises Active Directory (AD).

About this article

This article describes the required steps for configuring a connection between Citrix Cloud and your SAML provider. Some of these steps describe actions that you perform in your SAML provider's ad-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ministration console. The specific commands you use to perform these actions might vary from the commands described in the article, depending on your chosen SAML provider. These SAML provider commands are provided as examples only. Refer to your SAML provider's documentation for more information about the corresponding commands for your SAML provider.

Citrix SAML Logon Use Cases

- Login to stores for end users.
- Login to stores using a store custom domain for end users.
- Login to Citrix Cloud for admin users.

Choosing the right SAML flow for your use case

- **AD backed identities** imported into your SAML provider. These identities contain on-premise user attributes such as objectSIDs and objectGUIDs. These do not require AD shadow accounts as AD accounts corresponding to these imported users already exist in Active Directory.
- **Native Identities**, which exist only within the SAML provider directory such as Entra ID or Okta Users. These have no corresponding identity inside AD and require AD shadow accounts if AD domain joined VDAs and DaaS catalogs are to be used. These users do not have embedded objectSIDs.
- **Entra ID Guest/B2B users**, which are invited into Entra ID from other Entra ID tenants or using guest email addresses. These have no corresponding identity inside AD and require AD shadow accounts if AD domain joined VDAs and DaaS catalogs are to be used. These users may not have embedded objectSIDs. Some users may have incorrect objectSIDs in the wrong Active Directory.

Supported SAML providers

SAML providers that support the official SAML 2.0 specification are supported for use with Citrix Cloud.

Citrix has tested the following SAML providers for authenticating Citrix Cloud administrators and for authenticating Citrix® StoreFront Cloud end users using Single Sign-on (SSO) and Single Logout (SLO). SAML providers that don't appear in this list are also supported.

- Microsoft ADFS
- Microsoft Entra ID
- Duo
- Okta
- PingFederate

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When testing these providers, Citrix used the following settings to configure the SAML connection in the Citrix Cloud console:

In this field in Citrix Cloud	Enter this value
Entity ID	`https://entityid.com`
Sign Authentication Request	Yes
SSO Service URL	`https://yoursamlprovider/sso/saml2`
SSO Binding Mechanism	HTTP Post
SAML Response	Sign Either Response Or Assertion
Authentication Context	Unspecified, Exact
Logout URL	`https://yoursamlprovider/slo/saml2`
Sign Logout Request	Yes
SLO Binding Mechanism	HTTP Post

For more information about these settings, see Add SAML provider metadata to Citrix Cloud in this article.

Support for scoped Entity IDs

This article describes how to configure SAML authentication using a single SAML application and Citrix Cloud's default generic Entity ID.

If your SAML authentication requirements include the need for multiple SAML applications within a single SAML provider, refer to Configure a SAML application with a scoped Entity ID in Citrix Cloud.

Administrator authentication with SAML 2.0

Citrix Cloud supports using SAML 2.0 to authenticate individual administrators and members of administrator groups in AD. For more information about adding administrator groups to Citrix Cloud, see Manage administrator groups.

Using an existing SAML connection for administrator authentication

If you already have a SAML 2.0 connection in Citrix Cloud and want to use it to authenticate administrators, you must first disconnect SAML 2.0 in **Identity and Access Management** and then reconfigure

© 1997–2026 Citrix Systems, Inc. All rights reserved.

the connection. If you're using your SAML connection to authenticate StoreFront Cloud end users, you must also disable the SAML authentication method in **StoreFront Cloud**. After reconfiguring the SAML connection, you can add individual administrators or administrator groups to Citrix Cloud.

If you attempt to add individual administrators or administrator groups without first disconnecting and reconnecting SAML 2.0, the **Active Directory** identity option described in Add an administrator group to Citrix Cloud doesn't appear.

Task overview for setting up a new SAML connection

To set up a new SAML 2.0 connection in Citrix Cloud, you perform the following tasks:

1. In **Identity and Access Management**, connect your on-premises AD to Citrix Cloud as described in Connect Active Directory to Citrix Cloud.
2. Integrate your SAML provider with your on-premises AD as described in SAML integration with Active Directory in this article.
3. Configure the sign-in URL that administrators can use to sign in to Citrix Cloud.
4. In **Identity and Access Management**, configure SAML authentication in Citrix Cloud. This task involves configuring your SAML provider with the SAML metadata from Citrix Cloud and then configuring Citrix Cloud with the metadata from your SAML provider to create the SAML connection.

Task overview for using an existing SAML connection for Citrix Cloud administrators

If you already have a SAML 2.0 connection in Citrix Cloud and want to use it for administrator authentication, perform the following tasks:

1. If applicable, disable SAML 2.0 store authentication: In **StoreFront Cloud > Authentication**, select a different authentication method and then select **Confirm** when prompted.
2. Disconnect your existing SAML 2.0 connection: In **Identity and Access Management > Authentication**, locate the SAML connection. From the ellipsis menu at the far right, select **Disconnect**. Select **Yes, disconnect** to confirm the action.
3. Reconnect SAML 2.0 and configure the connection: From the ellipsis menu for **SAML 2.0**, select **Connect**.
4. When prompted, enter a unique identifier for the sign-in URL that administrators will use to sign in.
5. Configure the SAML connection as described in Configure the SAML provider metadata in this article.

After configuring your SAML connection, you can add your AD administrator groups to Citrix Cloud as described in Manage administrator groups. You can also reenable SAML for end users as described in this article.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create and map custom SAML attributes

If you already have custom attributes for the SID, UPN, OID, email, and displayName attributes configured in your SAML provider, you don't have to perform this task. Proceed to Create a SAML connector application and use your existing custom SAML attributes in Step 5.

> **Note:**
>
> The steps in this section describe actions that you perform in your SAML provider's administration console. The specific commands you use to perform these actions might vary from the commands described in this section, depending on your chosen SAML provider. The SAML provider commands in this section are provided as examples only. Refer to your SAML provider's documentation for more information about the corresponding commands for your SAML provider.

1. Sign in to the administration console of your SAML provider and select the option for creating custom user attributes. For example, depending on your SAML provider's console, you might select **Users > Custom User Fields > New User Field**.
2. Add attributes for the following AD properties. Name the attributes using the default values shown.

AD Property	Required or optional	Default value
userPrincipalName	Required if not adding an attribute for SID (recommended).	`cip_upn`
objectSID	Required if not adding an attribute for UPN.	`cip_sid`
objectGUID	Optional for authentication	`cip_oid`
mail	Optional for authentication	`cip_email`
displayName	Required by the store UI	`displayName`
givenName	Required by the store UI	`firstName`
sn	Required by the store UI	`lastName`
AD Forest	Optional for authentication	`cip_forest`
AD Domain	Optional for authentication	`cip_domain`

3. Select the AD that you connected with Citrix Cloud. For example, depending on your SAML provider's console, you might select **Users > Directories**.
4. Select the option for adding directory attributes. For example, depending on your SAML provider's console, you might select **Directory Attributes**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Select the option for adding attributes and map the following AD attributes to the custom user attributes you created in Step 2:

    - If you added the attribute for SID in Step 2 (for example, `cip_sid`), select **objectSid** and map to the attribute that you created.
    - If you added the attribute for UPN in Step 2 (for example, `cip_upn`), select **userPrincipalName** and map to the attribute that you created.
    - If you added the attribute for ObjectGUID in Step 2 (for example, `cip_oid`), select **ObjectGUID** and map to the attribute that you created.
    - If you added the attribute for Mail in Step 2 (for example, `cip_email`), select **mail** and map to the attribute that you created.
    - If you added the attribute for Display Name in Step 2 (for example, `displayName`), select **displayName** and map to the attribute that you created.

Configure the administrator sign-in URL

1. Sign in to Citrix Cloud at https://citrix.cloud.com.
2. From the Citrix Cloud menu, select **Identity and Access Management**.
3. Locate **SAML 2.0** and select **Connect** from the ellipsis menu.
4. When prompted, enter a short, URL-friendly identifier for your company and select **Save and continue**. The **Configure SAML** page appears.
5. Proceed to the next section to configure the SAML connection to Citrix Cloud.

Configure the SAML provider metadata

In this task, you create a connector application using SAML metadata from Citrix Cloud. After you configure the SAML application, you use the SAML metadata from your connector application to configure the SAML connection to Citrix Cloud.

> **Note:**
>
> Some steps in this section describe actions that you perform in your SAML provider's administration console. The specific commands you use to perform these actions might vary from the commands described in this section, depending on your chosen SAML provider. The SAML provider commands in this section are provided as examples only. Refer to your SAML provider's documentation for more information about the corresponding commands for your SAML provider.

Create a SAML connector application

1. From your SAML provider's administration console, add an application for an identity provider with attributes and sign response. For example, depending on your provider's console, you

© 1997–2026 Citrix Systems, Inc. All rights reserved.

might select **Applications > Applications > Add App** and then select **SAML Test Connector (IdP w/ attr w/ sign response)**.

2. If applicable, enter a display name and save the app.
3. From the **Configure SAML** screen in Citrix Cloud, in **SAML Metadata**, select **Download**. The metadata XML file appears in another browser tab.

   > **Note:**
   >
   > If needed, you can also download this file from `https://saml.cloud.com/saml/metadata.xml`. This endpoint might be more friendly to some identity providers when importing and monitoring the SAML provider metadata.

4. Enter the following details for the connector application:
   - In the **Audience** field, enter `https://saml.cloud.com`.
   - In the **Recipient** field, enter `https://saml.cloud.com/saml/acs`.
   - In the field for ACS URL validator, enter `https://saml.cloud.com/saml/acs`.
   - In the field for ACS URL, enter `https://saml.cloud.com/saml/acs`.
5. Add your custom SAML attributes as parameter values in the application:

Create this field	Assign this custom attribute
cip_sid	The custom attribute you created for SID. Example: cip_sid
cip_upn	The custom attribute you created for UPN. Example: cip_upn
cip_oid	The custom attribute you created for ObjectGUID. Example: cip_oid
cip_email	The custom attribute you created for Mail. Example: cip_email
displayName	The custom attribute you created for Display Name. Example: displayName

6. Add your end users as users to allow them to access the application.

Add SAML provider metadata to Citrix Cloud

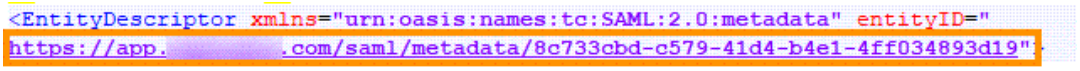
1. Acquire the SAML metadata from your SAML provider. The following image is an example of what this file might look like:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. In the **Configure SAML** screen in Citrix Cloud, enter the following values from your SAML provider's metadata file:

   - In **Identity Provider Entity ID**, enter the **entityID** value from the **EntityDescriptor** element in the metadata.

   - In **Sign Authentication Request**, select **Yes** to allow Citrix Cloud to sign authentication requests, certifying they came from Citrix Cloud and not a malicious actor. Select **No** if you prefer to add the Citrix ACS URL to an allow list that your SAML provider uses for posting SAML responses safely.

   - In **SSO Service URL**, enter the URL for the binding mechanism you want to use. You can use either HTTP-POST or HTTP-Redirect binding. In the metadata file, locate the **SingleSignOnService** elements with Binding values of either **HTTP-POST** or **HTTP-Redirect**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In **Binding Mechanism**, select the mechanism that matches the binding for the SSO Service URL you chose from the metadata file. By default, **HTTP Post** is selected.
- In **SAML Response**, select the signing method your SAML provider uses for the SAML Response and SAML Assertion. By default, **Sign Either Response or Assertion** is selected. Citrix Cloud rejects any responses that aren't signed as specified in this field.

3. In your SAML provider's administration console, perform the following actions:
   - Select **SHA-256** for the SAML signing algorithm.
   - Download the X.509 certificate as a Base64-encoded PEM, CRT, or CER file.
4. On the **Configure SAML** page in Citrix Cloud, in **X.509 Certificate**, select **Upload File** and select the certificate file you downloaded in the previous step.
5. Select **Continue** to complete the upload.
6. In **Authentication Context**, select the context you want to use and how strictly you want Citrix Cloud to enforce this context. Select **Minimum** to request authentication at the selected context without enforcing authentication at that context. Select **Exact** to request authentication at the selected context and enforce authentication only at that context. If your SAML provider doesn't support authentication contexts or you choose not to use them, select **Unspecified** and **Minimum**. By default, **Unspecified** and **Exact** are selected.
7. For **Logout URL** (optional), decide whether or not you want users signing out of their store or Citrix Cloud to also sign out of all web applications that they previously signed in to through the SAML provider.
   - If you want users to stay signed in to their web applications after signing out of their store or Citrix Cloud, leave the **Logout URL** field blank.
   - If you want users to sign out of all web applications after signing out of their store or Citrix Cloud, enter the SingleLogout (SLO) endpoint from your SAML provider. If you're using Microsoft ADFS or Microsoft Entra ID as your SAML provider, the SLO endpoint is the same as the single sign-on (SSO) endpoint.



8. Verify that the following default attribute values in Citrix Cloud match the corresponding attribute values configured in your SAML provider. For Citrix Cloud to find these attributes within the SAML assertion, the values entered here must match those in your SAML provider. If you

© 1997–2026 Citrix Systems, Inc. All rights reserved.

didn't configure a certain attribute in your SAML provider, you can use the default value in Citrix Cloud or leave the field blank, unless noted otherwise.

- **Attribute name for User Display Name**: Default value is `displayName`.
- **Attribute name for User Given Name**: Default value is `firstName`.
- **Attribute name for User Family Name**: Default value is `lastName`.
- **Attribute name for Security Identifier (SID)**: You must enter this attribute name from your SAML provider if you didn't create an attribute for UPN. The default value is `cip_sid`.
- **Attribute name for User Principal Name (UPN)**: You must enter this attribute name from your SAML provider if you didn't create an attribute for SID. The default value is `cip_upn`.
- **Attribute name for Email**: Default value is `cip_email`.
- **Attribute name for AD Object Identifier (OID)**: Default value is `cip_oid`.
- **Attribute name for AD Forest**: Default value is `cip_forest`.
- **Attribute name for AD Domain**: Default value is `cip_domain`.

9. Select **Test and Finish** to verify you configured the connection successfully.

Add administrators to Citrix Cloud from AD

For instructions for adding and managing AD groups in Citrix Cloud, see Manage administrator groups.

Enable SAML authentication for stores

1. From the Citrix Cloud menu, select **StoreFront Cloud**.
2. Select the **Authentication** tab
3. Select **SAML 2.0**.

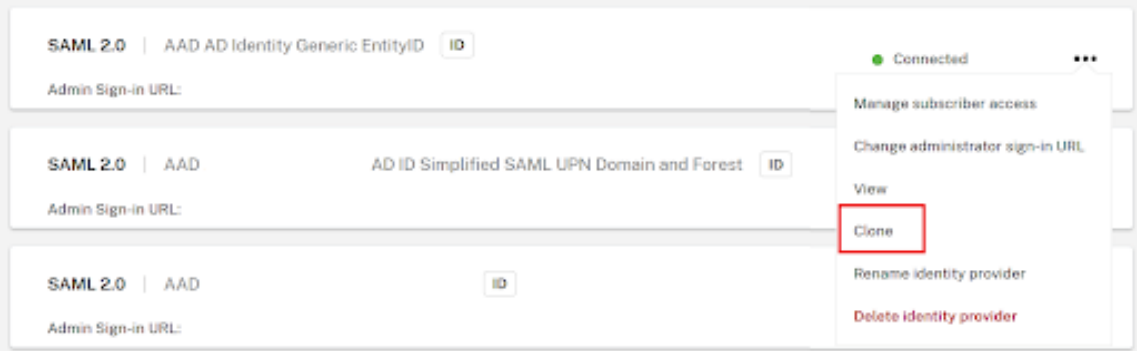
Cloning an Existing SAML Connection within Identity and Access Management

> **Important:**
>
> Cloning SAML connections does not clone the existing Scoped Entity ID. You may need to update your SAML application configuration if you add a Scoped Entity ID or generate a new one during the cloning process.

To clone an existing SAML connection follow the steps below:

1. Select the 3 dots to the right of an existing SAML connection and select **Clone** from the list of actions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Enter a new and unique GO URL for the new SAML connection. This can be changed later if needed.
3. Enter a new unique nickname for the new SAML connection.



4. Update any settings within the connection such as enable scoped entity ID, signing needs to be enabled, add a missing logout URL, or update the SAML provider cert which has recently expired ….
5. Click “Test and finish”to save the new SAML connection.
6. Switch store to use the new SAML connection within **StoreFront Cloud -> Authentication**.
7. Update your SAML application configuration with a new scoped entity ID (not always necessary)



Prerequisites

July 21, 2026

Author:
Mark Dear

© 1997–2026 Citrix Systems, Inc. All rights reserved.

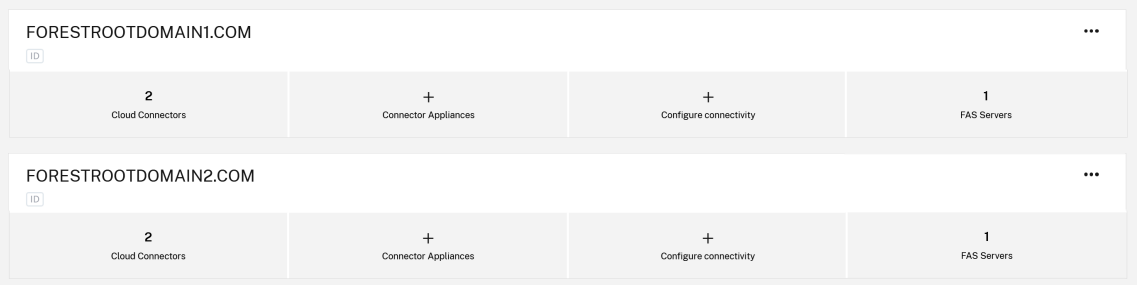
Using SAML authentication with Citrix Cloud has the following requirements:

- SAML provider that supports SAML 2.0.
- On-premises AD domain.
- Two Cloud Connectors deployed to a resource location and joined to your on-premises AD domain. The Cloud Connectors are used to ensure Citrix Cloud can communicate with your resource location.
- AD integration with your SAML provider.

Cloud Connectors

You need at least two (2) servers on which to install the Citrix Cloud Connector™ software. Citrix recommends at least two servers for Cloud Connector high availability. These servers must meet the following requirements:

- Meets the system requirements described in Cloud Connector system requirements.
- Does not have any other Citrix® components installed, is not an AD domain controller, and is not a machine critical to your resource location infrastructure.
- Joined to the AD domain where your AD users and resources reside. If users access resources in multiple domains, you need to install at least two Cloud Connectors in each domain.



- Connected to a network that can contact the resources that end users access through their stores.
- Connected to the Internet. For more information, see System and Connectivity Requirements.

For more information about installing the Cloud Connector, see Cloud Connector Installation.

Active Directory (Default AD Identities SAML Flow)

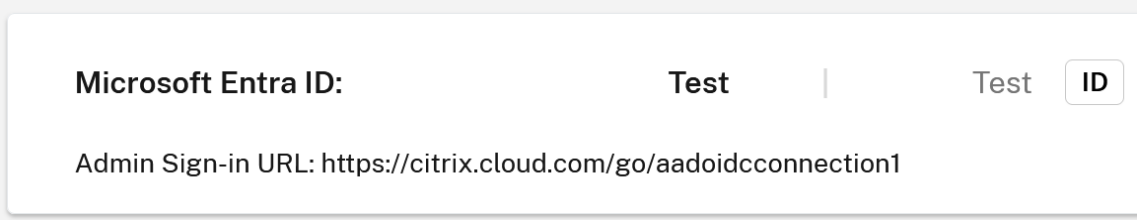
- Verify that your end users have user accounts in your AD. End users without AD accounts can't sign in to their stores successfully when SAML authentication is configured.
- Connect your AD to your Citrix Cloud account by deploying Cloud Connectors in your on-premises AD.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Synchronize your AD users to the SAML provider. Citrix Cloud requires the AD user attributes for your end users so they can sign in successfully.
- Only Universal AD groups should be used.
- You MUST define any UPN suffixes inside Active Directory that your SAML users are configured to use. Citrix Cloud connectors cannot use undefined or ambiguous UPN suffixes to determine Active Directory domain context.
- An EntraID OIDC IdP connection is NOT required for the default SAML flow as this uses AD identities.

EntraID Directory (EntraID Identities SAML Flow)

- EntraID B2B and external user support require AD shadow accounts with UPNs that match the FrontEnd users inside EntraID.
- If using the SAML using Entra ID identities SAML flow as documented in SAML with Entra ID identities then you must also connect the correct EntraID tenant inside **identity and Access Management > Authentication**.



AD user attributes

The following attributes are required for all Active Directory user objects and must be populated:

- Common name
- SAM account name
- User Principal Name (UPN)
- Object GUID
- SID

Citrix Cloud uses the Object GUID and SID attributes from your AD to establish the user context when end users sign in to their store. If either of these properties isn't populated, end users can't sign in.

The following attributes aren't required for using SAML authentication with Citrix Cloud, but Citrix recommends populating them to ensure the best user experience:

- Email address

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Display Name

Citrix Cloud uses the Display Name attribute to show end users' names correctly in their store. If this attribute isn't populated, end users can still sign in, but their names might not be displayed as expected.

SAML integration with Active Directory

Before enabling SAML authentication, you must integrate your on-premises AD with your SAML provider. This integration allows the SAML provider to pass the following required AD user attributes to Citrix Cloud in the SAML assertion:

- objectSID (SID)
- objectGUID (OID)
- userPrincipalName (UPN)
- Mail (email)
- Display Name (displayName)

You can configure a subset of these attributes, provided either the SID or UPN attributes are included in the SAML assertion. Citrix Cloud retrieves the other attributes from your AD as needed.

> **Note:**
>
> To ensure the best performance, Citrix recommends configuring all of the attributes mentioned in this section.

Although the precise integration steps vary among SAML providers, the integration process typically includes the following tasks:

1. Install a synchronization agent in your AD domain to establish a connection between your domain and your SAML provider. If you're using ADFS as your SAML provider, this step isn't required.
2. Create custom attributes and map them to the required AD user attributes mentioned earlier in this section. For reference, the general steps for this task are described in Create and map custom SAML attributes in this article.
3. Synchronize your AD users to your SAML provider.

For more information about integrating your AD with your SAML provider, consult your SAML provider's product documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Which SAML Binding Mechanism should I choose to use?

March 31, 2026

Author:
Mark Dear

Whether to use HTTP POST or HTTP Redirect for SSO and SLO is determined by the SAML bindings your SAML IdP supports. If your SAML provider supports multiple binding mechanisms then Citrix recommends you choose HTTP Post over HTTP Redirect as the SAML binding. There is no need to enable both SAML binding mechanisms on your SAML provider if it supports both. It is recommended you choose a single SAML binding type for both SSO and SLO.

SAML Binding Support

SAML Binding	Supported by Citrix Cloud
HTTP POST	Recommended.
HTTP Redirect	Supported.
SAML Artifact binding	Not Supported.
SOAP	Not Supported.

> **Important:**
>
> **HTTP Post** is the recommended binding mechanism for both SSO and SLO requests for two reasons.
>
> **HTTP Post** is easier to debug when signing enforcement is enabled on both sides of the SAML connections as the SAML XML contains easily identifiable sections that show the signature and certificate used. This is easier for humans to see and debug than if this signature data is embedded inside a very long Redirect URI which needs to be URL decoded.
>
> **HTTP Redirect** URIs can grow very long and exceed a critical threshold which then leads to errors during SAML authentication and can cause login or logout failure. The GET binding type is limited to a maximum of **2,048 characters**, minus the number of characters in the actual path. The POST method is not limited by the size of the URL for submitting name and value pairs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Service Provider Initiated SSO vs Identity Provider Initiated SSO

June 22, 2026

Author:
Mark Dear

SP-initiated SSO - the end user logs in directly from the web application (SP) such as stores and/or Citrix Cloud, which then redirects them to the SAML IdP for authentication, and if authentication is successful, then redirects the end user back to the web app (SP) and logs them in.

IdP-initiated SSO - the end user logs in first to their SAML IdP and then selects the app (SP) they want to launch from the IDP portal.

Can Identity Provider Initiated SSO be used with store or Citrix Cloud?

No. Stores and Citrix Cloud both only support SAML **Service Provider Initiated SSO** logon. All logon flows must be initiated via either a store URL for end user access, or a Citrix Cloud GO URL for Citrix Cloud admin access.

Directly Connecting the SAML Provider to Citrix Cloud VS IDP Chaining

June 22, 2026

Author:
Mark Dear

Is IDP chaining supported for SAML login to stores or Citrix Cloud?

IDP chaining is supported provided the closest SAML IDP in the IDP chain is configured correctly and forwards SAML requests from Citrix Cloud onwards in the IDP chain, and the IDP chain returns the correct SAML response to Citrix Cloud.

Examples of IDP chains

- Citrix Cloud → F5 (directly connected to Citrix Cloud as the SAML provider) → Federated to Entra ID

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Cloud → Entra ID (directly connected to Citrix Cloud as the SAML provider) → Federated to ADFS
- Citrix Cloud → Entra ID (directly connected to Citrix Cloud as the SAML provider) → Federated to PingFederate
- Citrix Cloud → Entra ID (directly connected to Citrix Cloud as the SAML provider) → Federated to Okta

Can I get assistance and support from Citrix when debugging SAML issues if I am using an IDP chain?

Citrix support and Citrix Engineering can only debug SAML connections directly between Citrix Cloud and the closest SAML IDP in the chain.

> **Important:**
>
> Citrix is not responsible for debugging issues within a complex IDP chain upstream of the directly connected SAML provider.

Should I avoid IDP chaining if possible?

Citrix recommends directly connecting your SAML IDP to Citrix Cloud as this greatly reduces configuration and debugging complexity and minimises end user logon delays which can be introduced whilst Citrix Cloud waits for responses from the complex IDP chain. Many issues can arise with both SSO and SLO when multiple IDPs are chained together particularly when different SAML bindings are used by different IDPs within the IDP chain. A directly connected SAML provider will always be easier to debug and more performant than one that relies on upstream IDPs.

SAML Logout Considerations

June 22, 2026

Author:
Mark Dear

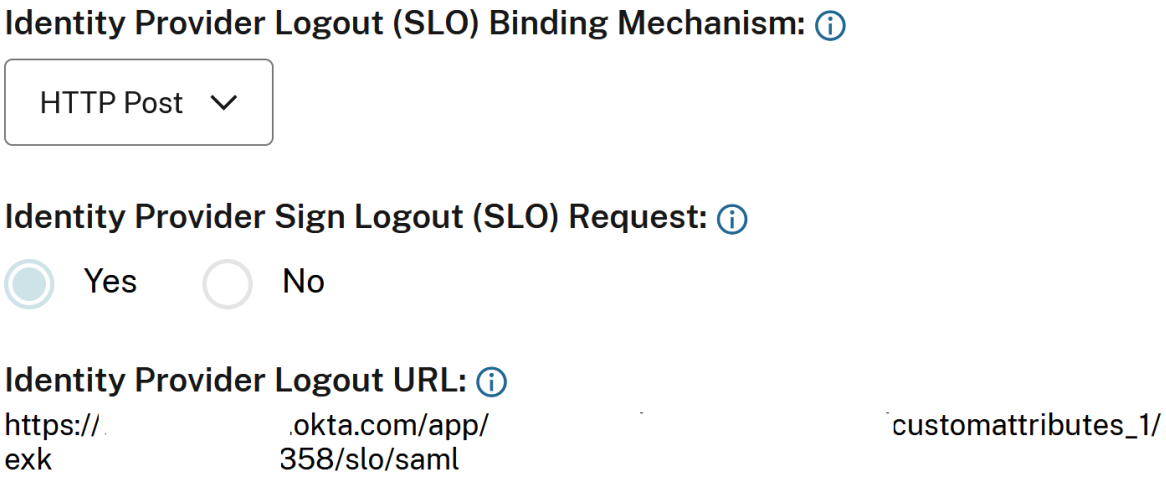
For Identity Provider Logout URL (SLO), decide the SAML logout behaviour most appropriate for your organization based on whether the SAML application you wish to connect to Citrix Cloud is also shared by other service providers (SPs) or not.

Citrix recommends creating a new dedicated SAML application within your SAML provider, which is used by only store and/or Citrix Cloud. If you have followed one of Citrix's SAML application setup

© 1997–2026 Citrix Systems, Inc. All rights reserved.

guides and you are using a dedicated SAML application for store and/or Citrix Cloud then configuring a Logout URL is always the correct course of action.

Option1 SLO Configured (Recommended): Users signing out of store and/or Citrix Cloud also sign out of the connected SAML IDP.



> **Important:**
>
> For SAML SLO to succeed you must configure both sides of the SAML connection to support it. Citrix Cloud expects to receive an SLO response from the SAML application indicating the logout succeeded and the user was logged out of the SAML IDP. Ensure your SAML application is configured to send the SLO response back to Citrix Cloud using this SAML logout endpoint `https://saml.cloud.com/saml/logout/callback`.

OR

Option 2 SLO not configured: If you want users to stay signed into your SAML application after signing out of store and/or Citrix Cloud, leave the Logout URL field empty inside the Citrix Cloud SAML connection. When an end user performs an explicit logout in the store or Citrix Cloud UI this will only log the user out of store or Citrix Cloud. The user will not be logged out of the SAML IDP and no SLO request will be sent from Citrix Cloud to the SAML application.



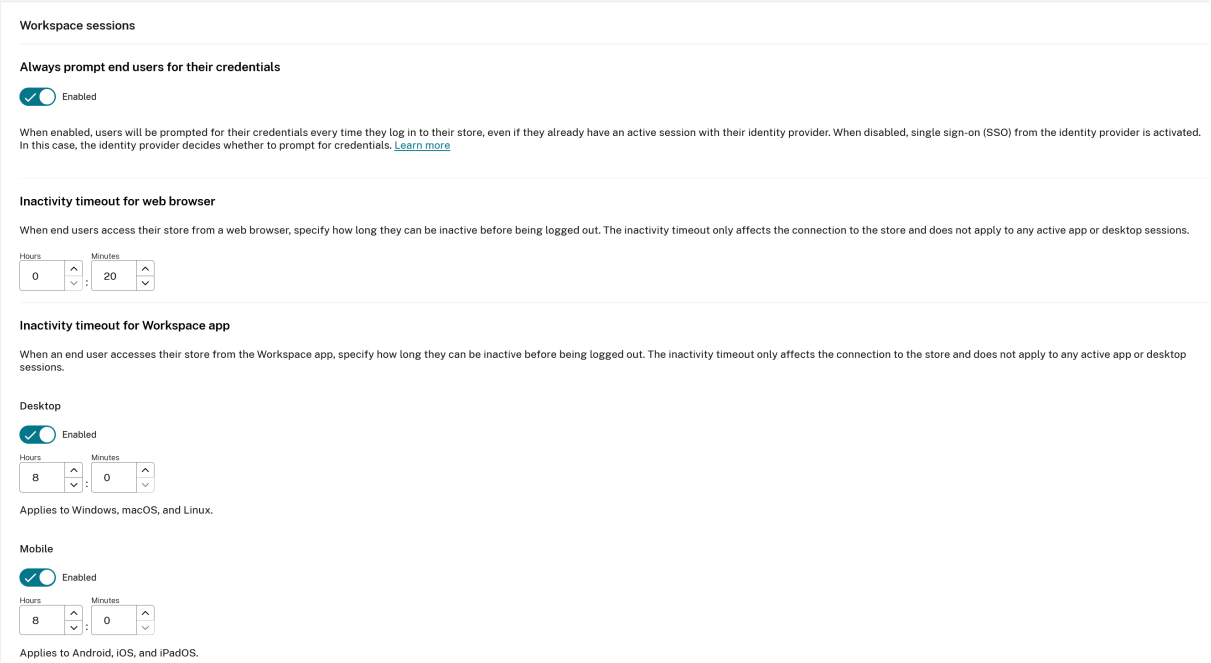
> **Important:**
>
> This SAML Connection configuration without a logout URL configured is only recommended if

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> the SAML application connected to Citrix Cloud is shared by other non Citrix service providers (SPs)

Store Session Inactivity Timeout Behaviour

When an end user does not perform any action within stores then the session inactivity timeout will trigger a log off from stores. The stores inactivity timeout is defined in **StoreFront Cloud → Customize → Preferences → Store sessions**.



The stores inactivity timeout does not trigger an SLO request to log the end user out of the SAML IdP. The SAML IdP idle session timeout may be a different value to what is set inside store. It is recommended you should set them to be the same duration if possible.

Set **Always Prompt End Users for their credentials** to **Enabled** within **toreFront Cloud → Customize → Preferences** to ensure the end user is always prompted to reauthenticate even if a SAML provider session still exists for the user.

Setting **Always Prompt End Users for their credentials** to **Enabled** also sets **ForceAuthn** to **True** within the SAML request.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Create a SAML Connection using Metadata URL Mode

March 31, 2026

Author:
Mark Dear

Citrix recommends that all new SAML connections be created using metadata URL mode. Obtain the metadata URL for your SAML application from inside your IdP. Citrix Cloud can consume SAML IdP metadata to configure a SAML connection automatically.

Why is Metadata URL mode the recommended way to create a Citrix Cloud SAML connection?

Simplicity. The SAML connection inside Citrix Cloud is set up automatically using a combination of default connection setting values and values obtained from inside the metadata.

IdP metadata contains all the following information required to set up the SAML connection inside Citrix Cloud:

- SAML Entity ID
- SSO Endpoint
- SLO Endpoint (if configured inside the IdP)
- Supported SAML bindings

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Public keys and signing certificates

Reduced Maintenance. Automatic handling of changes made inside the SAML IdP and IdP certificate rotations.

How does Citrix Cloud handle IdP certificate rotations when Metadata URL mode is used?

Automatically. When your SAML IdP admin updates the SAML application to include a new IdP signing certificate, or replace the existing certificate, Citrix Cloud implicitly trusts all SAML signing certificates provided inside the IdP metadata. Metadata URL mode eliminates the need for manual IdP certificate rotations within Citrix Cloud. Any changes made by IdP admins are automatically detected. Your SAML application's metadata URL is used during each SAML logon to get the latest copy of your SAML application's signing certificates.

Configure the Citrix Cloud SAML connection using your IdP Metadata URL

1. Obtain the link to your SAML application's metadata and enter it into a browser to prove it is contactable and there are no firewall rules blocking Citrix Cloud's access to it.

   Example:
   `https://tenant.okta.com/app/zxv1r8qo70l2q5LNT359/sso/saml/metadata`

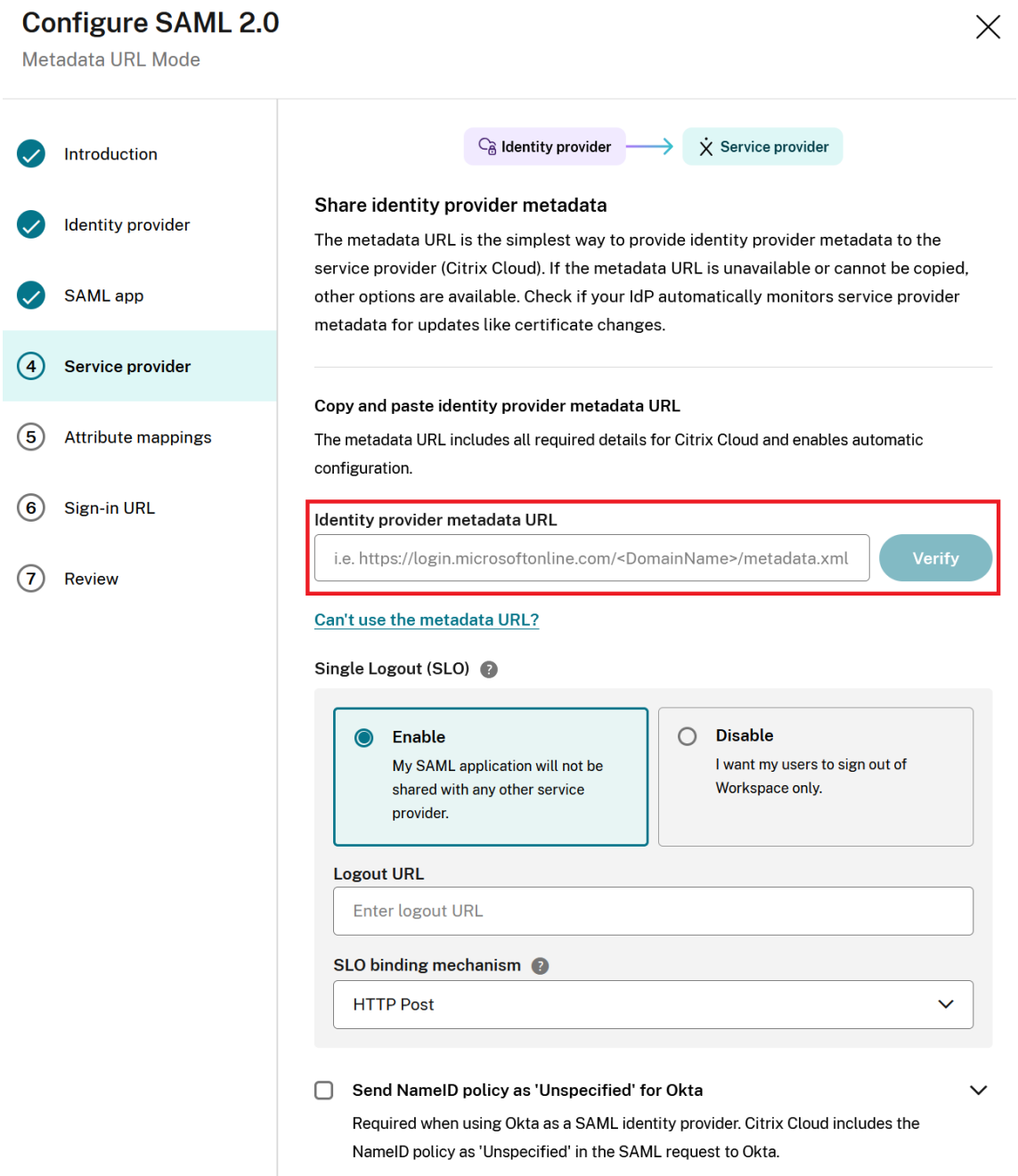
2. When you reach the **Section 4 Service Provider** section of the SAML wizard, enter your SAML application's metadata URL here and click **Verify**.

   > **IMPORTANT:**
   > If your SAML application exists on an on-premise server such as an ADFS or PingFederate server and SAML IdP metadata URL fails to verify, check your firewall rules. Verify your metadata URL is contactable inside a browser from any client outside of your organization.

3. After Citrix Cloud has parsed the metadata URL you should see this success message and Re-Verify.

   Here is an Okta example of a successfully imported metadata connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



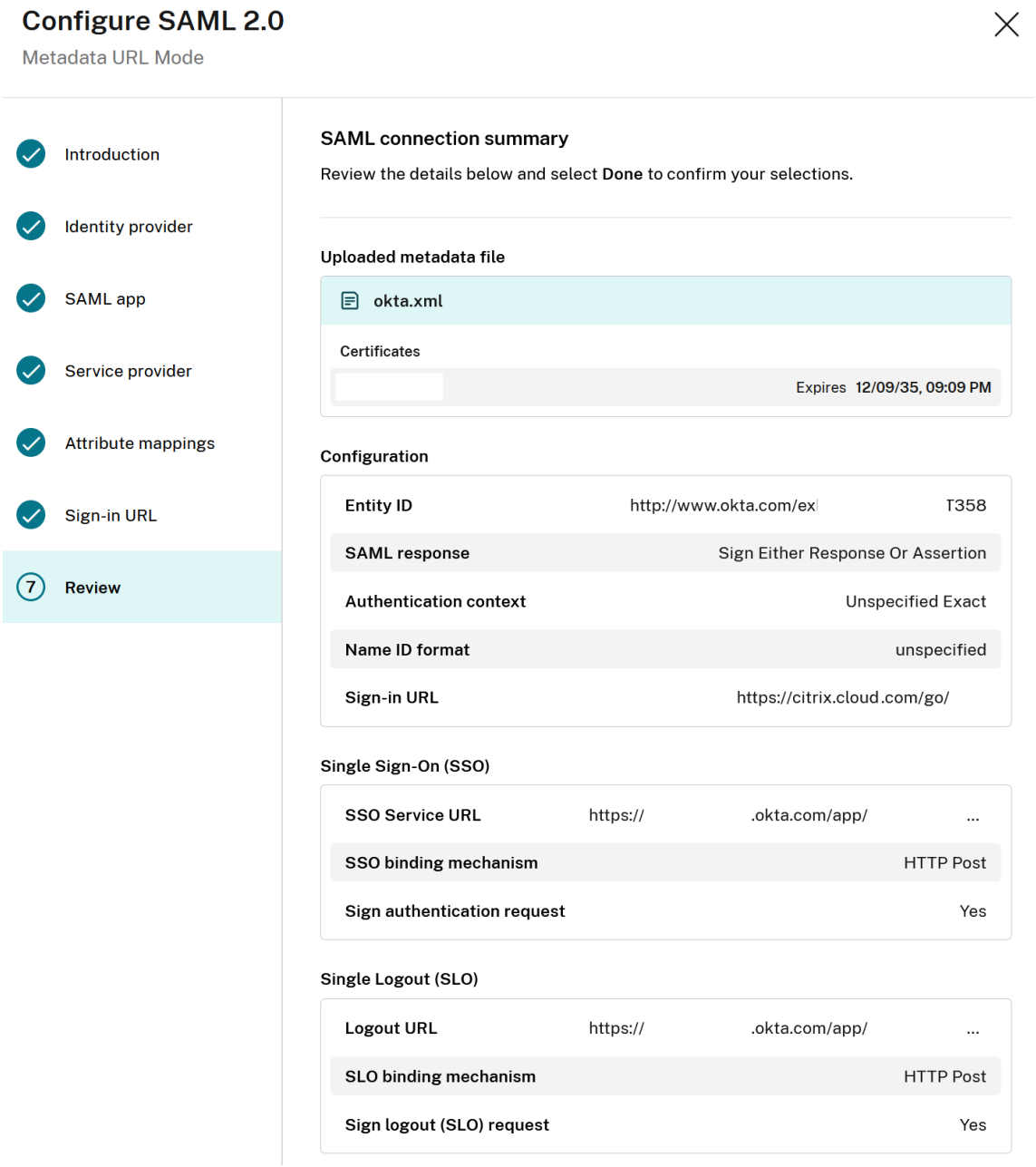
4. Configure the SAML logout behaviour you want by either enabling or disabling SLO. Refer to this in-depth article for Logout Considerations.

> **Important:**
>
> **Okta SAML connections ONLY**. If the metadata URL contains an SSO endpoint and a DNS domain string containing "okta"then Send NameID Policy as Unspecified for Okta will be automatically enabled. Okta SAML applications that use an Okta custom domain like my-tenant.domain.com cannot be autodetected and Send NameID Policy as Unspecified for

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> Okta must be manually enabled by the Citrix admin by clicking the check box.

5. Accept the default attribute mappings.
6. Configure your Citrix Cloud Admin Sign-In URL.
7. Examine the SAML wizard summary inside the Review section and verify the SAML configuration matches your expectations after parsing of the IdP metadata URL.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a SAML Connection using Metadata File Mode

March 31, 2026

Author:
Mark Dear

How does Metadata File mode differ from Metadata URL mode?

On premise SAML IdPs such as an ADFS or PingFederate server may have restrictions that block public access to their SAML metadata URL endpoint, so using metadata URL mode is not possible. Citrix Cloud administrators can still benefit from automatic configuration of Citrix Cloud SAML connections if they are provided with a metadata.xml file exported from the SAML IdP. Citrix Cloud administrators can still upload this file within the SAML connection creation wizard.

How is Metadata File mode less useful than Metadata URL mode?

Metadata File mode is a static configuration stored inside Citrix Cloud. Citrix Cloud SAML connections that were created using metadata file mode cannot detect changes in the SAML application AFTER it has been uploaded into Citrix Cloud.

Metadata URL mode is a dynamic configuration obtained on demand. Metadata URL mode continuously polls your SAML IdP and can detect changes made inside the SAML application configuration immediately after they are made.

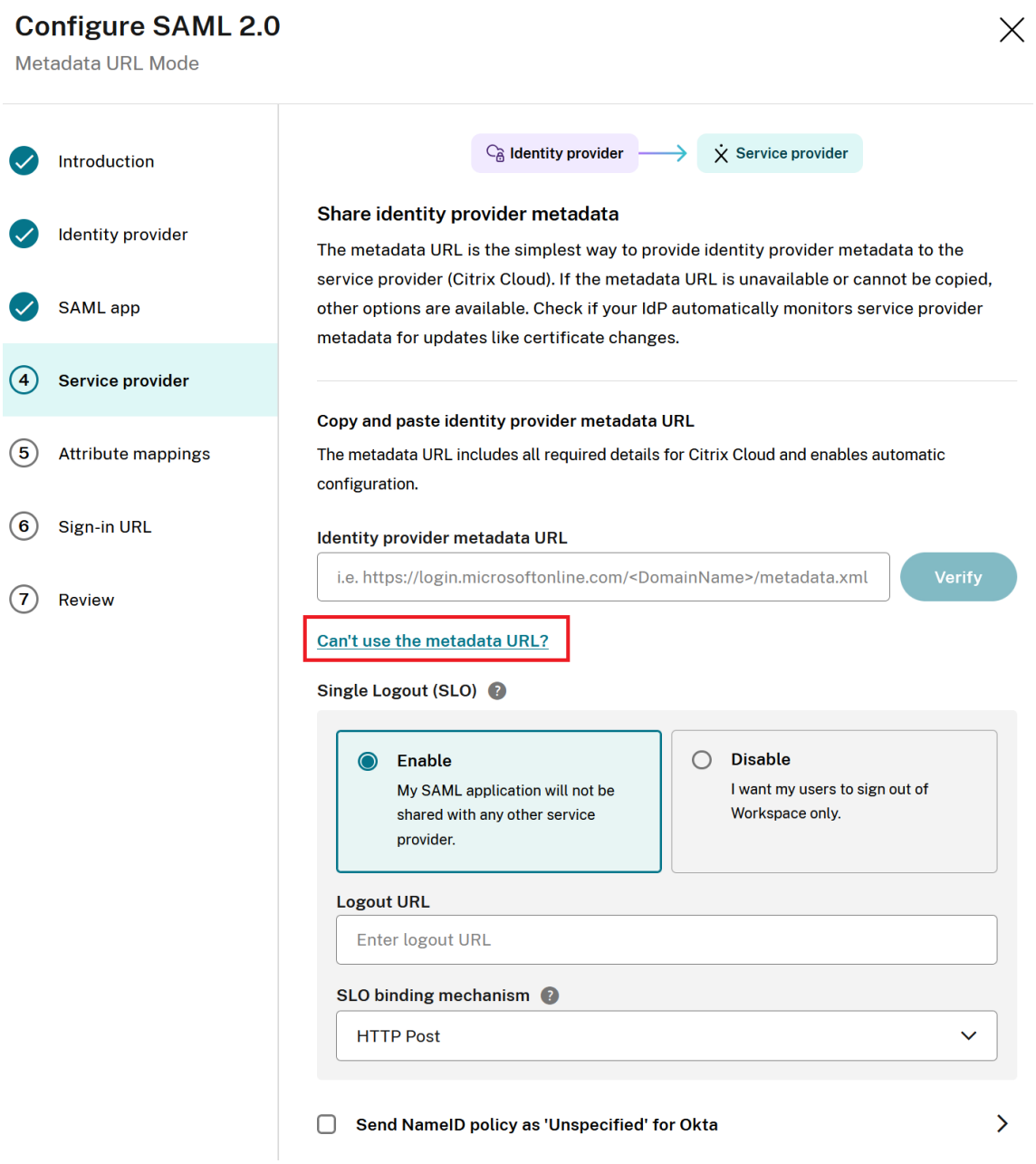
Configure the Citrix Cloud SAML connection using your IdP Metadata File

1. Download the metadata.xml file from the SAML application you wish to configure inside Citrix Cloud as a new SAML IdP connection.
2. Save the file to disk as `<filename>.xml` and do not make any changes to its XML formatting or its contents. It is recommended you use completely unchanged and unformatted metadata.xml files taken directly from the SAML IdP after export.

   > **Important:**
   >
   > metadata.xml files are often signed by the IdP to prevent tampering. Any changes to the data inside the metadata.xml such as reformatting it using XML beautifying tools will invalidate the embedded signature and cause a failure to upload and parse the metadata.xml.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

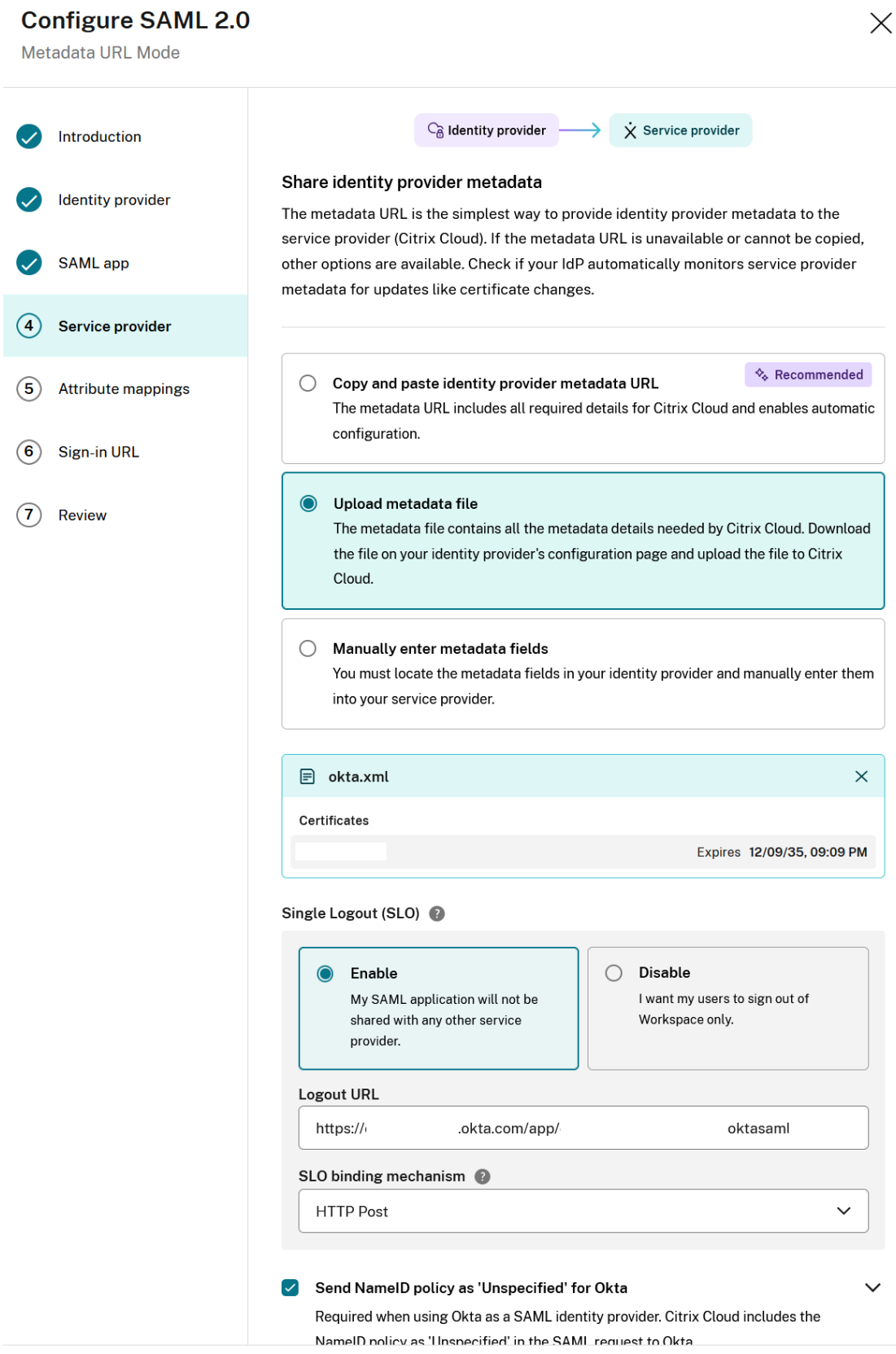
3. When you reach the **Section 4 Service Provider** section of the SAML wizard select *Can't use the metadata URL?*.



4. Select Upload metadata file and drag and drop the metadata.xml file into the file upload dialogue or browse to the metadata.xml file on disk.

   Here is an **Okta** example of a successfully imported metadata file.

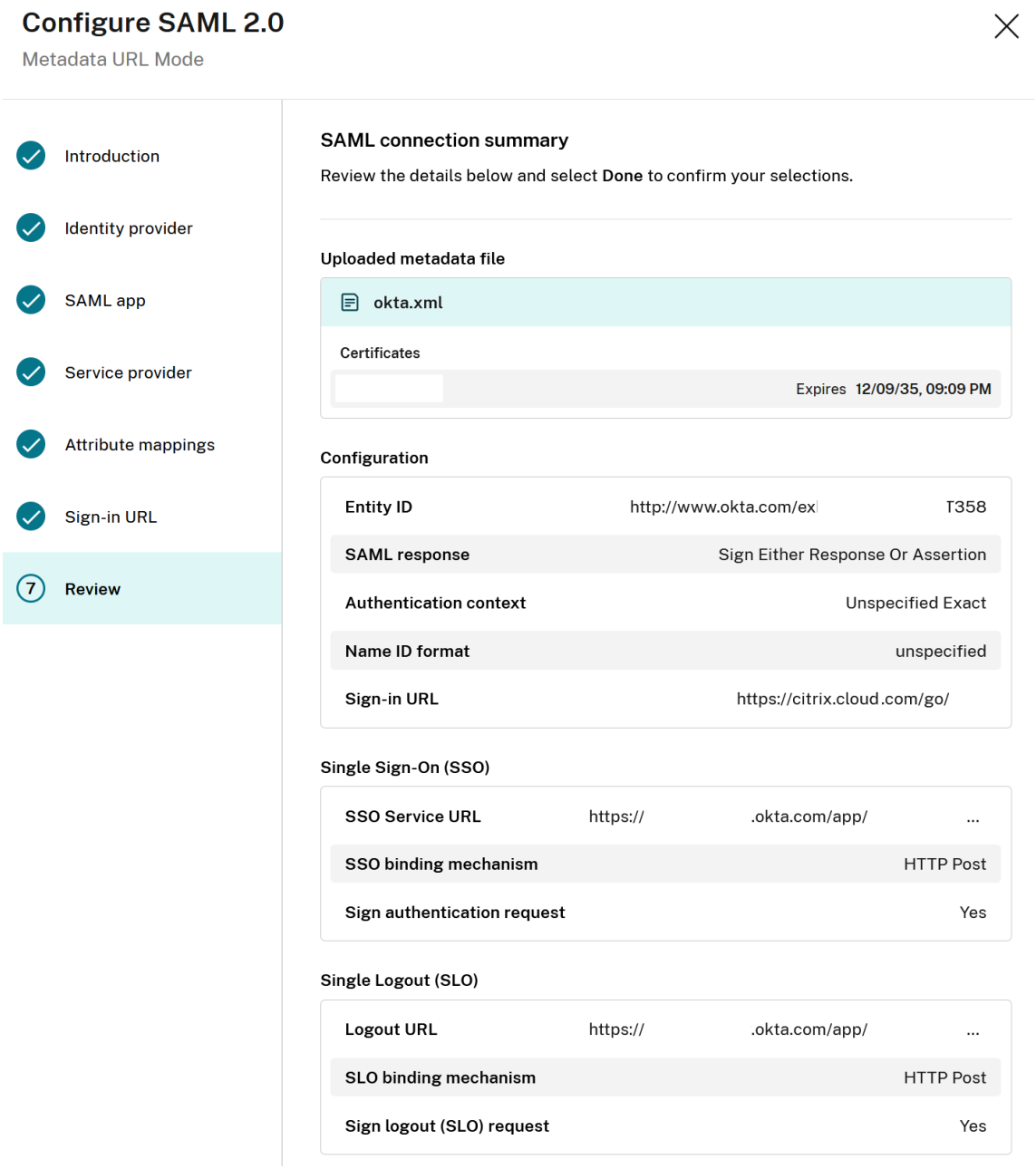
© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Configure the SAML logout behaviour you want by either enabling or disabling SLO.
   Refer to this in-depth article for Logout Considerations.
6. Okta SAML connections ONLY. If the metadata file contains an SSO endpoint and a DNS domain string containing "okta"then **Send NameID Policy as Unspecified for Okta** will be automatically enabled. Okta SAML applications that use an Okta custom domain like mytenant.domain.com cannot be autodetected and **Send NameID Policy as Unspecified for Okta** must be manually enabled by the Citrix admin by clicking the check box.
7. Accept the default attribute mappings.
8. Configure your Citrix Cloud Admin Sign-In URL.
9. Examine the SAML wizard summary inside the Review section and verify the SAML configuration matches your expectations after parsing of the IdP metadata file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Create a SAML Connection using Manual Mode

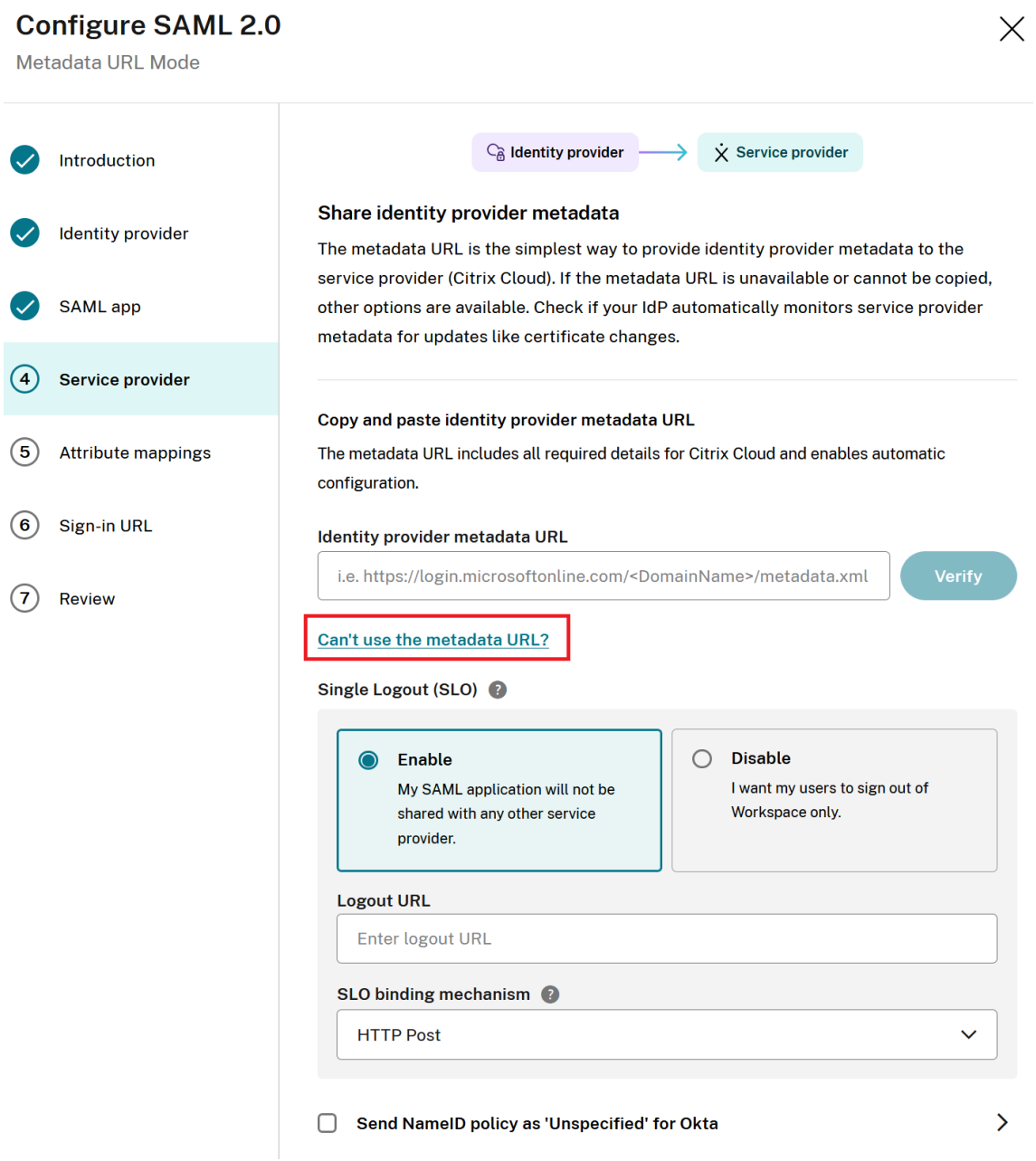
March 31, 2026

Author:
Mark Dear

1. Obtain details of your SAML application and its SAML endpoints.

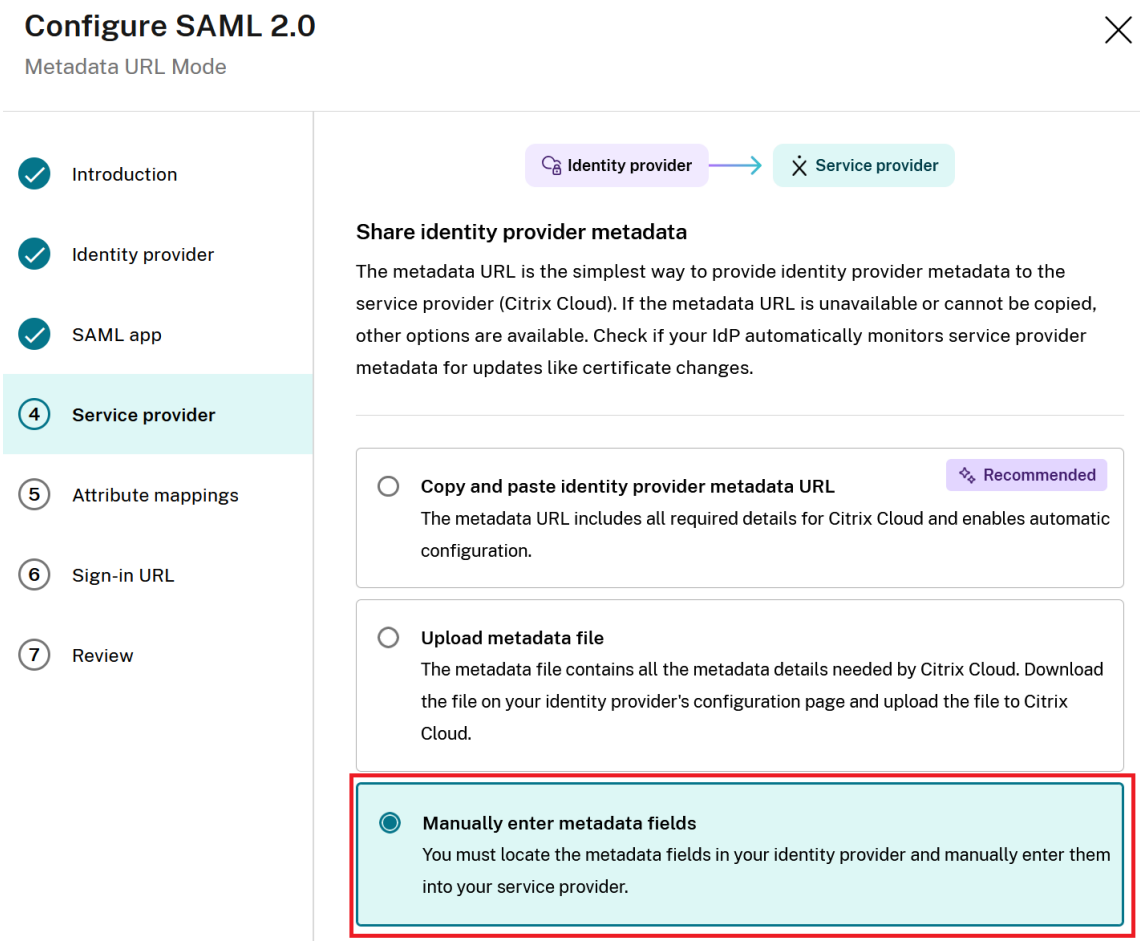
© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Download the SAML signing certificate from your SAML application.
3. When you reach the **Section 4 Service Provider section** of the SAML wizard select *Can't use the metadata URL?*.

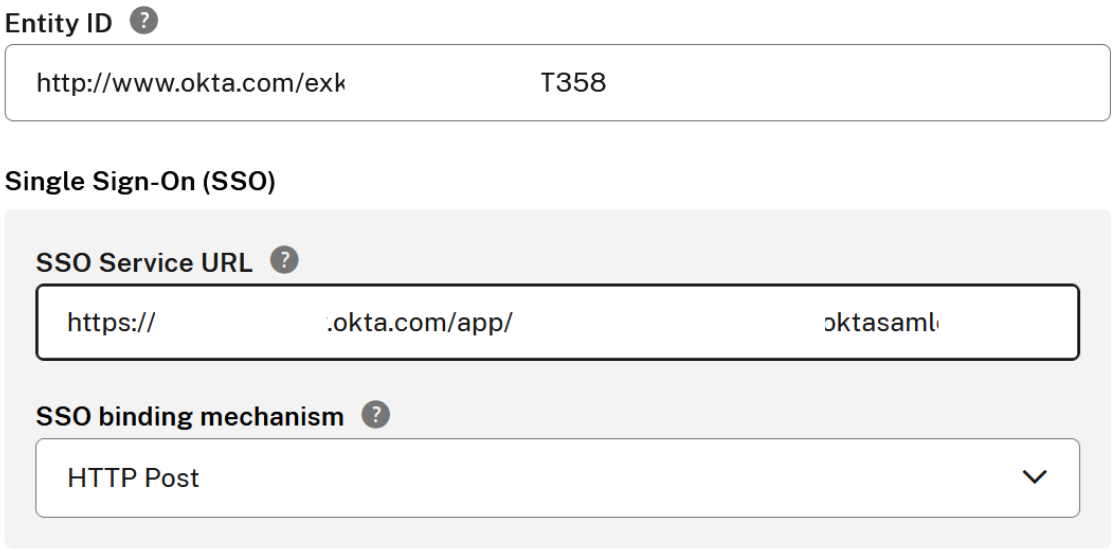


4. Select **Manually enter metadata fields**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Enter your SAML application's Entity ID and SSO URL.

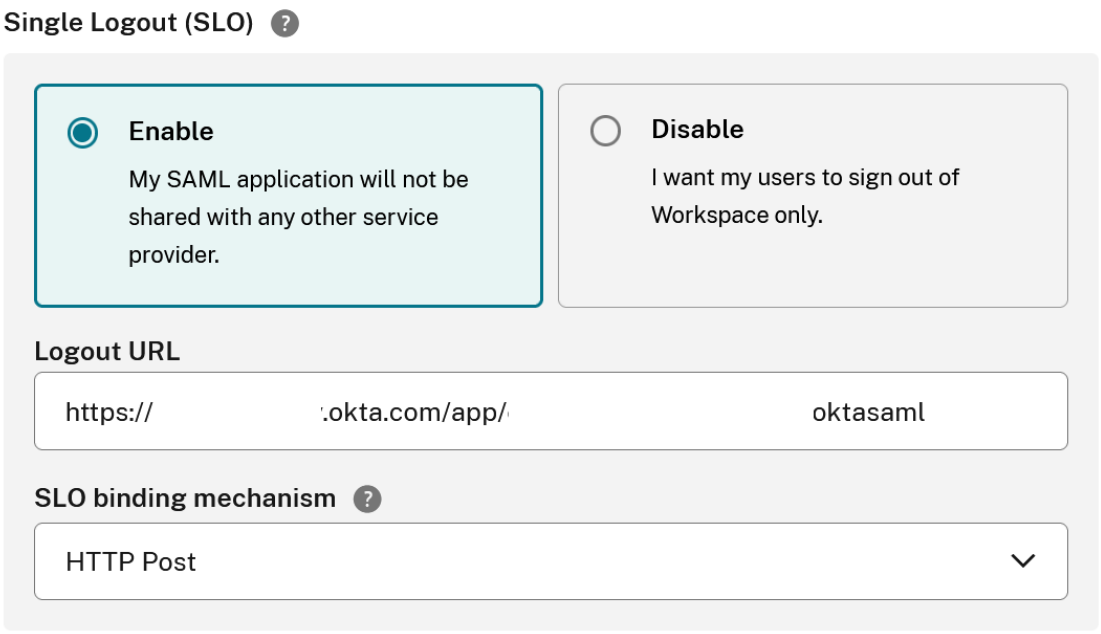


6. Upload your SAML application's signing certificate by dragging and dropping the file into the file upload dialogue or browse to the samlapp.cer file on disk.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

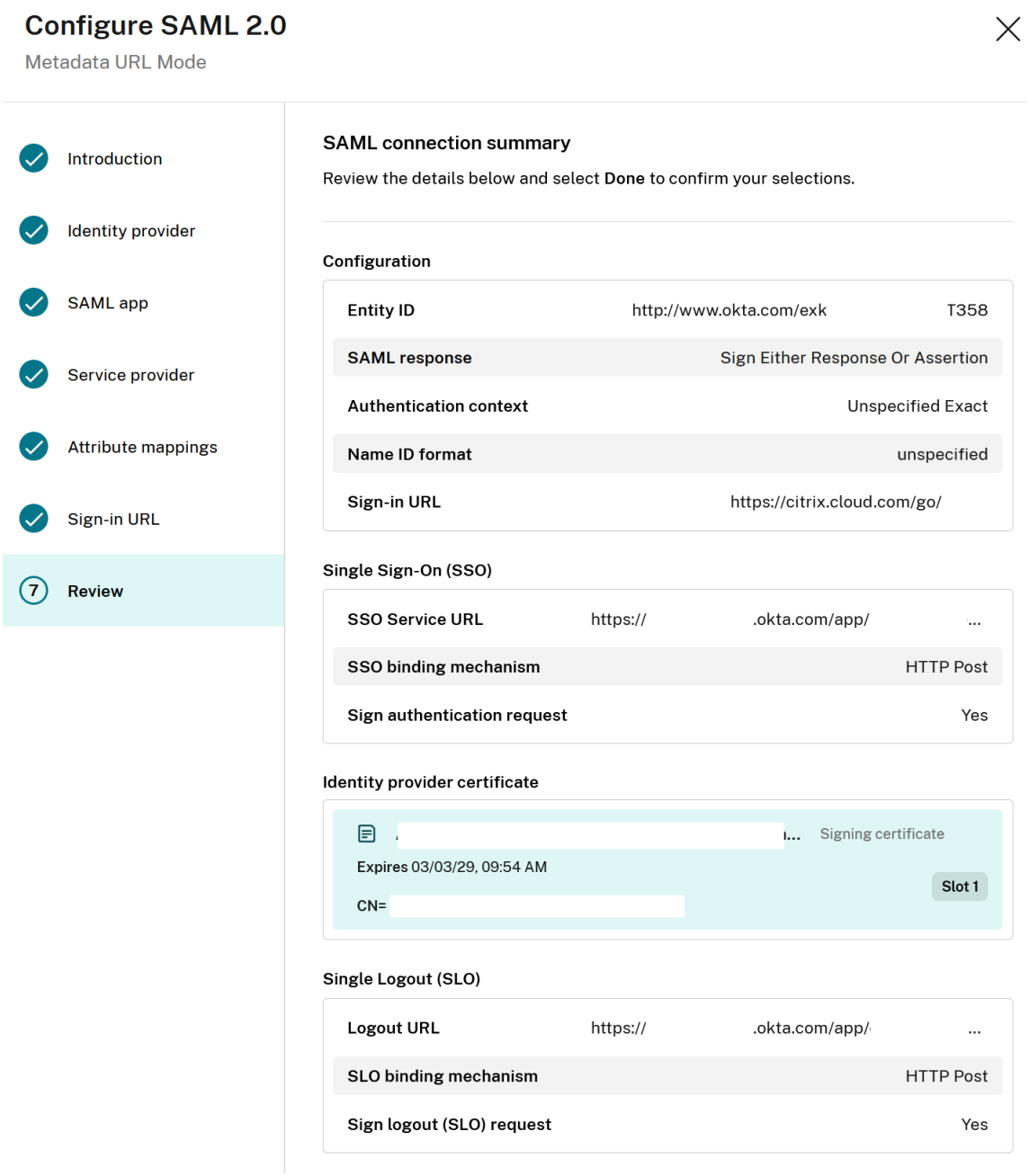
7. Configure the SAML logout behaviour you want by either enabling or disabling SLO. Refer to this in-depth article for Logout Considerations.

   Enter your SAML application's SLO URL (recommended).



8. Okta SAML connections ONLY. If the SSO URL entered contains a DNS domain string containing "okta"then **Send NameID Policy as Unspecified for Okta** will be automatically enabled. Okta SAML applications that use an Okta custom domain like mytenant.domain.com cannot be autodetected and **Send NameID Policy as Unspecified for Okta** must be manually enabled by the Citrix admin by clicking the check box.
9. Accept the default attribute mappings.
10. Configure your Citrix Cloud Admin Sign-In URL.
11. Examine the SAML wizard summary inside the Review section and verify the SAML configuration matches your expectations after manually configuring the connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Troubleshooting

June 22, 2026

Author:
Mark Dear

© 1997–2026 Citrix Systems, Inc. All rights reserved.

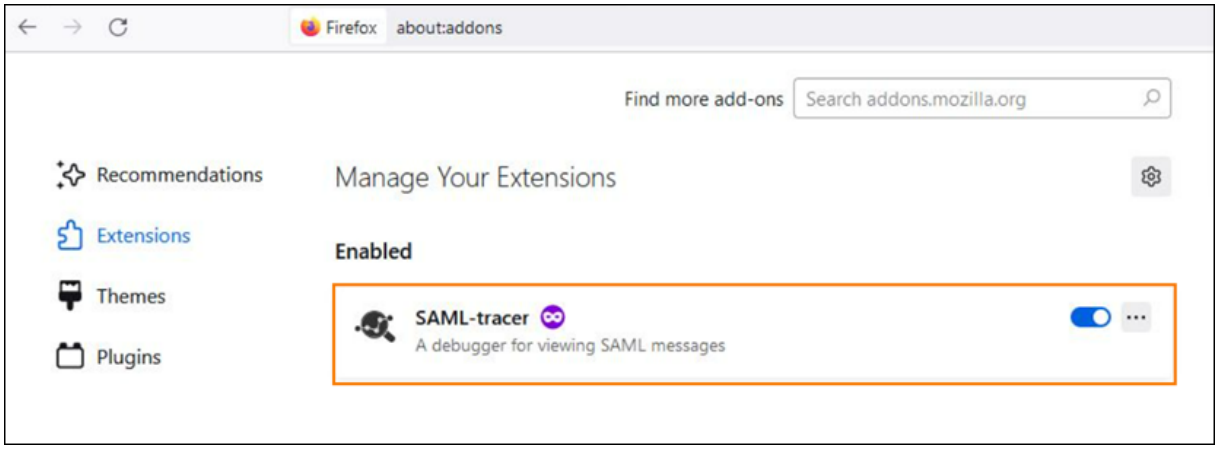
What do I need to provide to Citrix Support and Engineering when I open a SAML support case?

In the event you need assistance with a SAML-related issue, Citrix Support and Engineering requires the following information:

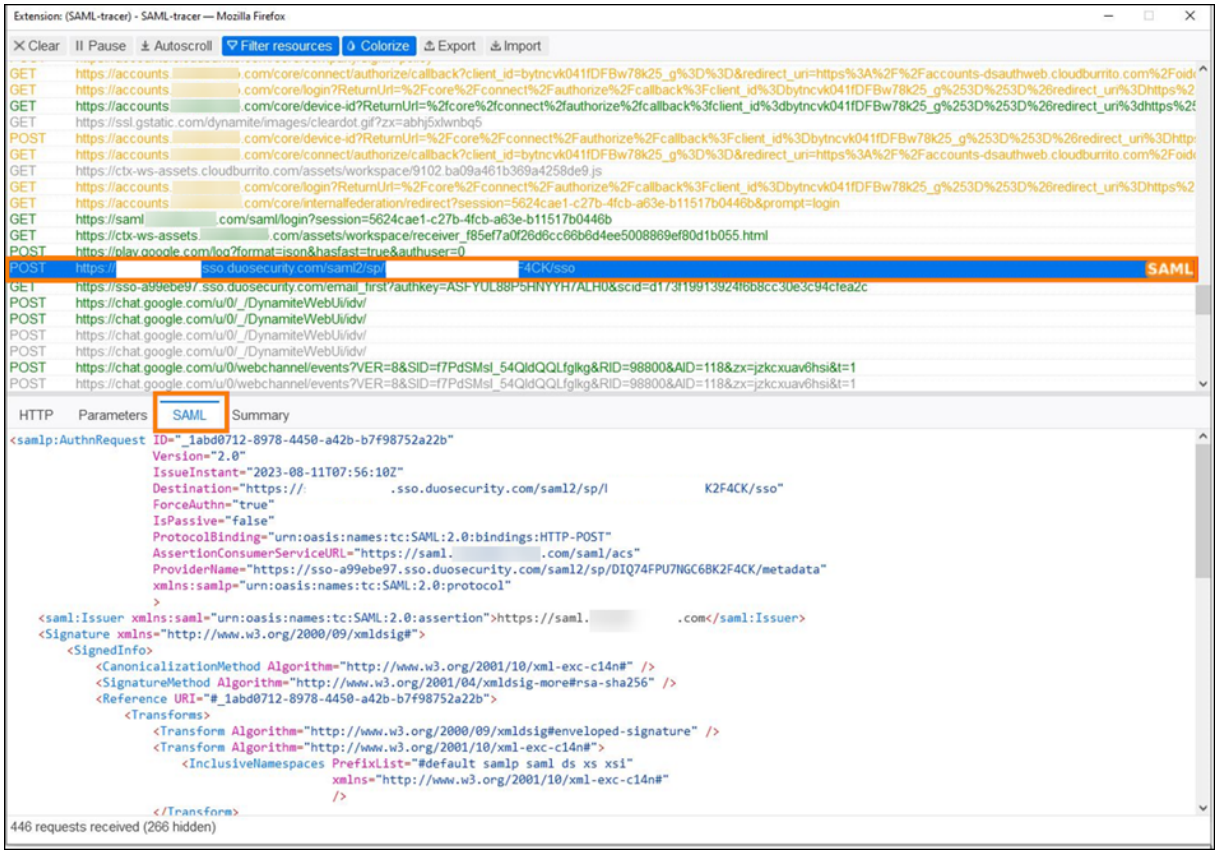
- Include sufficient context and describe your logon scenario and Citrix or Active Directory environment.
- Which Citrix eDocs you followed during initial configuration.
- Screenshots and details of your SAML application inside your IdP.
- Details of your Active Directory.
- A SAML-tracer file (`.json`) file from the SAML tracer browser extension.
- A HAR file (`.har`) from your browser dev tools.
- Details of both working and failing end users or Citrix Cloud admin users.
- The public caller IP of the machine performing a SAML logon to store or Citrix Cloud.

Capture SAML Traces for Citrix Support and Engineering

Citrix Engineering and Support recommends the use of the SAML-tracer browser extension for all SAML debugging as well as `.HAR` files generated by browser developer tools. This extension is available for most common web browsers and exports `.JSON` files. The extension decodes SAML requests and responses into XML, which renders them human-readable and much easier to understand and debug.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



How do I collect a HAR file from my browser to send to Citrix Support and Engineering?

For more information, see article Collect HAR file

Useful 3rd party SAML debugging tools

> **IMPORTANT:**
>
> Citrix does not provide any liability when 3rd party tools are used for debugging purposes. Use and access 3rd party tools and websites at your own risk.

Tool	Purpose
https://www.samltool.io/	Decodes base 64 SAML requests and responses
https://www.sslshopper.com/certificate-decoder.html	Decodes certificate data
https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract	Extracts Signing and Encryption certificates as files from SAML metadata

© 1997–2026 Citrix Systems, Inc. All rights reserved.

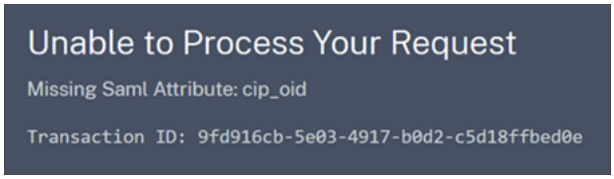
Tool	Purpose
https://www.whatismyip.com/	Provides the caller IP of the client that is attempting a SAML logon.

Attribute Errors

Attribute errors might arise under any of the following conditions:

- The required attributes in your SAML configuration are not encoded correctly.
- The `cip_sid` and `cip_upn` attributes are missing from SAML assertion.
- The `cip_sid` or `cip_oid` attributes are missing from the SAML assertion and Citrix Cloud can't retrieve them from Active Directory due to a connectivity issue.

When an attribute error occurs, Citrix Cloud displays an error message that includes the faulty attributes.



To resolve this type of error:

1. Ensure that your SAML provider sends the required attributes with the correct encoding, as shown in the following table. At a minimum, either the SID or UPN attribute must be included.

Attribute	Encoding	Required
cip_email	Must be in String format (`user@domain`)	
cip_oid	Must be in Base64 or String format	
cip_sid	Must be in Base64 or String format	Yes, if not using `cip_upn`
cip_upn	Must be String format (`user@domain`)	Yes, if not using `cip_sid`

2. Verify the Cloud Connectors are online and healthy so Citrix Cloud can retrieve any missing attributes that it needs. For more information, see Cloud Connector advanced health checks.

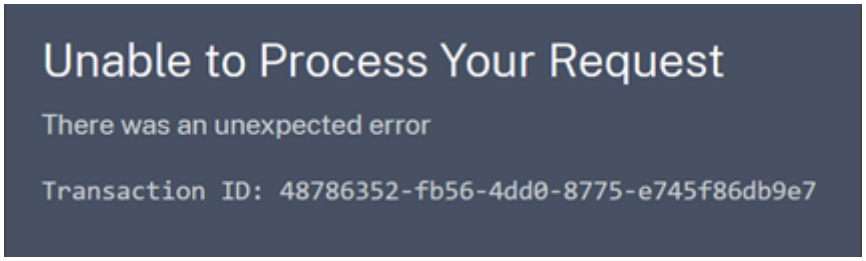
Unexpected errors

Citrix Cloud might experience an unexpected error when:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- A user initiates a SAML request using an IDP-initiated flow. For example, the request is made by selecting a tile through the identity provider's app portal instead of navigating directly to the store URL (`customer.cloud.com`).
- The SAML certificate is invalid or has expired.
- The authentication context is invalid.
- SAML assertion and response signature is mismatched.

When this error occurs, Citrix Cloud displays a generic error message.



If this error results from navigating to Citrix Cloud through an identity provider's app portal, you can use the following workaround:

1. Create a bookmark app in the identity provider's app portal that references your store URL (for example, `https://customer.cloud.com`).
2. Assign users to both the SAML app and the bookmark app.
3. Change the visibility settings of the SAML app and the bookmark app so that the bookmark app is visible and the SAML app is hidden in the app portal.
4. Disable the **Always prompt end users for their credentials** setting in Citrix® StoreFront Cloud to remove additional password prompts. For instructions, see Always prompt end users for their credentials.

Configure a SAML application with a scoped Entity ID in Citrix Cloud™

June 22, 2026

Author:
Mark Dear

This article describes how to provision multiple SAML applications within the same SAML provider.

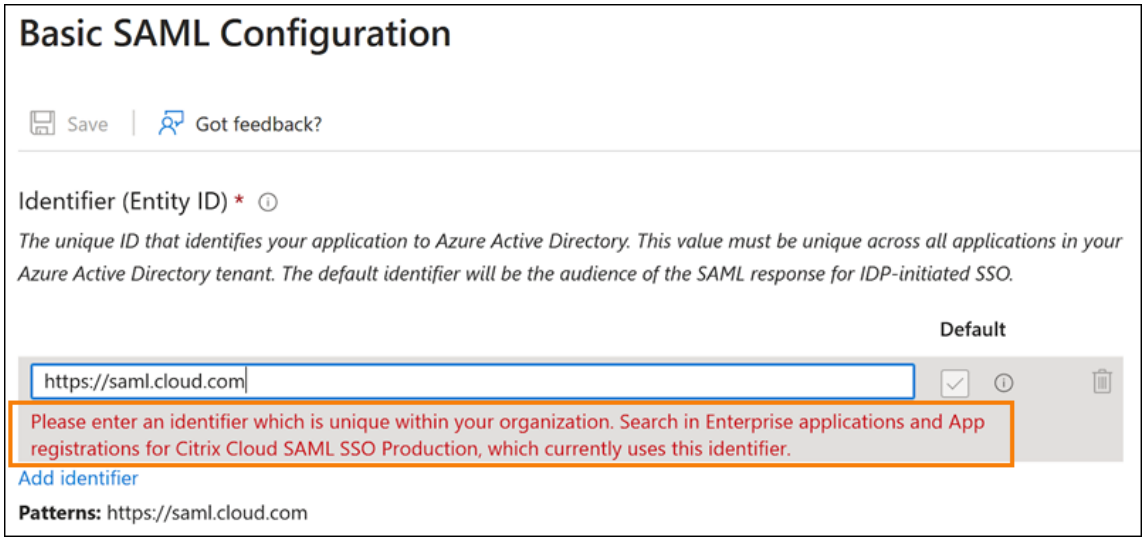
Some SAML providers, such as Microsoft Entra ID (ME-ID), Active Directory Federation Services (ADFS), PingFederate, and PingSSO, prohibit reusing the same Service Provider (SP) Entity ID within multiple SAML applications. As a result, administrators who create two or more different SAML applications within the same SAML provider can't link them to the same, or differing, Citrix Cloud tenants. Attempting to create a second SAML application using the same SP Entity ID, such as `https:\\saml`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

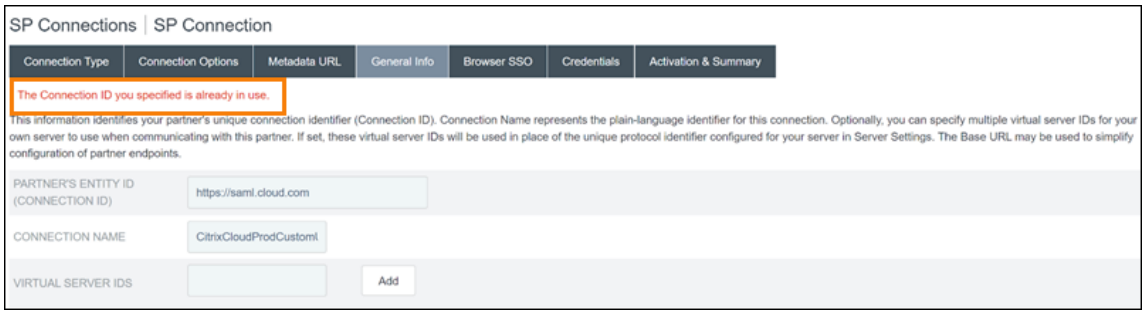
`.cloud.com`, when an existing SAML application is already using it triggers an error at the SAML provider, indicating the Entity ID is already in use.

The following images illustrate this error:

- In Microsoft Entra ID:



- In PingFederate:



The scoped Entity ID feature in Citrix Cloud addresses this limitation so you can create more than one SAML application within the SAML provider (such as an Microsoft Entra ID tenant) and link it to a single Citrix Cloud tenant.

What is an Entity ID?

A SAML Entity ID is a unique identifier that is used to identify a specific entity in the SAML authentication and authorization protocol. Typically, the Entity ID is a URL or URI that's assigned to the entity and used in SAML messages and metadata. Each SAML application that you create within your SAML provider is considered a unique entity.

Within a SAML connection between Citrix Cloud and Microsoft Entra ID, for example, Citrix Cloud is the Service Provider (SP) and Microsoft Entra ID is the SAML provider. Both have an Entity ID that must

© 1997–2026 Citrix Systems, Inc. All rights reserved.

be configured on the opposite side of the SAML connection. This means Citrix Cloud's Entity ID must be configured within Microsoft Entra ID, and Microsoft Entra ID's Entity ID must be configured within Citrix Cloud.

The following Entity IDs are examples of a generic Entity ID and a scoped Entity ID in Citrix Cloud:

- Generic: `https://saml.cloud.com`
- Scoped: `https://saml.cloud.com/67338f11-4996-4980-8339-535f76d0c8fb`

Generic and scoped SP Entity IDs by region

Existing SAML connections in Citrix Cloud (created before November 2023) use the same generic Entity ID for each SAML connection and Citrix Cloud tenant. Only new Citrix Cloud SAML connections provide the option of using a scoped Entity ID.

If you elect to use scoped Entity IDs for new connections, any existing SAML connections continue to function using their original generic Entity IDs.

The following table lists the generic and scoped SP Entity IDs for each Citrix Cloud region:

Citrix Cloud region	Generic SP Entity ID	Scoped Entity ID
United States, European Union, Asia Pacific-South	`https://saml.cloud.com`	`https://saml.cloud.com/67338f11-4996-4980-8339-535f76d0c8fb`
Japan	`https://saml.citrixcloud.jp`	`https://saml.citrixcloud.jp/db642d4c-ad2c-4304-adcf-f96b6aa16c29`
Government	`https://saml.cloud.us`	`https://saml.cloud.us/20f1cf66-cfe9-4dd3-865c-9c59a6710820`

Generating unique SP Entity IDs for new and existing SAML connections

When you create a new SAML connection, Citrix Cloud generates a unique ID (GUID). To generate a scoped Entity ID, you enable the **Configure scoped SAML Entity ID** setting when you create the new connection.

If you want to update an existing SAML connection to use scoped Entity IDs, you must disconnect and then reconnect your SAML provider from the **Identity and Access Management > Authentication**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

page in Citrix Cloud. Citrix Cloud doesn't allow you to edit existing SAML connections directly. However, you can clone the configuration and modify the clone.

> **Important:**
>
> Closing the SAML connection process before completing it discards the Entity ID that Citrix Cloud automatically generates. When you restart the SAML connection process, Citrix Cloud generates a new scoped Entity ID GUID. Use this new scoped Entity ID when you configure the SAML provider. If you're updating an existing SAML connection to use scoped Entity IDs, you must update the SAML application for that connection with the scoped Entity ID that Citrix Cloud generates.

Frequently asked questions about scoped Entity IDs

Can I create more than one Microsoft Entra ID SAML application within the same Microsoft Entra ID tenant and link it to one or more Citrix Cloud tenants?

Citrix Cloud's scoped Entity ID feature addresses the limitation of preventing duplicate Entity IDs that some SAML providers impose. With this feature, you can provision more than one SAML application within your Microsoft Entra ID tenant and configure each one with a scoped Entity ID from a single Citrix Cloud tenant.

Can I still link the same Microsoft Entra ID SAML application to multiple Citrix Cloud tenants?

This scenario is a common one among Citrix Cloud customers and Citrix continues to support it. To implement this scenario, you must meet the following requirements:

- Use a generic Entity ID, such as `https://saml.cloud.com`.
- Don't enable scoped Entity IDs for your SAML connection.

How do I decide whether or not to use a scoped Entity ID within my SAML provider?

Scoped Entity IDs in Citrix Cloud offer the flexibility to use a generic or a scoped Entity ID, depending on your requirements. Consider the number of SAML applications you need and the number of Citrix Cloud tenants you have. Also, consider whether or not each tenant might share an existing SAML application or require its own scoped SAML application.

> **Important:**
>
> If your SAML provider already allows you to create multiple SAML applications with the same Entity ID (such as `https://saml.cloud.com`), you don't need to enable scoped Entity IDs or make any changes to your existing SAML configuration. You don't need to update any settings

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> either in Citrix Cloud or in your SAML application.

Affected SAML providers

The following table lists the SAML providers that allow or limit the use of duplicate Entity IDs.

SAML Provider	Supports duplicate Entity IDs
Microsoft Entra ID (cloud)	No
ADFS (on-premises)	No
PingFederate (on-premises)	No
PingOneSSO (cloud)	No
Okta (cloud)	Yes
Duo (cloud)	Yes
OneLogin (cloud)	Yes

Affected use cases

The following table indicates whether a generic or scoped Entity ID is supported based on the SAML applications that your use case requires and whether your SAML provider supports duplicate Entity IDs.

Use case requirement	SAML provider supports duplicate Entity IDs?	Supported configuration
Only one SAML application	Yes	Generic or scoped Entity ID
Only one SAML application	No	Generic or scoped Entity ID
Two or more SAML applications	Yes	Generic or scoped Entity ID
Two or more SAML applications	No	Scoped Entity ID
store custom URL and SAML application pairs	Yes	Generic or scoped Entity ID
store custom URL and SAML application pairs	No	Scoped Entity ID
Link the same SAML application to multiple Citrix Cloud tenants	Yes	Generic Entity ID

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use case requirement	SAML provider supports duplicate Entity IDs?	Supported configuration
Link the same SAML application to multiple Citrix Cloud tenants	No	Generic Entity ID

Configure the primary SAML connection with a scoped Entity ID

In this task, you create a SAML connection in Citrix Cloud using a scoped Entity ID for the primary SAML application (SAML App 1).

1. From the Citrix Cloud menu, select **Identity and Access Management**.
2. On the **Authentication** tab, locate **SAML 2.0** and select **Connect** from the ellipsis menu.
3. When prompted to create your unique sign-in URL, enter a short URL-friendly identifier for your company (for example, `https://citrix.cloud.com/go/mycompany`) and select **Save and continue**. This identifier must be unique across Citrix Cloud.
4. Under **Configure SAML Identity Provider**, select **Configure scoped SAML Entity ID**. Citrix Cloud automtically generates scoped Entity IDs and populates the fields for Entity ID, Assertion Consumer Service, and Logout URL.
5. Under **Configure a SAML Connection to Citrix Cloud**, enter the connection details from your SAML provider.
6. Accept the default SAML attribute mappings.
7. Select **Test and Finish**.

Configure the primary SAML connection with a generic Entity ID

In this task, you create a SAML connection in Citrix Cloud using the default, generic Entity ID for the primary SAML application (SAML App 1).

1. From the Citrix Cloud menu, select **Identity and Access Management**.
2. On the **Authentication** tab, locate **SAML 2.0** and select **Connect** from the ellipsis menu.
3. When prompted to create your unique sign-in URL, enter a short URL-friendly identifier for your company (for example, `https://citrix.cloud.com/go/mycompany`) and select **Save and continue**. This identifier must be unique across Citrix Cloud.
4. Under **Configure SAML Identity Provider**, verify that **Configure scoped SAML Entity ID** is disabled.
5. Under **Configure a SAML Connection to Citrix Cloud**, enter the connection details from your SAML provider.
6. In **Service Provider SAML Metadata**, click **Download** to acquire a copy of the generic SAML metadata, if needed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Accept the default SAML attribute mappings.
8. Select **Test and Finish**.

Configure a SAML connection using Citrix® StoreFront Cloud custom domains

This section includes for configuring a SAML connection using a custom store URL with either a scoped or generic Entity ID.

The tasks in this section are applicable only if you have an existing custom store URL that you're using with SAML. If you're not using a custom store URL with SAML authentication, you can skip the tasks in this section.

For more information, refer to the following articles:

- Configure a custom domain
- Sign in to stores with SAML using custom domains

Configure a SAML connection with a store custom URL and a generic Entity ID

In this task, the **Configure scoped Entity ID** setting is disabled.

1. From the Citrix Cloud menu, select **Store Authentication**.
2. In **Custom store URL**, select **Edit** from the ellipsis menu.
3. Select **Use both [customerName].cloud.com URL and custom domain URL**.
4. Enter the generic Entity ID, SSO URL and optional SLO URL for SAML App 2 and upload the signing certificate that you downloaded earlier from your SAML provider.
5. If needed, in **Service Provider SAML Metadata for custom domain**, click **Download** to acquire a copy of the generic SAML metadata for the store custom URL SAML application.
6. Click **Save**.

Configure a SAML connection with a store custom URL and a scoped Entity ID

In this task, the **Configure scoped Entity ID** setting is enabled.

1. From the Citrix Cloud menu, select **Store Authentication**.
2. In **Custom store URL**, select **Edit** from the ellipsis menu.
3. Select **Use both [customerName].cloud.com URL and custom domain URL**.
4. Enter the scoped Entity ID, SSO URL, and optional SLO URL for SAML App 2 and upload the SAML signing certificate that you downloaded earlier from your SAML provider.
5. Click **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After you save the configuration, Citrix Cloud generates the scoped SAML metadata containing the correct GUID. If needed, you can obtain a copy of the scoped metadata for the store custom URL SAML application.

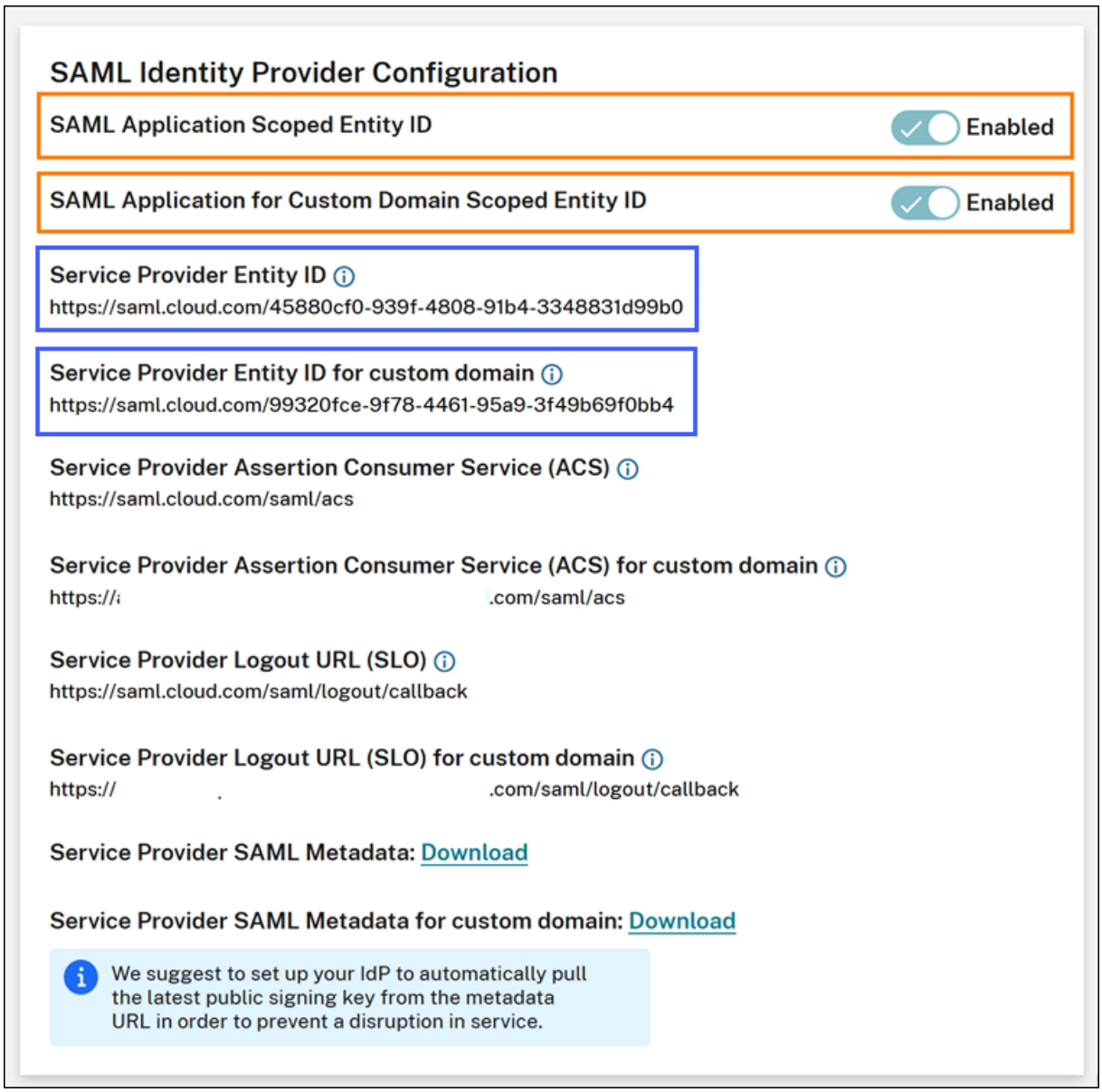
1. On the **Identity and Access Management** page, locate the SAML connection and select **View** from the ellipsis menu.
2. In **Service Provider SAML Metadata for custom domain**, click **Download**.

View the SAML configuration of both the primary and custom store URL SAML applications

When viewing the configuration details for your scoped SAML connection, Citrix Cloud displays the scoped Entity ID settings for both the primary SAML application and the store custom domain SAML application.

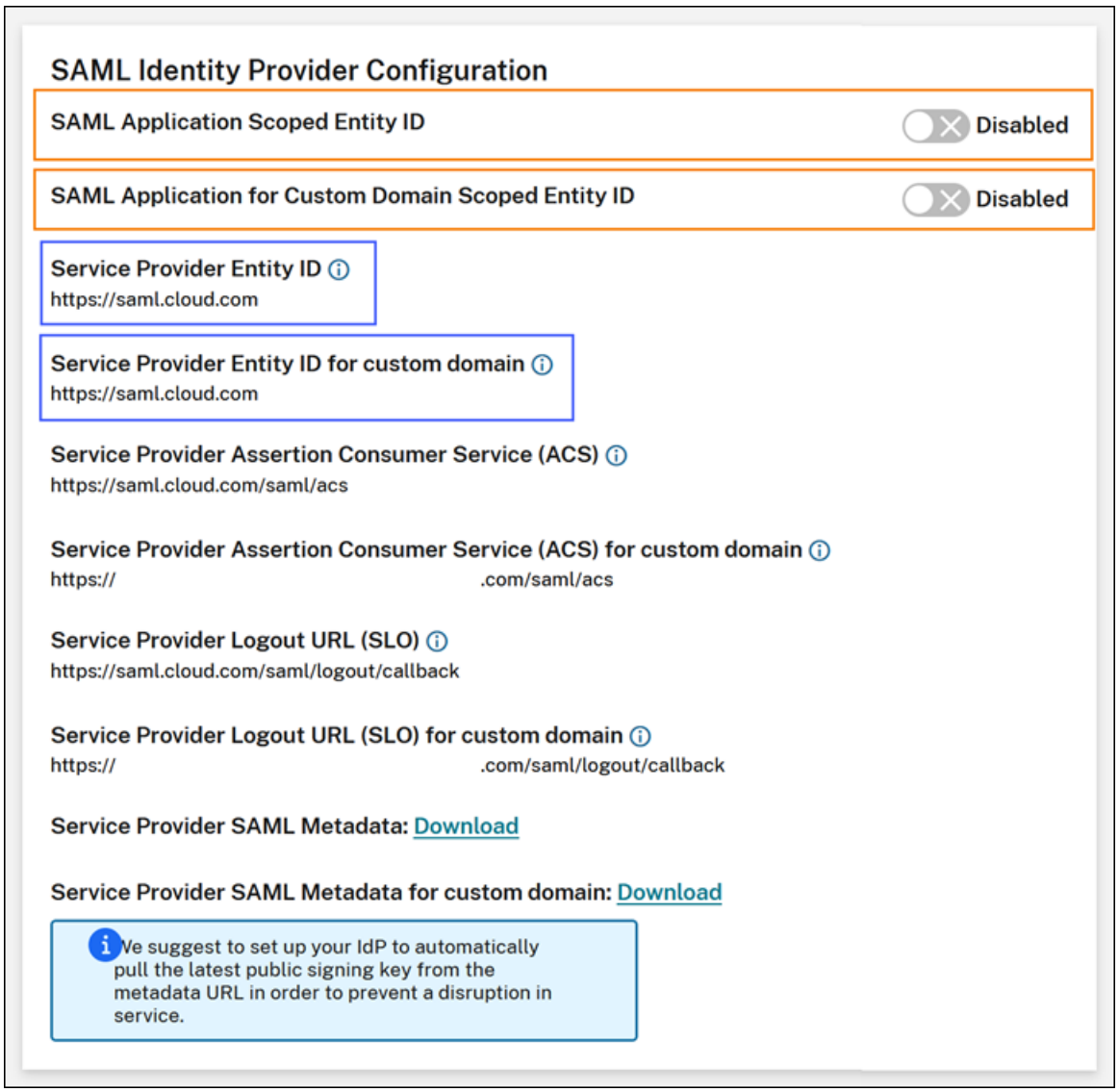
For example, when scoped Entity IDs are enabled, the **Service Provider Entity ID** and **Service Provider Entity ID for custom domain** fields contain the scoped Entity IDs that Citrix Cloud generates.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



When scoped Entity IDs are disabled, the **Service Provider Entity ID** and **Service Provider Entity ID for custom domain** fields contain the generic Entity IDs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



You can update existing SAML applications within your SAML provider by appending the scoped Entity ID to the existing Entity ID value.

SAML provider configuration with scoped Entity IDs

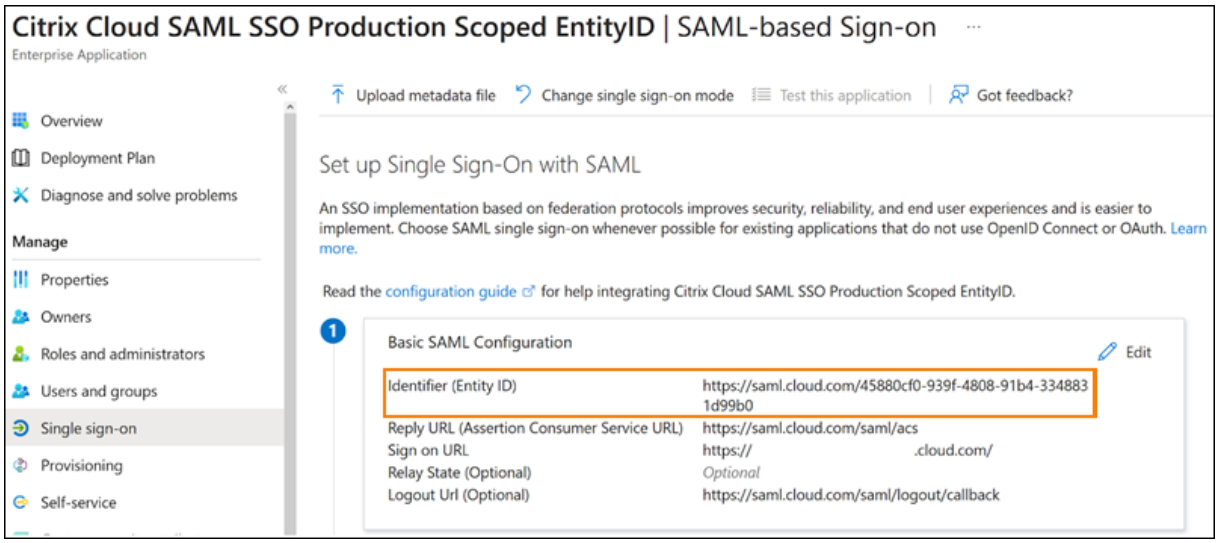
After configuring the SAML connection in Citrix Cloud with scoped Entity IDs, you can add the scoped Entity ID to your SAML provider.

This section includes configuration examples from Microsoft Entra ID and PingFederate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Entra ID SAML configuration with scoped Entity ID

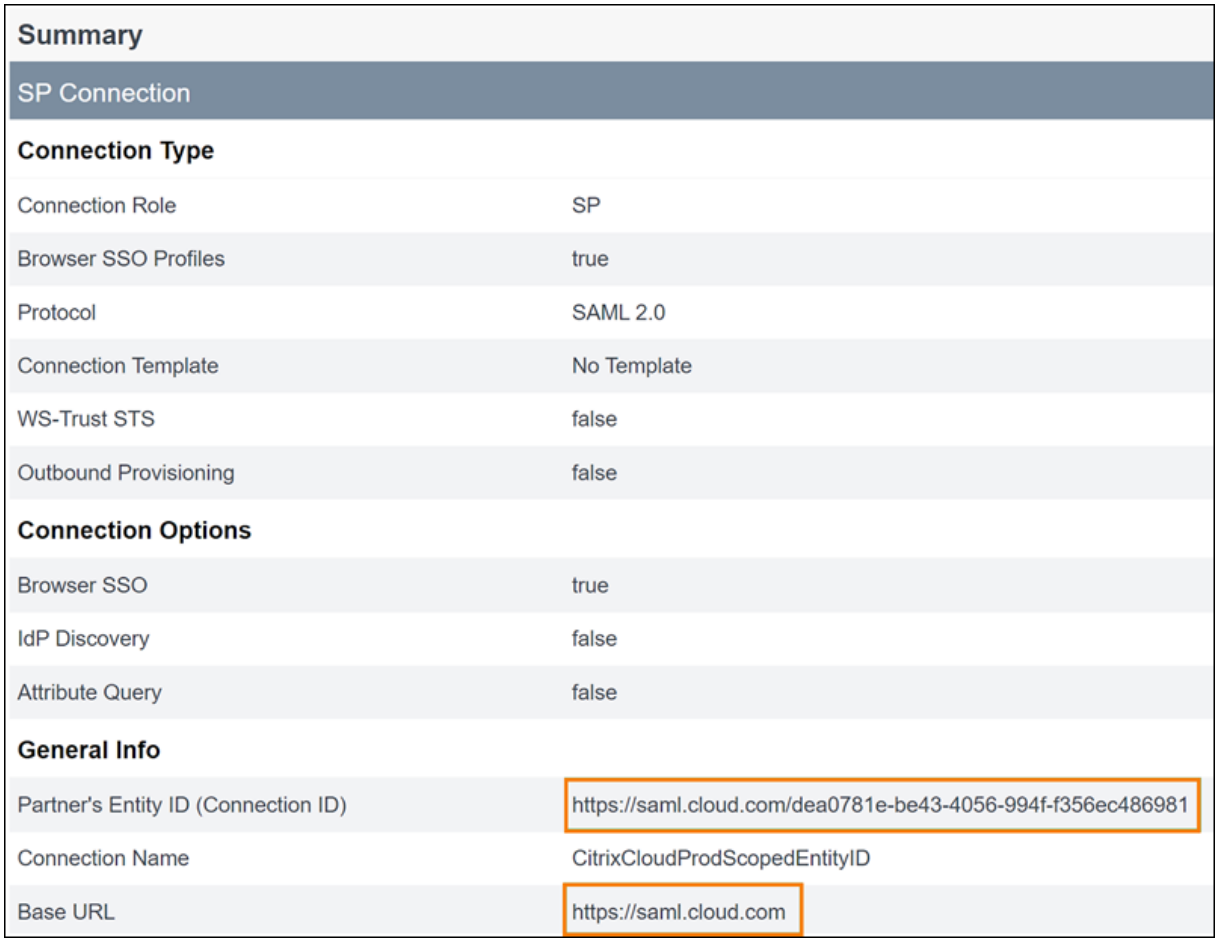
In this example, the scoped Entity ID from Citrix Cloud is entered in the **Identifier** field in Microsoft Entra ID.



PingFederate SAML configuration with scoped Entity ID

In this example, the scoped Entity ID and the generic Entity ID from Citrix Cloud are populated in the **Partner's Entity ID** field and the **Base URL** field, respectively.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Summary	
SP Connection	
Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
Connection Options	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
General Info	
Partner's Entity ID (Connection ID)	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981
Connection Name	CitrixCloudProdScopedEntityID
Base URL	https://saml.cloud.com

Troubleshooting

Citrix recommends using the SAML-tracer browser extension to troubleshoot any issues with your SAML configuration. This extension decodes Base64-encoded requests and responses into SAML XML, rendering the information human-readable. You can use the SAML-tracer extension to examine both the SSO and SLO SAML requests that Citrix Cloud (the Service Provider) generates and sends to your SAML provider (the identity provider). The extension can show whether the Entity ID scope (GUID) is included in both requests.

1. From the Extensions panel in your web browser, install and enable the SAML-tracer extension.
2. Perform a SAML sign-in and sign-out operation and capture the entire flow with the SAML-tracer extension.
3. Locate the following line within either the SAML SSO request or SLO request.

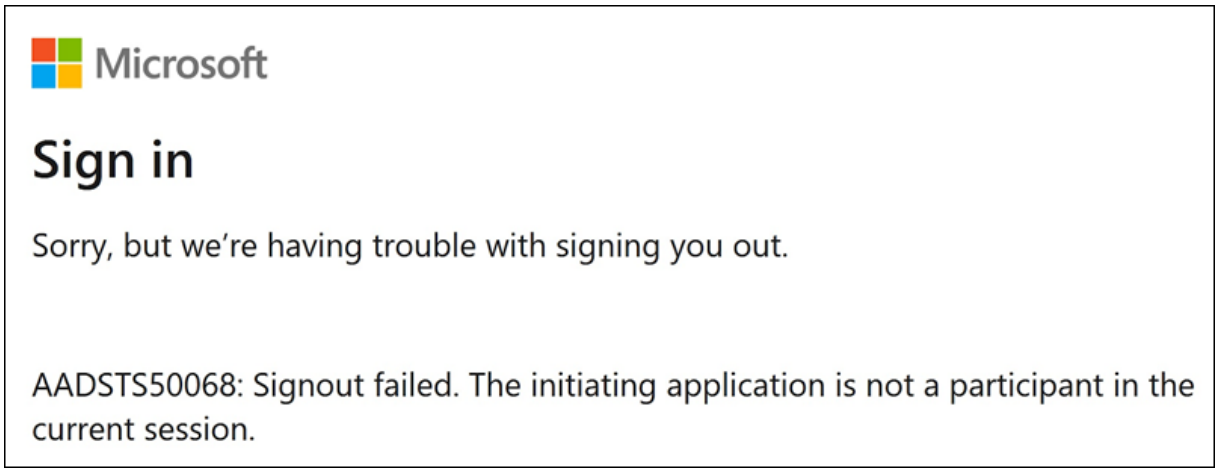
```
<saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
    https://saml.cloud.com/cfee4a86-97a8-49cf-9bb6-fd15ab075b92</
    saml:Issuer>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Verify that the Entity ID matches the configured Entity ID in your SAML provider application.
5. Verify that the scoped Entity ID is present in the **Issuer** field and verify that it's configured correctly in your SAML provider.
6. Export and save the SAML-tracer JSON output. If you're working with Citrix Support to resolve an issue, upload the output to your Citrix support case.

Microsoft Entra ID troubleshooting

Issue: Signing out of Microsoft Entra ID fails when SLO is configured. Microsoft Entra ID displays the following error to the user:



If scoped Entity IDs are enabled for the SAML connection in Citrix Cloud, the scoped Entity ID must be sent in both the SSO and SLO requests.

Cause: The scoped entity is configured but the Entity ID is missing from the SLO request. Verify the scoped Entity ID is present in the SLO request in the SAML-tracer output.

On-premises PingFederate troubleshooting

Issue: Signing in or signing out of PingFederate fails after enabling the scoped Entity ID setting.

Cause: The PingFederate administrator added the scoped Entity ID to the SP connection base URL.

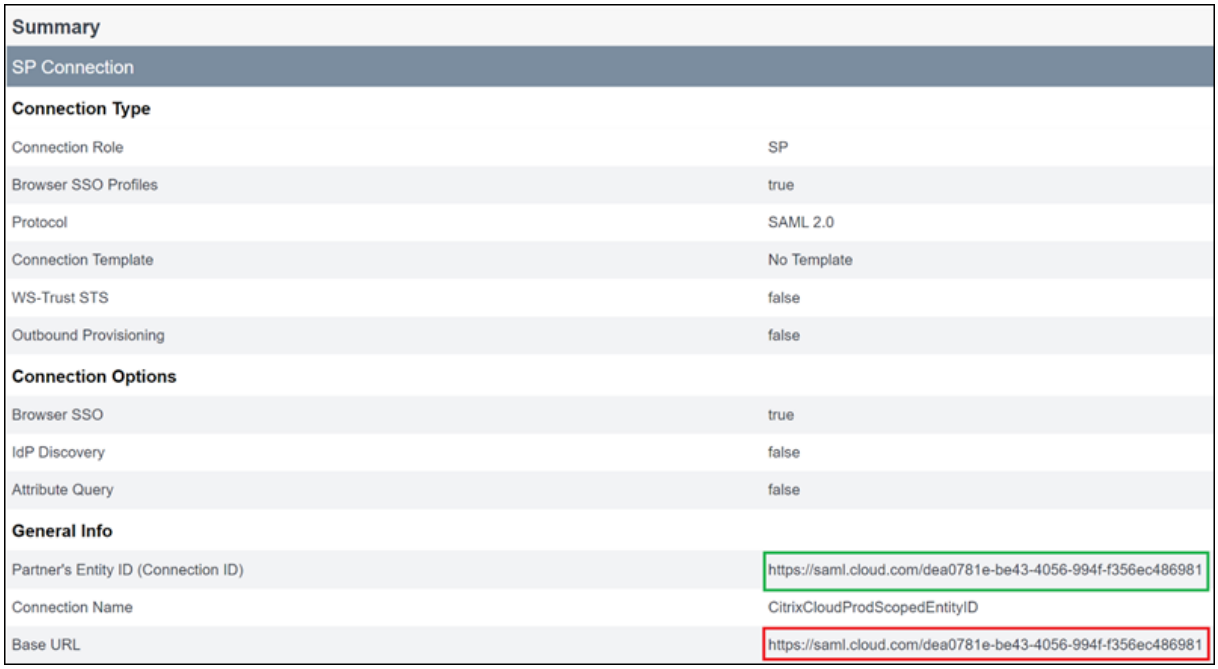
To correct this issue, add the scoped Entity ID to the **Partner's EntityID** field only. Adding the scoped Entity ID to the base URL results in a malformed SAML endpoint. If the Citrix Cloud base URL is incorrectly updated, all other SAML endpoint relative URLs that are derived from the base URL produce sign-in failures.

The following endpoints are examples of malformed Citrix Cloud SAML endpoints that might appear in the SAML-tracer output:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `https://saml.cloud.com/<GUID>/saml/acs`
- `https://saml.cloud.com/<GUID>/saml/logout/callback`

The following image shows a misconfigured PingFederate SAML application. The correctly configured field is shown in green. The incorrectly configured field is shown in red.



Summary	
SP Connection	
Connection Type	
Connection Role	SP
Browser SSO Profiles	true
Protocol	SAML 2.0
Connection Template	No Template
WS-Trust STS	false
Outbound Provisioning	false
Connection Options	
Browser SSO	true
IdP Discovery	false
Attribute Query	false
General Info	
Partner's Entity ID (Connection ID)	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981
Connection Name	CitrixCloudProdScopedEntityID
Base URL	https://saml.cloud.com/dea0781e-be43-4056-994f-f356ec486981

Sign in to stores with SAML using Multiple Custom URLs

June 22, 2026

Author:
Mark Dear

The architecture to support SAML with a store Custom URL has been simplified and updated to support multiple custom domains using **just one SAML application** configured inside your SAML IdP. Changes have been made within Citrix Cloud's authentication platform and within the store custom URL service to support up to 10 custom URLs with SAML and Conditional Authentication. Historically, it was necessary to configure one SAML application with `cloud.com` SAML endpoints, and another with SAML endpoints containing your Custom URLs. It is no longer necessary to create and maintain multiple different SAML applications to support all SAML use cases.

Advantages of the New Architecture to Support Multiple Custom URLs.

Create just 1x SAML application containing Citrix Cloud SAML endpoints matching your Citrix Cloud

© 1997–2026 Citrix Systems, Inc. All rights reserved.

region such as saml.cloud.com (US, EU and APS), saml.citrixcloud.jp (Japan) or saml.cloud.us (GOV).

Example SAML Application Endpoints:

- Entity ID https://saml.cloud.com or https://saml.cloud.com/<guid>
- Assertion Consumer Service (SSO): https://saml.cloud.com/saml/acs
- Logout (SLO): https://saml.cloud.com/saml/logout/callback

Supported SAML Logon Use Cases:

- Logon to store using either of your Store URLs with a single SAML application
  store.cloud.com
  OR
  store.mycustomer.com
- Logon to Citrix Cloud using SAML for admin access also uses the same generic SAML application.
- A single SAML application inside your IdP can now support up to 10 store custom URLs without the need to create and maintain multiple different SAML applications. Citrix Cloud no longer needs additional SAML applications with custom URL SAML endpoints to support all SAML use cases.

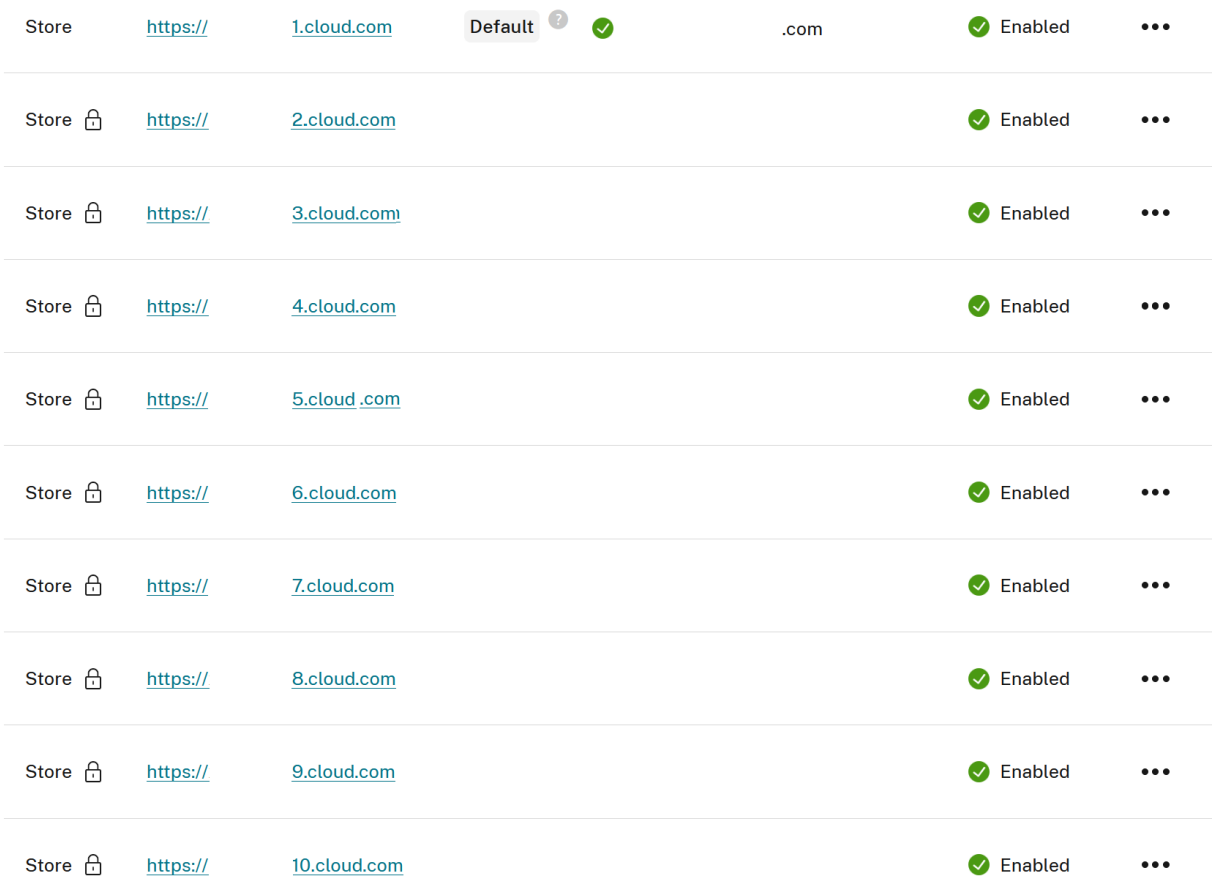
FAQ

What is the multi custom URL feature in stores?

Historically, Citrix Cloud only supported a single custom URL linked to the first Store cloud.com URL. Now a custom URL can be configured for each of your Store cloud.com URLs up to a maximum of 10. These form pairs of URLs where each custom URL is a CNAME in DNS for its corresponding cloud.com URL.

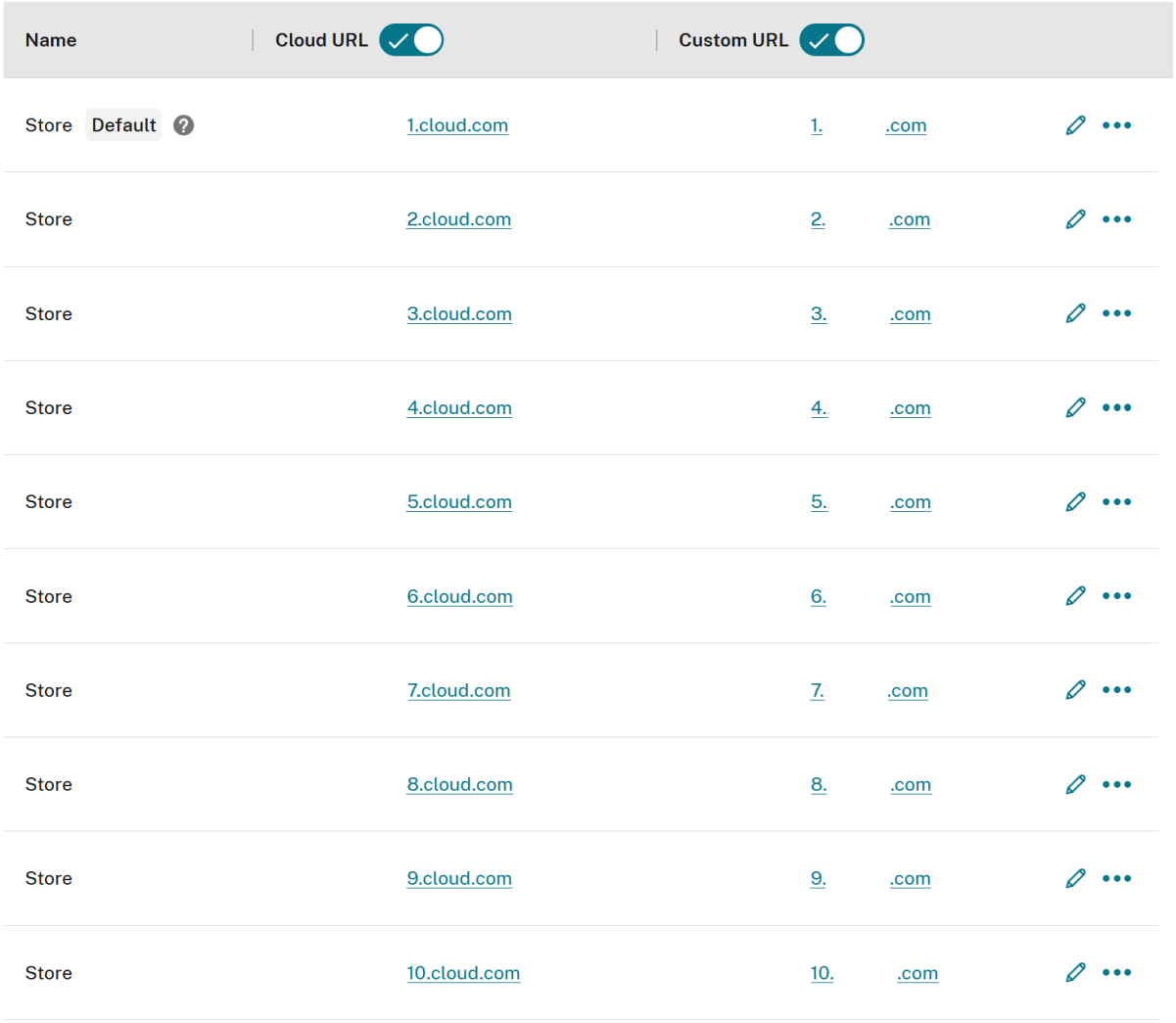
Before the release of multi custom URL, only 1 custom URL associated with the primary cloud.com store URL was supported within **StoreFront Cloud > Access**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



StoreFront Cloud > Access after release of multi custom URL. 1 –10 custom URLs are now supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



How do I decide if I need to migrate my custom URL or not?

This is dictated by the combination of authentication features you wish to use in Citrix Cloud and store, the logon scenarios you currently have and your current SAML solution. Use the table below for guidance.

SAML Logon Scenario	Unmigrated Custom URL	Migrated Custom URLs
Logon to store with 1x SAML App with **custom URL endpoints**	Supported (1 Custom URL)	Not Supported (1–10 Custom URLs)
Logon to store with 2x SAML Apps	Supported (1 Custom URL)	Supported (1–10 Custom URLs)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SAML Logon Scenario	Unmigrated Custom URL	Migrated Custom URLs
Citrix Cloud admin logon with SAML 1x App with **`cloud.com` URL endpoints**	Supported	Supported
Citrix Cloud admin logon with 2x SAML Apps	Supported	Supported
Citrix Cloud admin logon with SAML 1x App with **custom URL endpoints**	Unsupported	Unsupported
Conditional Authentication Policy using store URL and SAML end users enter a **`cloud.com` URL** into the browser or Citrix Workspace app	Supported	Supported
Conditional Authentication Policy using store URL and SAML end users enter a **custom URL** into the browser or Citrix Workspace app	Unsupported (1 Custom URL)	Supported (1–10 URLs)

Why did the SAML and Custom URL architecture need to change to support multiple custom URLs?

Scalability. The introduction of multi custom URLs within Citrix Cloud means that the legacy architecture requiring a SAML app per custom URL does not scale and is impractical for both Citrix Cloud and IdP administrators.

Legacy SAML custom URL requirements:

- 1 x `cloud.com` SAML application for Citrix Cloud admin logon using SAML.
- 1 x SAML application per custom URL.

IdP Configuration Complexity. It was necessary for each SAML application to be configured identically apart from their SAML endpoints leading to additional work within your SAML IdP. This increased deployment and configuration complexity. The new multi custom domain architecture eliminates the need to do this and only one SAML application is needed inside your IdP to support 1 –10 custom URLs.

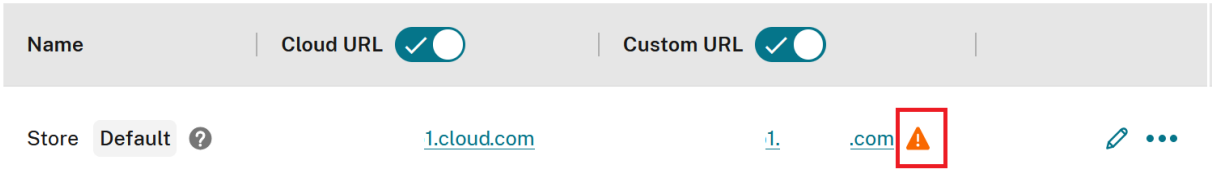
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Ongoing IdP Maintenance Tasks. Configuring and maintaining multiple SAML applications and having to perform ongoing yearly certificate rotation tasks on multiple SAML applications is labour intensive and undesirable for both Citrix Cloud and IdP administrators. This problem only increases for administrators as more custom domains are added and more SAML applications are required. The new architecture eliminates this maintenance problem as only one SAML application is needed for all SAML and Custom URL use cases.

Why is Citrix asking me to migrate from my current custom URL SAML solution to the new simpler solution?

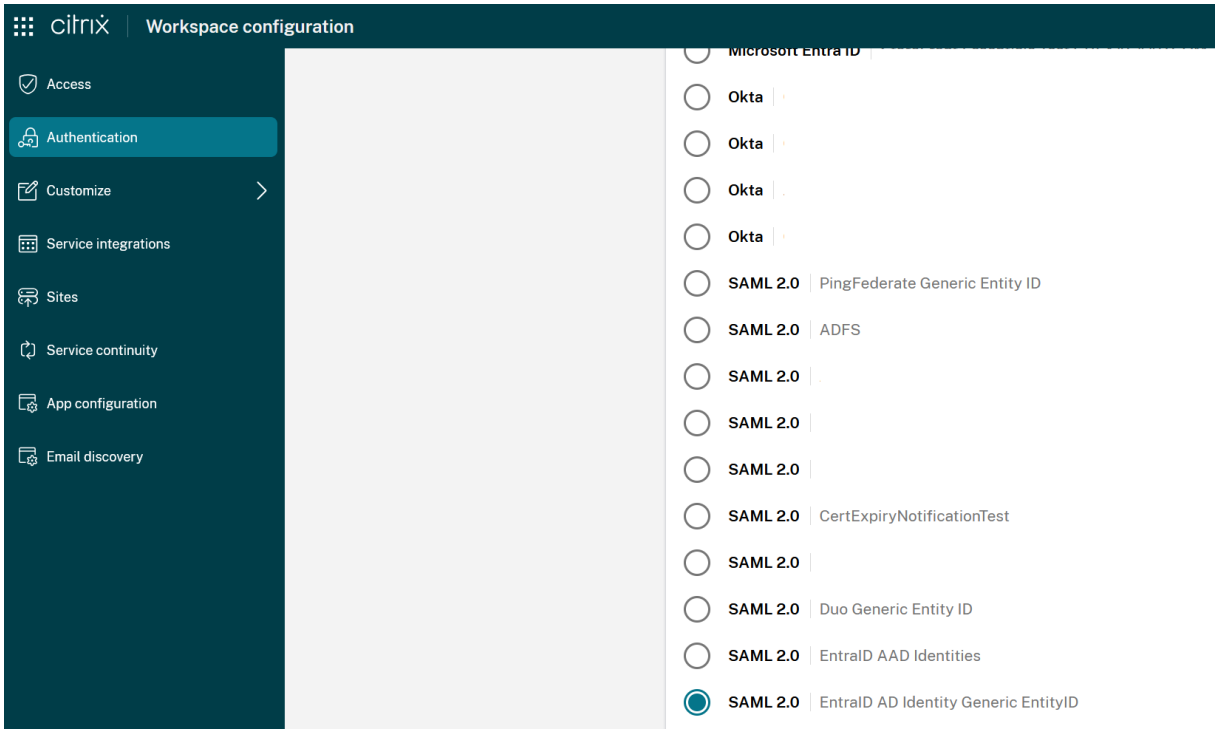
The use of both the Multi Custom URL feature and the use of Conditional Authentication with custom URLs, requires legacy 1x and 2x SAML application configurations to be updated and migrated. This document contains instructions on how to perform migrations for customers using either of the legacy 1x or 2x SAML application solutions.

This warning inside **StoreFront Cloud > Access** indicates you have one or more custom URLs in need of migration.



This warning will only appear if you have enabled either SAML or Conditional Authentication within **StoreFront Cloud > Authentication**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Is the SAML IdP configuration the same to support all my new custom URLs up to a maximum of 10?

Yes. Configure your SAML application identically if your intent to use just one, or more than one custom URL to access store.

Is Conditional Authentication now supported with multiple SAML apps and multiple custom domains?

Yes. This is a common scenario that many large enterprises will wish to use. It has always been possible to create Conditional Authentication policies that resolve to different SAML applications using any of your 1-10 `cloud.com` URLs. Now each of your `cloud.com` URLs can have its own custom URL (pairs of URLs).

For detailed instructions on switching between different IdPs based on store URL used by your end users, refer to this article Conditional Authentication article.

Will my legacy unmigrated SAML connections continue to function if I don't wish to use multiple custom URLs or to use Conditional Authentication with a custom URL and SAML?

Yes. Backwards compatibility with existing legacy 1x and 2x SAML app solutions will be maintained, and existing SAML application solutions will continue to function and be supported. You will NOT be

© 1997–2026 Citrix Systems, Inc. All rights reserved.

able to use custom URLs with SAML or with Conditional Authentication if any of your custom URLs remain in an unmigrated state.

If I onboard new custom URLs after the release of the multi custom URL feature do I need to perform any migrations on these new URLs?

No. All newly onboarded custom domains after the multi custom URL feature has been released will support the new architecture and do not need to be migrated. Migration only applies to custom URL configurations that were created before the release of the multi custom URL feature. This is typically for the first and only custom URL you have configured within your Citrix Cloud tenant which existed before support for multiple custom URLs was introduced.

Migrating Legacy Custom URLs and SAML Configurations

It is required you read the entire Legacy Custom URL SAML Configurations section so you understand your current custom URL and SAML configuration and whether you are currently operating with a **1x or 2x SAML application** solution before taking any migration actions. Migration actions should be conducted in a planned maintenance window and testing conducted after migration to ensure SAML logons have not been impacted before you remove any obsolete SAML applications from your IdP.

> **Important:**
>
> If your legacy SAML configuration in both Citrix Cloud and your SAML IdP does not exactly match either of the 1x or 2x SAML app solutions described in the Legacy Custom URL SAML Configurations section in this document, you are in an unsupported state.

What do I have to do to migrate from my current 2x SAML application Custom URL solution to the new simpler solution?

1. Citrix Cloud administrators must coordinate with IdP administrators to make the necessary changes within both Citrix Cloud's custom URL service and within your SAML IdP.
2. Within your SAML IdP verify the existence and configuration of both the primary and secondary SAML applications. This is different for every SAML IdP such as EntraID, Okta, Duo, PingFederate ect.
3. Do not change the existing primary SAML application Citrix Cloud SAML endpoints. This is the SAML application that appears inside **Identity and Access Management > Authentication** and will be used for all SAML logon use cases after migration of the custom URL.

   Primary Application Example from Citrix Cloud Commercial US, EU and APS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

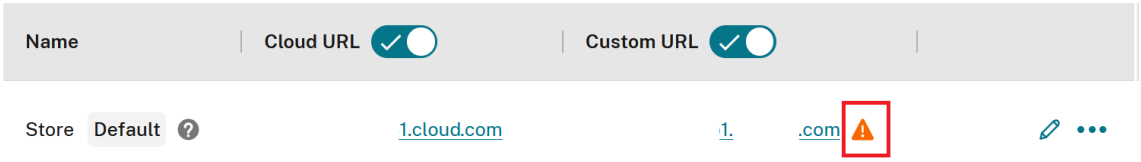
- Entity ID: `https://saml.cloud.com` or `https://saml.cloud.com/<guid>`
- Assertion Consumer Service (SSO): `https://saml.cloud.com/saml/acs`
- Logout (SLO): `https://saml.cloud.com/saml/logout/callback`

4. Identify this obsolete secondary SAML application. This SAML application's configuration is specified inside the **StoreFront Cloud > Access** menu.

   Secondary Application Example

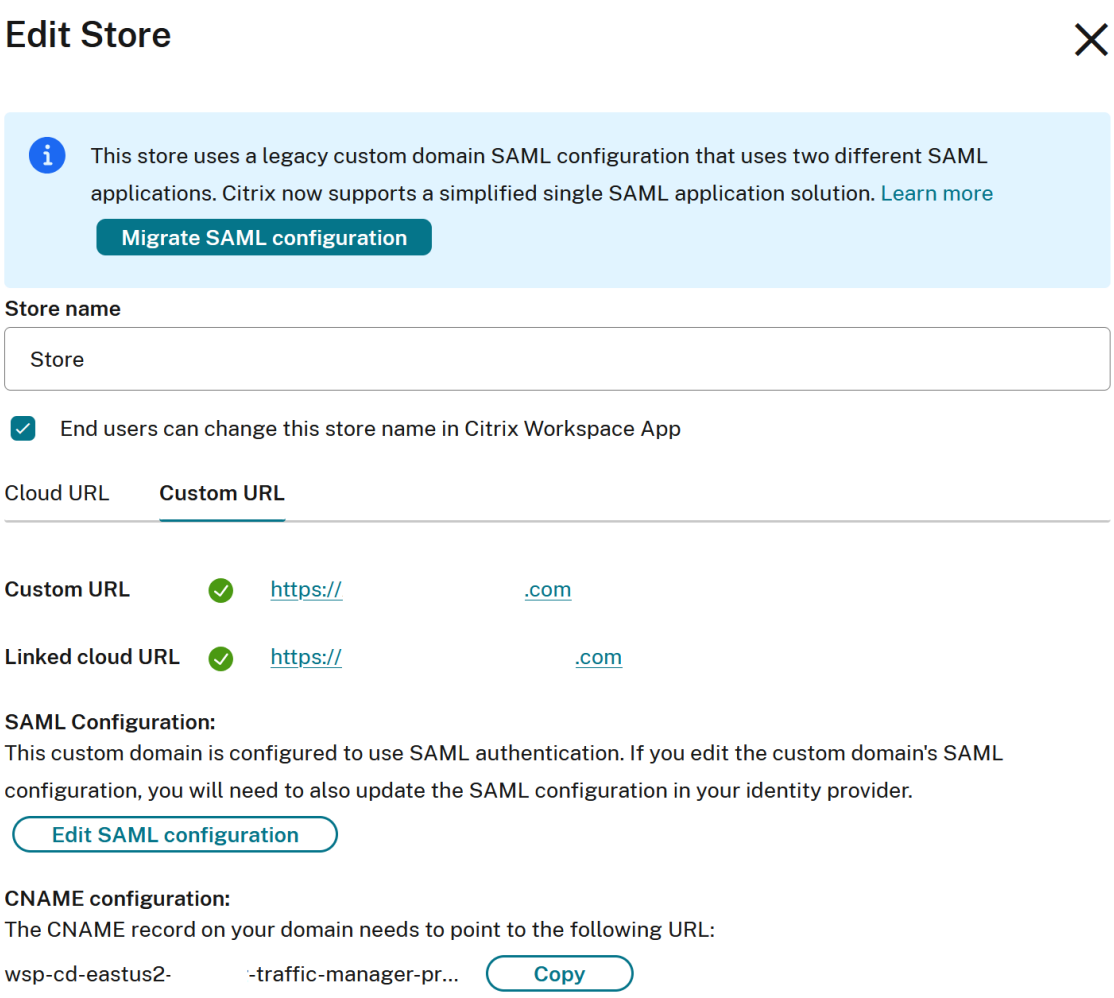
   - Entity ID: `https://saml.cloud.com` or `https://saml.cloud.com/<guid>`
   - Assertion Consumer Service (SSO): `https://workspaces.mycompany.com/saml/acs`
   - Logout (SLO): `https://workspaces.mycompany.com/saml/logout/callback`

5. Navigate to **StoreFront Cloud > Access** and click on the **warning icon** to open the migration UI.



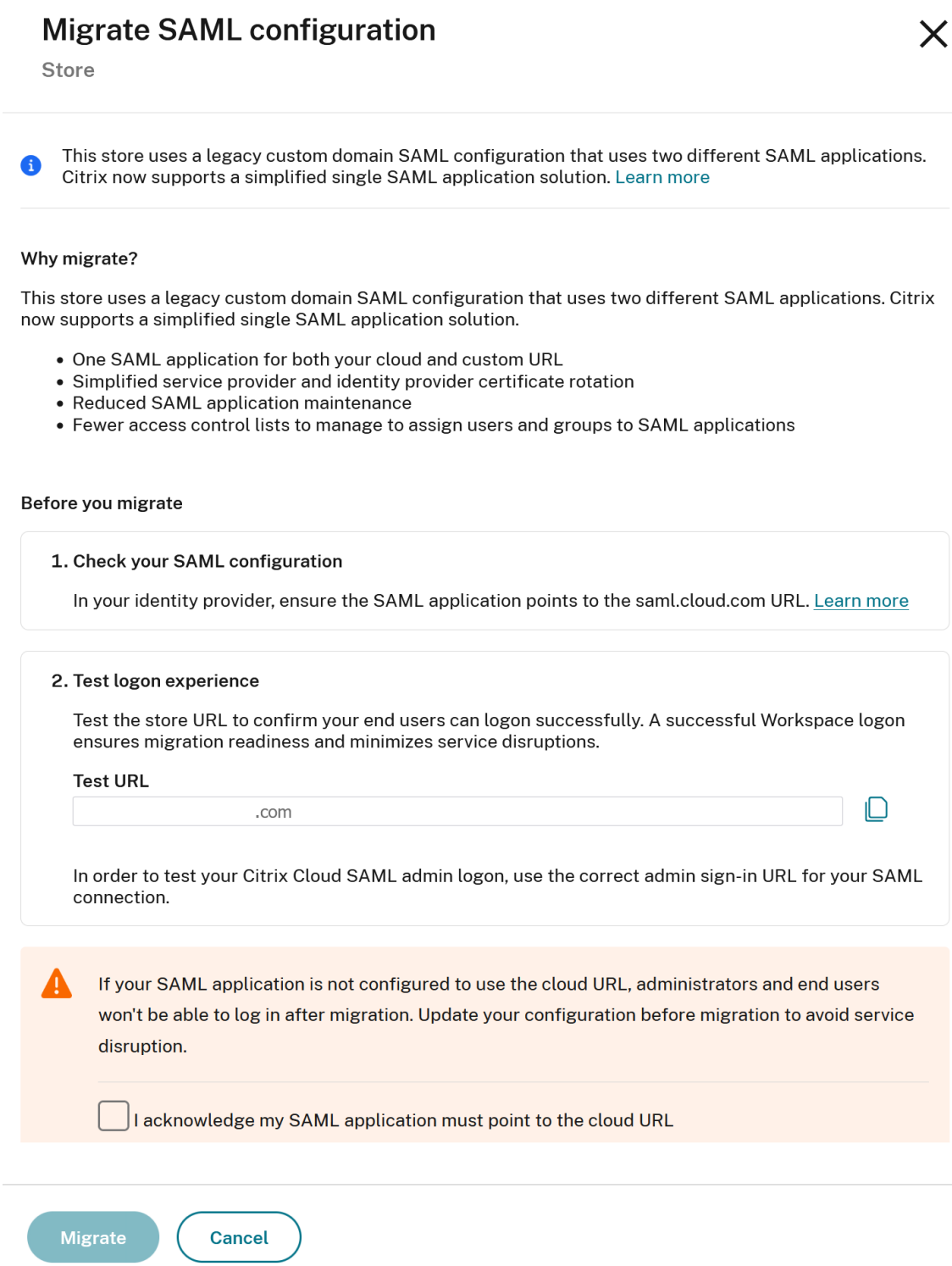
6. Click the **Migrate SAML Configuration** button shown below.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. Accept the warning and perform the migration from within this UI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. Click **Migrate**.

> **Important:**
>
> The migration updates legacy backend data within the store Custom URL service. This is

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> an irreversible operation on the store custom URL service record and cannot be reverted once performed.

9. The warning icon shown in step 4 next to your custom URL should disappear once migration has been successful. This indicates the backend data within the store Custom URL service has been updated.

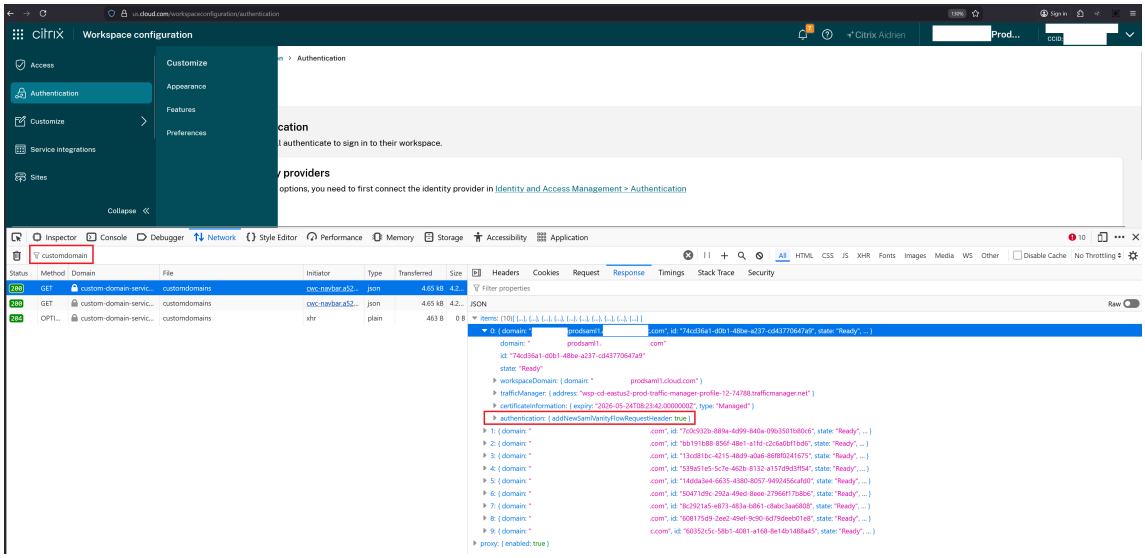
   Verify all your SAML logon use cases are still successful after migration.

   - Test the SAML logon to store using any `cloud.com` URLs. This uses the Primary SAML Application.
   - Test the SAML logon to store using all your custom URLs. This previously used the Secondary SAML Application **BEFORE** migration but now uses the unchanged Primary SAML Application.
   - Test the SAML logon to Citrix Cloud using your admin sign in URL using any AD admin users and groups that were configured before migration. This uses the Primary SAML Application.

10. Verify the backend store Custom URL service data was successfully updated.

    For example using FireFox Developer Tools.

    Open developer tools on your browser by pressing F12 on your keyboard and then navigate to **StoreFront Cloud > Access** from any other page in the Citrix Cloud UI with developer tools already running. This will capture all REST API calls made by the Citrix Cloud console to return a list of Custom URLs.



    Enter `customdomain` into the network search dialogue to filter for the correct REST API calls.

    Locate this REST API call:
    `GET https://custom-domain-service.us.wsp.cloud.com/services/`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
custom-domain-service/customers/<CCID>/stores/<storeID>/customdomains
```

Migrated custom URL objects will contain this additional data.

```
"addNewSamlVanityFlowRequestHeader":true
```

Example Custom URL Object:

```
"items": [
    {

        "domain": "stores.mycompany.com",
        "id": "74cd36a1-d0b1-48be-a237-cd43770647a9",
        "state": "Ready",
        "workspaceDomain": {

            "domain": "stores.cloud.com"
         }
 ,
        "trafficManager": {

            "address": "wsp-cd-eastus2-prod-traffic-manager-
               profile-12-74788.trafficmanager.net"
         }
 ,
        "certificateInformation": {

            "expiry": "2026-05-24T08:23:42.0000000Z",
            "type": "Managed"
         }
 ,
        "authentication": {

            "addNewSamlVanityFlowRequestHeader": true
         }

     }

]
```

11. Delete the secondary application from within your SAML IdP that uses custom URL SAML endpoints. The secondary SAML application is no longer used during the SAML logon flow.

> **Important:**
>
> Only delete the secondary SAML application once you have proven the migration has been successful and all the required SAML logon scenarios have been tested.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What do I have to do to migrate from my current 1x SAML application Custom URL solution to the new simpler solution?

1. Citrix Cloud administrators must coordinate with IdP administrators to make the necessary changes within both Citrix Cloud's custom URL service and within your SAML IdP.
2. Within your SAML IdP verify the existence and configuration of a custom URL SAML application. You should only have one SAML application configured inside your SAML IdP. This is different for every SAML IdP such as EntraID, Okta, Duo, PingFederate ect…

   Your existing primary SAML application's Citrix Cloud SAML endpoints should look like this example.

   Primary Application Example

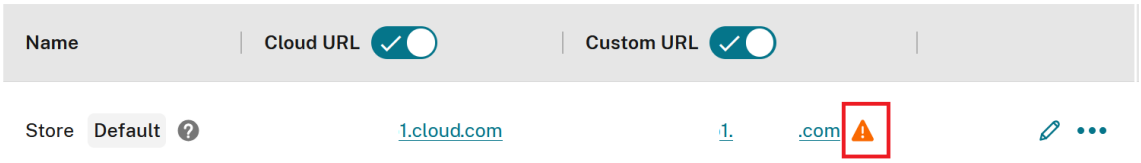
   - Entity ID: `https://saml.cloud.com` or `https://saml.cloud.com/<guid>`
   - Assertion Consumer Service (SSO): `https://workspaces.mycompany.com/saml/acs`
   - Logout (SLO): `https://workspaces.mycompany.com/saml/logout/callback`
3. Raise a support case and contact Citrix Support and Engineering to schedule assistance with migrating your custom domain. Citrix engineering will migrate your custom URL on your behalf after a review of your SAML configuration.
4. Step 3 must be completed before you can safely make changes to your SAML application. Update your existing **primary SAML application's** Citrix Cloud SAML endpoints to look like this example.

   > **Important:**
   >
   > Do NOT update or alter the existing EntityID SAML endpoint on your **primary** SAML application. There is no need to change this. Only the ACS and logout SAML endpoints need to be updated.

   Primary Application Example

   - Entity ID: `https://saml.cloud.com` or `https://saml.cloud.com/<guid>` (Do not change)
   - Assertion Consumer Service (SSO): `https://saml.cloud.com/saml/acs` (Update)
   - Logout (SLO): `https://saml.cloud.com/saml/logout/callback` (Update)
5. Navigate to **StoreFront Cloud > Access** and click on the **warning icon** to open the migration UI.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. The warning icon shown in step 4 next to your custom URL should disappear once Citrix support and engineering have completed the migration. This indicates the backend data within the store Custom URL service has been successfully updated.
7. Test the SAML logon to store using all your custom URLs (previously used the Secondary SAML Application before migration).

    - Test the SAML logon to store using any `cloud.com` URLs (continues to use the Primary SAML Application).
    - Test the SAML logon to store using all your custom URLs (previously used the Secondary SAML Application before migration).

Legacy Custom URL SAML Configurations

To determine whether you have deployed either a **1x or 2x SAML application** solution in your Citrix Cloud environment, identify which combination of SAML sign-in scenarios you currently use and examine your current SAML applications inside your SAML IdP.

The following sign-in scenarios share the same SAML application (SAML App 1) by default:

- SAML authentication where the store sign-in URL for your region (`cloud.com`, `citrixcloud.jp`, `cloud.us`) is configured in your SAML provider as the SP Entity ID.
- SAML authentication for Citrix Cloud using your unique sign-in URL (for example, `https://citrix.cloud.com/go/mycompany`). In this scenario, administrators are authenticated to Citrix Cloud using SAML, based on their Active Directory (AD) group membership.

Adding SAML authentication for users through a custom domain (for example, `https://workspaces.mycompany.com`) that you configure in Citrix® StoreFront Cloud requires a second SAML application (SAML App 2).

> **Note:**
>
> Adding a custom URL and configuring SAML will take up to 24 hours for provisioning in Citrix Cloud.

The following table lists the supported combinations of SAML sign-in scenarios and the required SAML apps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Sign in to store with store URL	Sign in to store with custom domain URL	Sign in to Citrix Cloud using SAML sign-in URL	SAML App 1 required?	SAML App 2 required?
Yes	No	No	Yes - Use cloud.com SAML endpoints	No
No	Yes	No	Yes - Use custom domain SAML endpoints	No
No	No	Yes	Yes - Use cloud.com SAML endpoints	No
Yes	No	Yes	Yes - Use cloud.com SAML endpoints	No
No	No	Yes	Yes - Use the cloud.com SAML endpoints	Yes - Use custom domain SAML endpoints
Yes	Yes	Yes	Yes - Use cloud.com SAML endpoints	Yes - Use custom domain SAML endpoints

1x SAML Application Configuration (Legacy SAML Config)

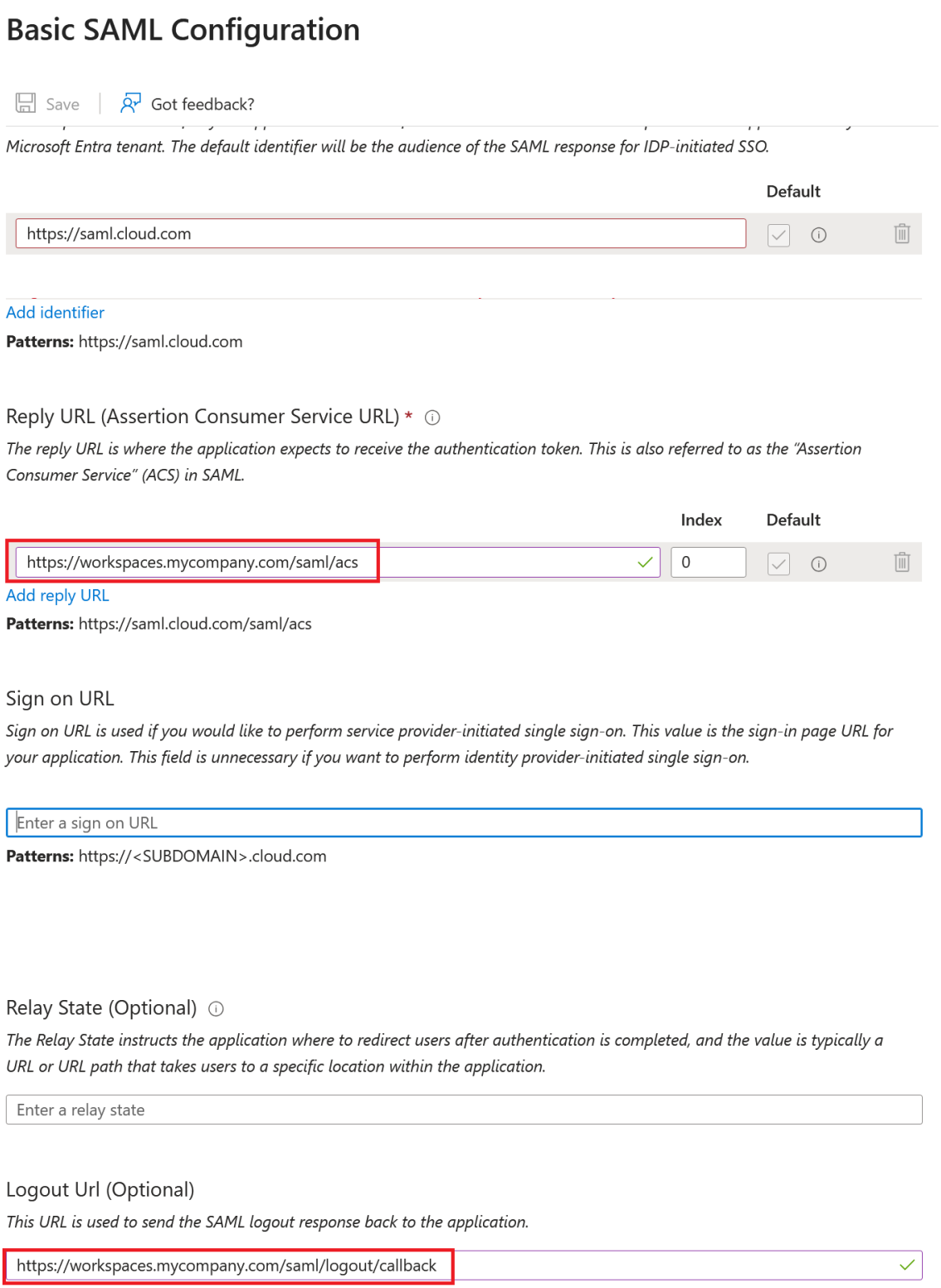
1. In Citrix Cloud, you configured a custom URL inside **StoreFront Cloud > Access**.
2. In your SAML provider's management console, you configured **1x SAML application** using the store custom URL as the SP endpoints.

   Example Legacy Custom URL SAML Application Endpoints

   - Entity ID: `https://saml.cloud.com` or `https://saml.cloud.com/<guid>`
   - Assertion Consumer Service (SSO): `https://workspaces.mycompany.com/saml/acs`
   - Logout (SLO): `https://workspaces.mycompany.com/saml/logout/callback`

   The following example illustrates the Custom URL SAML endpoint configuration for Entra ID:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The following example illustrates the Custom URL SAML endpoint configuration for Okta, where Audience Restriction contains the Entity ID value:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. You selected **Use only the custom domain** within **StoreFront Cloud > Access > Edit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Edit domain

This is an alternate URL that can be used to access Workspace.

Remember:

- You will need to distribute the new workspace URL to your subscribers.
- You will need to manually update Citrix Workspace apps to the new workspace URL.
- If you are using Okta or Netscaler as your identity provider, you will need to add this domain as the redirect URL on your side.

Configure Custom Domain SAML Identity Provider

Configure scoped SAML Entity ID

Enabled

Enabling this feature will generate a unique ID for this SAML connection. You should enable this feature if your SAML provider does not allow creation of multiple SAML apps with the same Entity ID. Learn More

Service Provider Entity ID

https://saml.cloud.com/a6aad814- 106378

Service Provider Assertion Consumer Service (ACS)

https:// .com/saml/acs

Service Provider Logout URL (SLO)

https:// .com/saml/logout/callback

Service Provider SAML Metadata: Download

We suggest that you set up your IdP to automatically pull the latest public signing key from the metadata URL in order to prevent a disruption in service.
Learn more

Configure SAML Connection to Citrix Cloud for Custom Domain:

Select the preferred configuration for SAML authentication. Changes may take up to 10 minutes to go into effect.

- ○ Use both .cloud.com URL and custom domain URL
- ◉ **Use only the custom domain URL**

1. Download the custom domain SAML metadata.
2. Update the existing SAML identity-provider application configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2 x SAML Application Configuration (Legacy SAML Config)

1. In Citrix Cloud you configured a custom domain inside **StoreFront Cloud > Access**.
2. Within your SAML provider's management console, you configured **2x SAML applications**.
3. Within the **primary SAML application**, you configured the following cloud.com SP endpoints:

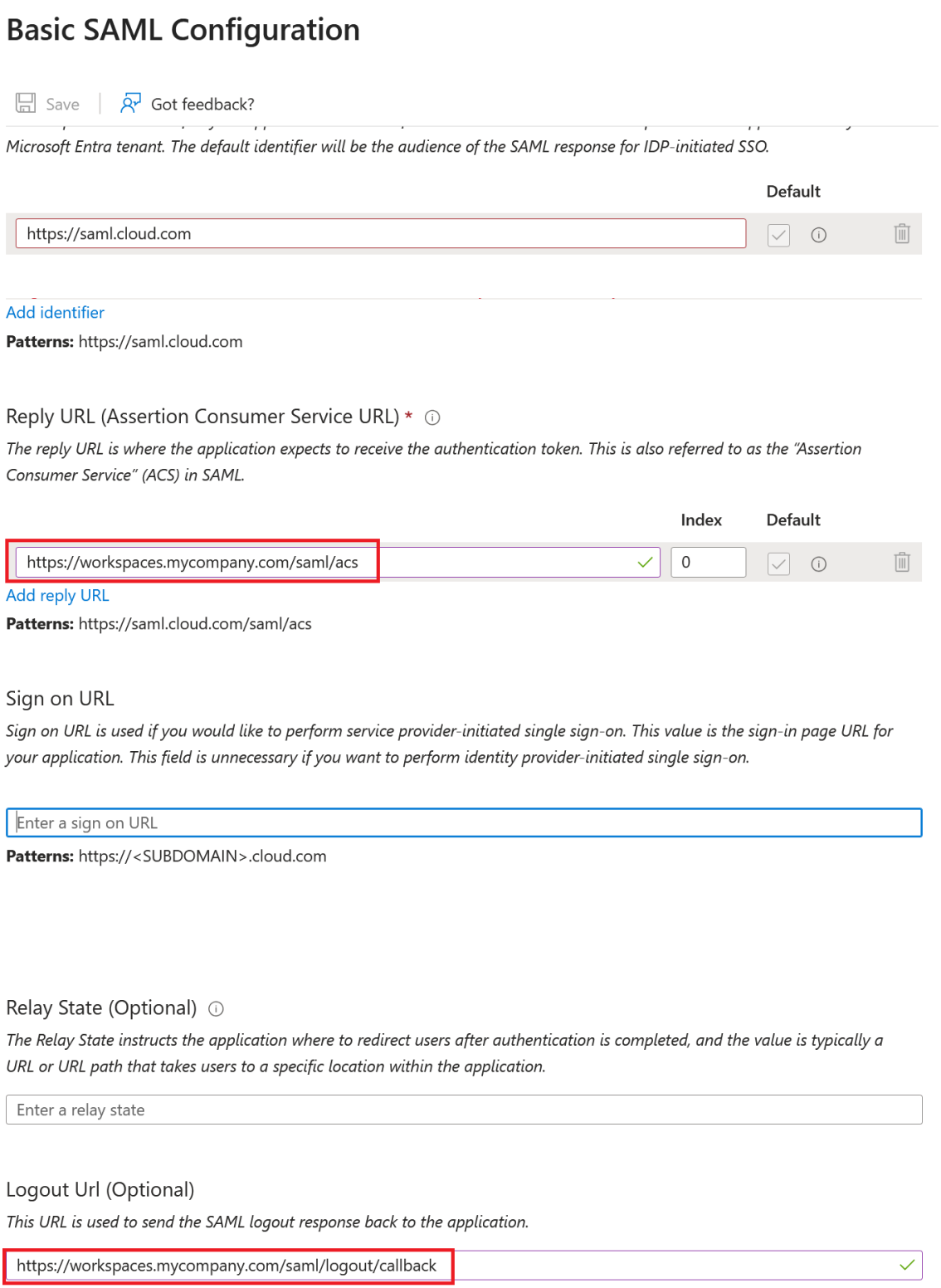
   - Entity ID: `https://saml.cloud.com` or `https://saml.cloud.com/<guid>`
   - Assertion Consumer Service (SSO): `https://saml.cloud.com/saml/acs`
   - Logout (SLO): `https://saml.cloud.com/saml/logout/callback`

   The following example shows this endpoint configuration in the Okta management console:



   The following example shows this Service Provider endpoint configuration in the Entra ID management console:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Within the **secondary SAML application**, you configured the following store custom domain SP endpoints.

    - Entity ID: `https://saml.cloud.com`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

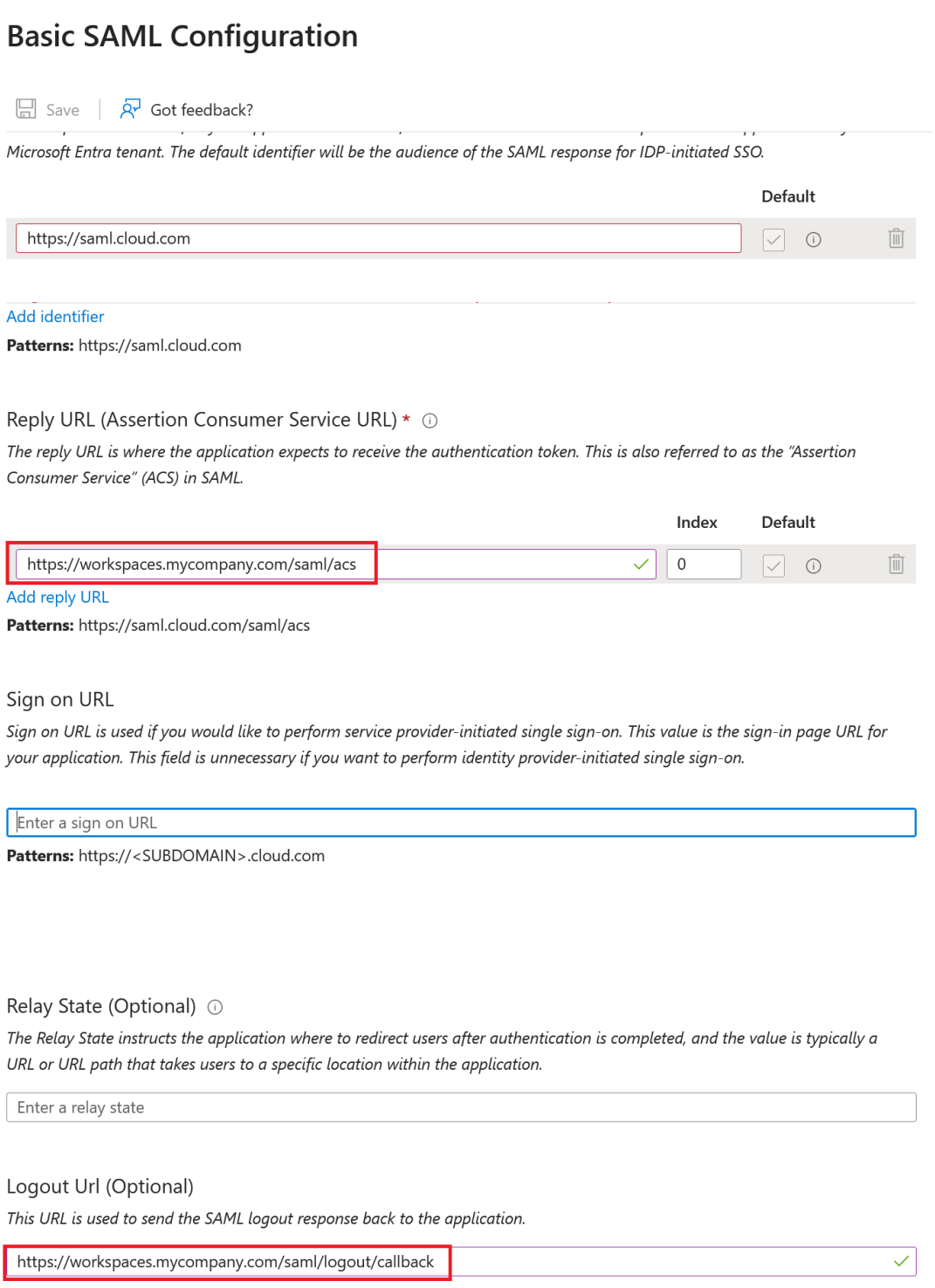
- Assertion Consumer Service (SSO): `https://workspaces.mycompany.com/saml/acs`
- Logout (SLO): `https://workspaces.mycompany.com/saml/logout/callback`

  The following example shows this Service Provider endpoint configuration in the Okta console.



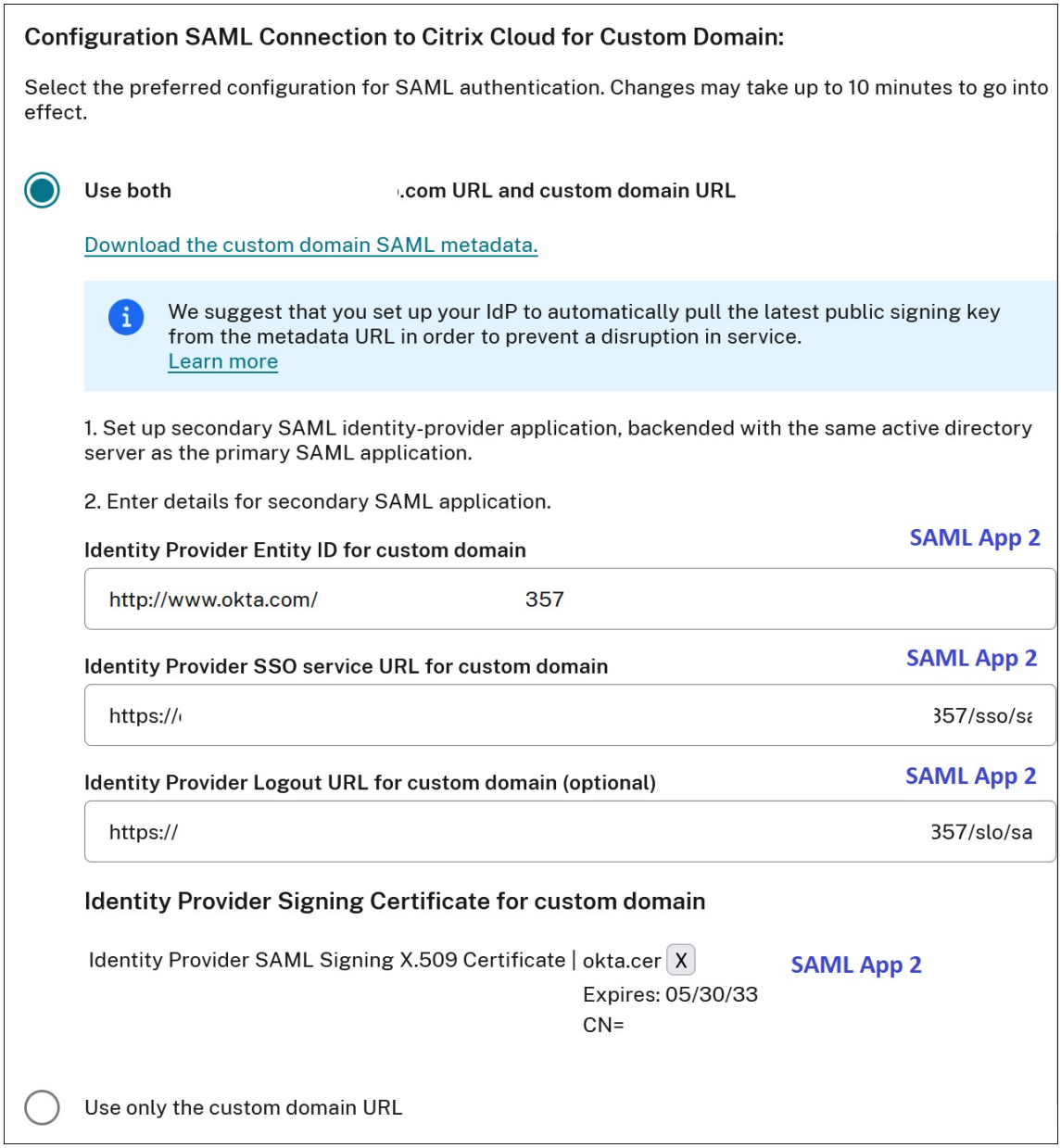
- The following example shows this Service Provider endpoint configuration in the **Entra ID** console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



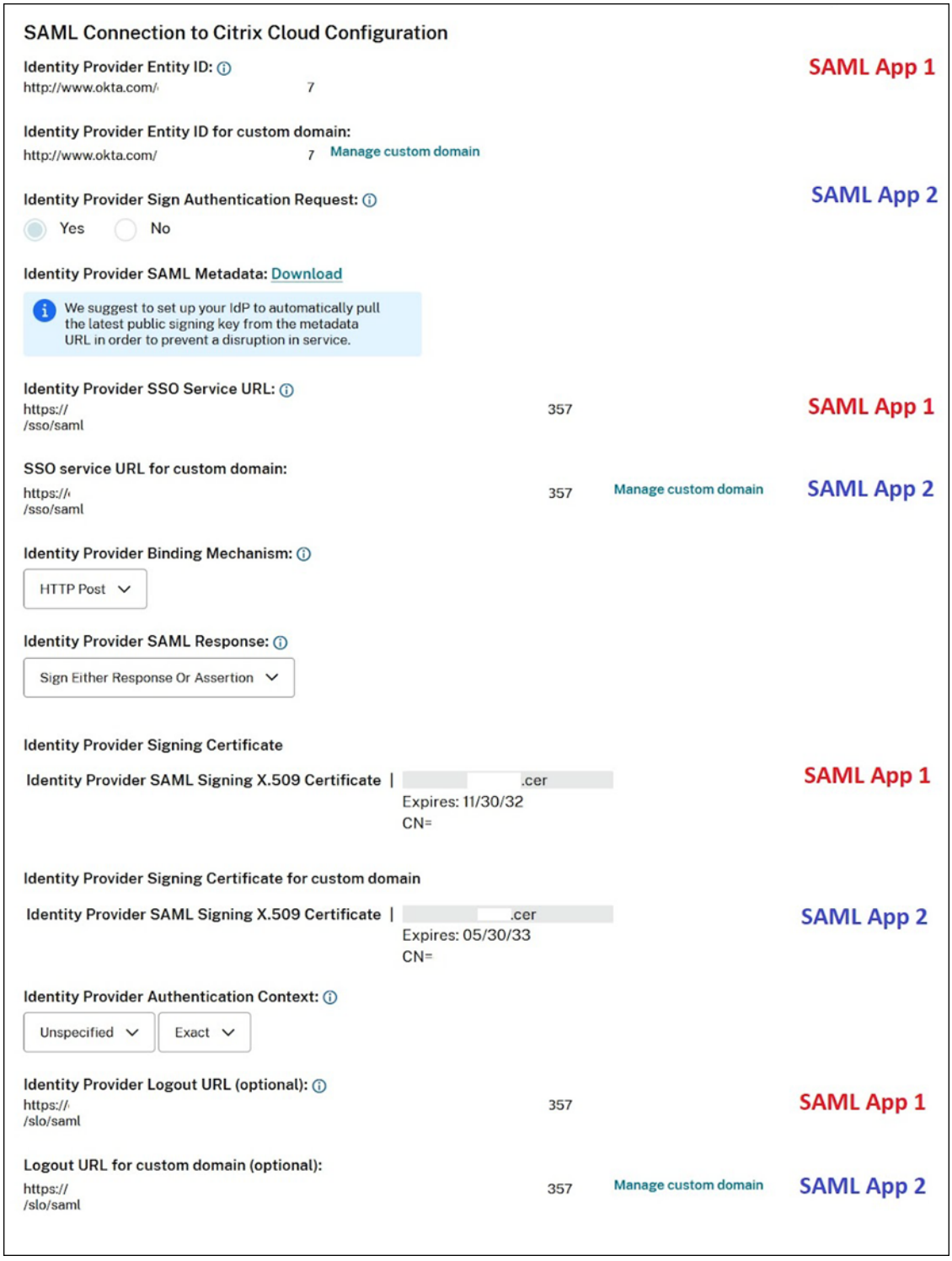
5. You selected **Use both `customer.cloud.com` URL and Custom URL** within **StoreFront Cloud > Access > Edit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Within **Identity and Access Management > Authentication** select **Select SAML Provider > View** from the ellipsis menu. The SAML Configuration page should display pairs of SAML end-points configured for Entity ID, SSO URL, and Logout URL.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Update the Service Provider SAML Signing Certificate

September 23, 2026

Author:
Mark Dear

SAML connections which use signed requests and responses depend on two different SAML signing certificates. One for each side of the SAML connection.

Service Provider signing certificate

This certificate is provided by Citrix via the Citrix Cloud™ SAML metadata and is updated during the advertisement phase of the SP signing certificate rotation. This occurs at least once per calendar year.

SAML signing certificates need to be rotated before their expiration date occurs to give Citrix Cloud administrator's time to prepare for deployment. Certificate rotation is required by both Service Providers and Identity Providers to ensure alignment and prevent any downtime.

If a selected SAML provider does not support automated rotation of the SP SAML signing certificate, a manual rotation of the SAML signing certificate within your SAML provider must be performed in order to replace the expiring certificate.

> **Important:**
>
> All existing guides within this SAML eDoc section include details of how to configure signing on both sides of the SAML connection. Citrix® only recommends signed SAML configurations as these are more secure and are required by some SAML providers for logout (SLO) to succeed.

FAQ

What is SAML signing?

The SAML Protocol uses messages to request authentication and to send assertions of identity. The security of these messages depends on both transport and message level security. The messages are XML documents which are signed in accordance with the XML Signature syntax. This provides both integrity assurance of the message, but also authentication of the sender by proving they hold the private key. The trust model is described by: SAML Security and Privacy Considerations. The public keys used to define which private keys are trusted can be distributed in any suitable format. Citrix uses X.509 certificates as suitable containers to distribute and consume keys.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What is SAML signed request enforcement?

Just because Citrix Cloud is configured to send signed requests within the SAML connection this does not guarantee that the SAML provider will enforce the use of signatures and reject any unsigned incoming SAML requests. Most SAML IdPs have an option to enforce signed requests. If an unsigned request to log into the SAML provider is received then the SAML logon will fail. Some SAML IdPs like Duo do not even offer this option. It is the responsibility of the SAML IdP admin to check the status of the SAML IdP configuration. Citrix support does not control or have any visibility of whether signed requests are enforced within your SAML application.

How frequently does Citrix rotate its Service Provider SAML signing certificate?

In order to allow plenty of overlap between the active Service Provider signing certificate and the newly issued one, Citrix rotates the Service Provider signing certificate approximately every 11 months. This is to ensure a valid certificate is available to Citrix Cloud customers 30 days before the new certificate is to be activated.

What is the Service Provider SAML signing certificate advertisement phase?

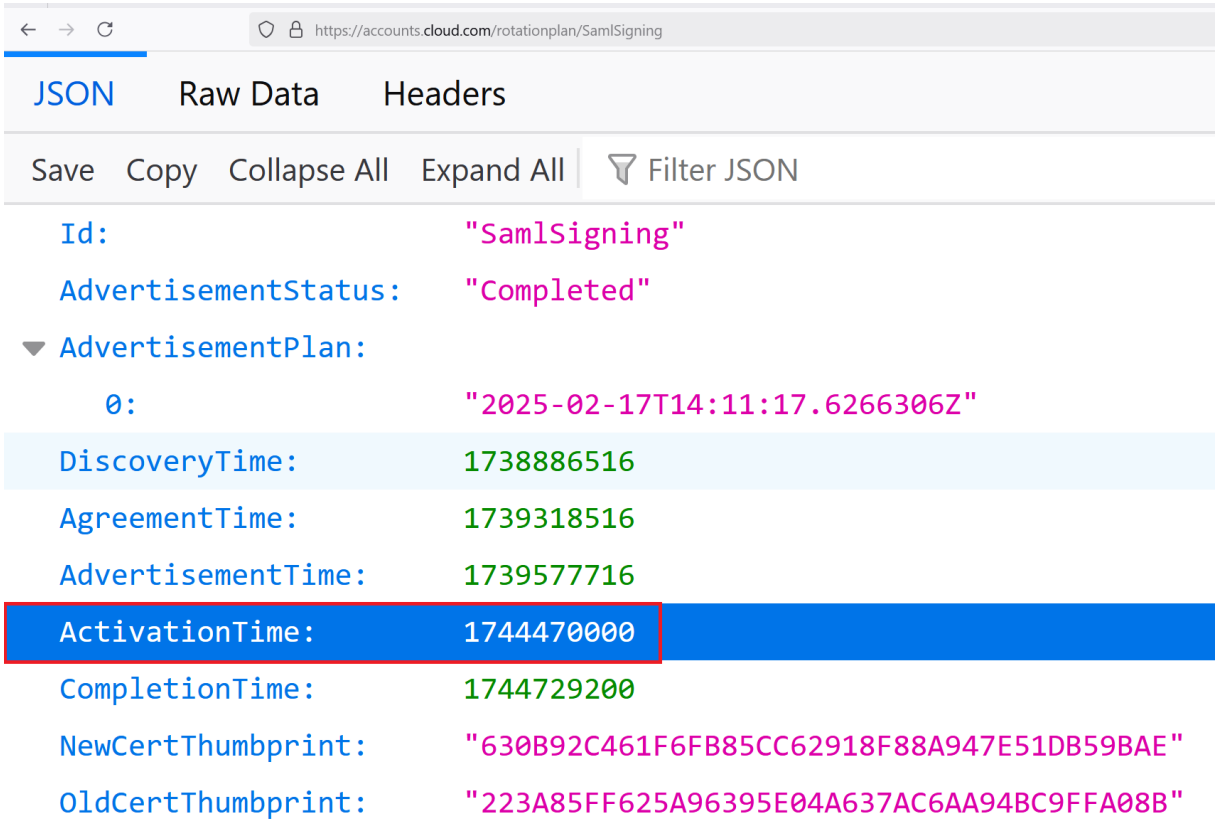
During the advertisement phase the current and replacement SAML signing certificates will be present in the Citrix Cloud metadata. Only the active certificate can be used for SAML request verification until the rotation date and time. This is the date and time specified within the Citrix Cloud emails and Citrix Cloud console notifications.

> **Important:**
>
> The date of signing certificate expiry is not the same as the date of activation. It is the activation date that the Citrix and IdP admins need to pay attention to NOT the date of certificate expiry. The Citrix Cloud signing cert will always be rotated before it expires.

You can check the advertisement and activation date and time using this link Rotation plan.

The date and times are provided as Unix epoch time stamps for each event in the service provider signing certificate rotation process.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Use Epoch converter to convert unix epoch time stamps into a human readable date and time format.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



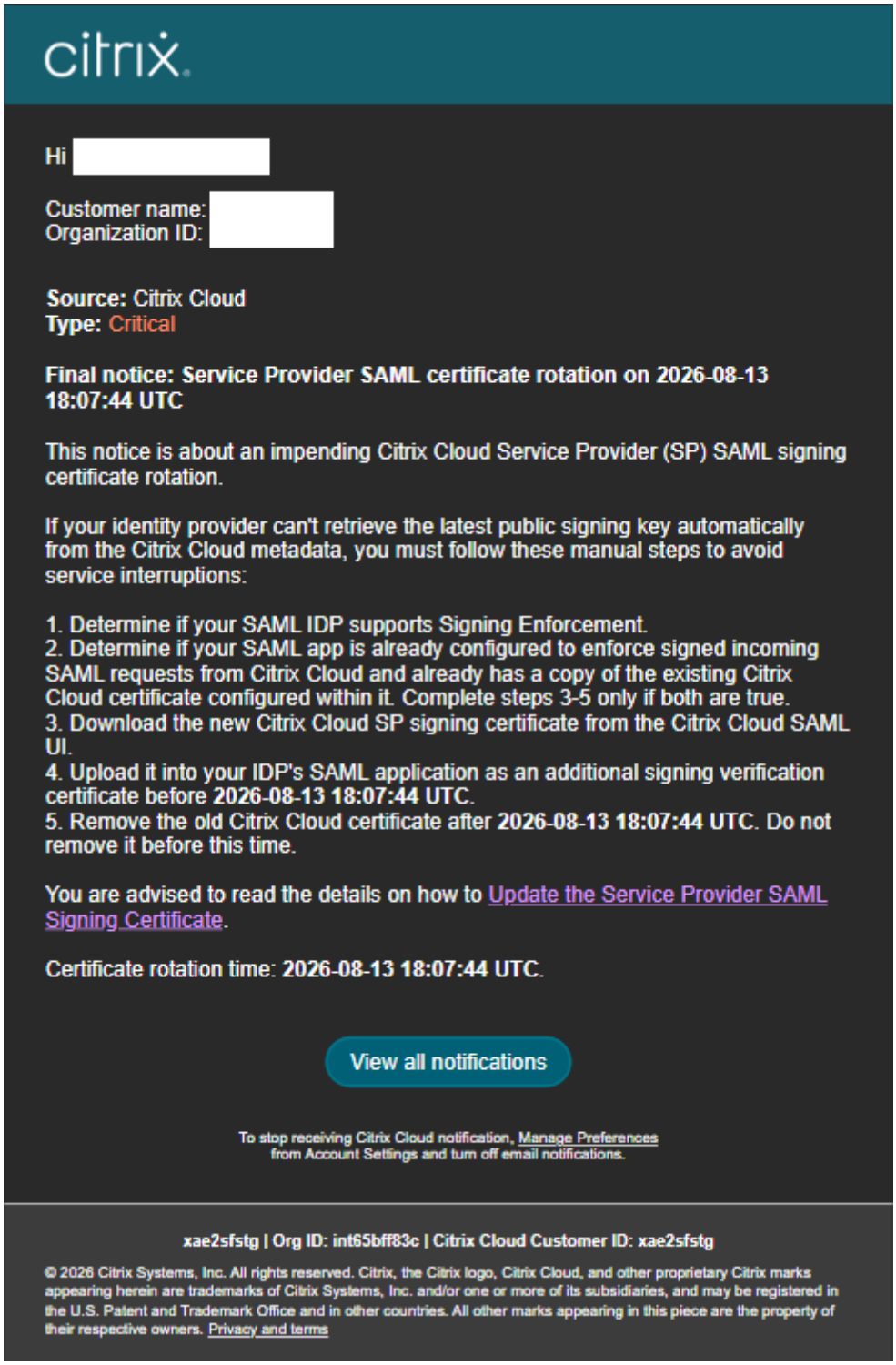
Why has Citrix decided to use a self signed Citrix Cloud SAML signing certificate rather than a certificate signed by a public certificate authority such as Digitcert?

The **Issuer**: within the latest version of the SAML signing certificate you should upload into your SAML applications is now "samlsigning.cloud.com, Citrix Systems Inc."instead of a public certificate authority like Digicert. The use of self signed SP signing certificates is to mitigate against a known SAML vulnerability with externally issued certificates, referred to as "Silver SAML".

Why have I received a notification via email and within the Citrix Cloud console indicating that the current Citrix Cloud SAML signing certificate is about to expire and must be replaced?

SAML providers (IdP) require a valid and in date certificate to verify the signature of incoming SAML requests from Service Providers such as store and the Citrix Cloud console. Citrix Cloud customers using SAML for store or Citrix Cloud console logon will be contacted to advise them of an imminent SAML signing certificate rotation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



citrix.

Hi

Customer name:
Organization ID:

Source: Citrix Cloud
Type: Critical

Final notice: Service Provider SAML certificate rotation on 2026-08-13 18:07:44 UTC

This notice is about an impending Citrix Cloud Service Provider (SP) SAML signing certificate rotation.

If your identity provider can't retrieve the latest public signing key automatically from the Citrix Cloud metadata, you must follow these manual steps to avoid service interruptions:

1. Determine if your SAML IDP supports Signing Enforcement.
2. Determine if your SAML app is already configured to enforce signed incoming SAML requests from Citrix Cloud and already has a copy of the existing Citrix Cloud certificate configured within it. Complete steps 3-5 only if both are true.
3. Download the new Citrix Cloud SP signing certificate from the Citrix Cloud SAML UI.
4. Upload it into your IDP's SAML application as an additional signing verification certificate before **2026-08-13 18:07:44 UTC**.
5. Remove the old Citrix Cloud certificate after **2026-08-13 18:07:44 UTC**. Do not remove it before this time.

You are advised to read the details on how to Update the Service Provider SAML Signing Certificate.

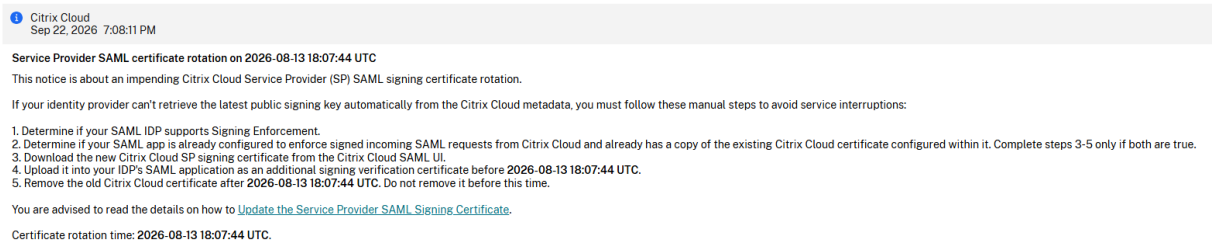
Certificate rotation time: **2026-08-13 18:07:44 UTC**.

View all notifications

To stop receiving Citrix Cloud notification, Manage Preferences from Account Settings and turn off email notifications.

xae2sfstg | Org ID: int65bff83c | Citrix Cloud Customer ID: xae2sfstg

© 2026 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, Citrix Cloud, and other proprietary Citrix marks appearing herein are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries. All other marks appearing in this piece are the property of their respective owners. Privacy and terms


Citrix Cloud
Sep 22, 2026 7:08:11 PM

Service Provider SAML certificate rotation on 2026-08-13 18:07:44 UTC

This notice is about an impending Citrix Cloud Service Provider (SP) SAML signing certificate rotation.

If your identity provider can't retrieve the latest public signing key automatically from the Citrix Cloud metadata, you must follow these manual steps to avoid service interruptions:

1. Determine if your SAML IDP supports Signing Enforcement.
2. Determine if your SAML app is already configured to enforce signed incoming SAML requests from Citrix Cloud and already has a copy of the existing Citrix Cloud certificate configured within it. Complete steps 3-5 only if both are true.
3. Download the new Citrix Cloud SP signing certificate from the Citrix Cloud SAML UI.
4. Upload it into your IDP's SAML application as an additional signing verification certificate before **2026-08-13 18:07:44 UTC**.
5. Remove the old Citrix Cloud certificate after **2026-08-13 18:07:44 UTC**. Do not remove it before this time.

You are advised to read the details on how to Update the Service Provider SAML Signing Certificate.

Certificate rotation time: **2026-08-13 18:07:44 UTC**.

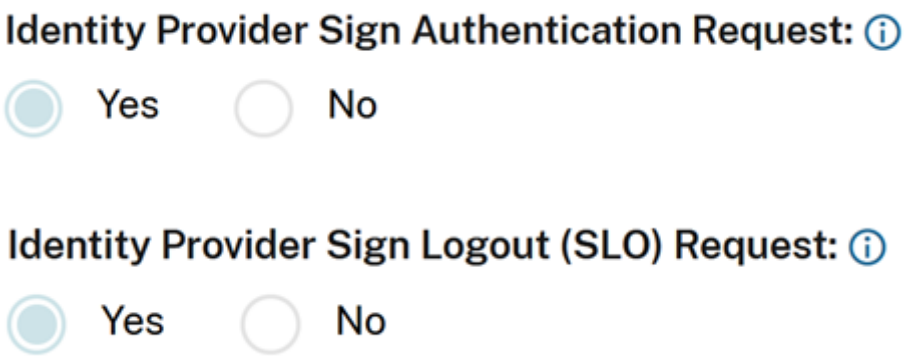
How do I know if my Citrix Cloud customer is affected by the Citrix Cloud SAML signing certificate rotation or not?

This will affect Citrix Cloud customers with the following SAML configuration.

- Your SAML connection within Citrix Cloud is configured with **Sign Authentication Requests = Yes**
- You have configured your SAML provider such as Microsoft Entra ID, ADFS, or Okta to reject unsigned SAML requests (signing enforcement).
- You have Single Logout (SLO) configured within your Citrix Cloud SAML connection and within your SAML provider. SLO requests need to be signed as part of security best practice.

How do I check the signing configuration of my Citrix Cloud SAML connection?

Navigate to **Identity and Access Management** > **SAML 2.0** > **Edit** to check if you have **Sign Authentication Requests** enabled within your Citrix Cloud SAML connection. All new SAML connections within Citrix Cloud will default to **Identity Provider Sign Authentication/Logout Requests = Yes** for both logon (SSO) and logout (SLO).

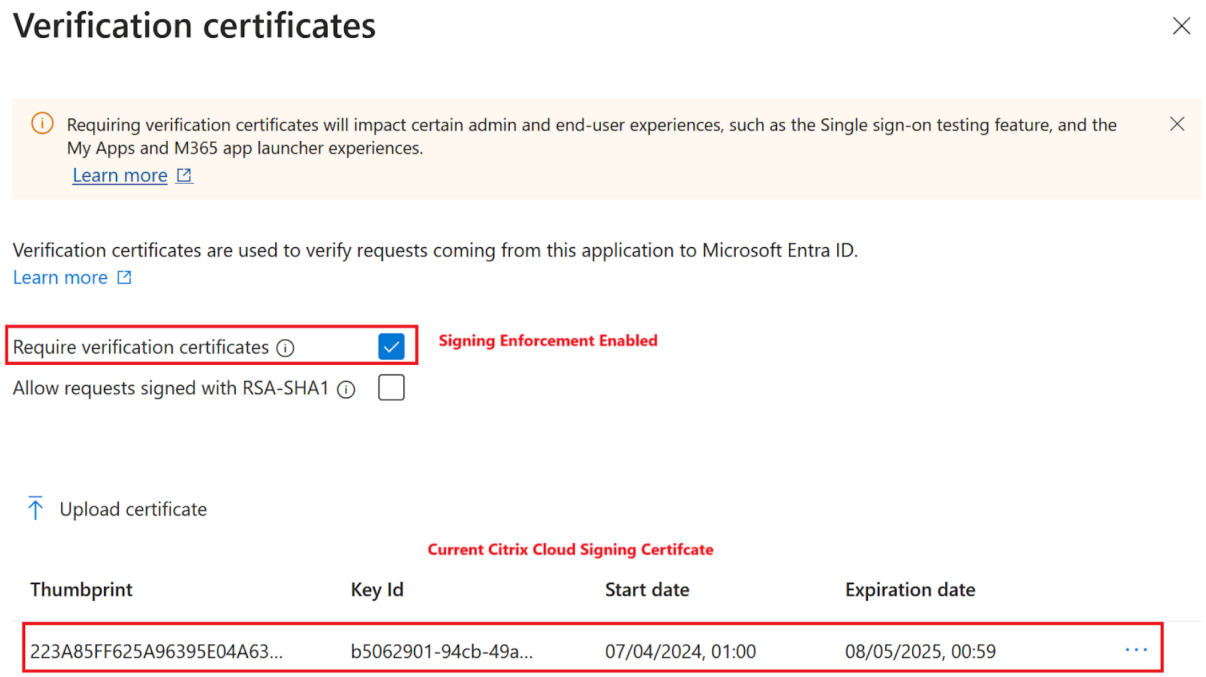


© 1997–2026 Citrix Systems, Inc. All rights reserved.

How do I check whether signing enforcement is configured within my SAML app?

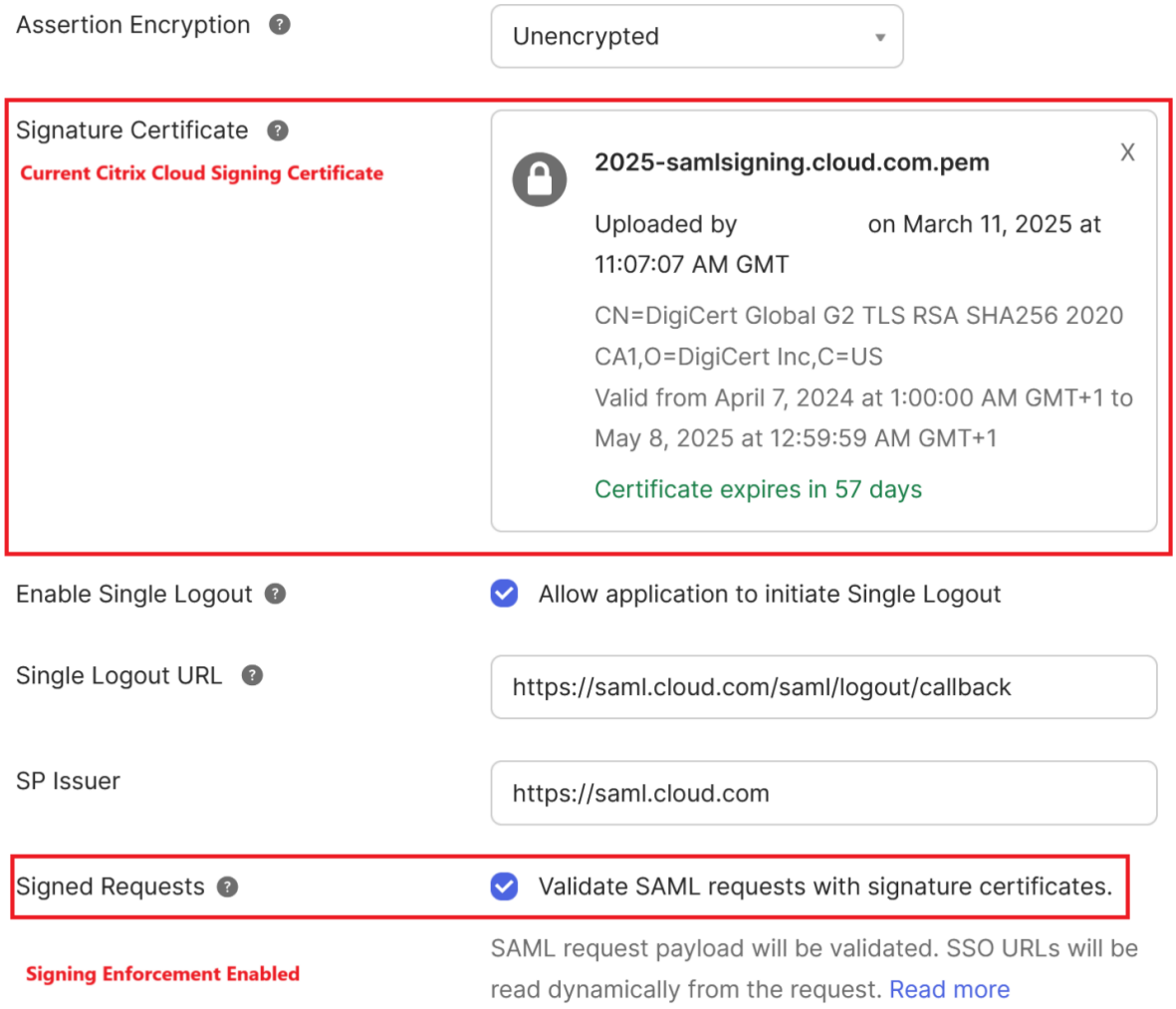
This varies depending on the SAML provider you are using. All Citrix documented SAML solutions include steps to enable Signing Enforcement as part of security best practice.

EntraID Signing Enforcement Example:



Okta Signing Enforcement Example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Where do I obtain a copy of the latest Service Provider (SP) signing certificate?

This certificate is provided by Citrix through the Citrix Cloud SAML metadata and is updated periodically during the advertisement phase of the SP signing certificate rotation. This occurs at least once per calendar year.

US, EU, and APS: https://saml.cloud.com/saml/metadata

JP: https://saml.citrixcloud.jp/saml/

GOV: https://saml.cloud.us/saml/metadata

© 1997–2026 Citrix Systems, Inc. All rights reserved.

When is it safe to remove the old Citrix Cloud SAML signing certificate if my SAML app supports multiple verification certificates?

Only remove the old Citrix Cloud signing certificate from your SAML applications after the certificate activation date and time given in the email and Citrix Cloud console notification. Some SAML IdPs such as Okta only allow one signing certificate to be uploaded at a time. In this situation there is no choice but to overwrite the current certificate with the new one after the activation date and time. This should not be done before the activation date and time.

Use metadata exchange to automatically update the SAML Provider with the latest Citrix Cloud SP SAML Signing Certificate

Using SAML metadata exchange, the SAML provider consumes the Citrix Cloud SAML metadata automatically by monitoring the metadata URL, such as https://saml.cloud.com/saml/metadata. If your SAML provider supports SAML metadata exchange, then the SP signing certificate might already be updated automatically.
Verify that your SAML provider supports metadata exchange. Afterward, you can verify whether the update has occurred before the current SAML signing certificate expires.



> **Important**
>
> There is a large amount of variation regarding the SAML features that each third-party SAML provider supports. It is the Citrix Cloud administrator's responsibility to know and understand the capabilities and requirements of the SAML provider you are using. This is necessary to ensure that both the Citrix Cloud SAML connection configuration (SP) and SAML provider (IdP) configuration match. Refer to your SAML provider's documentation to determine if it supports signature verification and whether SAML requests and responses need to be signed.

Manually update the SAML Provider with the latest Citrix Cloud SP SAML Signing Certificate

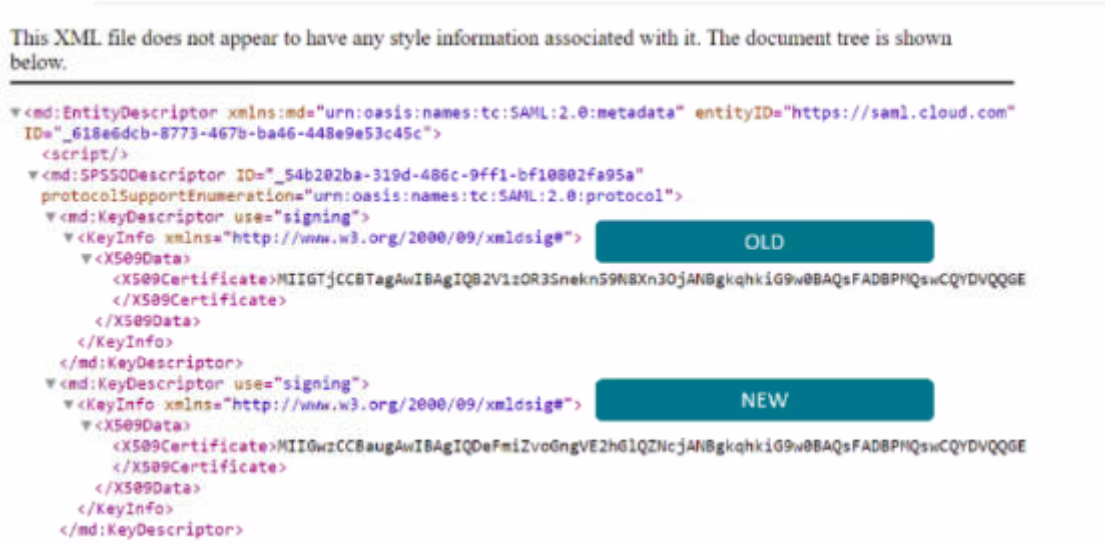
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important**
>
> SP Certificate rotation must be done every time a new certificate is published from Citrix Cloud otherwise SAML logon will be impacted and you will incur downtime.

Obtain a Copy of the future Service Provider Certificate from the Citrix Cloud metadata

1. Acquire the latest SAML metadata from Citrix Cloud by viewing your current SAML connection within **Identity and Access Management**, click **Authentication**, select **SAML Connection** and click **View**.
   The following image is an example of what this file might look like for Citrix Cloud regions such as US, EU and APS:

   https://saml.cloud.com/saml/metadata

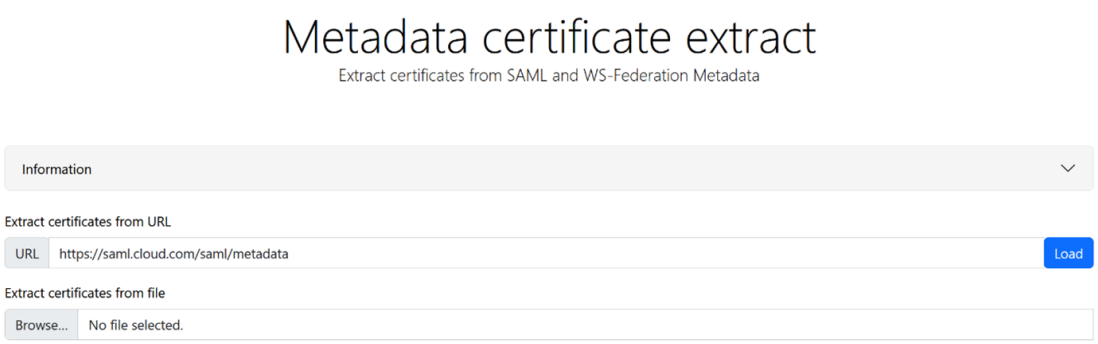


   In this metadata XML file example, there are two x.509 Citrix Cloud SAML signing certificates.

2. It is possible to extract the x.509 certificate from the metadata by uploading the XML file to a third-party tool or providing the metadata URL.
3. Navigate to https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract
4. Enter the SAML metadata URL that corresponds to your Citrix Cloud customer region:

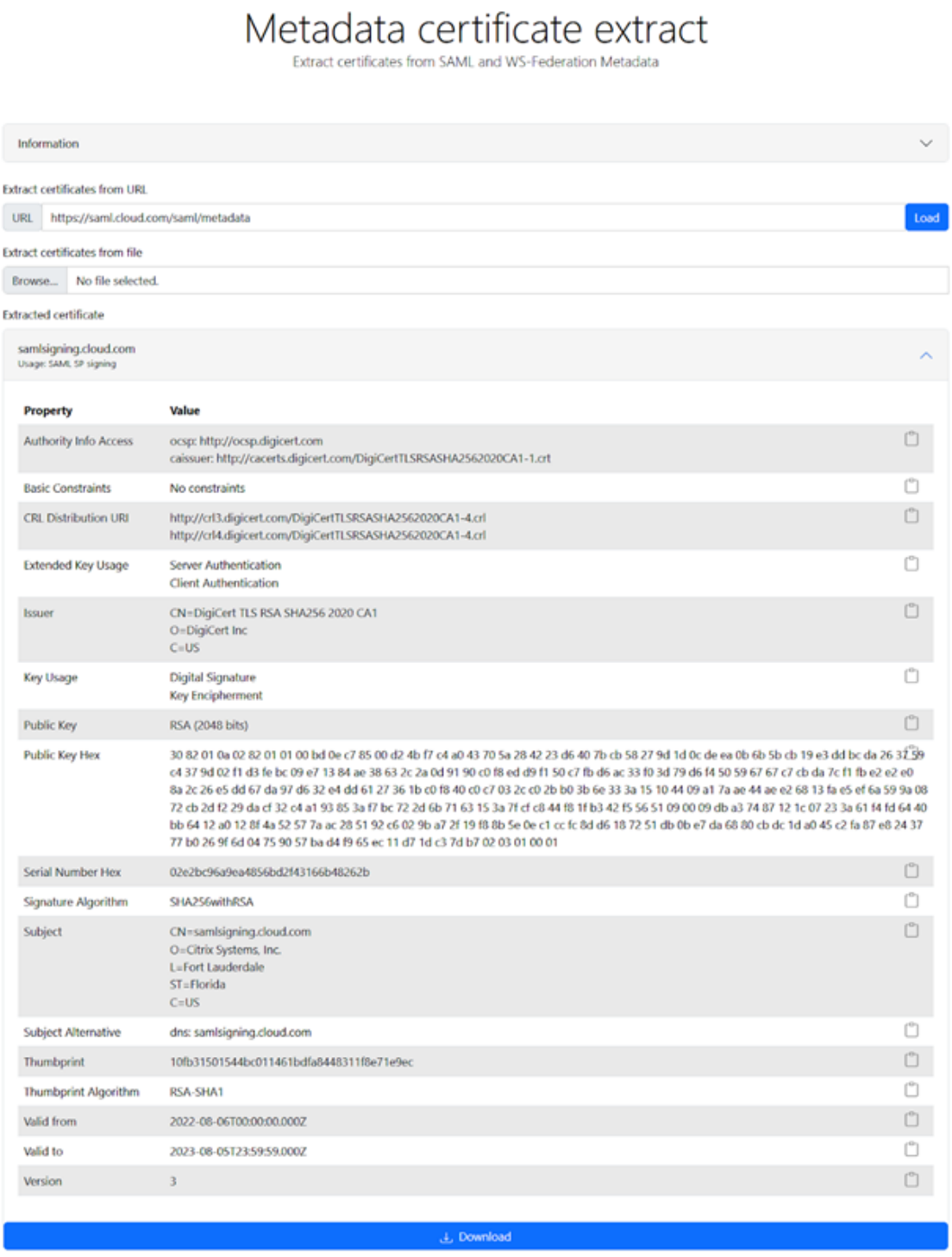
   - US, EU and APS: https://saml.cloud.com/saml/metadata
   - JP: https://saml.citrixcloud.jp/saml/metadata
   - GOV: https://saml.cloud.us/saml/metadata

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Download the SAML signing certificate from https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Upload the newly extracted Citrix Cloud SP SAML certificate to your SAML provider. This process will be different for every SAML provider. Verify the proper SP signing certificate rotation procedure using your specific SAML provider documentation.

   Depending on your SAML provider, the existing SAML signing certificate might need to be replaced by the new one. In some cases, the SAML provider might support multiple SP signing cer-

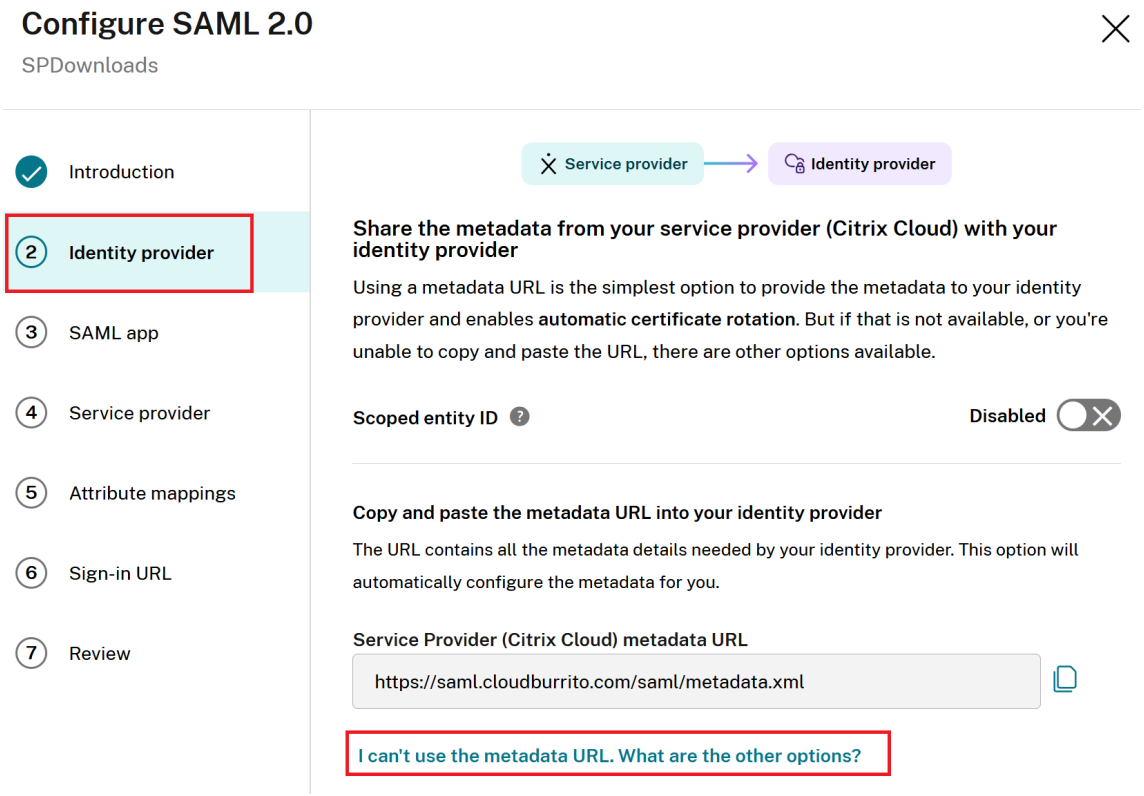
© 1997–2026 Citrix Systems, Inc. All rights reserved.

tificates at the same time, thus only uploading the new one will be enough. It is recommended you remove the old certificate once it has expired.

OR,

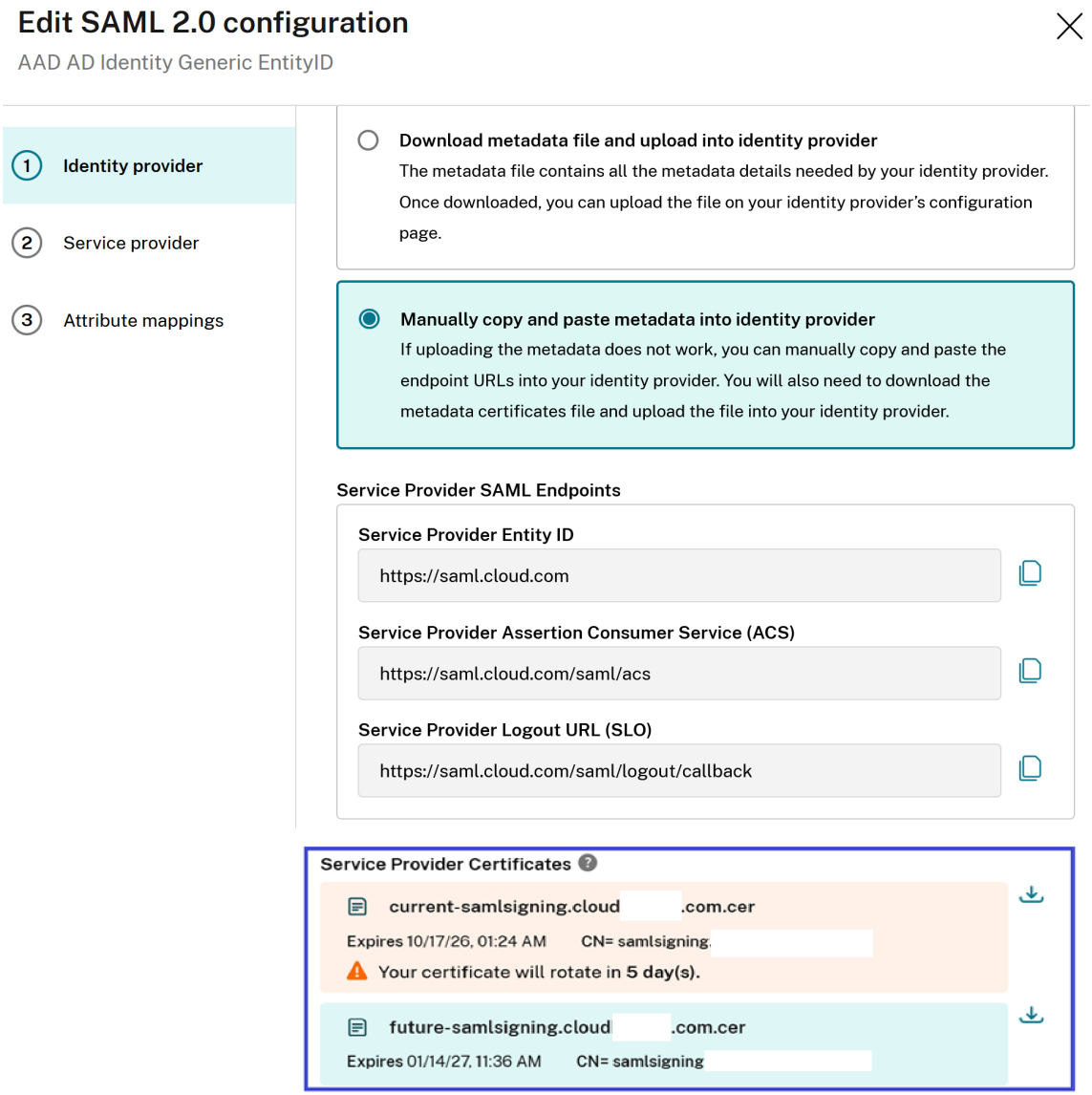
Obtain a Copy of the future Service Provider Certificate from inside the Citrix Cloud UI

1. Within the Configure SAML 2.0 wizard for new manually created connections.
2. Navigate to the **Identity Provider** page within the wizard flow.
3. Select **I can't use the metadata URL. What are the other options?**



4. Select **Manually enter metadata fields** and navigate to the **Service Provider Certificates** section.
5. Download the future version of the Citrix Cloud signing certificate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

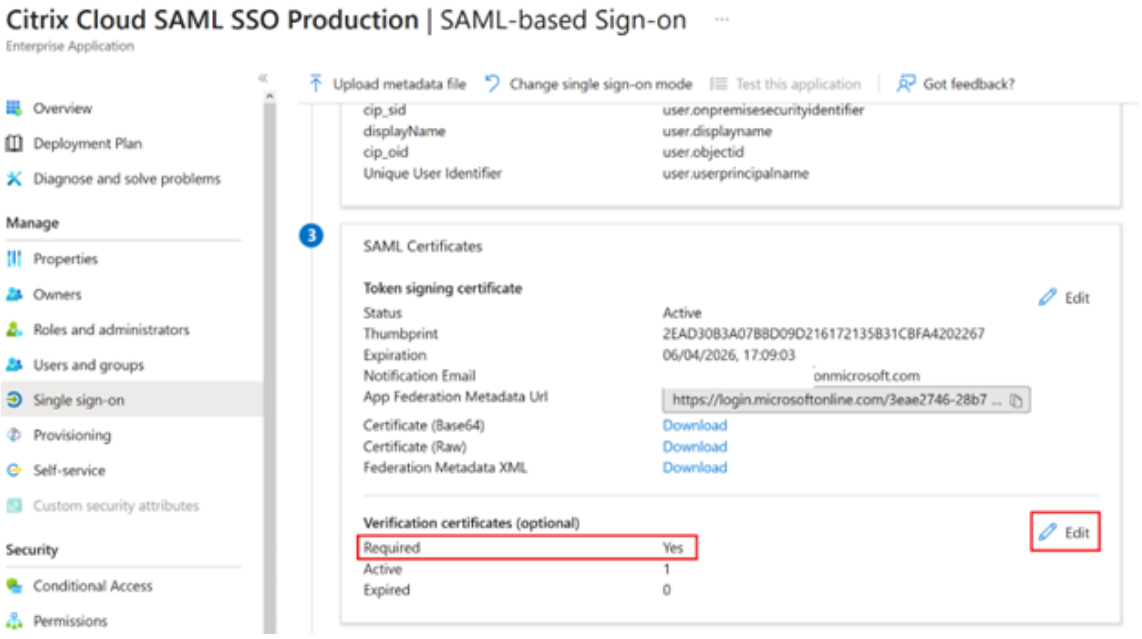


Upload a replacement Citrix Cloud SAML signing certificate to your Microsoft Entra ID SAML application

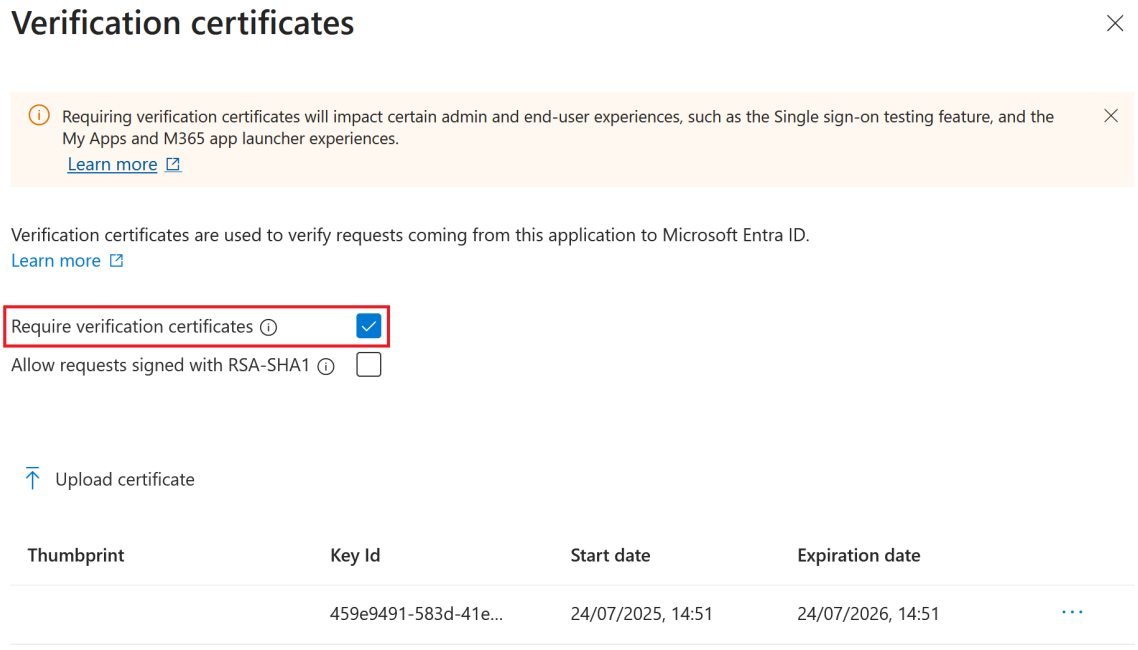
Before configuring the Microsoft Entra ID SAML app, see SAML Request Signature Verification for more information.

1. Navigate to **Microsoft Entra ID**, select **Enterprise Applications** and click Your SAML App.
2. Locate the SAML certificates section within the SAML application.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



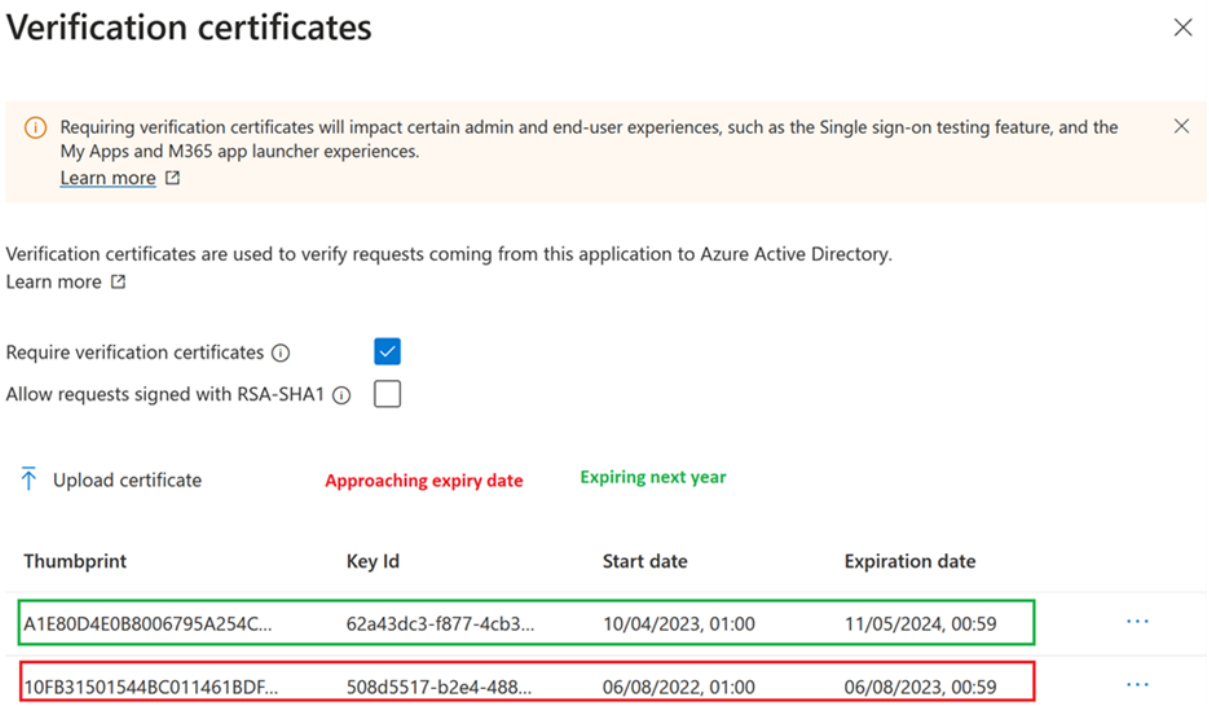
3. Select **Upload Certificate** and upload the replacement Citrix Cloud SAML signing certificate obtained from the SAML metadata.



> **Note:**
>
> Microsoft Entra ID SAML apps can have multiple signing verification certificates configured so it is possible to upload a replacement certificate long before the current certificate has expired. The following screenshot shows two valid certificates. One of the certificates is due to expire in the near future. Provided at least one of the uploaded certificates is valid and has not yet expired,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> a SAML login to a store or Citrix Cloud will continue to succeed and you will not experience an outage.



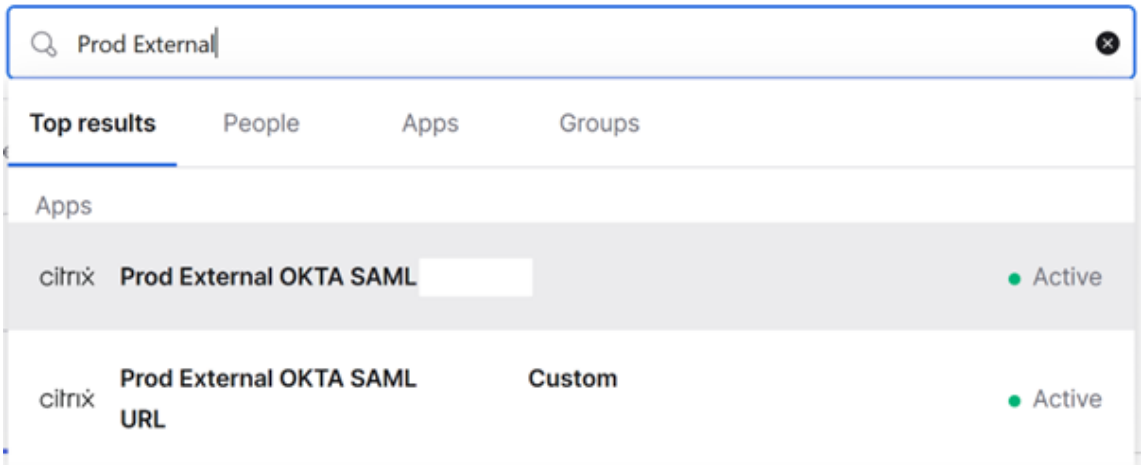
> **Important:**
>
> Do not remove the existing verification certificate until after the SAML rotation date and time given in the email and Citrix Cloud console notification has passed. The new Citrix Cloud certificate becomes active only on the date and time given within those two notifications.

Upload a replacement Citrix Cloud SAML signing certificate to your Okta SAML application

Okta does not support multiple SP SAML signing certificates at the same time. You have no choice but to overwrite the existing Citrix Cloud SP signing certificate you are currently using with the new one. It is recommended you do this in a scheduled maintenance window.

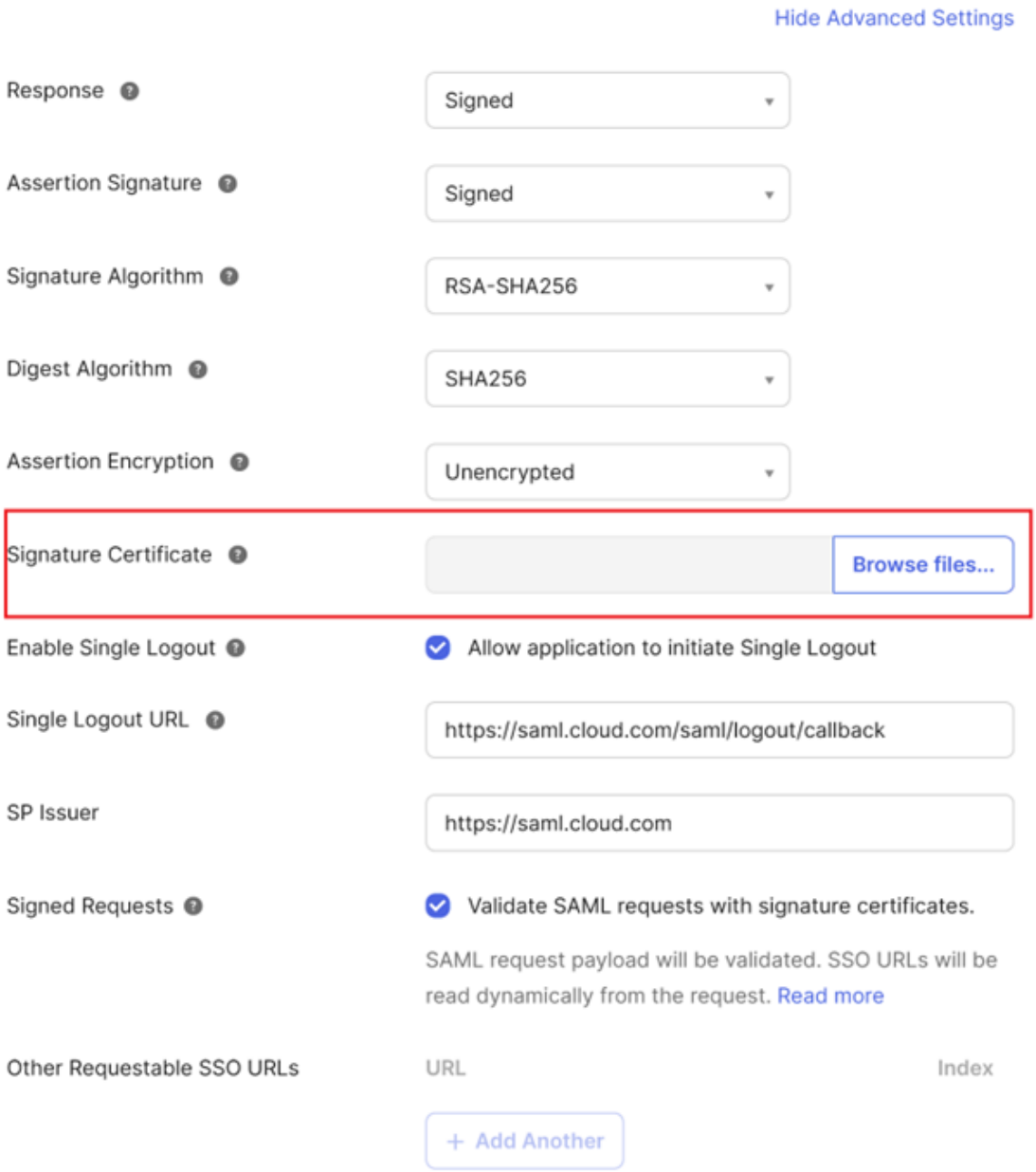
1. Navigate to **Applications**, select **Applications** and search for your Okta SAML App

© 1997–2026 Citrix Systems, Inc. All rights reserved.



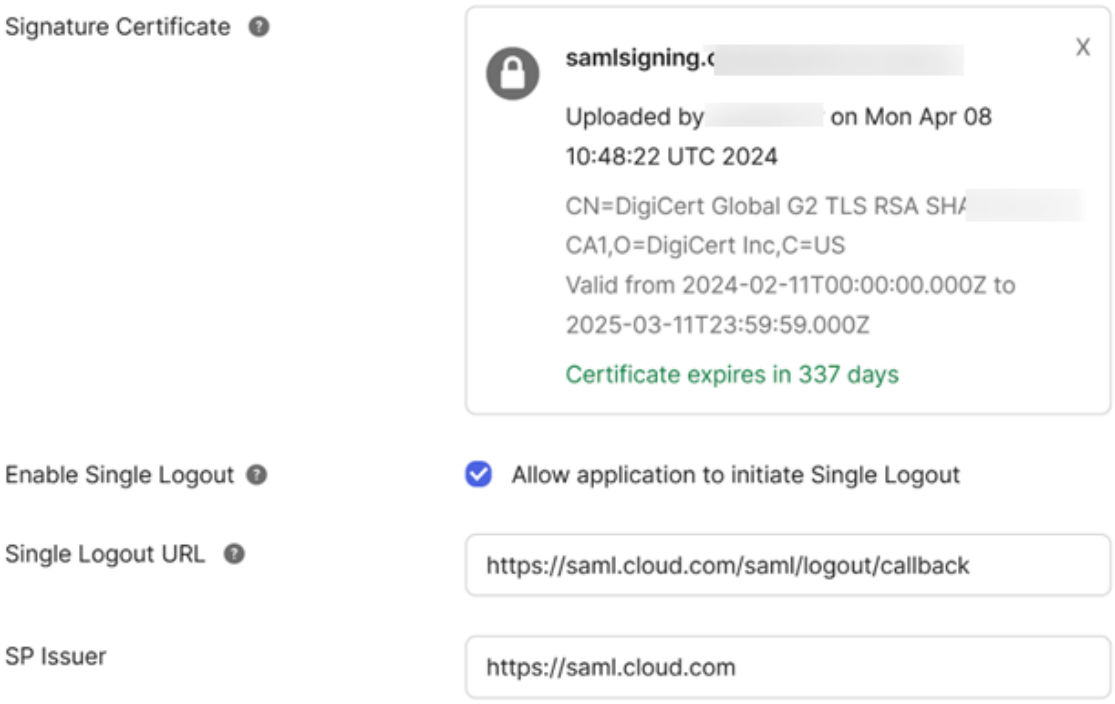
2. From **General**, navigate to **SAML Settings**, click **Edit**, select **Configure SAML**, select **Show Advanced Settings**, and click **Signature Certificate** in order to upload a replacement. Okta does not display the current Citrix Cloud SAML signing certificate in the upload UI. It will only display the replacement certificate after this has been uploaded.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Select **Signature Certificate**, click **Browse Files** and upload the replacement Citrix Cloud SAML signing certificate obtained from the Citrix Cloud SAML metadata.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Important**
>
> Do not overwrite the existing verification certificate until the SAML rotation date and time given in the email and Citrix Cloud console notification. The new Citrix Cloud certificate only becomes active on the date and time given within those two notifications.

Update the Identity Provider SAML Signing Certificate

June 22, 2026

Author:
Mark Dear

SAML connections which use signed requests and responses depend on two different SAML signing certificates. One for each side of the SAML connection. The **IdP certificate rotation** process is not to be confused with the **Service Provider** yearly rotation of the `samlsigning.cloud.com` certificate in use by all Citrix Cloud customers. Citrix does not control the rotation of your SAML application's IDP certificate. Your Citrix Cloud and IdP administrator does.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FAQ

What is the SAML application's signing certificate used for?

Your SAML application's signing certificate is uploaded into Citrix Cloud when you initially create the SAML connection. During the initial SAML connection creation process only one IdP signing certificate needs to be provided. The IdP certificate is obtained from within your SAML provider such as Microsoft Entra ID, Okta, PingFederate, or ADFS. Citrix Cloud uses the IdP signing certificate to verify the signature of SAML responses sent from your SAML application to Citrix Cloud during the SAML authentication process. The IdP certificate will be trusted by Citrix Cloud until its date of expiry.

What is a SAML application signing certificate rotation?

An IdP Signing Certificate Rotation is a planned maintenance task that is required when your SAML application's signing certificate is approaching its date of expiry. Admins need to pay attention to the IdP signing certificate used by SAML connections within Citrix Cloud. When the certificate is about to expire within 30 days, upload an in-date replacement certificate into your Citrix Cloud SAML connection. Do this replacement before the current certificate expires.

How frequently do I need to rotate my SAML application's signing certificate?

Cloud SAML application certificates typically have very long lifespans such as 16 years for Duo, 10 years for Okta and 3 years for Entra ID SAML applications. Certificates used within on premise SAML IdPs such as PingFederate or ADFS are created and maintained like any other x509 certificate in your environment so are typically replaced yearly by commercial certificate authorities such as Digicert.

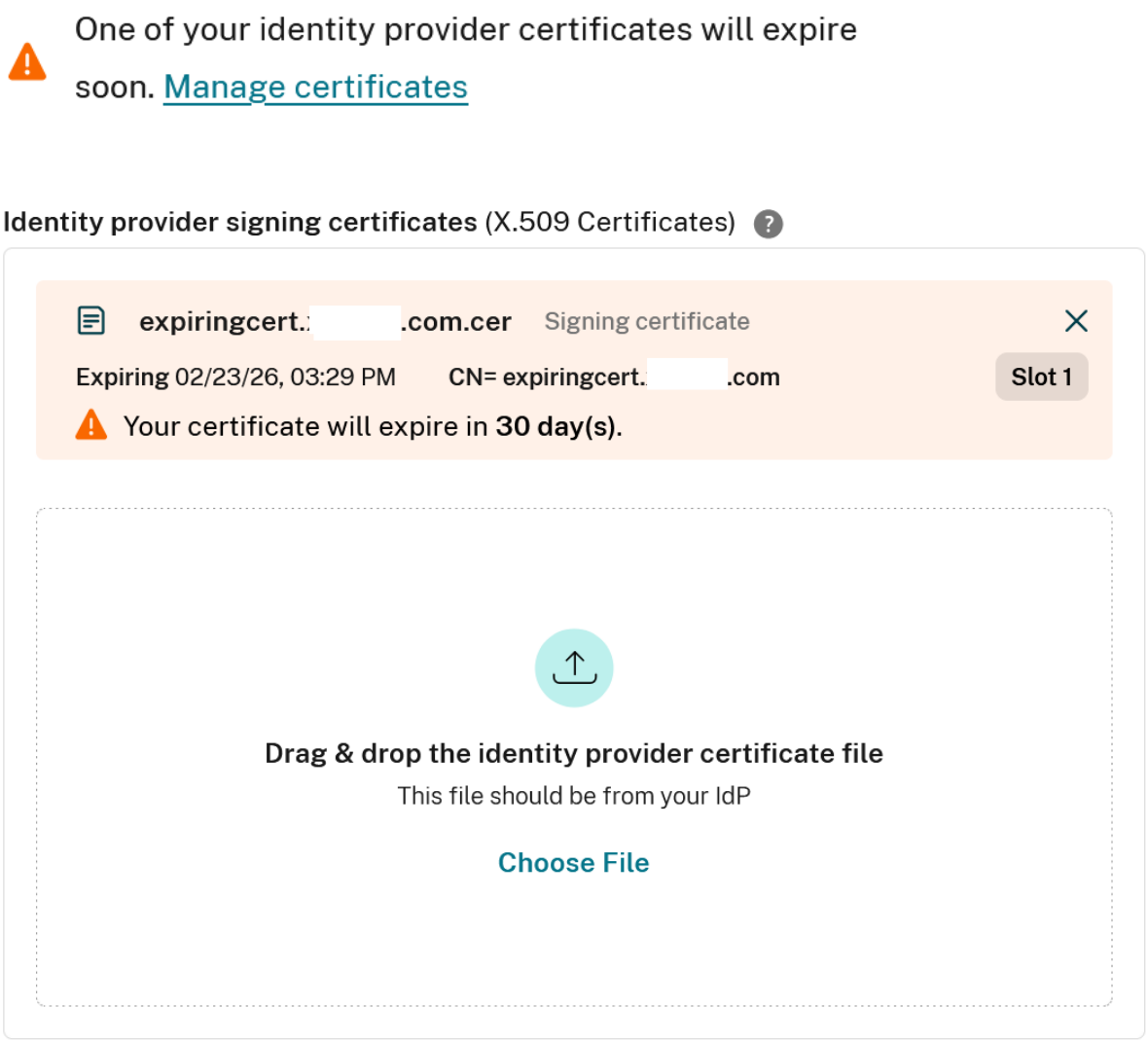
How will I know if my SAML application's signing certificate is about to expire?

You are required to check the date of expiry of the certificate that is currently active inside your IdP's SAML application.

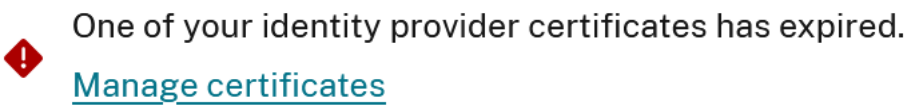
Citrix Cloud will display a warning on your SAML IDP connection within **Identity and Access Management > Authentication** on the SAML connection 30 days before your SAML application's signing certificate expires.

Click **manage Certificates** to be redirected to the **View > SAML connection** page where you can upload a new or remove an expired certificate.

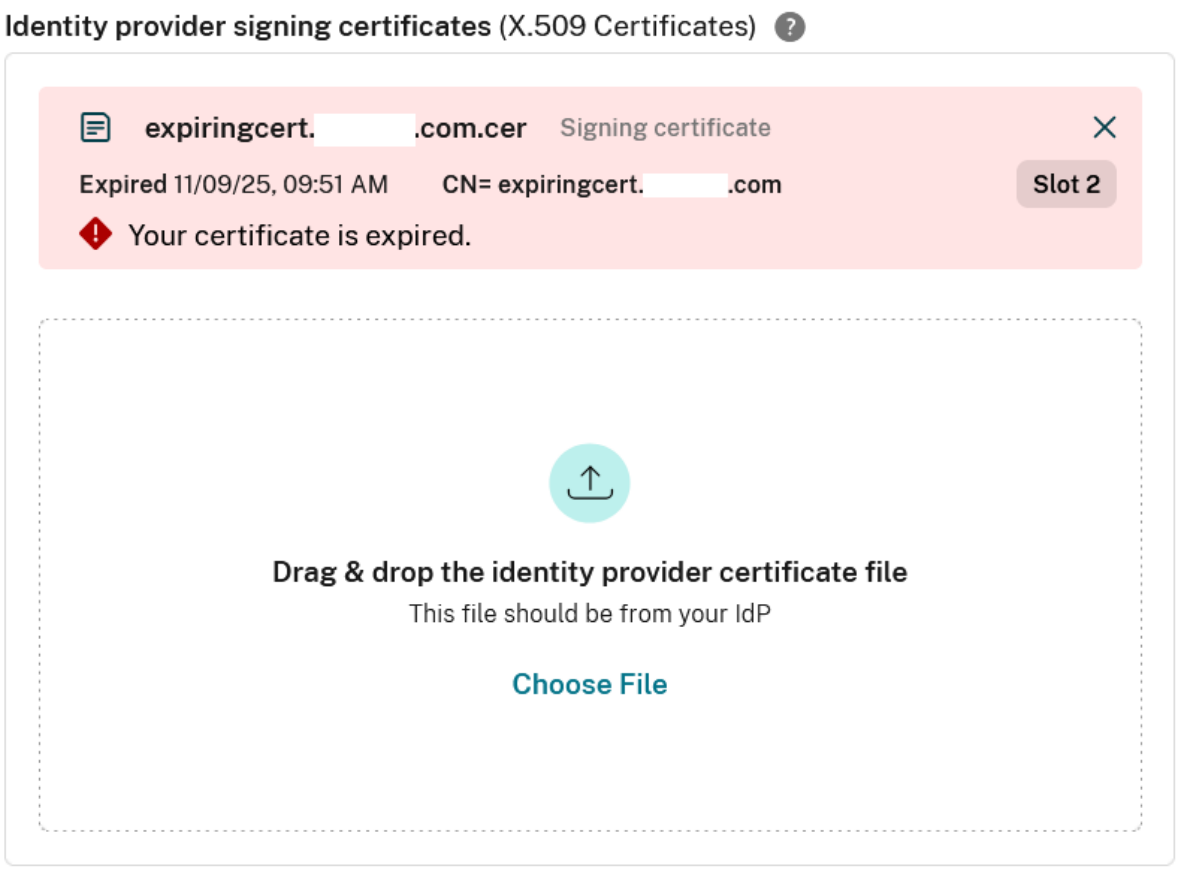
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Citrix Cloud will also display an error on the SAML connection if the IdP certificate has actually already expired as shown below. An expired IdP certificate renders the SAML connection unusable until the certificate is replaced.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



What notifications will I receive from Citrix Cloud when my SAML application's signing certificate is about to expire?

Citrix Cloud admins will receive a **critical notification** if they have one or more SAML connections with IDP certificates that are due to expire in the **next 30 days**. Citrix Cloud monitors all SAML connections and will detect any that contain a certificate that is about to expire in the next 30 days. You may also receive notifications from your SAML IdP about SAML app certificates that are due to expire in addition to notifications from your Citrix Cloud tenant.

> **Important:**
>
> If your Citrix Cloud admins have chosen to disable all email and Citrix Cloud console notifications you may miss these critical warnings as your SAML IdP certificate approaches its date of expiry. Your Citrix Cloud administrators are responsible for ensuring at least one or more active admin users can receive these critical notifications. See this article regarding how Citrix Cloud admins manage their notifications

Every IdP certificate expiry notification contains details to help you identify the SAML connection within Citrix Cloud and the IdP certificate that is due to expire within your Identity Provider. Navigate

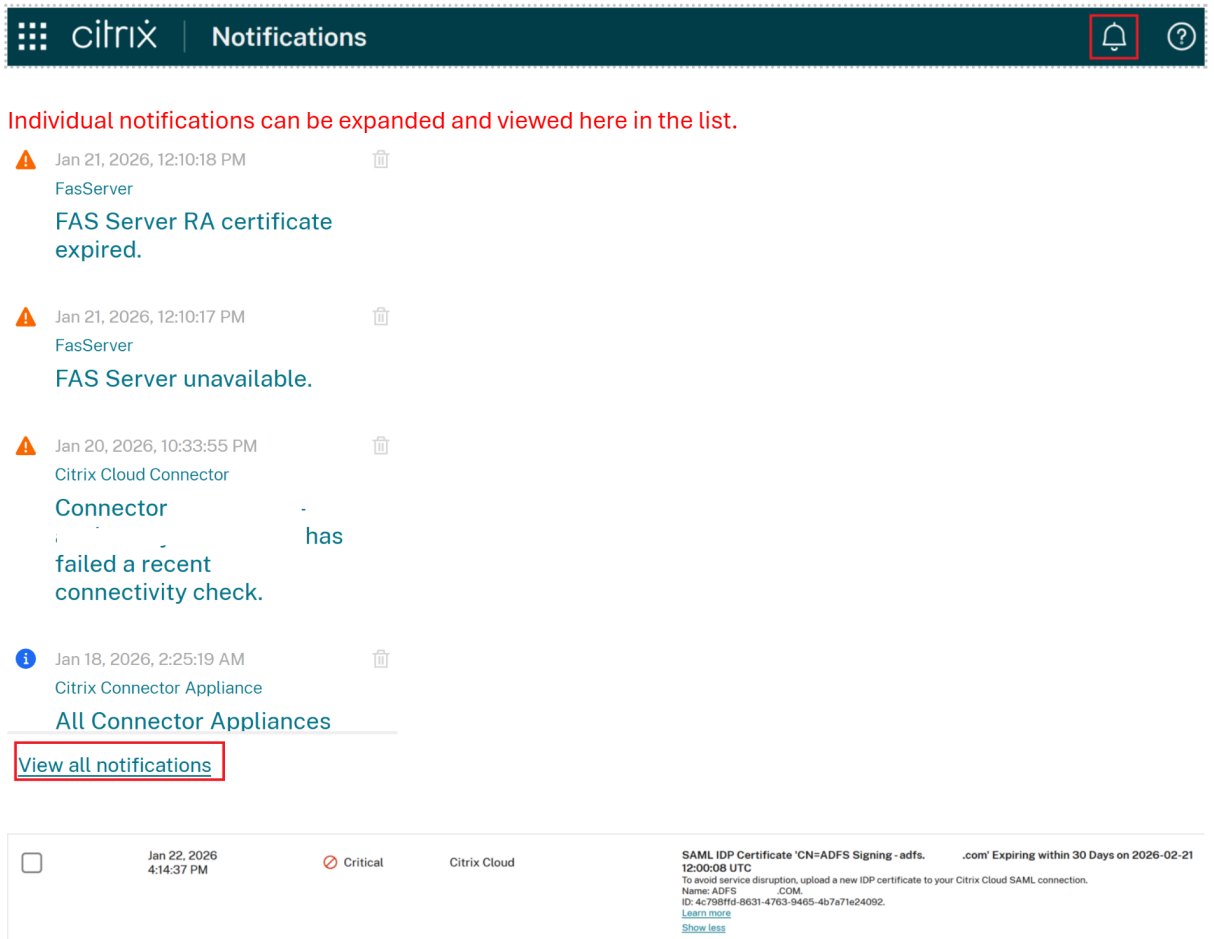
© 1997–2026 Citrix Systems, Inc. All rights reserved.

further to **Identity and Access Management > Authentication**.



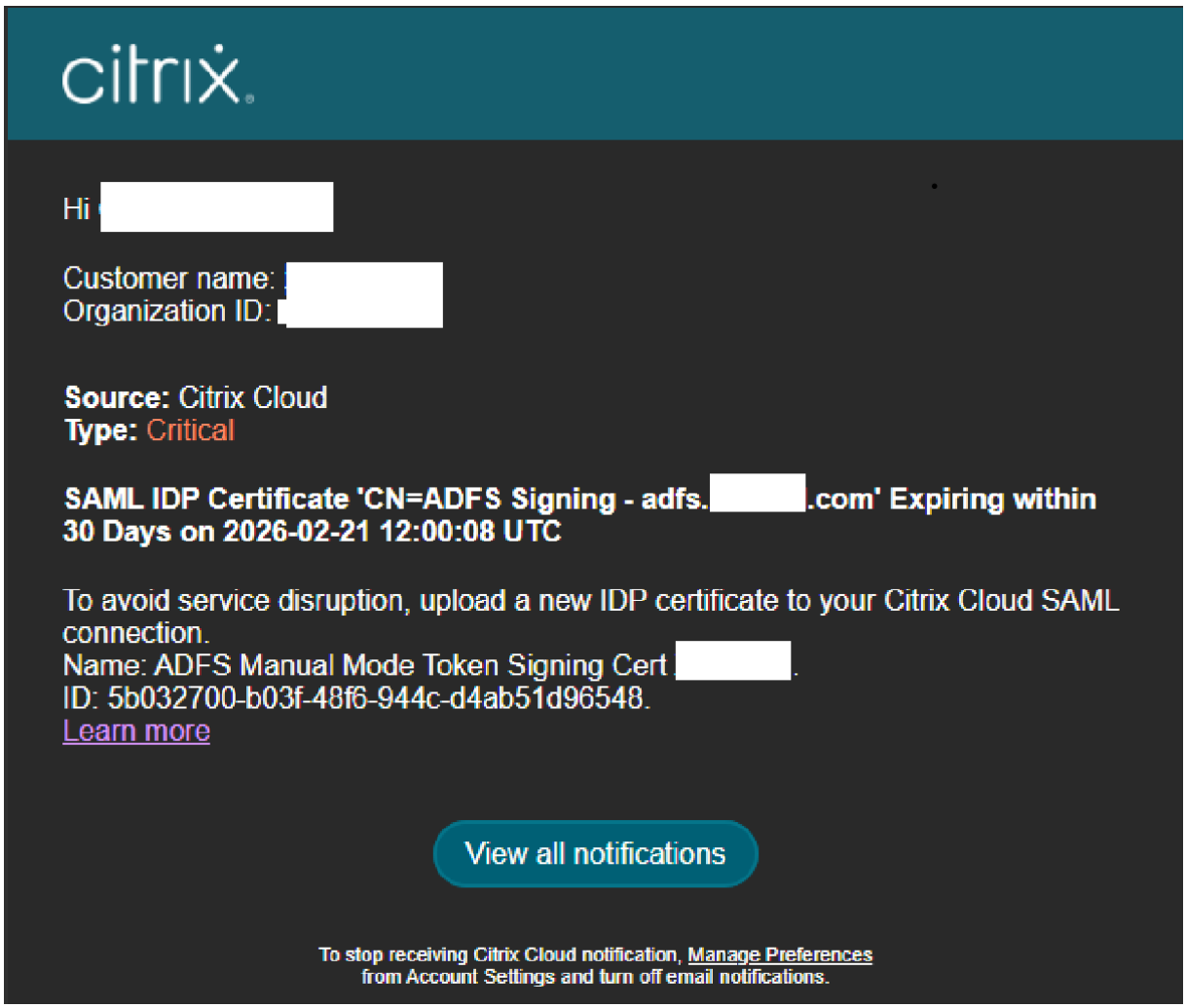
- SAML Connection Nickname: `ExpiringIdPCert`
- SAML Connection ID: `e65e3d1d-f4fa-40f4-a53e-de84a270011c`
- Certificate Common Name: `CN=expiringcert.domain.com`
- Date of Expiry: `2025-12-27`

Admin Notifications within the Citrix Cloud Portal Navigate to the Citrix Cloud Home page and click the bell icon and select view all notifications. Look for critical alerts that indicate the certificate and SAML connection that is due to expire in the next 30 days.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Email Notifications Once an IdP certificate expiry notification has been **sent once**, it will not be resent again. This is to prevent unnecessary email spamming and ensure Citrix Cloud admins only receive the notification email once and not another email every day for the entire 30 day period as expiry approaches. If the Citrix Cloud notification is dismissed it will not be resent.



Can I update the SAML IdP certificate while still using the Citrix Cloud SAML connection without triggering an outage?

Yes. The introduction of a second IdP certificate to the SAML IdP connection allows for seamless SAML application certificate rollovers. **Upload the new certificate at least 24 hours** before the current certificate expires. **Your end users or Citrix Cloud admin users should be unaffected provided you have followed this article correctly**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Where do I obtain a copy of the latest Identity Provider (IdP) signing certificate from my SAML application?

Certificates used within on-premise SAML IdPs such as PingFederate are obtained from either private certificate authorities within your organization or from commercial certificate authorities like Digicert. Cloud-based SAML IdP SAML apps can generate new IdP certificates on demand at any time within the SAML app UI. New IdP signing certificates can be generated at any time and set to Inactive.

Can Citrix Cloud trust two different IdP signing certificates at the same time?

Yes. Seamless IdP certificate rollovers depend on this. Citrix Cloud SAML connections trust SAML responses. These responses must be signed with either of the two trusted IdP signing certificates that have been uploaded into the SAML connection. If one of the certificates has expired it can no longer be trusted by Citrix Cloud and should not be used by your SAML application anymore.

Citrix Cloud SAML connections can store either one or two SAML application certificates.

Slot1: contains the certificate you uploaded into the Citrix Cloud SAML connection when you first created it. This certificate needs to be replaced before it expires to prevent outages.

Slot2: is always empty after your SAML connection has been created but can be used to upload a new SAML app certificate before the certificate in **Slot1** expires. It is intended to provide an alternative trusted certificate to take over from the expiring **Slot1** signing certificate.

When should I remove the "old"Identity Provider (IdP) signing certificate from my SAML connection inside Citrix Cloud?

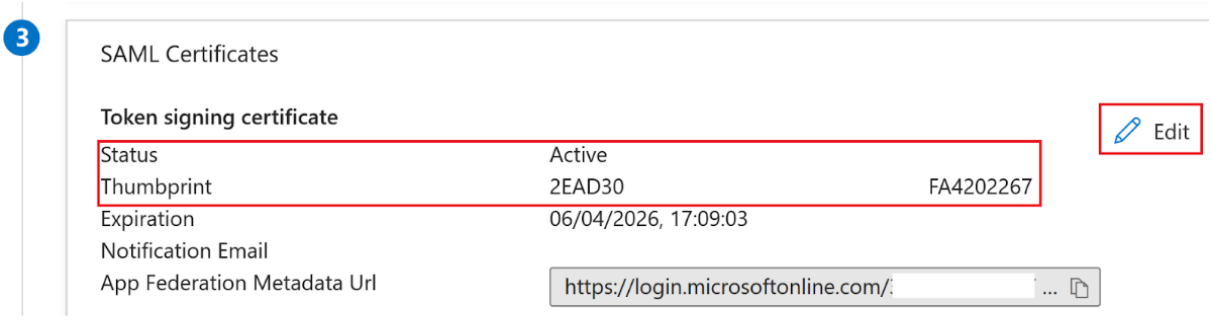
The **old** Identity Provider (IdP) signing certificate should only be removed from the Citrix Cloud SAML connection **AFTER** you have proven that the "new"signing certificate has been **activated** within your SAML application AND you have successfully logged into store and/or Citrix Cloud using it. It is easier to rollback a failed IdP certificate rotation maintenance task if both IdP certificates are still present in the Citrix Cloud connection. Citrix Cloud can trust both certificates provided they are both still in date. If the IdP certificate has already expired then rolling back to it is not possible.

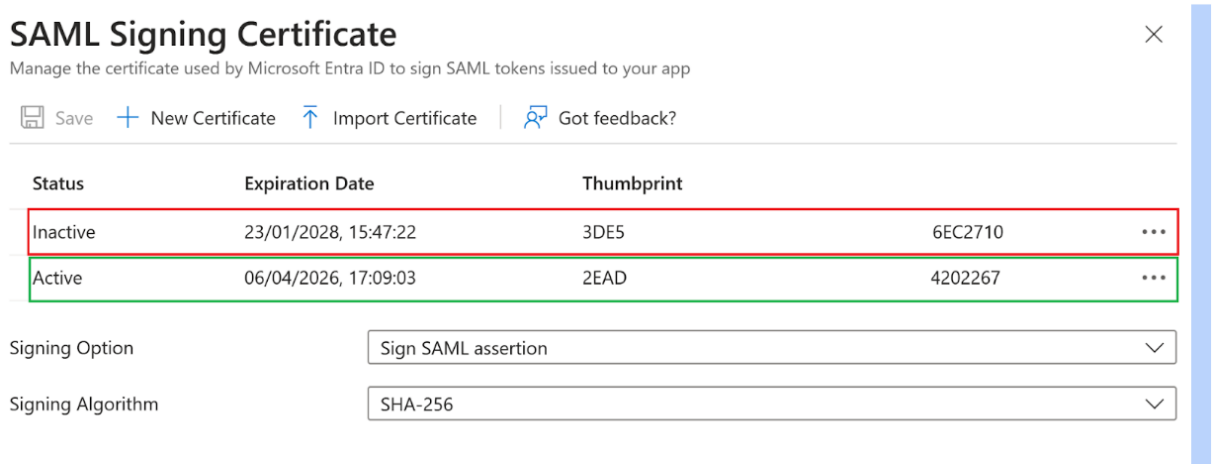
How can I tell which IdP signing certificate my SAML application is currently using to sign the SAML response?

Your SAML application uses only one certificate at a time to sign the SAML response. It uses the certificate that is currently set as **active** in your SAML application. The **active** IdP signing certificate is also present in the SAML application metadata.

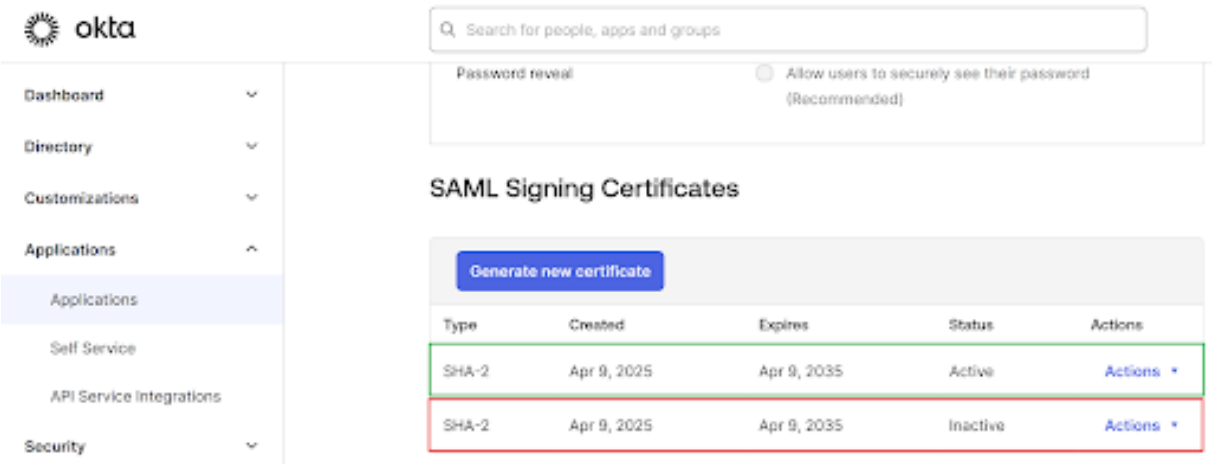
The screenshots below show examples from Entra ID.

© 1997–2026 Citrix Systems, Inc. All rights reserved.





The screenshot below shows an example from Okta.



Perform a SAML Application IdP Certificate Rotation as a Scheduled Maintenance Task

> **Important:**
>
> At least one of your IdP certificates within your SAML Connection must be in date and active within your IdP to prevent an outage. If you have just a single IdP certificate configured within

© 1997–2026 Citrix Systems, Inc. All rights reserved.

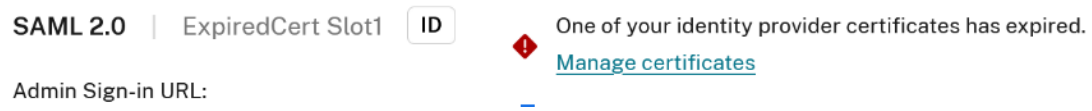
> the Citrix Cloud certificate and that certificate expires, your users will experience an outage and your SAML logon will fail. This situation impacts store users and/or Citrix Cloud admin users depending on how your SAML connection is used.

1. Plan to perform the IdP certificate rotation several days before the date of expiry of your current certificate.
2. Obtain a copy of the replacement IdP certificate from within your SAML application that you want to rotate to. Ensure the IdP certificate is in either PEM, CER or CRT format ready for upload into your Citrix Cloud SAML connection.
3. Upload the replacement IdP certificate into your Citrix SAML connection at least 24 hrs before you want to trigger the rotation of the certificate within your SAML application.

   Navigate to your SAML connection inside **Identity and Access Management > Authentication**. Select the 3 dots on a SAML connection with a certificate expiring in the next 30 days and Click **View**.

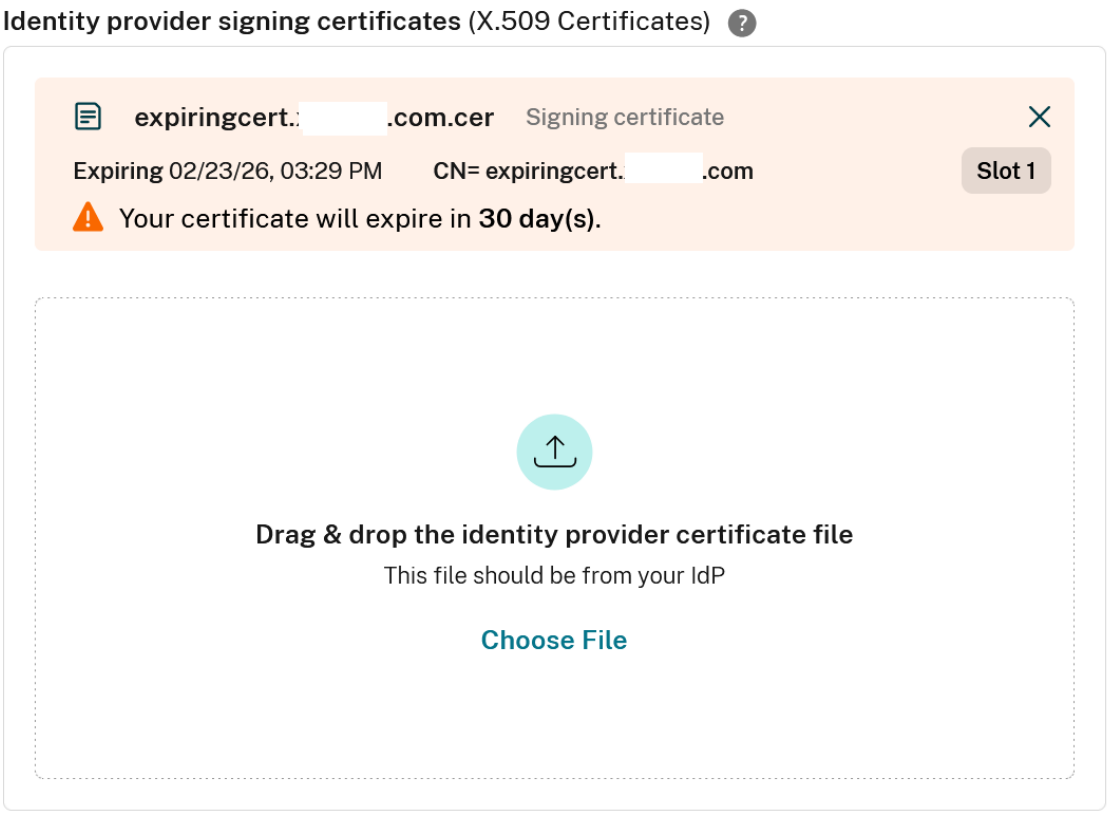
   OR,

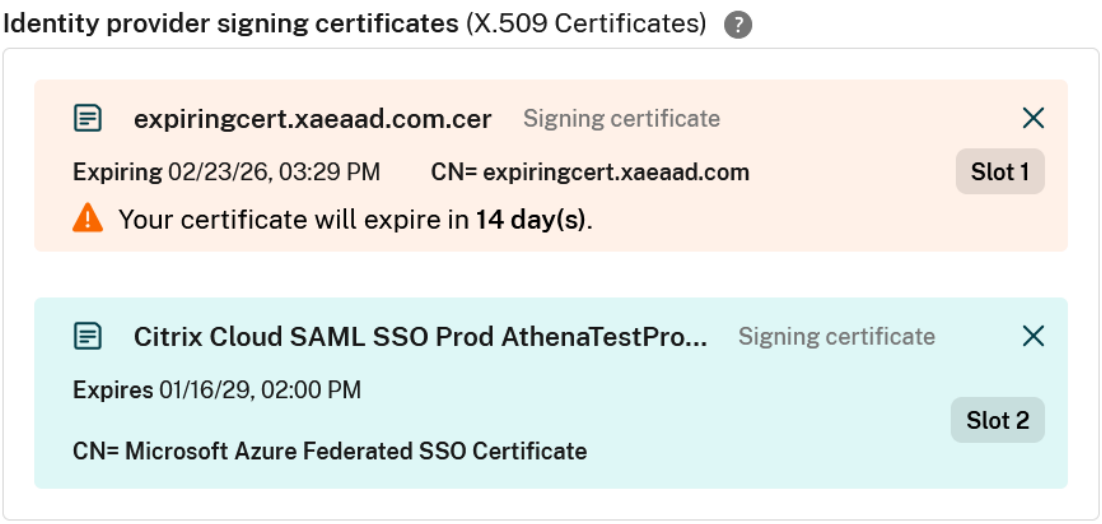
   Click **Manage certificates**.



4. Upload the second IdP certificate using the **Slot2** upload option within the Citrix Cloud SAML connection.

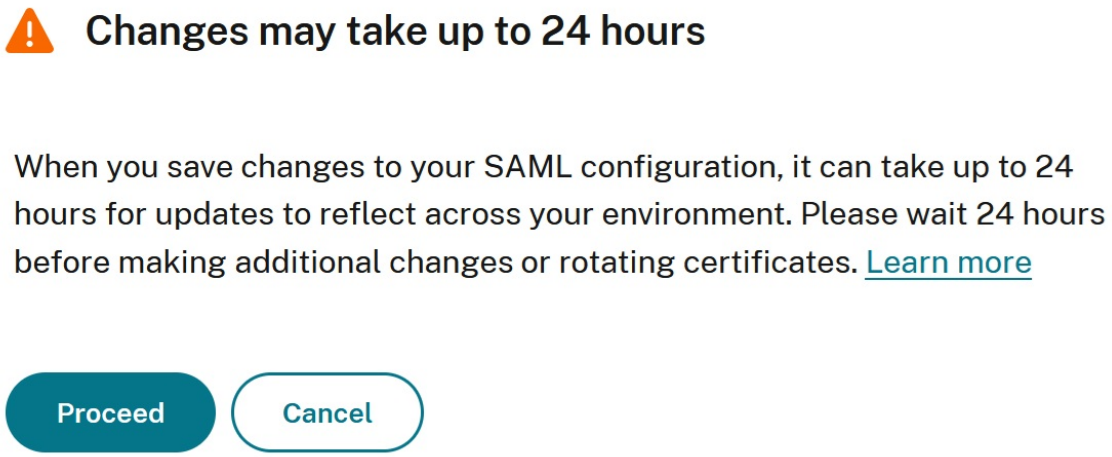
© 1997–2026 Citrix Systems, Inc. All rights reserved.





5. Save the SAML connection after you have uploaded the new certificate.

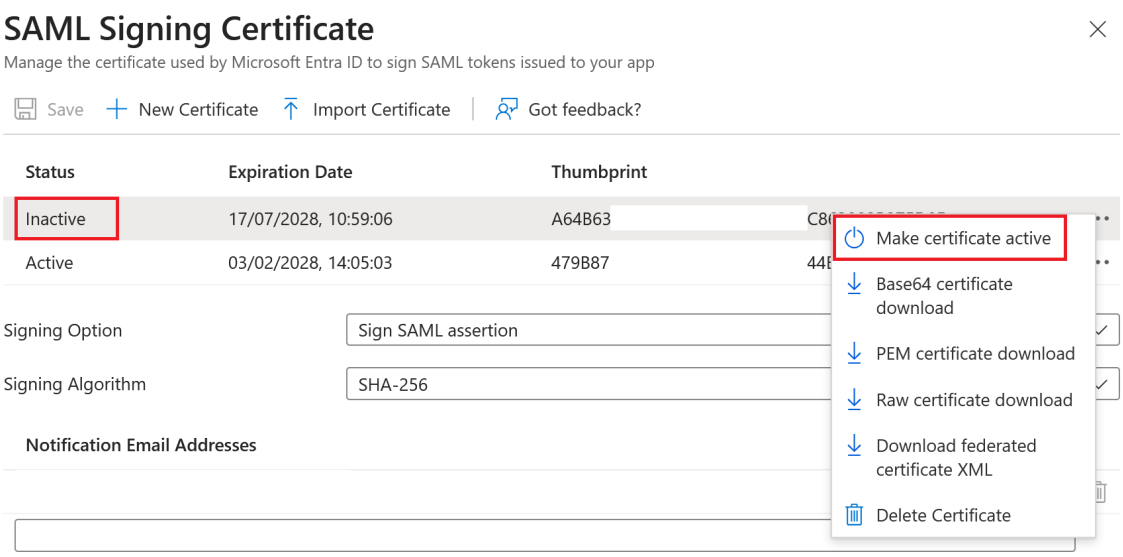
© 1997–2026 Citrix Systems, Inc. All rights reserved.



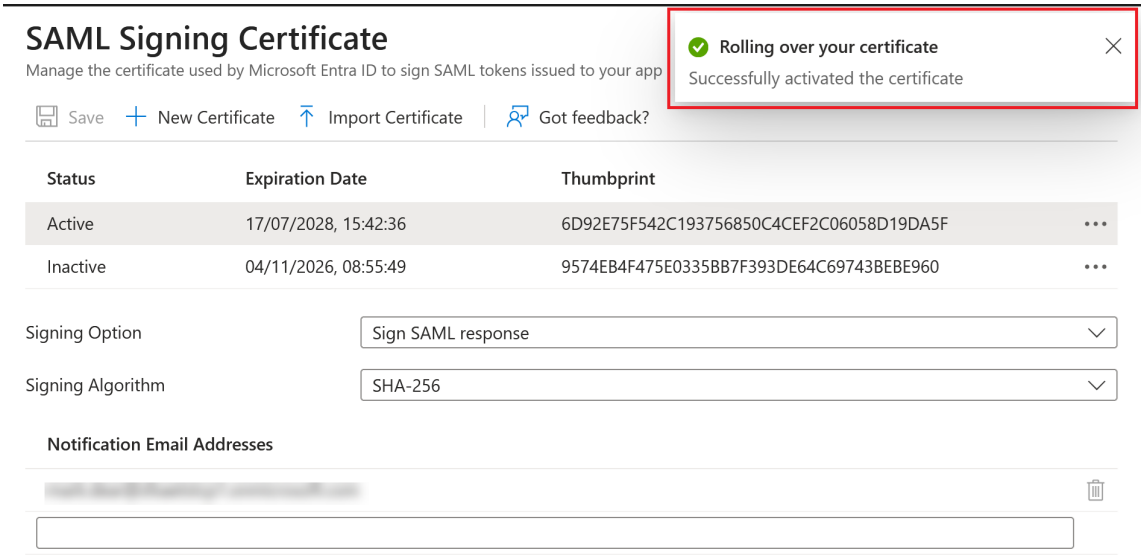
6. **Wait approximately 24 hours** then perform the **rollover action** inside your IdP and set the secondary IdP certificate to **active**. The method to rollover the certificate is different for every SAML IdP.

   > **Important:**
   >
   > Citrix's authentication platform performs caching of all IDP settings for resiliency and performance reasons. You cannot upload the replacement certificate into Citrix Cloud and then immediately rotate the certificate within your SAML application due to cached values. A delay between upload of the new certificate and activation of the new certificate within your SAML app is required. This delay allows the Citrix authentication cache to be updated with the newly uploaded certificate. A 24-hour delay is longer than the TTL value of the cache. This duration ensures that the new certificate is available when the SAML application switches to use it the next day.

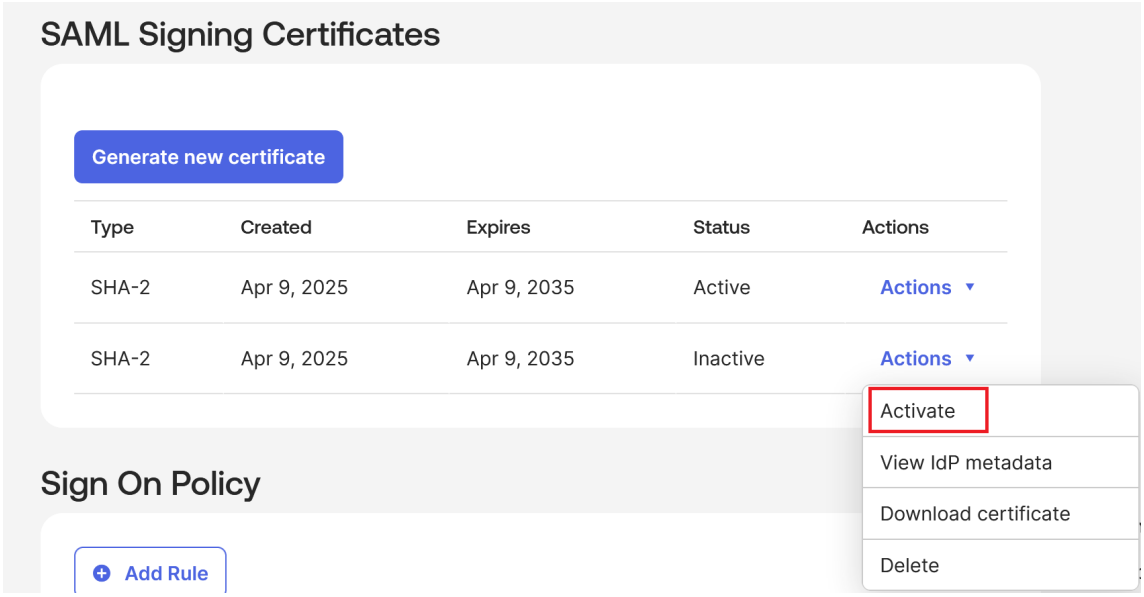
   Entra ID SAML Application:



© 1997–2026 Citrix Systems, Inc. All rights reserved.



Okta SAML Application:



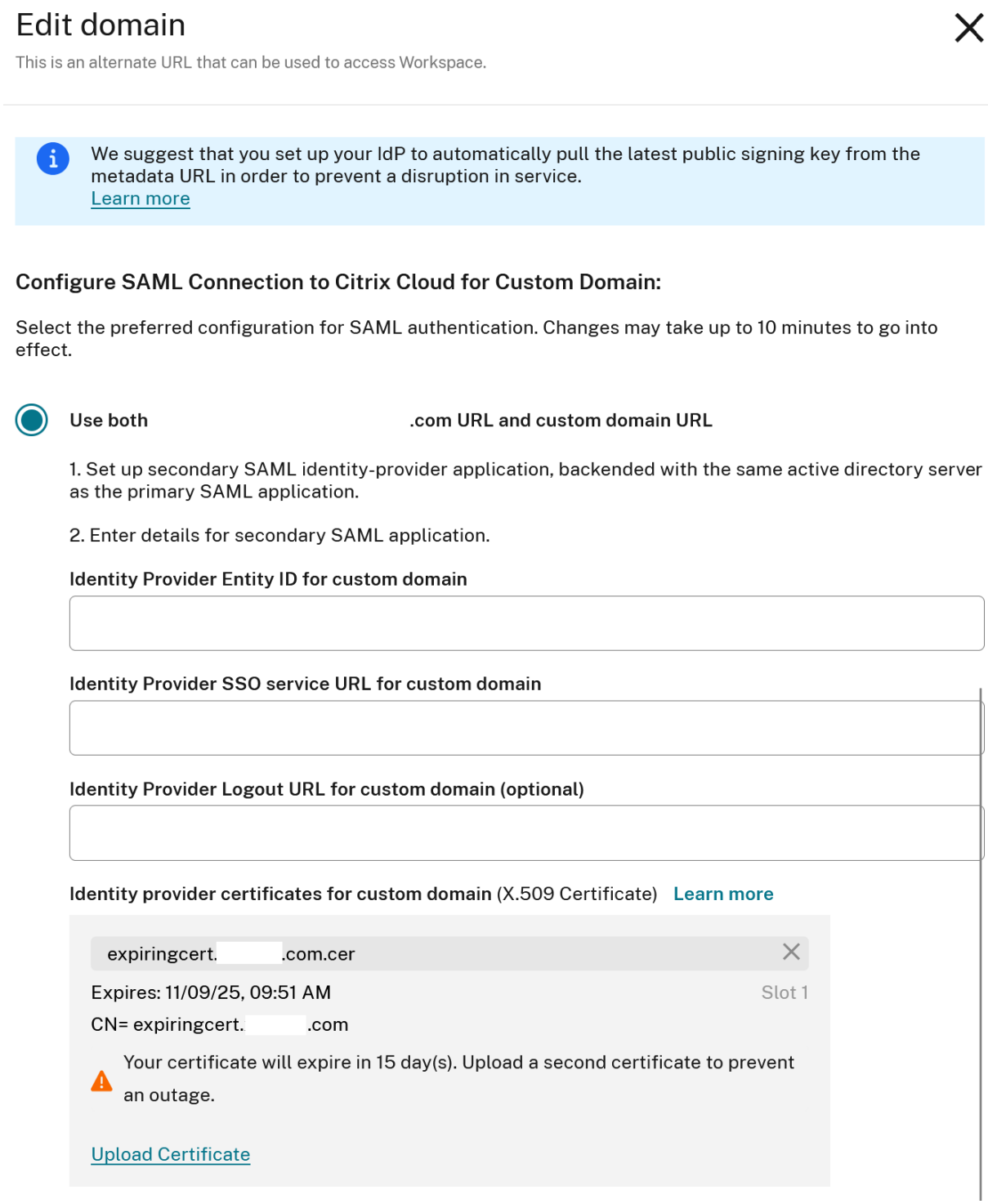
7. Test the SAML logon succeeds using either your store URL and/or the Citrix Cloud SAML Sign In URL and check the value of the signing certificate inside the SAML assertion.

Upload a Secondary SAML IdP certificate to an existing store Custom Domain SAML connection?

If you are required to update the IDP certificate in use by a secondary SAML application that is configured to support a store Custom domain then follow the same steps as documented above.

1. Navigate to **StoreFront Cloud > Access > Custom store URL > Select the 3 dots > Edit**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



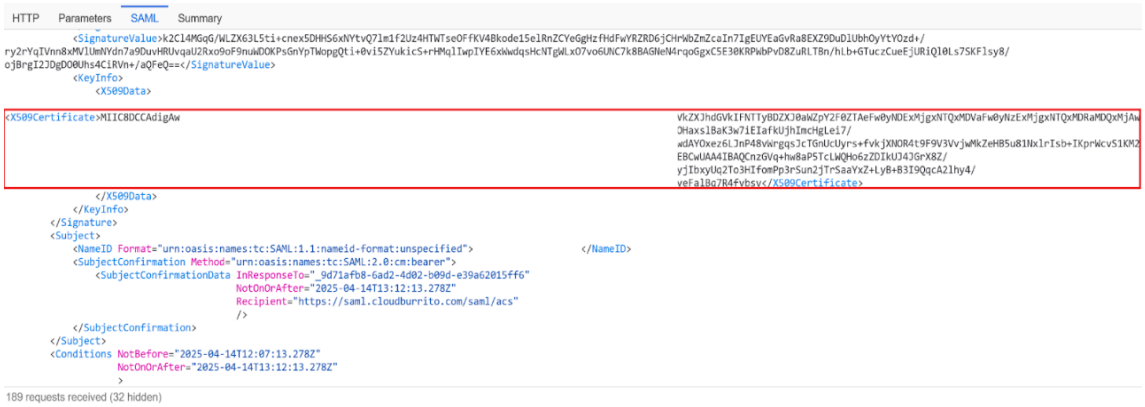
Troubleshooting IdP Signing Certificate Rotations If you encounter any SAML logon issues after performing an IdP certificate rotation then collect a SAML tracer file and examine the certificate base64 data inside the SAML response.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Start the SAML tracer capture **before** entering either the store URL or Citrix Cloud GO URL into your browser. Ensure you capture the entire authentication process from start to end.
2. Perform a SAML logon to either store or Citrix Cloud using your IdP and complete the authentication step when you are prompted for credentials.
3. Locate the SAML response from your IdP sent to the Citrix Cloud SAML endpoint `https://saml.cloud.com/saml/acs` and the entry inside SAML tracer file here.



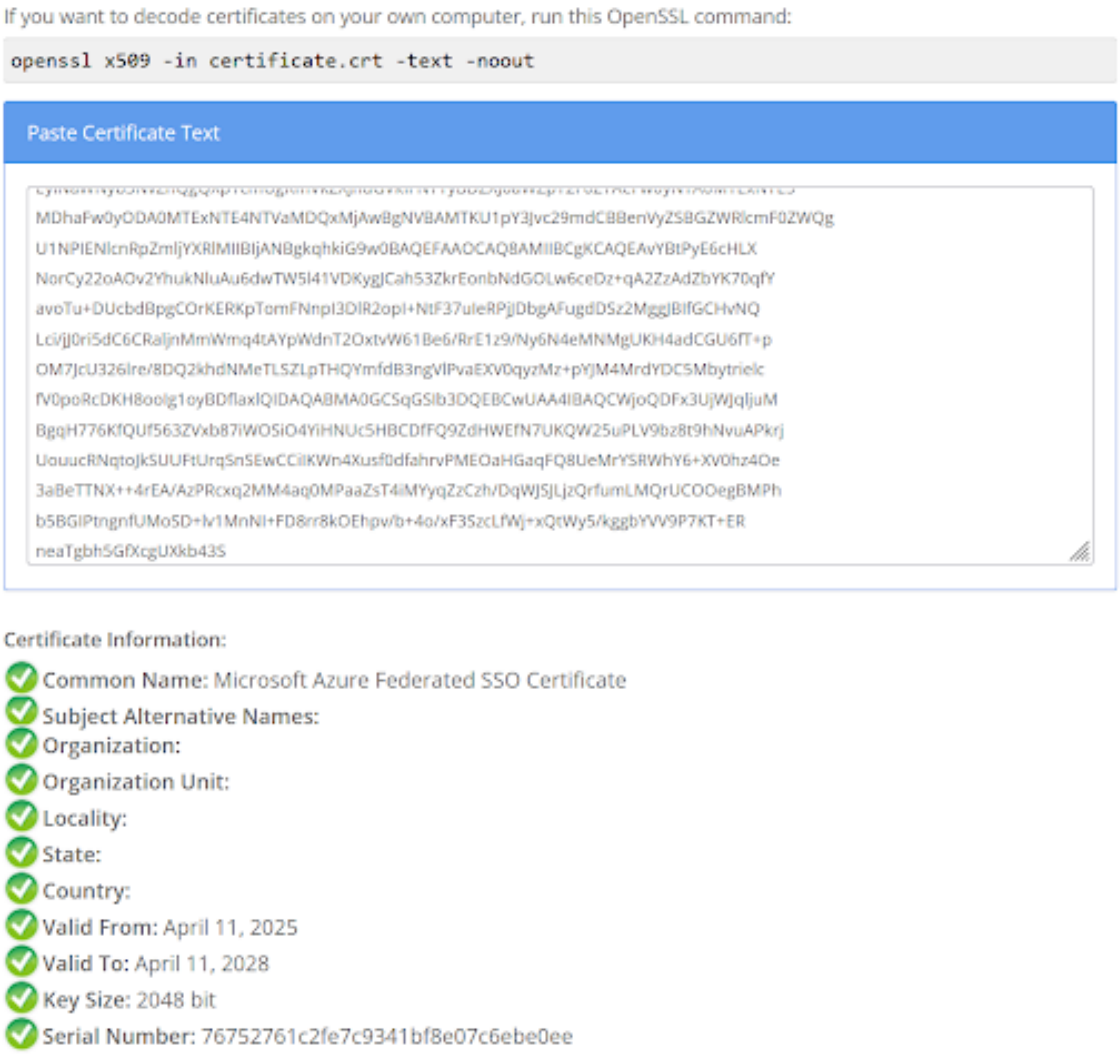
4. Locate the certificate section within the SAML XML and copy the IDP signing certificate's base64 data to a suitable tool to decode it.



> **Important:**
>
> This step assumes that you have followed Citrix's SAML recommended configuration and used HTTP POST as the SAML binding within your Citrix Cloud SAML Connection.

5. Decode the certificate from its base64 data and check it corresponds to the active certificate in the SAML IdP with the correct date and time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. If the certificate obtained from the SAML response in steps 4 and 5 is not as expected, activate the correct certificate inside your IdP. Check the active certificate within your SAML application. This certificate is included in the SAML response.

Advanced SAML Scenarios and correct use of cip_forest and cip_domain within the SAML Assertion

June 22, 2026

Author:
Mark Dear

This article describes Citrix Cloud or store advanced SAML configurations involving multiple con-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

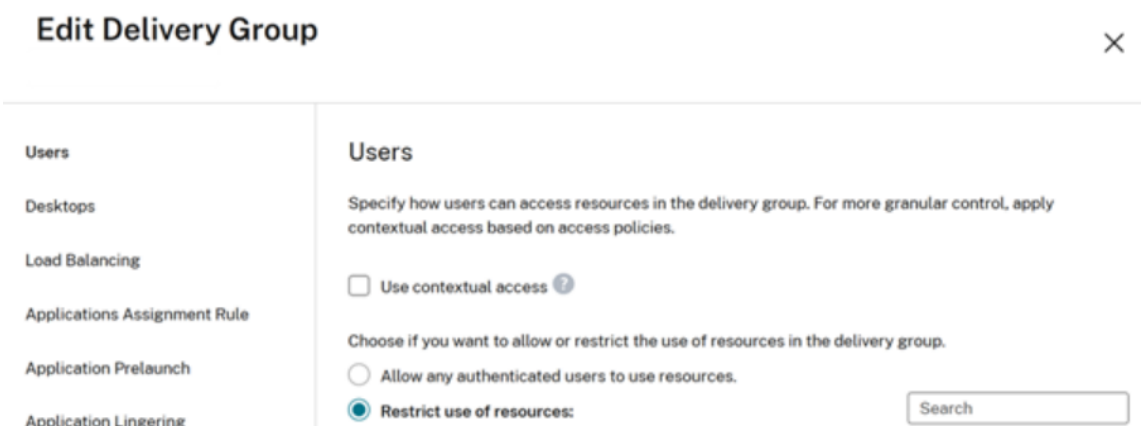
nected Active Directory Forests and Domains. This article is intended for large enterprises with complex AD deployments and should be implemented by architect-level Citrix Cloud, IdP, and AD administrators. The most common use of this advanced SAML configuration is in Mergers and Acquisitions scenarios where a large enterprise is formed from many smaller organizations with different AD infrastructure, multiple forests, and different populations of AD BackEnd users with different UPNs. Conditional Authentication is also often required in Mergers and Acquisitions scenarios.

The optional cip_forest and cip_domain claims give the Citrix Cloud administrator greater control over which Citrix Cloud Connectors are used to look up AD backend user accounts during SAML authentication. Citrix Cloud with SAML supports many advanced account mapping use cases, which are not possible with other Citrix Cloud federated OIDC authentication methods such as Okta IdP or Entra ID IdP.

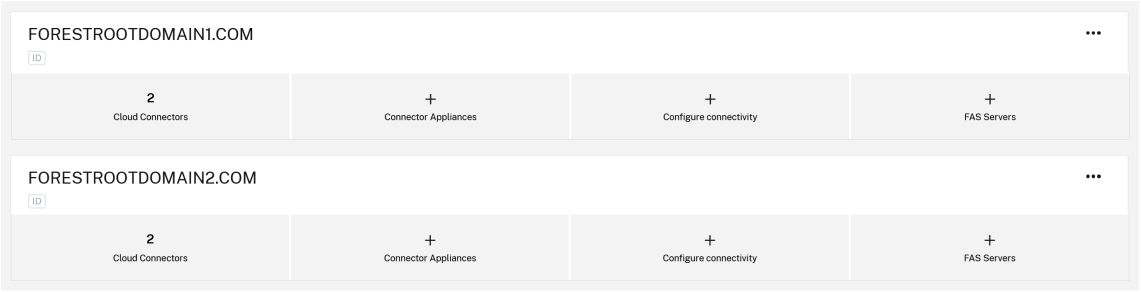
Prerequisites

- Use the default Citrix Cloud SAML flow, which uses AD identities to authenticate the end user.
- An extensive understanding of your AD forest or domain infrastructure and where your store end user's identities are.
- Citrix Cloud Connectors joined to the correct AD forest and domain and joined at the correct AD domain level.
- Knowledge of the existing resource locations and Citrix Cloud Connectors that are already configured within your Citrix Cloud tenant.
- Multiple AD forests connected to Citrix Cloud should not have any Active Directory trusts between them.
- An understanding of what a front-end (Entra ID, Okta, Duo) and BackEnd user (AD) identity means.
- Front-end and BackEnd user identities must be linked through matching UPNs. Linking a pair of front end and BackEnd user identities that do NOT have matching UPNs is NOT supported.
- An understanding of where each UPN suffix resides inside Active Directory and whether a particular UPN suffix is ambiguous and exists in multiple connected AD forests.
- DaaS VDAs should be AD domain joined.
- DaaS Applications and Desktops should be published to AD Identities.
- Universal AD groups are mandatory when mapping delivery group resources to AD groups in DaaS.
- DaaS delivery groups must be set to "Restrict use of resources"and should be assigned to the correct Universal AD groups. The use of "Allow any authenticated users to use resources"within DaaS delivery groups is NOT supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- FAS servers joined to the correct AD Forest and domain joined at the correct AD level. FAS servers are needed for SSON to AD domain joined VDAs during DaaS launches.



- You might also be required to implement Conditional Authentication if you have multiple SAML apps and you require one SAML app per connected AD forest. Each SAML app might require a different set of values for cip_forest and cip_domain in Mergers and Acquisitions scenarios.

FAQ

If I am sending cip_sid in the SAML assertion do I need to also send cip_forest and cip_domain optional claims?

No. If your SAML application is configured to send the cip_sid claim and it is included in the SAML assertion, then Citrix Cloud will always be able to correctly identify which forest and domain the AD backend user is in. cip_forest and cip_domain are not required.

> **Important:**
>
> - SAML scenarios where sending cip_sid in the SAML assertion is not possible and might require the use of cip_forest and cip_domain instead.
> - Front-end users that contain the incorrect SID, which doesn't match the SID of the Backend AD user mapped inside DaaS delivery groups.
> - Front-end users that have no embedded SID at all such as native Okta, Entra ID, or Duo users

© 1997–2026 Citrix Systems, Inc. All rights reserved.

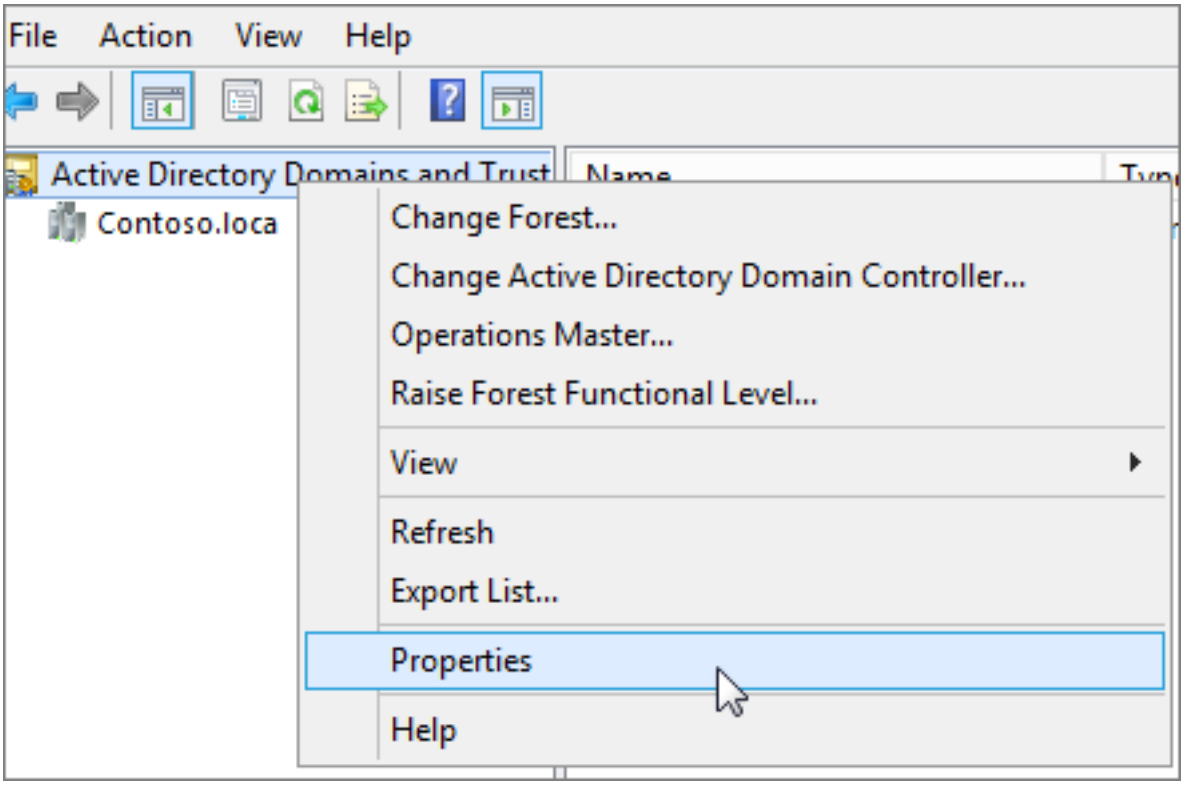
> that were not created inside the IdP through AD import tools.

What is an AD Implicit UPN suffix?

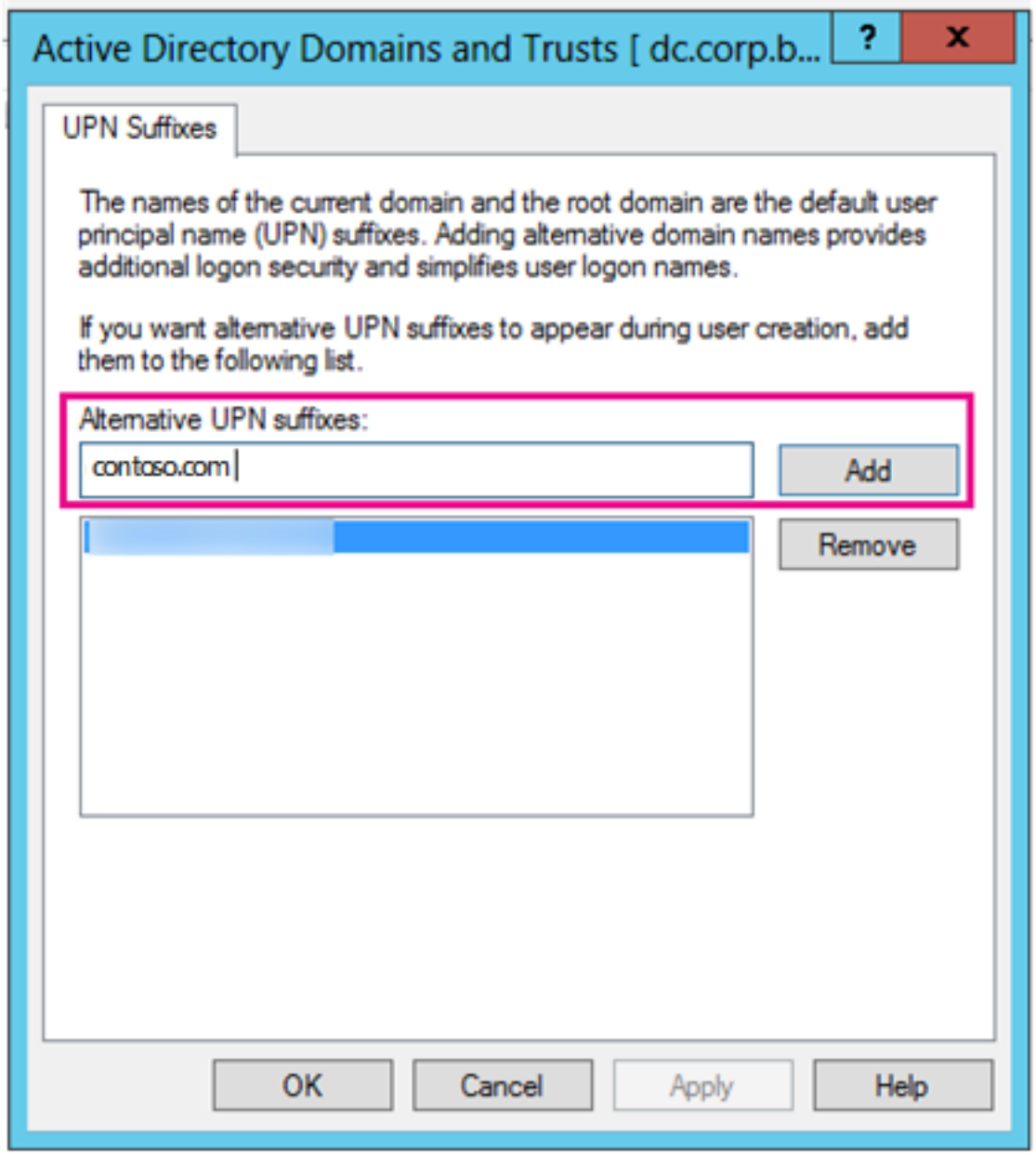
The implicit UPN is automatically created by Active Directory and is based on the user's sAMAccount-Name and the forest's DNS name. Implicit UPNs are always unique within an AD forest because they are derived from the sAMAccountName and the domain's DNS name, which are unique within the AD forest. For Example `@rootforestdomain.local`

What is an AD Explicit (ALT) UPN suffix?

An explicit UPN suffix is a custom domain name added by AD administrators in Active Directory Domains and Trusts. For Example `@rootforestdomain.local`



© 1997–2026 Citrix Systems, Inc. All rights reserved.



Important:

Windows AD PowerShell allows you to create AD users with any UPN suffix you specify even if that UPN suffix does not exist inside your AD forest. The alternative UPN Suffix that you want to use MUST exist within the AD forest as the Citrix Cloud Connectors depend on this list to look up the backend account users. If the alternative UPN suffix is not configured in the AD forest as shown in the screen shot above, then Citrix Cloud will not be able to match your front-end identity to an appropriate BackEnd AD account.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What is UPN ambiguity and why is it a problem for Citrix Cloud and DaaS?

UPN ambiguity is a situation that can arise if `duplicateuser@domain.com` exists in 2 or more AD forests connected to Citrix Cloud. The UPN suffix @domain.com alone, cannot be used to determine the correct AD backend user when two versions of `duplicateuser@domain.com` exist. This can cause DaaS resources to fail to enumerate at all, or incorrect DaaS resources published using AD domain joined VDAs might show inside the store.

Why are universal AD groups a requirement?

Universal AD groups are stored in the Global Catalog (GC), making them visible to all domain controllers throughout the forest. This allows them to be used for assigning permissions to resources located in any domain within the same forest.

> **Important:**
>
> The use of AD Universal Groups is a requirement for all SAML configurations not just advanced configurations involving cip_forest and cip_domain. Using other AD group types such as global can lead to failed resource enumerations in store.

It is recommended you read this Microsoft article regarding AD group scope.

Why is the use of "Allow any authenticated users to use resources"not recommended within DaaS delivery groups?

Configuring **Allow any authenticated users to use resources** will cause resources published using AD domain joined VDA's to appear inside store for AD user identities, which are not inside the same domain and forest. Launching resources from VDA's domain joined in Forest 2 using a store AD end user identity in Forest 1 will not succeed.

Can I send just cip_forest on its own or just cip_domain on its own in the SAML assertion?

No. If you want to specify a particular AD forest and domain context for the backend user lookup you must provide both optional claims in the SAML assertion.

When specifying a value for cip_forest what UPN suffix should I use?

The Implicit UPN suffix for the AD forest should be used. Do not specify a value of an ALT UPN suffix that has been added to the AD forest inside the cip_forest claim. This is because there are AD topologies where the same ALT UPN suffix might have been added to more than one AD forest connected to Citrix

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cloud. The Implicit UPN suffix and DN is never ambiguous to Citrix Cloud unless two different AD forests with the same DN such as DC=duplicate,DC=com are connected to Citrix Cloud (an unlikely scenario).

When should the values for cip_forest and cip_domain be the same or different from each other?

Scenario 1: Your Citrix Cloud Connectors are domain joined at the forest root level and the backend AD account users reside within the root domain within the connected AD forest.

cip_domain and cip_forest should have the same value.

cip_forest = "forestrootdomain.com"

cip_domain = "forestrootdomain.com"

Scenario 2: Your Citrix Cloud Connectors are domain joined to a child domain in the AD forest hierarchy. The backend AD users exist within "childdomain.forestrootdomain.com"within your AD forest.

cip_domain and cip_forest should have different values.

cip_forest = "forestrootdomain.com"

cip_domain = "childdomain.forestrootdomain.com"

Can I hardcode the values of cip_forest and cip_domain within the SAML assertion?

Yes, but only if the entire population of BackEnd AD users, which are mapped to DaaS resources reside in the same AD forest. Hard coding the values of cip_forest and cip_domain requires every front-end user to have their corresponding backend AD accounts in the same AD forest and domain.

Can I specify different values for cip_forest and cip_domain within the SAML assertion dynamically?

Yes if your SAML provider allows this through claims transformation rules. If you have different populations of front-end users with different UPN suffixes it is possible to specify the values of cip_forest and cip_domain dynamically using switching conditions like group membership. This is possible within Entra ID SAML applications and might also be possible in other SAML IdPs that support claims transform rules.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

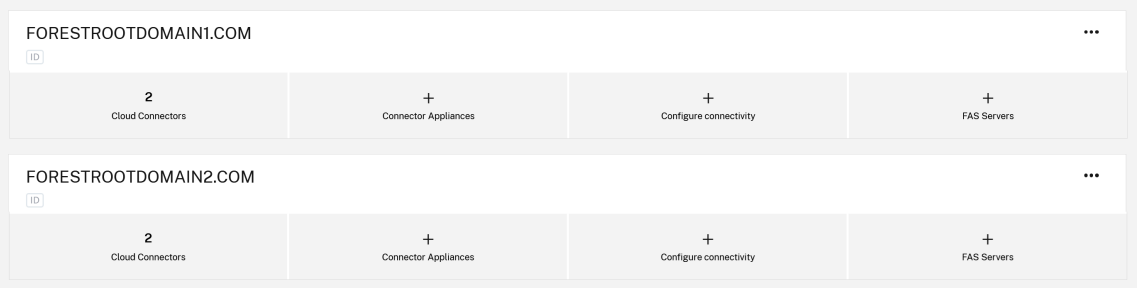
Where should I put my FAS servers so launch SSON to AD domain joined VDAs succeeds?

FAS servers should be domain joined and configured within each of the backend AD forests where the BackEnd AD accounts reside. It is recommended you domain join your FAS servers at the AD forest root domain level.

AD Topologies where cip_forest and cip_domain are required in the SAML assertion

Scenario 1: The SAML end user's UPN is ambiguous and exists in multiple AD forests connected to Citrix Cloud

- The Citrix Cloud tenant has two or more resource locations and multiple AD forests or domains connected to Citrix Cloud.



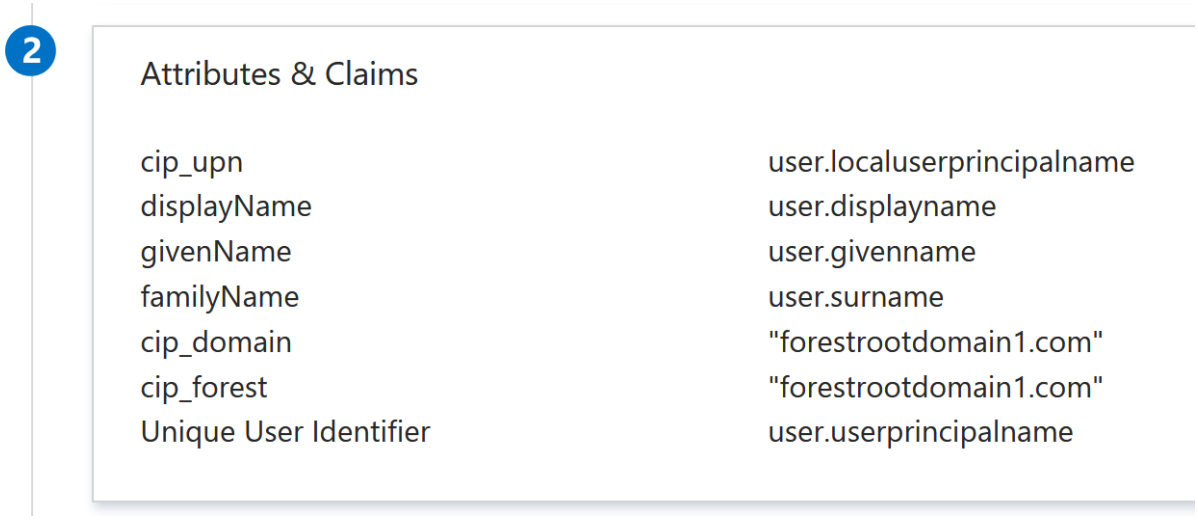
- ResourceLocation1 contains Citrix Cloud Connectors, which are domain joined to AD forestrootdomain1.com at the root forest level.
- ResourceLocation2 contains Citrix Cloud Connectors that are domain joined to AD forestrootdomain2.com at the root forest level.
- forestrootdomain1.com and forestrootdomain2.com both have the same UPN @domain.com suffix.
- Duplicate users might also exist inside forestrootdomain1.com and forestrootdomain2.com with the same UPN `duplicateuser@domain.com` but different SID and OID values.

Problem: the attempt to look up the correct backend AD account using `username@duplicatesuffix.com` does not always return the correct AD BackEnd user due to UPN ambiguity. Citrix Cloud cannot determine which AD forest and Citrix Cloud Connectors to use so the wrong DaaS resources might be shown in store or no DaaS resources are returned at all.

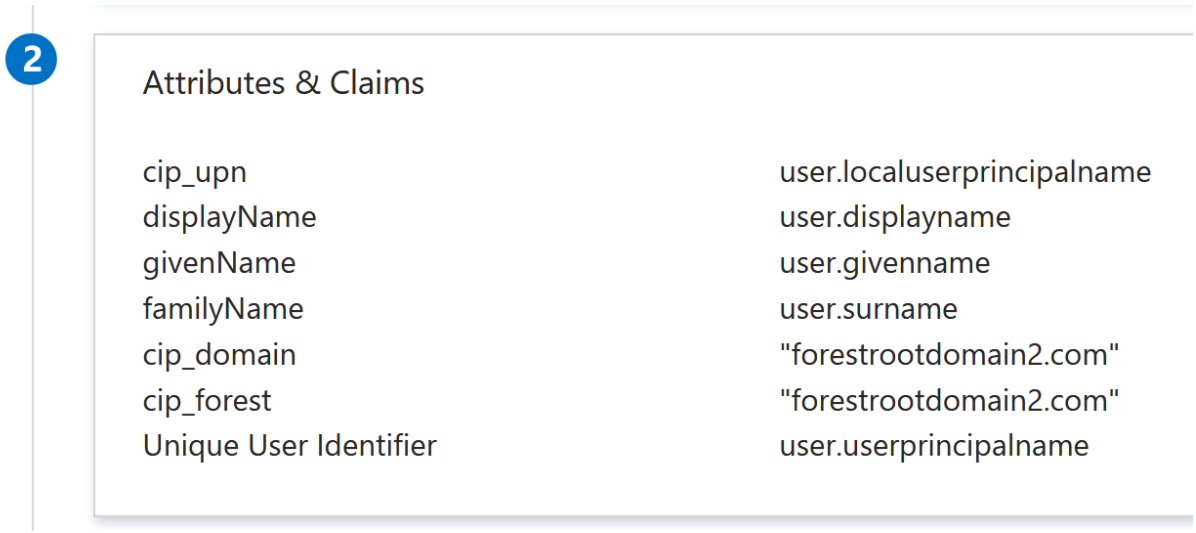
Solution: configure two different SAML applications, one for each connected AD forest and include the corresponding cip_domain and cip_forest values for the correct AD forest in the SAML assertion. This provides Citrix Cloud with the additional forest and domain context to ensure the correct BackEnd AD user is "looked up" when `username@duplicatesuffix.com` exists in multiple connected forests.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SAML App 1 forestrootdomain1.com:



SAML App 2 forestrootdomain2.com:



Map the two DaaS delivery groups correctly using the correct AD backend groups.

Scenario 2: Cloud Connectors joined at child domain level and store users at child domain level

Citrix Cloud tenant has a resource location, which contains two Citrix Cloud Connectors, which are domain joined at the "childdomain.forestrootdomain.com"level instead of the recommended "forestrootdomain.com"level. store users exist inside the childdomain.forestrootdomain.com child domain. Users are configured to use the root domain UPN suffix such as `username@forestrootdomain.com`.

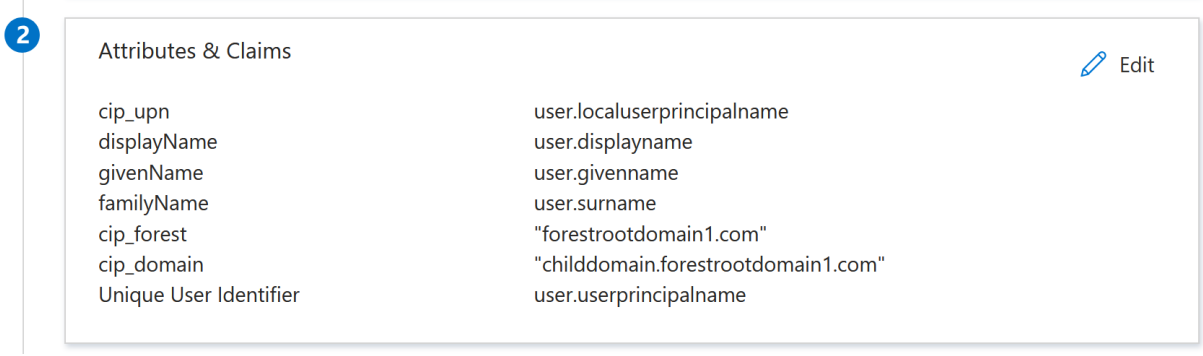
Problem: Citrix Cloud performs the AD account lookup using "forestrootdomain.com", which does not match a connected AD domain.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Solution: Specify the child domain context in the SAML assertion so that the AD account user is "looked up"from the correct AD child domain and forest context.

cip_forest = `forestrootdomain.com`

cip_domain = `childdomain.forestrootdomain.com`



Configure ADFS as a SAML provider for store authentication

June 22, 2026

Author:
Mark Dear

This article describes how to configure the relying party trust that Citrix Cloud™ requires for signing in to stores or Citrix Cloud using SAML.

After you complete the steps in this article, you can configure the SAML connection between your ADFS server and Citrix Cloud as described in Connect SAML as an identity provider in Citrix Cloud. For guidance for entering the correct ADFS values for your SAML connection, see SAML configuration in Citrix Cloud in this article.

Prerequisites

The instructions in this article assume that you have an operating ADFS server deployment with Citrix FAS in your environment. Citrix FAS is required to provide single sign-on to VDAs during session launch.

For more information, refer to the following articles:

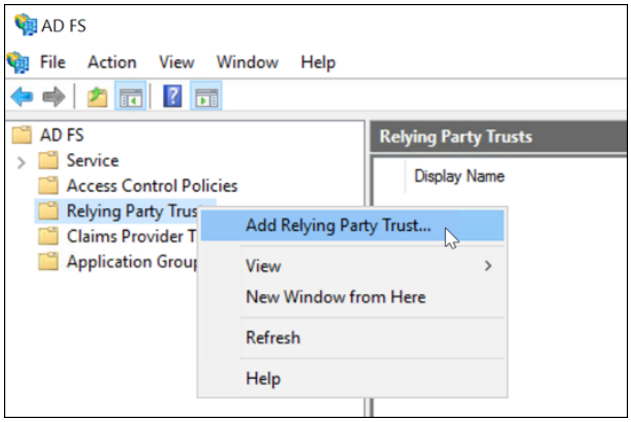
- Citrix FAS documentation:
  - Install and configure
  - ADFS deployment

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Tech Zone: Reference Architecture: Federated Authentication Service

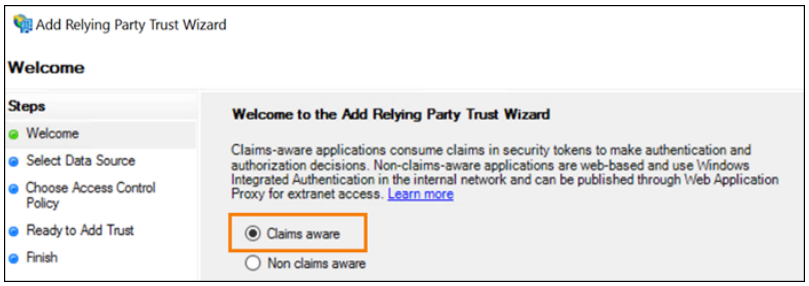
Configure a relying party trust for Citrix Cloud

1. From the AD FS management console, expand the **AD FS** node in the left pane.
2. Right-click **Relying Party Trust** and select **Add Relying Party Trust**.

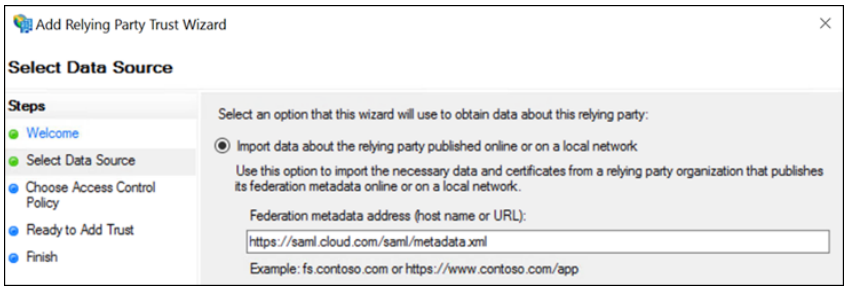


   The Add Relying Party Trust wizard appears.

3. Select **Claims aware** and then select **Next**.

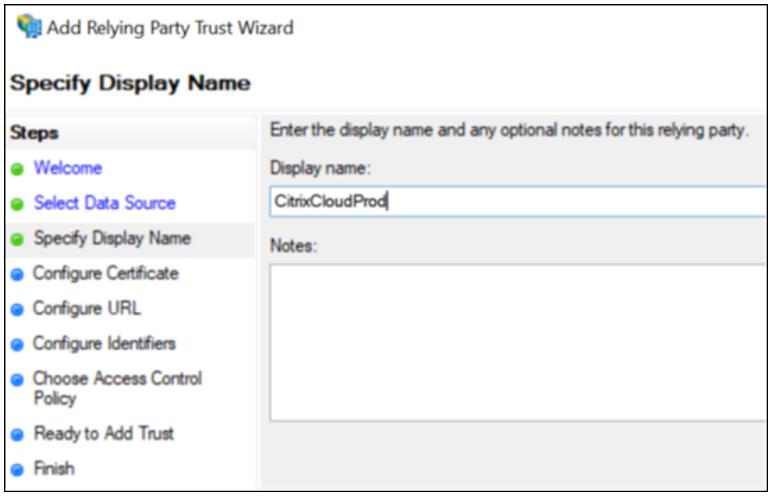


4. In **Federation metadata address**, enter `https://saml.cloud.com/saml/metadata.xml`. Select **Next**.

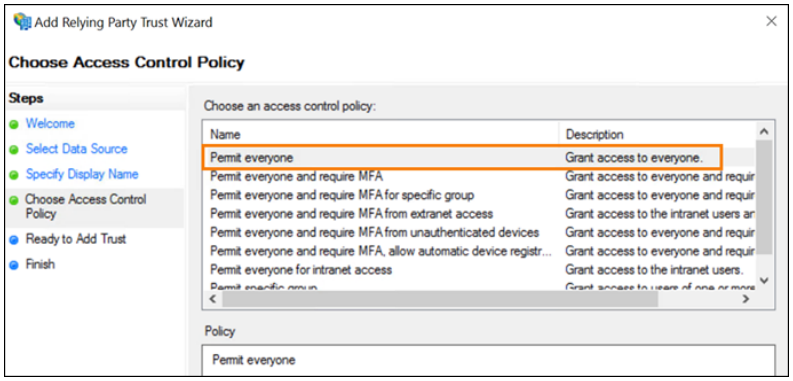


5. For the display name, enter `CitrixCloudProd`. Select **Next**.

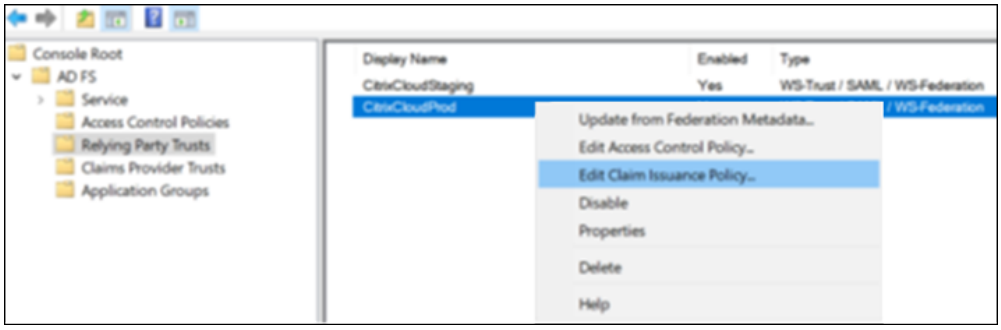
© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. For the access control policy, select **Permit everyone**. Select **Next**.



7. On the **Ready to Add Trust** screen, select **Next**.
8. On the **Finish** screen, select **Configure claims issuance policy for this application**. Select **Next**.



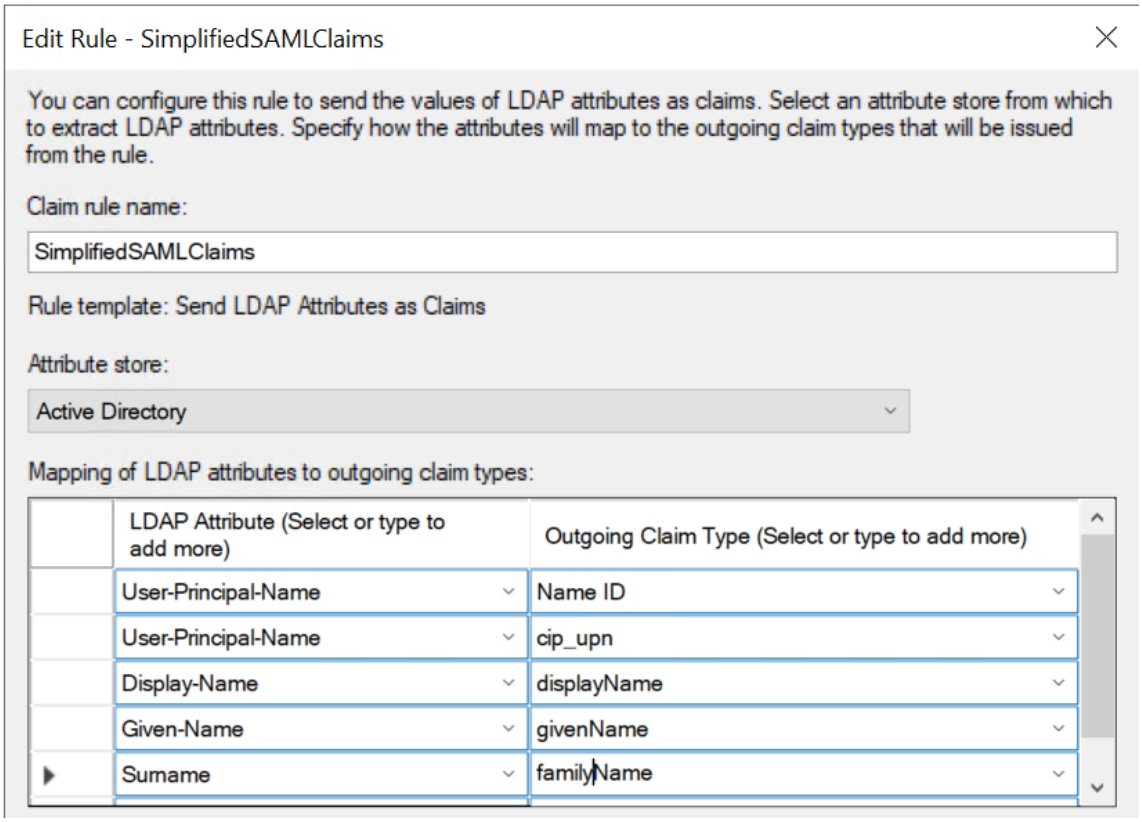
9. Right-click the newly-created relaying party trust and select **Edit Claim Issuance Policy**.
10. Click **Add Rule** and then select **Send LDAP Attributes as Claims**. Select **Next**.
11. In **Claim rule name**, enter `CitrixCloud`.
12. In **Attribute store**, select **Active Directory**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

13. Under **Mapping of LDAP attributes to outgoing claim types**, add the following LDAP attributes, exactly as shown:

LDAP attribute	Outgoing Claim Type
User-Principal-Name	Name ID
User-Principal-Name	cip_upn
Display-Name	displayName
Given-Name	givenName
Surname	familyName

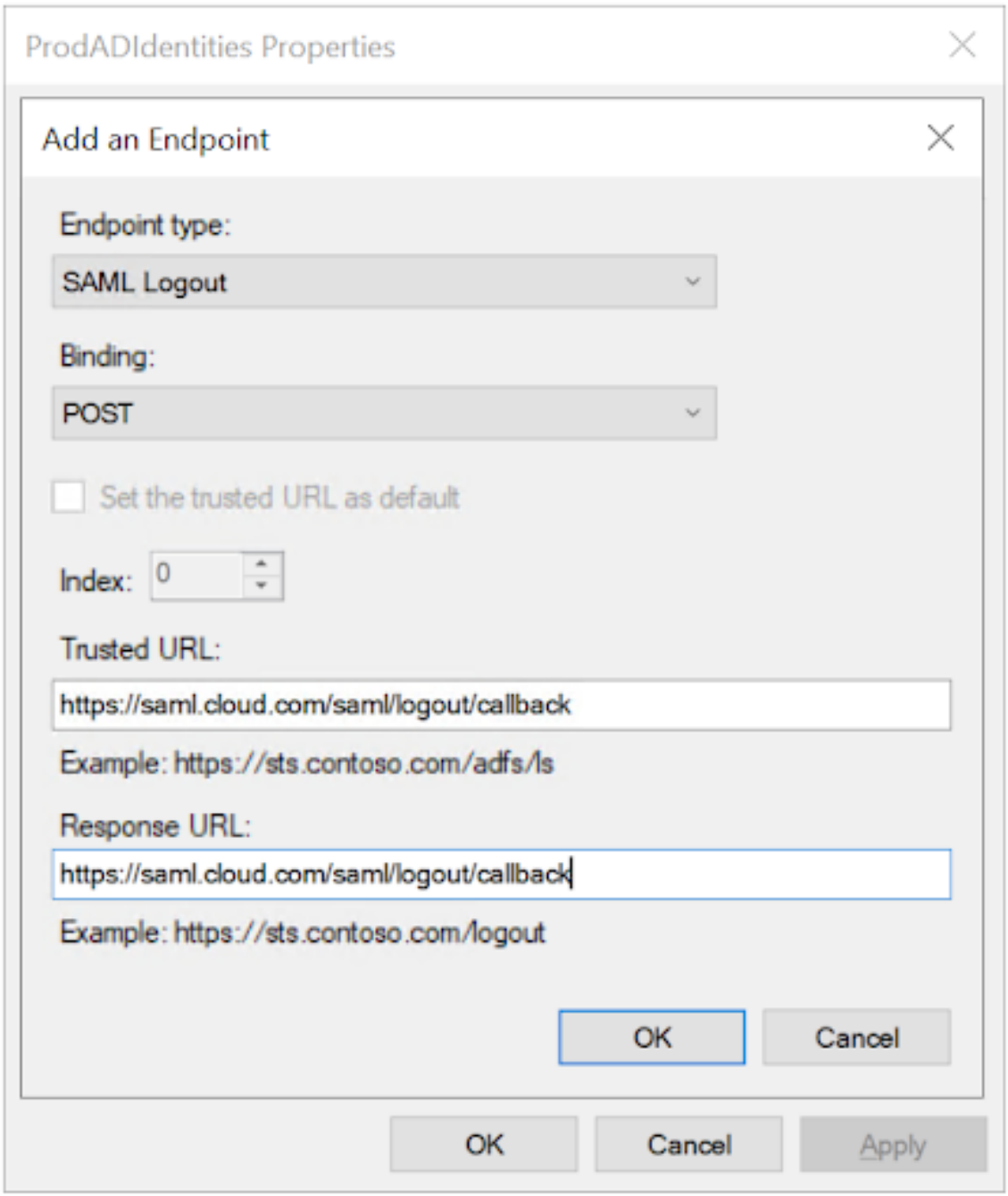
> **Important:**
>
> The NameID must always be the first claim added to the list of claims otherwise Single Logout (SLO) will not function correctly.



14. Select **Finish**.
15. Right click on the newly created Relaying Party trust called “CitrixCloudProd”and select properties.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

16. Select the **Endpoints** tab and click **Add SAML**.
17. Select the **SAML logout** from the endpoint type dropdown list.
18. Select the **POST** from the binding dropdown list.
19. Enter `https://saml.cloud.com/saml/logout/callback>` into both Trusted URL: and Response URL:



20. Click **OK** and **Apply**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Modify a Citrix Cloud relying party trust using PowerShell

If you've configured your ADFS server using the default "out of the box"configuration, the steps in this section enable you to update it so it meets the Citrix-recommended configuration. This task is required to resolve an issue where SAML Single Logout from Citrix Cloud or the store fails if the `nameidentifier` attribute isn't included in the claim rule set or isn't the first SAML attribute in the claim rule set.

> **Note:**
>
> You don't need to perform this task if you created your claim rule set using the steps in Configure a relying party trust for Citrix Cloud in this article.

To complete this task, you replace the existing rule set with a new claim rule set using PowerShell. The ADFS management console doesn't support this type of operation.

1. On the ADFS server, locate the PowerShell ISE. Right-click and select **Run as administrator**.
2. Back up your existing ADFS claim rules to a text file:

```
Get-ADFSRelyingPartyTrust -name "CitrixCloudProd" | Select-Object
    -ExpandProperty IssuanceTransformRules | Out-File "$env:
    USERPROFILE\desktop\claimrulesbackup.txt"
```

3. Download the claimrules.txt file that Citrix provides at https://github.com/citrix/sample-scripts/tree/master/citrix-cloud.
4. Copy the claimrules.txt file to your desktop.
5. Import the required claim rules using the claimrules.txt file:

```
Set-ADFSRelyingPartyTrust -Name "CitrixCloudProd" `
                      -MetadataUrl "https://saml.cloud.com/saml/
                         metadata" `
                      -AutoUpdateEnabled $True `
                      -IssuanceTransformRulesFile "$env:
                         USERPROFILE\desktop\claimrules.txt" `
                      -SignedSamlRequestsRequired $True `
                      -SamlResponseSignature "MessageAndAssertion"
                          `
                      -Enabled $True
```

Update SAML signing settings for the relying party trust using PowerShell

By default, ADFS relying party trusts have the following settings:

- EncryptClaims: True
- SignedSamlRequestsRequired: False

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- SamlResponseSignature: AssertionOnly

For increased security, Citrix recommends using signed SAML requests for both Single Sign-on (SSO) and Single Logout. This section describes how to update the signing settings of an existing relying party trust using PowerShell so they meet the Citrix-recommended configuration.

1. Obtain the current RelyingPartyTrust configuration on your ADFS server.

```
Get-ADFSRelyingPartyTrust -TargetName "CitrixCloudProd"
```

2. Update the **CitrixCloudProd** relying party trust settings.

```
Set-ADFSRelyingPartyTrust -Name "CitrixCloudProd" `
                          -SignedSamlRequestsRequired $True `
                          -SamlResponseSignature "MessageAndAssertion"
```

SAML configuration in Citrix Cloud

When you configure the SAML connection in Citrix Cloud (as described in Add SAML provider metadata to Citrix Cloud), you'll enter the values for ADFS as follows:

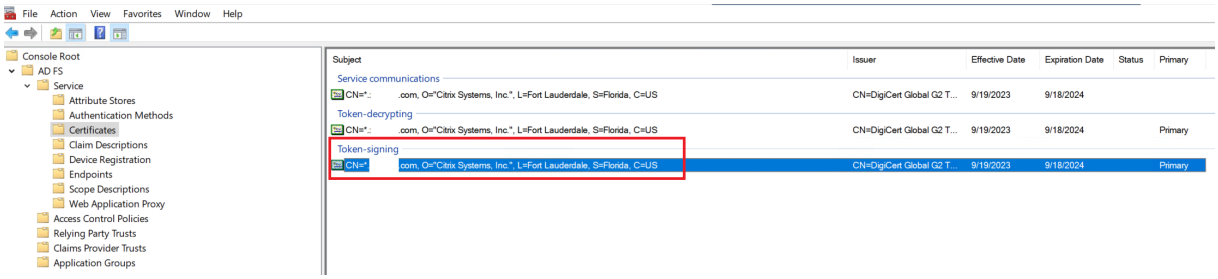
Use the default recommended values for the SAML connection within **Identity and Access Management > Authentication > Add an identity provider > SAML**.

In this field in Citrix Cloud	Enter this value
Entity ID	`https://adfs.YourDomain.com/adfs/services/trust`, where `YourDomain.com` is your ADFS server domain.
Sign Authentication Request	Yes
SSO Service URL	`https://adfs.YourDomain.com/adfs/ls`, where `YourDomain.com` is your ADFS server domain.
SSO Binding Mechanism	HTTP Post
SAML Response	Sign Either Response Or Assertion
Authentication Context	Unspecified, Exact
Logout URL	`https://adfs.YourDomain.com/adfs/ls`, where `YourDomain.com` is your ADFS server domain.
Sign Logout Request	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In this field in Citrix Cloud	Enter this value
SLO Binding Mechanism	HTTP Post

Export the ADFS signing certificate from within the MMC ADFS management console. See the screen shot below for which of the 3 certificates is the correct one to upload into Citrix Cloud within the SAML connection.



Configure Duo as a SAML provider for store authentication

June 22, 2026

Author:
Mark Dear

This article describes the required steps for configuring a Duo SAML application and SAML connection between Citrix Cloud™ and your SAML provider. Some of these steps describe actions that you perform in the Duo SAML provider's administration console.

Prerequisites

Before you complete the tasks in this article, ensure that you've met the following prerequisites:

- A Duo cloud tenant.
- A Duo authentication proxy inside your AD forest.
- An Active Directory LDAPS connection which syncs your AD users to Duo.

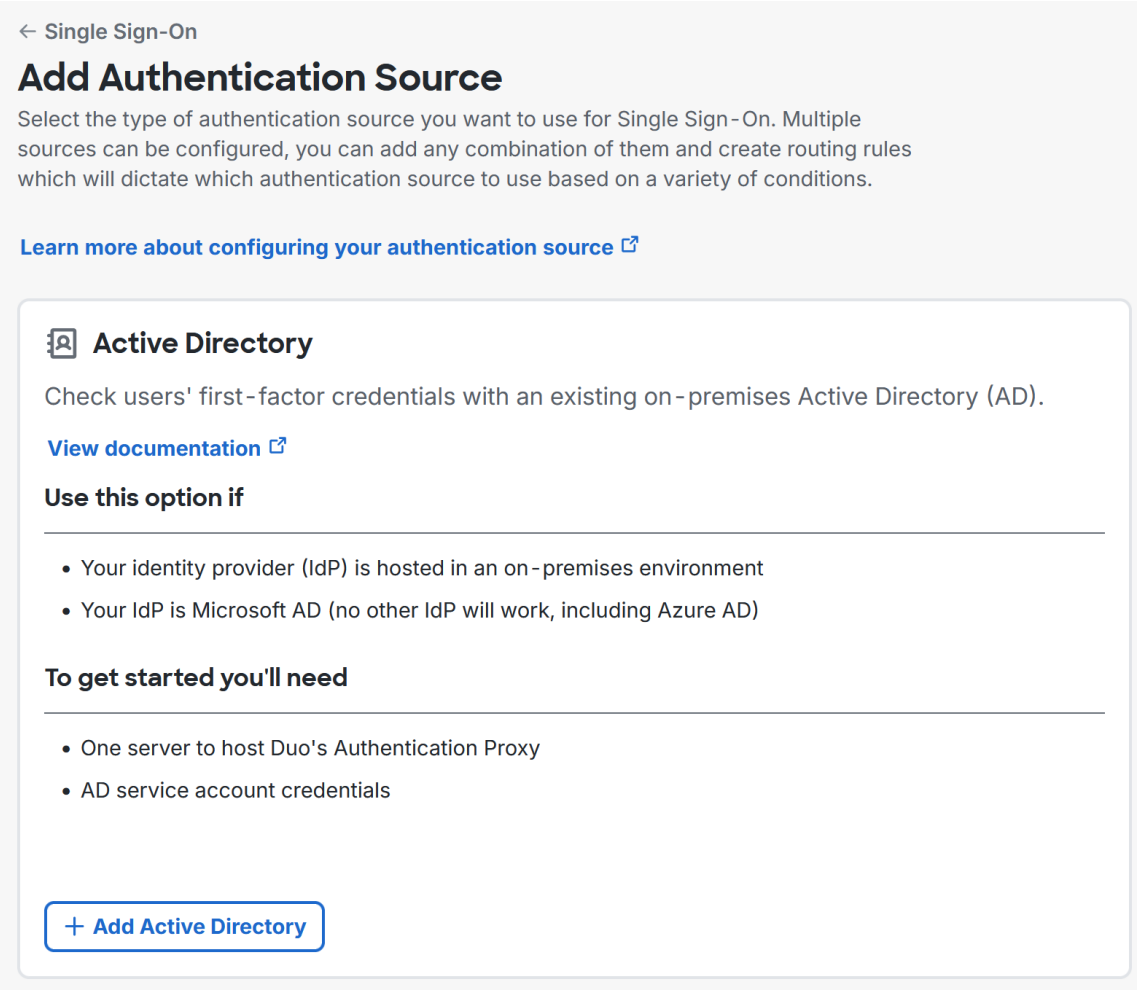
Configure Active Directory Synching to your Duo tenant

Follow the Duo documentation on connecting your on-premises AD to Duo and importing users for SAML.

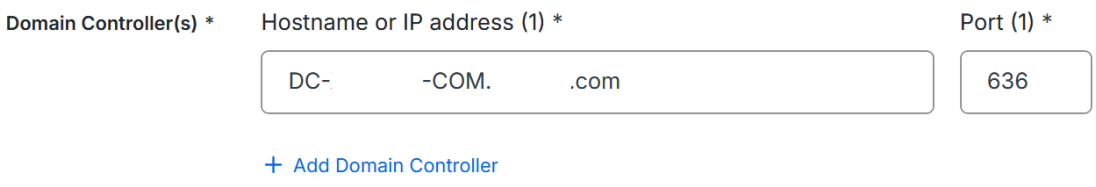
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create an Active Directory LDAPS Connection

1. Select **Applications > SSO Settings > Add Source > Active Directory > Add Active Directory** .

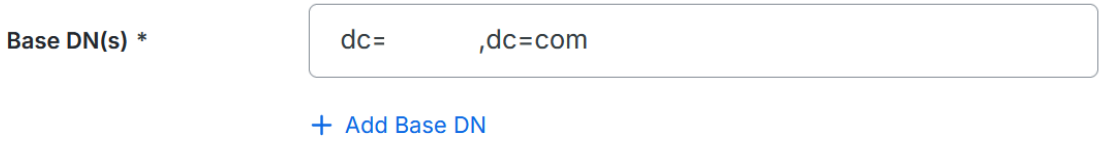


2. Enter a Display Name for the LDAPS connection to your AD forest.
3. Enter the FQDN of your domain controller.

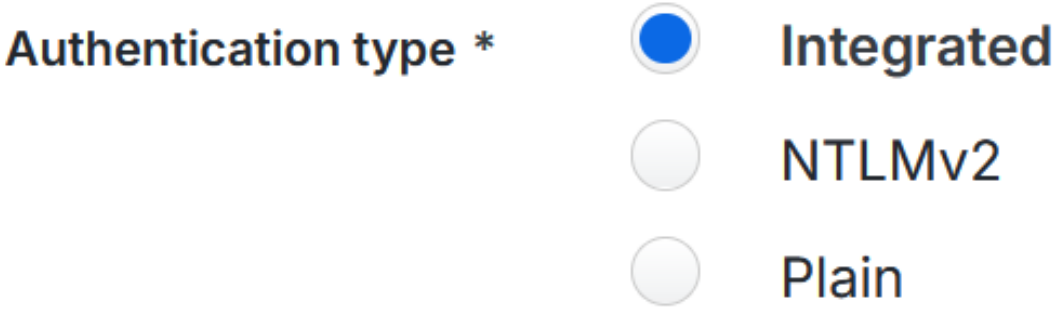


4. Configure the Base DN of your AD domain.

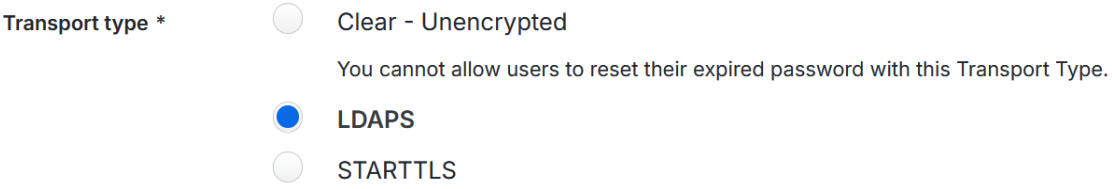
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Select Integrated as the Authentication Type.



6. Select LDAPS as the Transport Type.

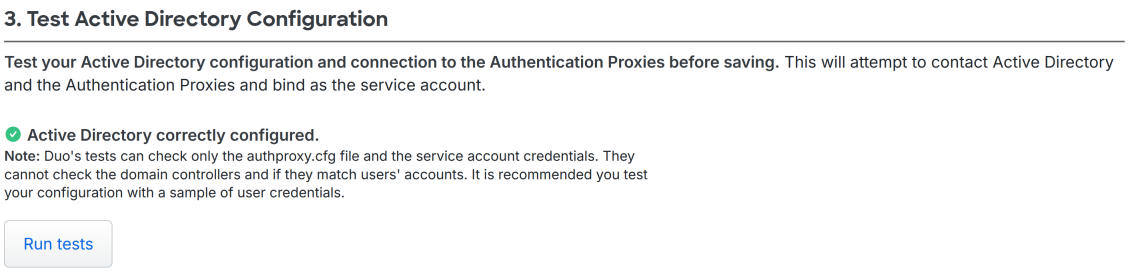


7. Tick SSL Verify Hostname.
8. Enter both the Domain Controller certificate and then the Private Enterprise certificate authority CA certificate that was used to sign your Domain certificate.
9. Enter the PEM formatted certificates according to the follow example

```
-----BEGIN CERTIFICATE-----
`<base64 Domain Controller Certificate>`
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
`<base64 Certificate Authority Certificate used to sign the Domain
    Controller Certificate above>`
-----END CERTIFICATE-----
```

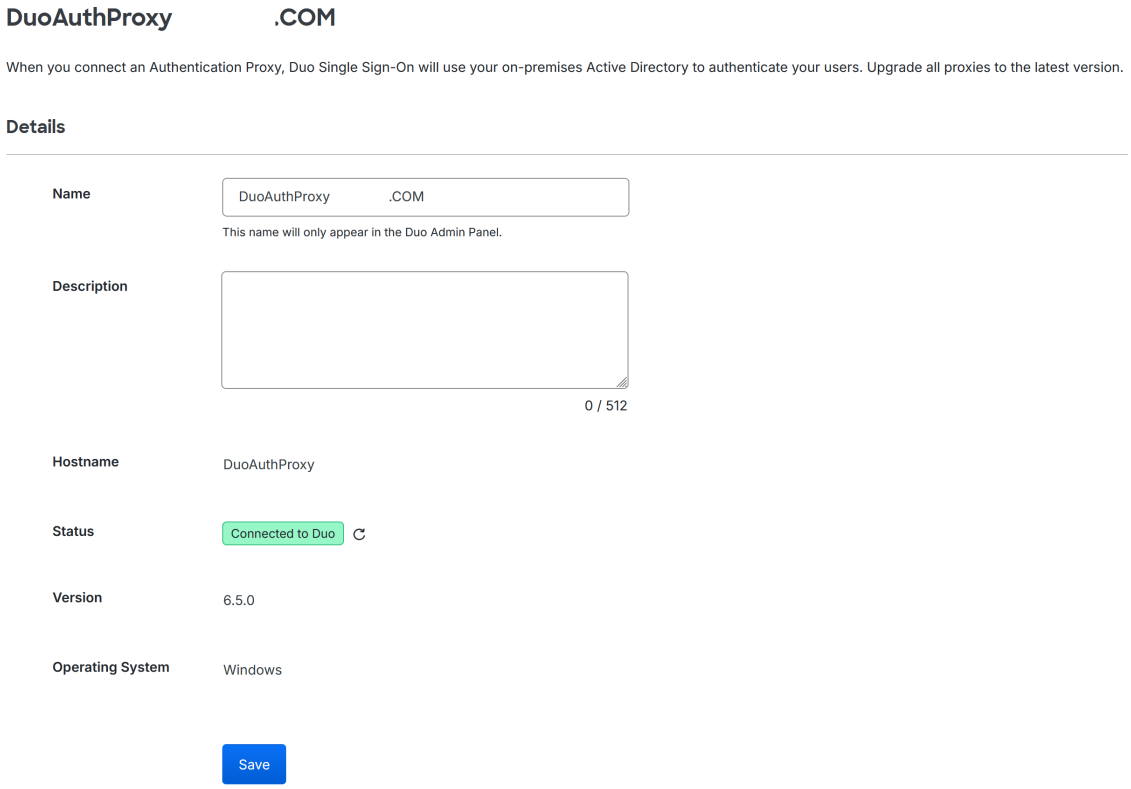
10. Test your LDAPS connection.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



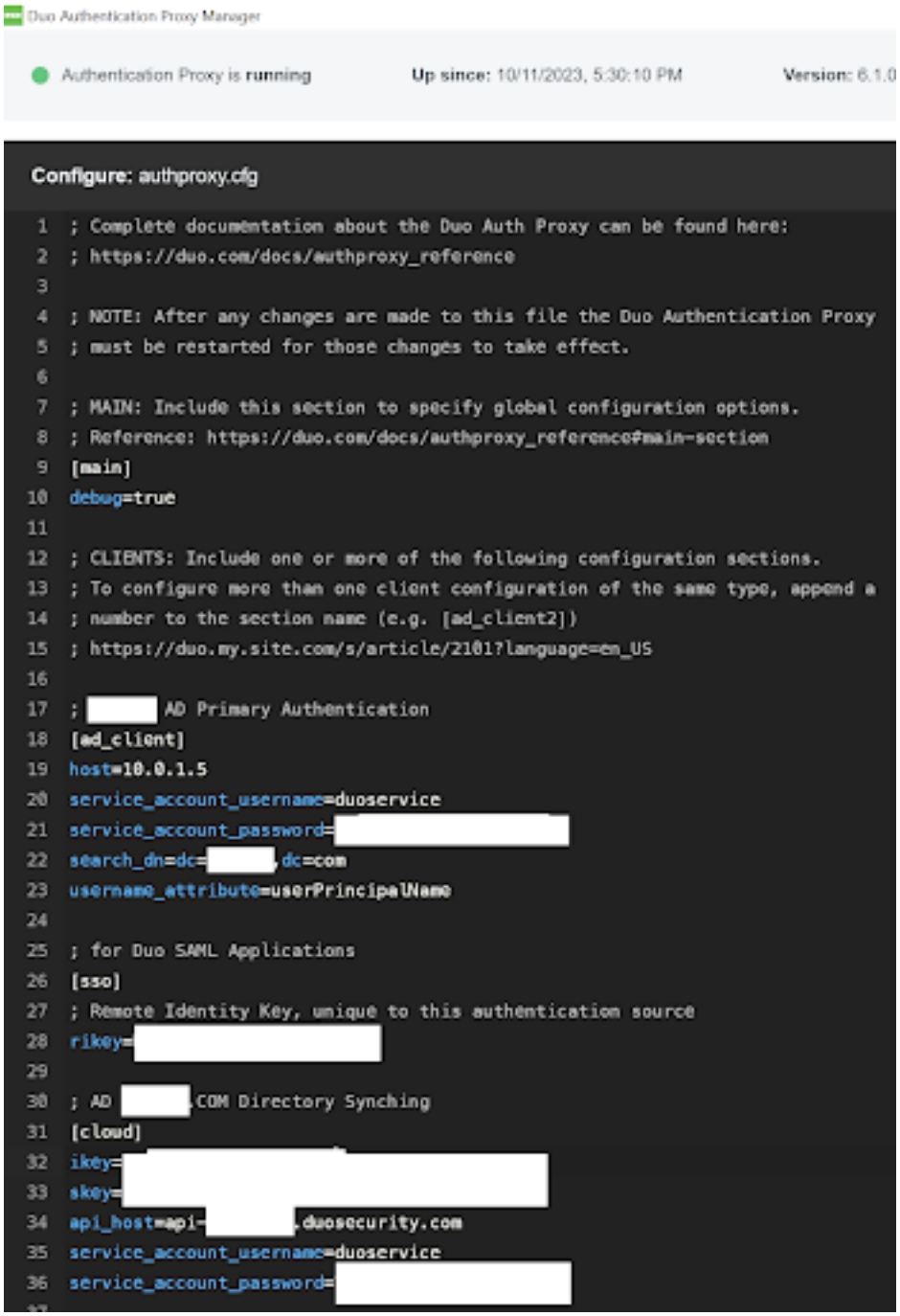
Configure your Duo authentication proxy config file for SAML

1. Check your Duo Auth Proxy configuration is healthy and showing as **Connected to Duo**.



2. Log into your Duo authentication proxy and add a SAML [sso] section to its config file using the **Remote Identity (rikey)** provided from the Duo admin console. The Duo Authentication Proxy uses a shared secret to communicate with the Duo cloud service. This secret is generated during the initial installation or configuration of the Authentication Proxy.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

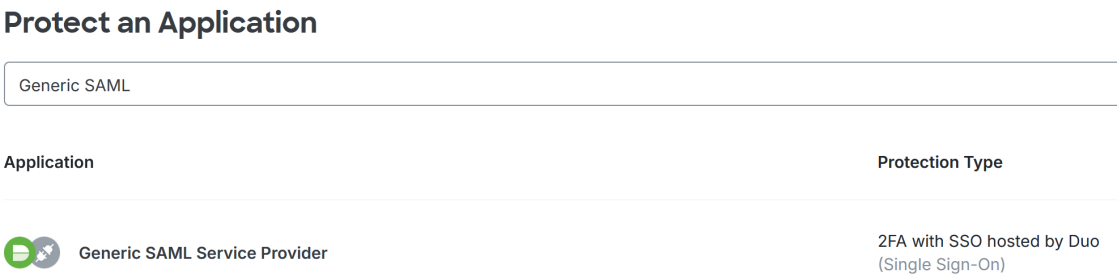


Configure a Duo SAML Application for use with stores

1. Select **Applications > Protect an Application**. Click **Add Application**.
2. Locate the entry for Generic SAML Service Provider Duo app template. Citrix® recommends the Generic SAML Service Provider Duo template as it is the most flexible and will allow you to configure different combinations of SAML attributes and different SAML flows according to your

© 1997–2026 Citrix Systems, Inc. All rights reserved.

needs.



> **Important:**
>
> The use of the Duo **Citrix Workspace** SAML template is not recommended as it is inflexible and only supports SAML using AD identities. The Duo **Citrix Workspace** SAML template will also not allow the addition of optional attributes like cip_domain and cip_forest which are needed for some advanced mergers and acquisitions SAML configurations. It also does not allow the configuration of the Citrix Cloud logout endpoint.

3. Specify a **Display Name** for your SAML application such as **Citrix Cloud Prod**.
4. Specify the **user access** such as **Enable for all users**.
5. Select **None (manual Input)** within **Metadata Discovery** and enter the following Citrix Cloud SAML endpoints.
6. Enter the **EntityID** according to the Citrix Cloud region your CC tenant is in.

URL	Region
`https://saml.cloud.com`	Commercial EU, US, and APS
`https://saml.citrixcloud.jp`	JP
`https://saml.cloud.us`	GOV

7. Configure the **Single sign-on URL (ACS URL)** according to the Citrix Cloud region your CC tenant is in.

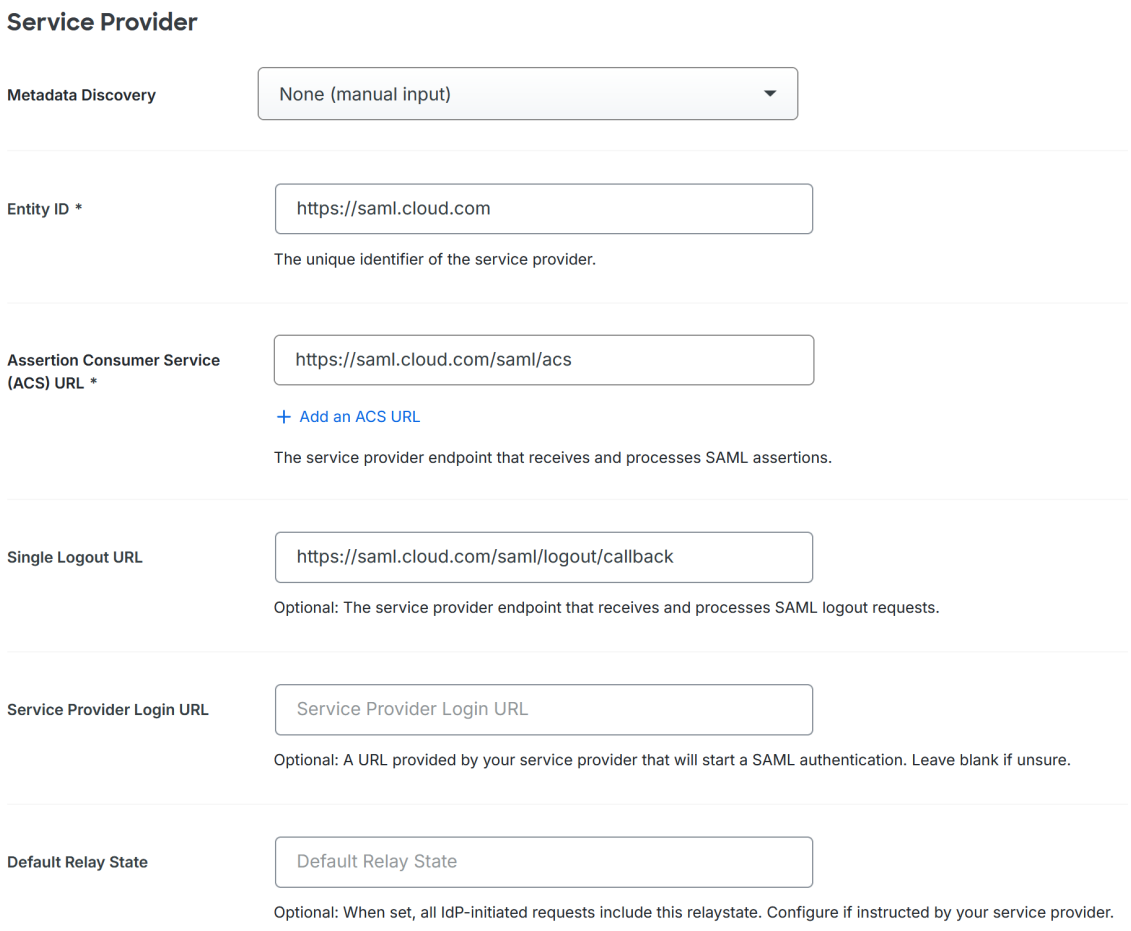
URL	Region
`https://saml.cloud.com/saml/acs`	Commercial EU, US, and APS
`https://saml.citrixcloud.jp/saml/acs`	JP
`https://saml.cloud.us/saml/acs`	GOV

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. Configure the **Single Logout URL** according to the Citrix Cloud region your CC tenant is in.

URL	Region
`https://saml.cloud.com/saml/logout/callback`	Commercial EU, US, and APS
`https://saml.citrixcloud.jp/samllogout/callback`	JP
`https://saml.cloud.us/saml/samllogout/callback`	GOV

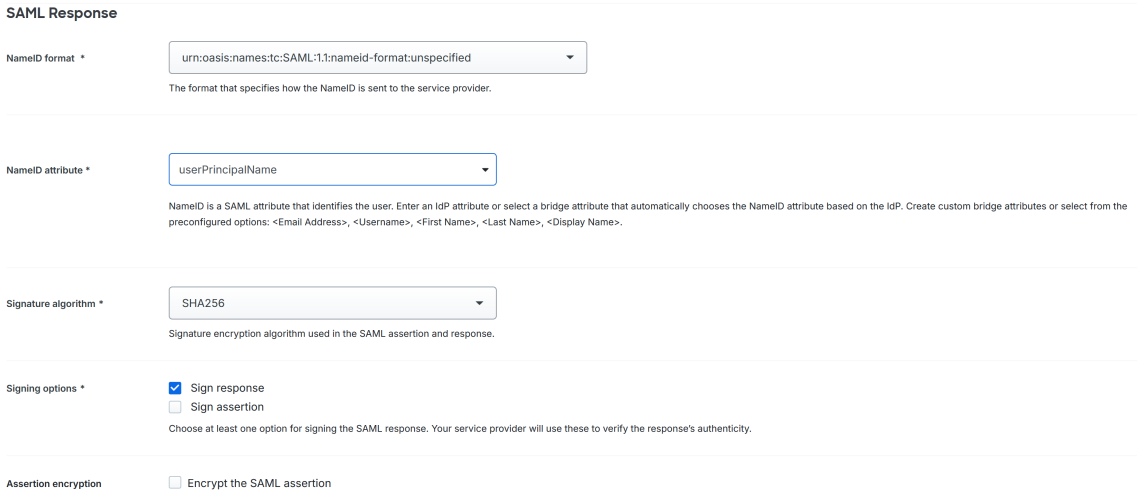
9. **Service Provider Login URL** is not required and can be left empty.
10. **Default Relay State** is not required and can be left empty.



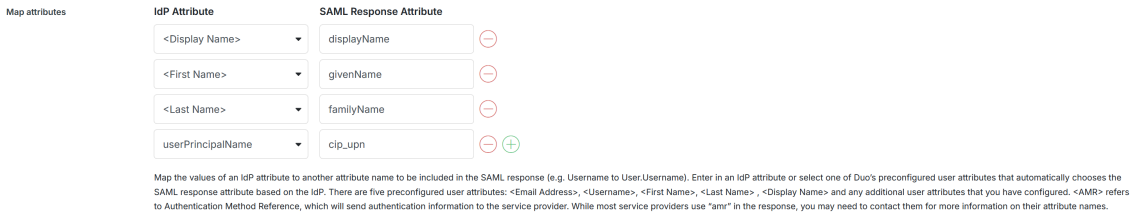
11. Configure the **Name ID Format** as **Unspecified**.
12. Configure the **Name ID Attribute** as **userPrincipalName** (case sensitive).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

13. Configure **Signature algorithm** as **SHA256**.
14. Configure **Signing options** as **Sign response**.
15. Configure **Assertion encryption** as **disabled**.



16. Configure **Map Attributes** with Duo bridging attributes on the left and Citrix Cloud SAML claim names on the right.



> **Important:**
>
> Duo bridge attributes (left) and SAML attribute claim names (right) are case sensitive. It is the claim names on the right that must match what is configured within the Citrix Cloud SAML connection.

Configure the Citrix Cloud SAML connection

1. All Citrix logon flows need to be Service Provider initiated using either a store URL or a Citrix Cloud GO URL.
2. Use the default recommended values for the SAML connection within **Identity and Access Management > Authentication > Add an identity provider > SAML**.
3. Obtain the Duo SAML application SAML endpoints to enter into the Citrix Cloud SAML connection from your Duo portal by visiting the Duo Active Directory Sync documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



In this field in Citrix Cloud	Enter this value
Entity ID	`https://sso-<id>.sso.duosecurity.com/saml2/sp/<samlappID>/metadata`
Sign Authentication Request	Yes
SSO Service URL	`https://sso-<id>.sso.duosecurity.com/saml2/sp/<samlappID>/sso`
SSO Binding Mechanism	HTTP Post
SAML Response	Sign Either Response Or Assertion
Authentication Context	Unspecified, Exact
Logout URL	`https://sso-<id>.sso.duosecurity.com/saml2/sp/<samlappID>/slo`
Sign Logout Request	Yes
SLO Binding Mechanism	HTTP Post

Duo SAML Logout Behaviour

Duo SAML does not currently support SAML SLO at the time this article was written but it is possible to configure Duo to terminate the IDP session when a user explicitly logs out of store and/or Citrix Cloud. It is recommended you read the SAML Logout Considerations section saml logout considerations in the main SAML article before choosing to configure your Duo SAML application's logout settings.

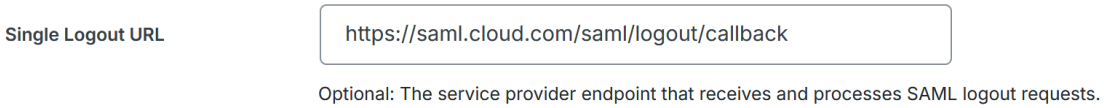
> **Important:**
>
> Taken from Duo documentation Duo SSO Logout Behavior and Session Management Details.
>
> ```
> Users that decide to log out and hit the SLO URL for Duo SSO will
>  be logged out of Duo SSO and have their MFA remembered devices
> ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> session deleted before redirecting them to the logout page.

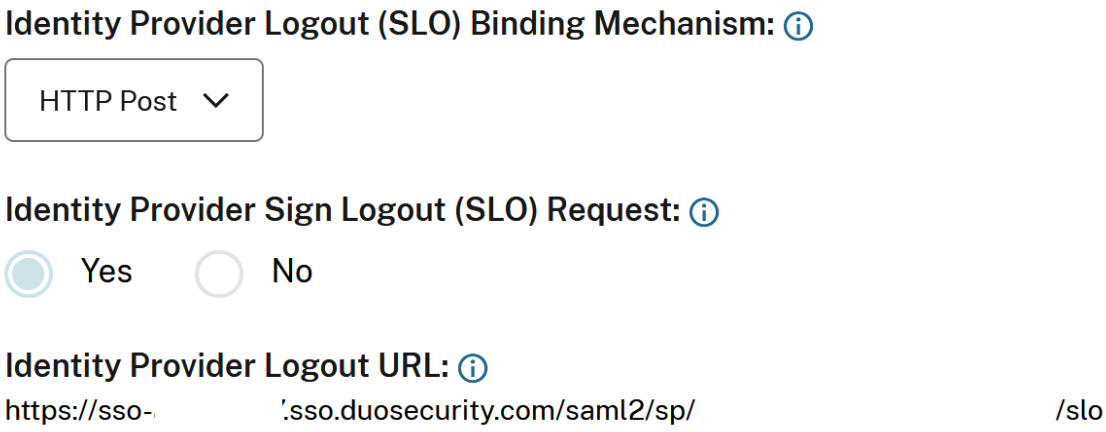
To configure explicit logout of the Duo IDP session when the end user logs out of store and/or Citrix Cloud follow the recommended steps below.

1. Configure the Citrix Cloud SAML logout endpoint within your Duo SAML app.



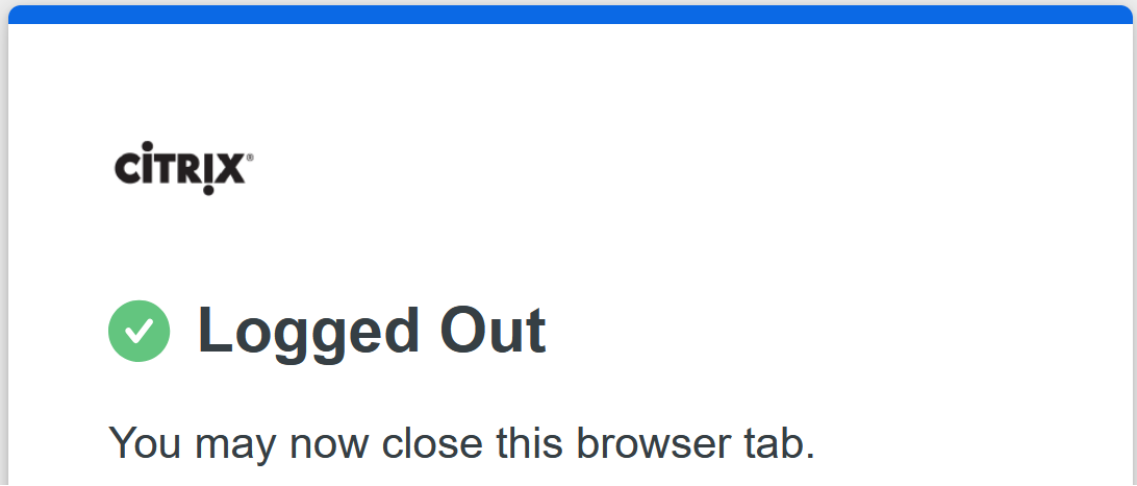
2. Configure the Duo SLO endpoint within the Citrix Cloud SAML connection.

> **Important:**
>
> If you have not used the **Generic SAML Provider** Duo app template you will be unable to complete this step as the option to enter the Citrix Cloud logout endpoint will not be available.

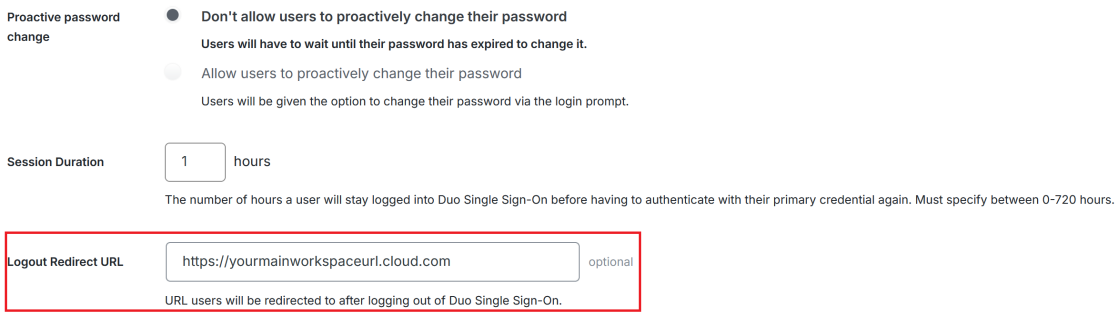


3. When logging out of store with both sides of the SAML connection configured for logout as per steps 1 and 2 the following UI will be shown by Duo indicating the IDP session has been terminated.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. **Optional**: To improve your store end user's logout experience it is possible to configure the Duo LDAPS connection with a single **Logout Redirect URL** which will redirect your end users back to the store logon page. This is done inside the your AD forest LDAPS connection.



> **Important:**
>
> The logout redirect URL field shown above will only allow the configuration of a single store URL. The use of multiple different store URLs within the Citrix Cloud tenant cannot be configured within a single Active Directory Forest connection in Duo.

SAML using Entra ID and AD identities for store authentication

June 22, 2026

Author:
Mark Dear

This article describes how you can configure SAML for store authentication using Active Directory (AD) identities. The default behavior for Citrix Cloud™ and SAML authentication to cloud stores or Citrix

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cloud, regardless of the SAML provider used, is to assert against an AD user identity. For the configuration described in this article, using Entra ID Connect to import your AD identities to your Entra ID is required.

> **Important:**
>
> It is crucial to determine the appropriate SAML flow for your end users, as it directly impacts their sign-in process and resource visibility. The chosen identity influences the types of resources accessible to a store end user.
> There is an associated article that provides instructions on utilizing Entra ID as the SAML provider for authenticating into store using ME-ID identities. You can find detailed instructions in SAML using Microsoft Entra ID and ME-ID identities for store authentication.
> Usually, end users typically need to open apps and desktops provided by AD domain joined VDAs. It is essential to carefully review the use cases outlined in both articles before deciding on the most suitable SAML flow for your organization. If uncertain, Citrix® recommends using the **AD SAML flow** and following the instructions in this article, as it aligns with the most common DaaS scenario.

Feature scope

This article applies to users who use the following combination of Citrix Cloud and Azure features:

- SAML for store authentication using AD identities
- SAML for Citrix Cloud admin login using AD identities
- Citrix DaaS™ and HDX resource enumeration of resources published using AD domain-joined VDAs
- AD domain-joined VDA resource enumeration

What's best: AD identities or Entra ID identities?

To determine whether your store users should authenticate using either SAML AD or SAML Entra ID identities:

1. Decide which combination of resources you intend to make available to your users in their stores.
2. Use the following table to determine which type of user identity is appropriate for each resource type.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Resource type (VDA)	User identity when signing in to stores	Needs SAML identity using Entra ID?	FAS provides single sign-on (SSO) to VDA?
AD joined	AD, Entra ID imported from AD (contains SID)	No. Use default SAML.	Yes

Configure the custom Entra ID Enterprise SAML application

By default, the behavior for SAML sign-in to stores is to assert against an AD user identity.

1. Sign in to the Azure portal.
2. From the portal menu, select **Entra ID**.
3. From the left pane, under **Manage**, select **Enterprise Applications**.
4. From the command bar in the working pane, select **New Application**.
5. From the command bar, select **Create your own application**. Don't use the Citrix Cloud SAML SSO enterprise application template. The template doesn't allow you to modify the list of claims and SAML attributes.
6. Enter a name for the application and then select **Integrate any other application you don't find in the gallery (Non-gallery)**. Click **Create**. The application overview page appears.
7. From the left pane, select **Single sign-on**. From the working pane, select **SAML**.
8. In the **Basic SAML Configuration** section, select **Edit** and configure the following settings:

    a) In the **Identifier (Entity ID)** section, select **Add identifier** and then enter the value associated with the region in which your Citrix Cloud tenant is located:
    - For European Union, United States, and Asia-Pacific South regions, enter `https://saml.cloud.com`.
    - For the Japan region, enter `https://saml.citrixcloud.jp`.
    - For the Citrix Cloud Government region, enter `https://saml.cloud.us`.

    b) In the **Reply URL (Assertion Consumer Service URL)** section, select **Add reply URL** and then enter the value associated with the region in which your Citrix Cloud tenant is located:
    - For European Union, United States, and Asia-Pacific South regions, enter `https://saml.cloud.com/saml/acs`.
    - For the Japan region, enter `https://saml.citrixcloud.jp/saml/acs`.
    - For the Citrix Cloud Government region, enter `https://saml.cloud.us/saml/acs`.

    c) In the **Logout URL (Optional)** section, enter the value associated with the region in which your Citrix Cloud tenant is located:

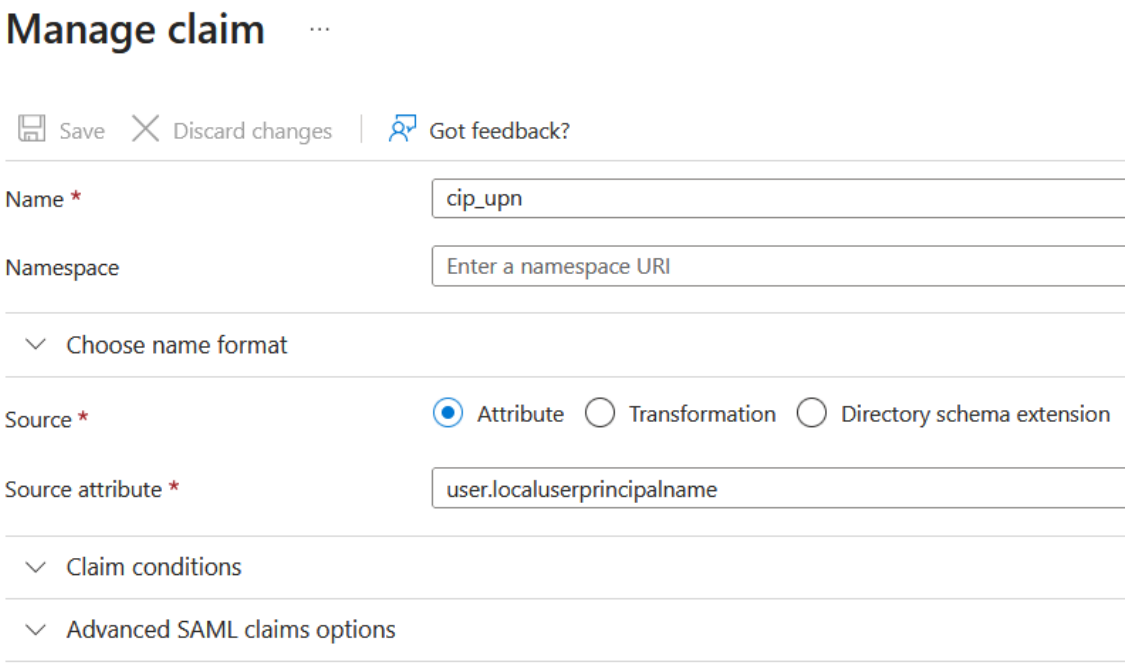
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For European Union, United States, and Asia-Pacific South regions, enter `https://saml.cloud.com/saml/logout/callback`.
- For the Japan region, enter `https://saml.citrixcloud.jp/saml/logout/callback`.
- For the Citrix Cloud Government region, enter `https://saml.cloud.us/saml/logout/callback`.

d) From the command bar, select **Save**.

9. In the **Attributes & Claims** section, click **Edit** to configure the following claims. These claims appear in the SAML assertion within the SAML response. After SAML app creation, configure the following attributes.

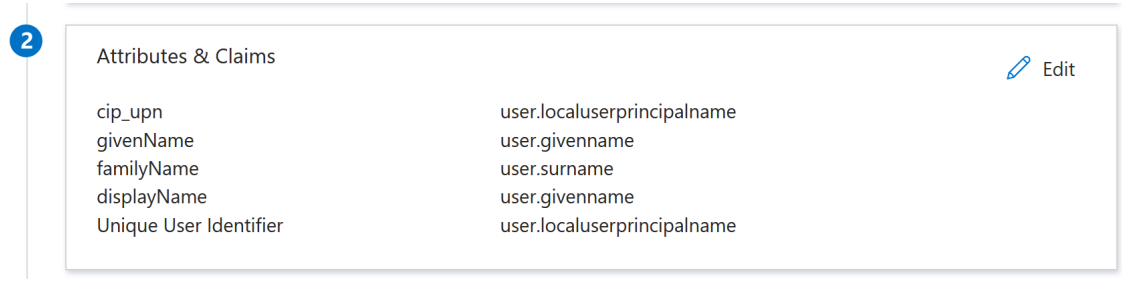
a) For the **Unique User Identifier (Name ID)** claim, update the default value to be `user.localuserprincipalname`.
b) For **cip_upn** claim, update the default value to be `user.localuserprincipalname`.



a) For **displayName**, leave the default value of `user.displayname`.
b) For **givenName** claim, update the default value to be `user.givenname`.
c) For **familyName** claim, update the default value to be `user.surname`.
d) In the **Additional claims** section, for any remaining claims with the `http://schemas.xmlsoap.org/ws/2005/05/identity/claims` namespace, click the ellipsis (…) button and click **Delete**. No need to include these claims as they are duplicates of the above user attributes.

When finished, the **Attributes & Claims** section appears as illustrated below:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

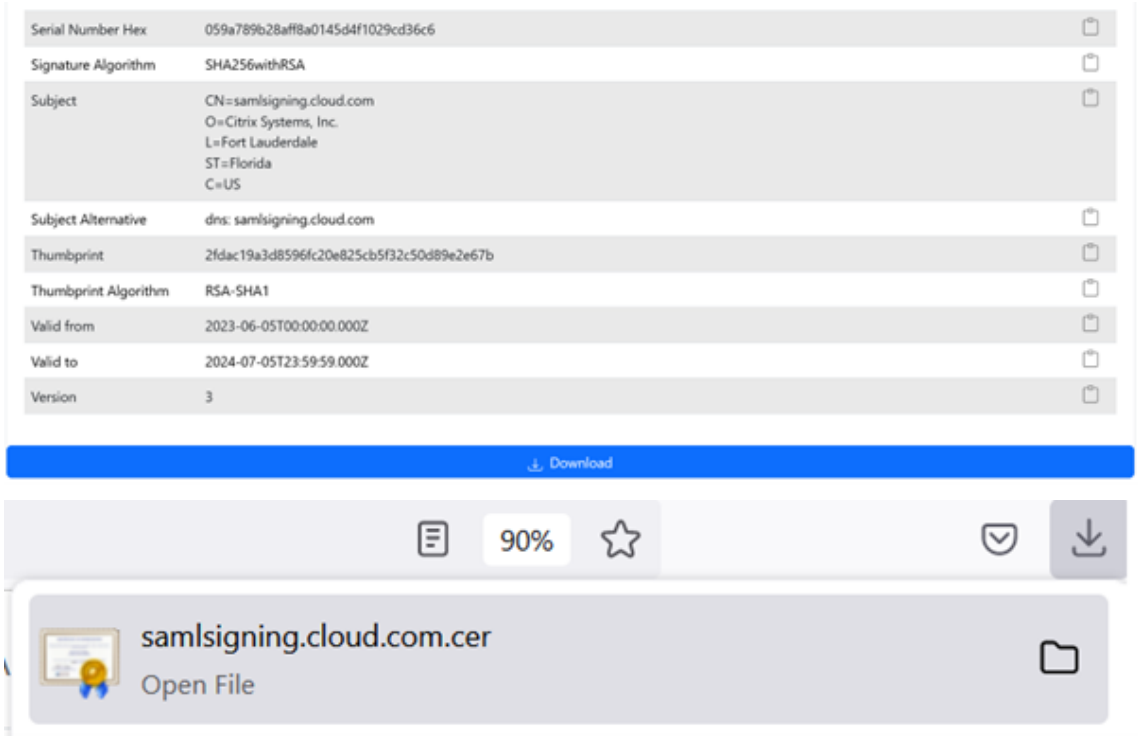


10. Obtain a copy of the Citrix Cloud SAML signing certificate using this third party online tool.

    a) Enter `https://saml.cloud.com/saml/metadata` in the URL field and click **Load**.



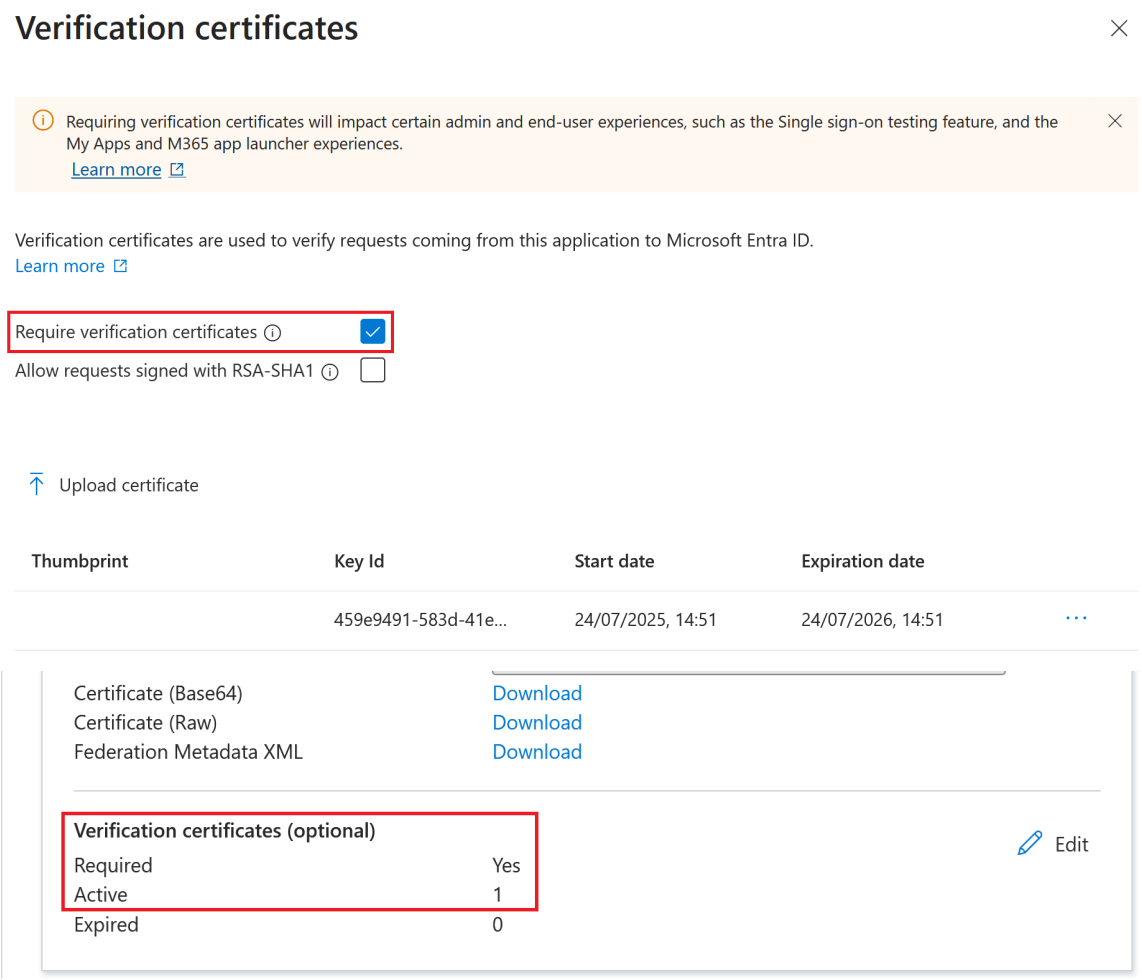
    a) Scroll to the bottom of the page and click **Download**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

11. Configure the Entra ID SAML application Signing Settings.

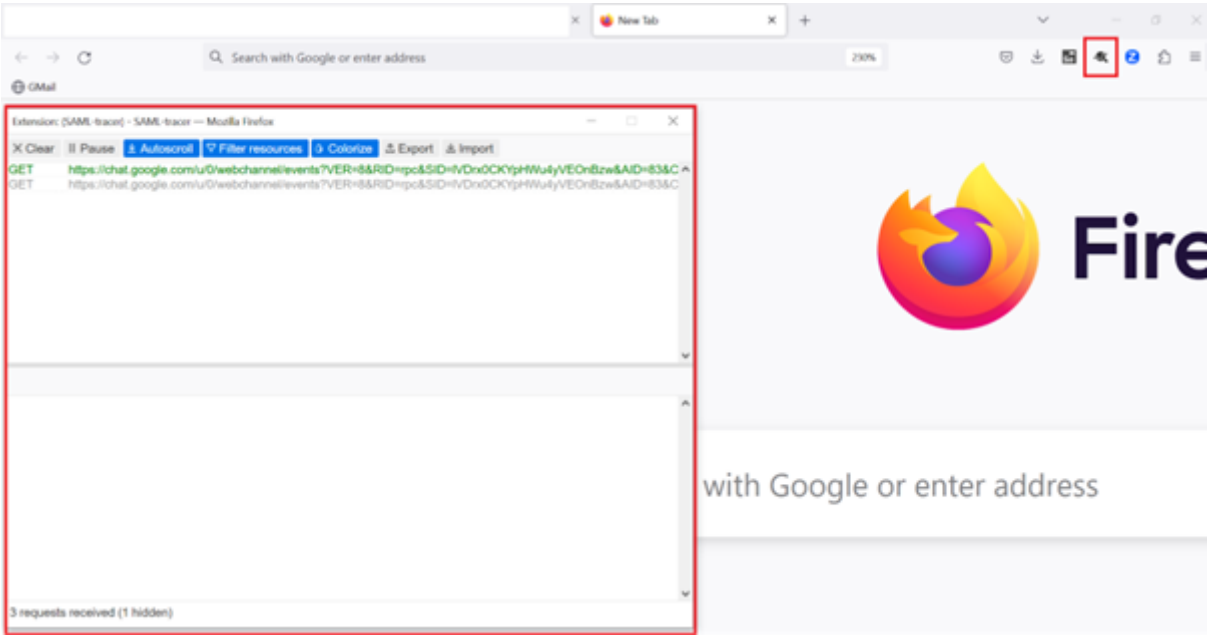
    a) Upload the production SAML signing certificate obtained in step 9 within the Entra ID SAML application.
    b) Enable **Require verification certificates**.



Troubleshooting

1. Verify your SAML assertions contain the correct user attributes using a SAML networking tool, such as the SAML-tracer browser extension.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

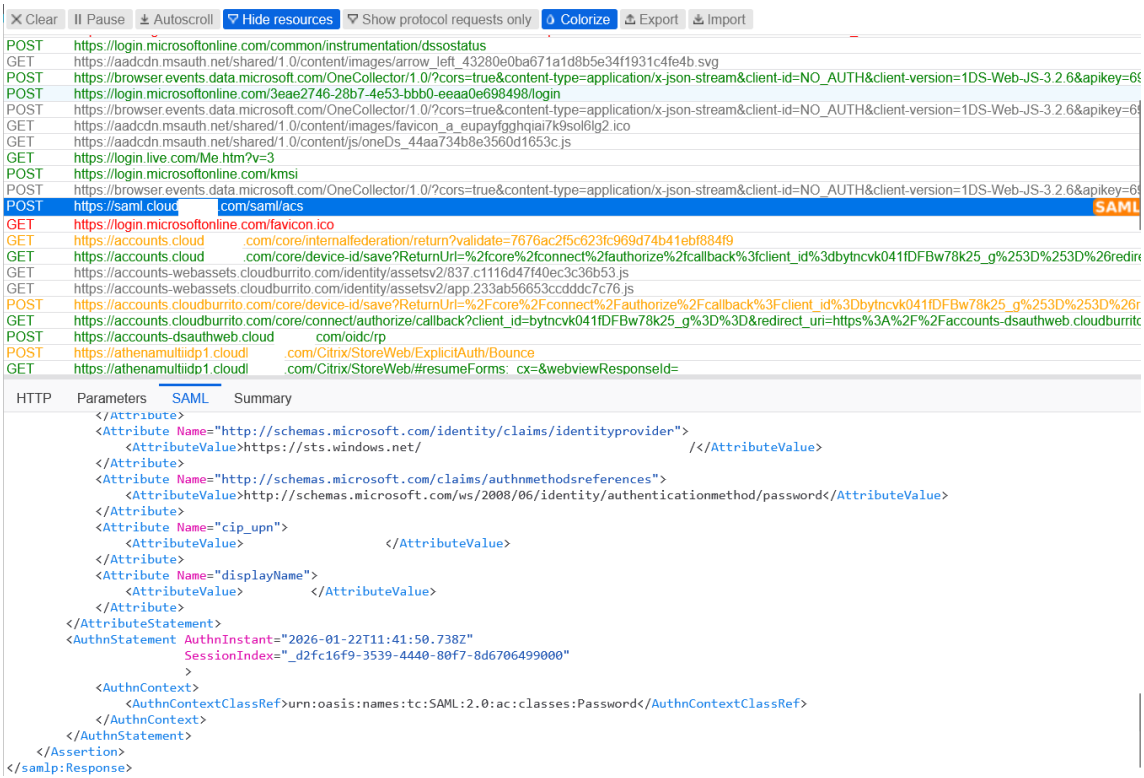


1. Locate the SAML response shown in yellow and compare to this example:



2. Click on the **SAML** tab in the bottom pane to decode the SAML response and view as XML.
3. Scroll to the bottom of the response and verify that the SAML assertion contains the correct SAML attributes and user values.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If your end users still can't sign in to their store or they can't see their Citrix HDX™ Plus for Windows 365 desktops, contact Citrix Support and provide the following information:

- SAML-tracer capture
- Date and time the sign-in to Citrix® StoreFront Cloud failed
- The affected user name
- The caller IP address of the client computer that you used to sign in to their store. You can use a tool like https://whatismyip.com to get this IP address.

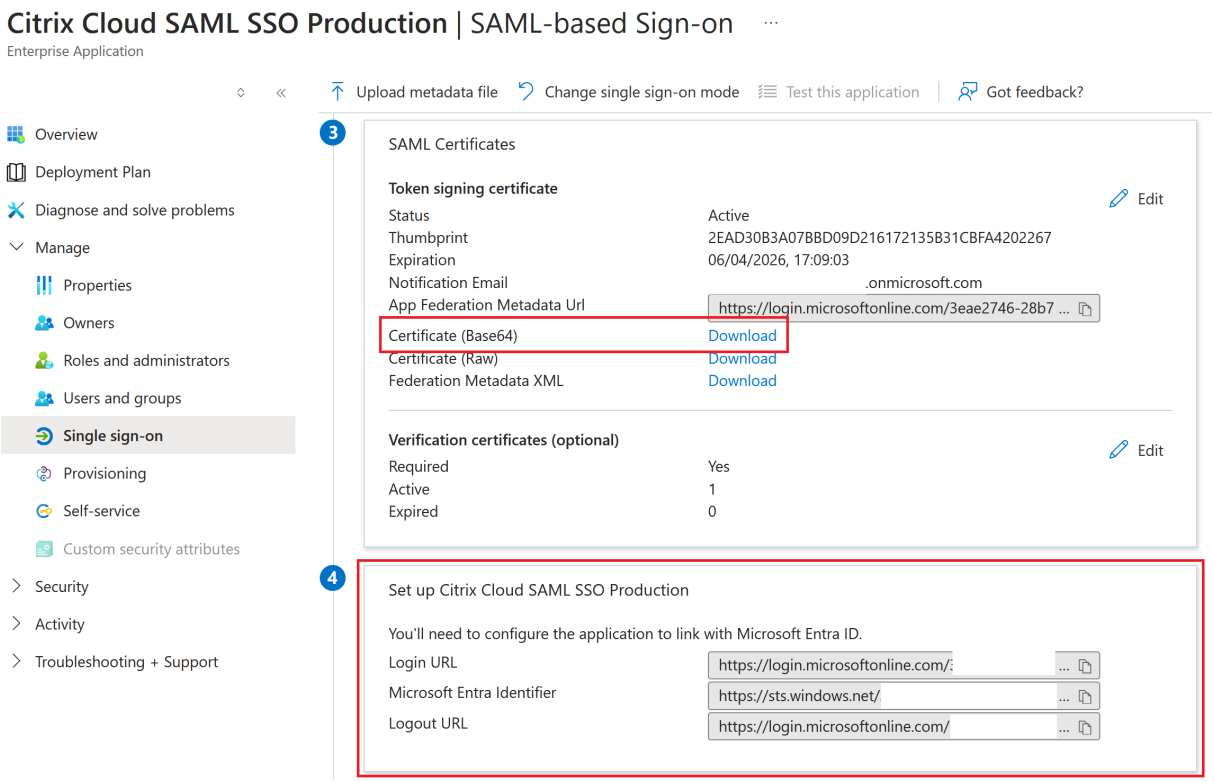
Configure the Citrix Cloud SAML Connection

All Citrix logon flows need to be Service Provider initiated using either a store URL or a Citrix Cloud GO URL.

Use the default recommended values for the SAML connection within **Identity and Access Management > Authentication > Add an identity provider > SAML**.

Obtain the Entra ID SAML application SAML endpoints from your Entra ID portal to enter into Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Entra ID SAML endpoint examples to be used within the Citrix Cloud SAML connection

> **Important:**
>
> EntraID SSO and Logout SAML endpoints are the same URL.

In this field in Citrix Cloud	Enter this value
Entity ID	`https://sts.windows.net/<yourEntraIDTenantID>`
Sign Authentication Request	Yes
SSO Service URL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`
SSO Binding Mechanism	HTTP Post
SAML Response	Sign Either Response Or Assertion
Authentication Context	Unspecified, Exact
Logout URL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In this field in Citrix Cloud	Enter this value
Sign Logout Request	Yes
SLO Binding Mechanism	HTTP Post

SAML using Entra ID and Entra ID identities for store authentication

July 17, 2026

Author:
Mark Dear

This article describes how you can configure SAML for store authentication using Entra ID identities instead of AD identities. Use this configuration if your Entra ID users can't enumerate Windows 365 Cloud PCs or Entra ID domain-joined VDAs after signing in to their store with the default SAML behavior. After completing the configuration, your users can sign in to their store using SAML authentication to access both HDX apps and desktops through Citrix DaaS™ and Windows 365 Cloud PCs through Azure.

The default behavior for Citrix Cloud™ and SAML authentication to Citrix® StoreFront Cloud is to assert against an AD user identity. For the configuration described in this article, using Entra ID Connect to import your AD identities to your Entra ID is required. The AD identities contain the user's SID, which StoreFront Cloud can send to Citrix DaaS and allows the HDX resources to be enumerated and launched. Because the Entra ID version of users' identities is used, users can also enumerate and launch Azure resources like Windows 365 Cloud PCs from within StoreFront Cloud.

> **Important:**
>
> Enumeration refers to the list of resources that users see after they sign in to their store. The resources that a given user is allowed to access depends on their user identity and which resources are associated with that identity in Citrix DaaS. There is an associated article that provides instructions on utilizing Entra ID and AD identities as the SAML provider for authenticating into store. You can find detailed instructions in SAML using Entra ID and AD identities for store authentication

Feature scope

This article applies to users who use the following combination of Citrix Cloud and Azure features:

- SAML for store authentication

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix DaaS and HDX™ resource enumeration of resources published using AD domain-joined VDAs
- Entra ID domain-joined VDA resource enumeration
- Azure hybrid domain-joined VDA resource enumeration
- W365 Cloud PC enumeration and launch

> **Important:**
>
> Do not use this ME-ID SAML flow for SAML login to Citrix Cloud as this requires the Citrix Cloud admin user to be a member of an AD group and therefore an AD user identity should be used. You can find detailed instructions in SAML using Entra ID and AD identities for store authentication

What's best: AD identities or Entra ID identities?

To determine whether your store users should authenticate using either SAML AD or SAML Entra ID identities:

1. Decide which combination of resources you intend to make available to your users in their stores.
2. Use the following table to determine which type of user identity is appropriate for each resource type.

Resource type (VDA)	User identity when signing in to their store	Needs SAML identity using Entra ID?	FAS provides single sign-on (SSO) to VDA?
AD joined	AD, Entra ID imported from AD (contains SID)	No. Use default SAML.	Yes
Hybrid joined	AD, Entra ID imported from AD (contains SID)	No. Use default SAML.	Yes, for AD as an identity provider. FAS isn't required if Entra ID is selected for VDA.
Entra joined	Entra ID native user, Entra ID imported from AD (contains SID)	Yes, use SAML through Entra ID.	No
Windows 365 Cloud PCs	Entra ID native user, Entra ID imported from AD (contains SID)	Yes, use SAML through Entra ID.	No
AD joined, Entra ID joined, Windows 365 Cloud PCs	Entra ID imported from AD (contains SID)	Yes, use SAML through Entra ID.	Yes, for AD joined. No, for Entra ID joined and Windows 365 Cloud PCs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

More information

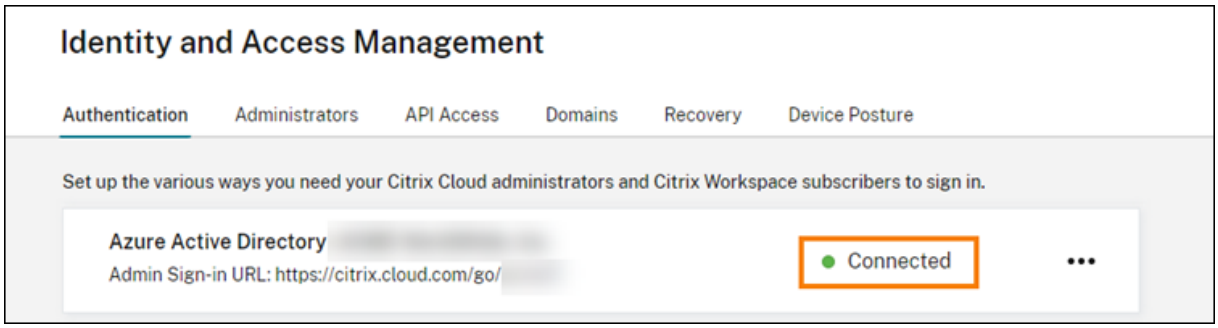
- Citrix DaaS documentation:
  - Machine identities
  - Citrix HDX Plus for Windows 365
- Citrix FAS documentation: Install and configure
- Microsoft Azure documentation: What is Entra ID Connect?

Requirements

- Your Entra ID tenant must be connected to your Citrix Cloud tenant. In the Citrix Cloud console, you can find your existing Entra ID connection by selecting **Identity and Access Management > Authentication**.

Or,

You can create a new Entra ID directory connection by selecting **Identity and Access Management > Authentication –> Add an identity provider –> Select Entra ID**.



> **Important:**
>
> You must connect the same Entra ID tenant where you intend to create the new SAML application which will use ME-ID identities.

- The store authentication method must be set to **SAML 2.0**. Don't use Entra ID as the authentication method. To change the store authentication method, go to **StoreFront Cloud > Authentication** in the Citrix Cloud console.
- The UPN suffix `@yourdomain.com` must be imported and verified within Entra ID as a custom domain name. In the Azure portal, this is located under **Entra ID > Custom Domain Names**.
- Entra ID user identities must be imported from AD using Microsoft Entra ID Connect. This ensures user identities are correctly imported and have the correct UPN suffix. Entra ID users with `@yourtenant.onmicrosoft.com` UPN suffixes aren't supported.
- Citrix FAS must be deployed and connected to the Citrix Cloud tenant and resource location. FAS provides single sign-on to HDX desktops and applications that are launched

© 1997–2026 Citrix Systems, Inc. All rights reserved.

from StoreFront Cloud. You don't have to configure AD shadow accounts because the UPN `user@customerdomain` for both the AD and Entra ID user identities must match. FAS generates the necessary user certificates with the correct UPN and performs a smart card sign-in when HDX resources are launched.

Configure the custom Entra ID Enterprise SAML application

By default, the behavior for SAML sign-in to stores is to assert against an AD user identity. The **cip_directory** SAML attribute is a hardcoded string value that's the same for all end users and acts as a switch. Citrix Cloud and StoreFront Cloud detect this attribute during sign-in and trigger SAML to assert against the Entra ID version of the user identity. Using the **azuread** parameter with this attribute overrides the default SAML behavior, this causes the store user to be authenticated using their Entra ID identity instead of their AD identity.

Although the steps in this section are for Entra ID, you can create a similar SAML application using a different SAML 2.0 provider (for example, ADFS, Duo, Okta, OneLogin, PingOneSSO, and so on), provided you perform the same tasks. Your SAML provider must allow you to configure a hardcoded SAML attribute (cip_directory = azuread) within the SAML application. Simply create the same SAML attribute mappings as described in this section.

1. Sign in to the Azure portal.
2. From the portal menu, select **Entra ID**.
3. From the left pane, under **Manage**, select **Enterprise Applications**.
4. From the command bar in the working pane, select **New Application**.
5. From the command bar, select **Create your own application**. Don't use the Citrix Cloud SAML SSO enterprise application template. The template doesn't allow you to modify the list of claims and SAML attributes.
6. Enter a name for the application and then select **Integrate any other application you don't find in the gallery (Non-gallery)**. Click **Create**. The application overview page appears.
7. From the left pane, select **Single sign-on**. From the working pane, select **SAML**.
8. In the **Basic SAML Configuration** section, select **Edit** and configure the following settings:

    a) In the **Identifier (Entity ID)** section, select **Add identifier** and then enter the value associated with the region in which your Citrix Cloud tenant is located:

    - For European Union, United States, and Asia-Pacific South regions, enter `https://saml.cloud.com`.
    - For the Japan region, enter `https://saml.citrixcloud.jp`.
    - For the Citrix Cloud Government region, enter `https://saml.cloud.us`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

b) In the **Reply URL (Assertion Consumer Service URL)** section, select **Add reply URL** and then enter the value associated with the region in which your Citrix Cloud tenant is located:

- For European Union, United States, and Asia-Pacific South regions, enter `https://saml.cloud.com/saml/acs`.
- For the Japan region, enter `https://saml.citrixcloud.jp/saml/acs`.
- For the Citrix Cloud Government region, enter `https://saml.cloud.us/saml/acs`.

c) In the **Logout URL (Optional)** section, enter the value associated with the region in which your Citrix Cloud tenant is located:

- For European Union, United States, and Asia-Pacific South regions, enter `https://saml.cloud.com/saml/logout/callback`.
- For the Japan region, enter `https://saml.citrixcloud.jp/saml/logout/callback`.
- For the Citrix Cloud Government region, enter `https://saml.cloud.us/saml/logout/callback`.

d) From the command bar, select **Save**.

9. In the **Attributes & Claims** section, select **Edit** to configure the following claims. These claims appear in the SAML assertion within the SAML response.

a) For the **Unique User Identifier (Name ID)** claim, update the default value to be `user.localuserprincipalname`.

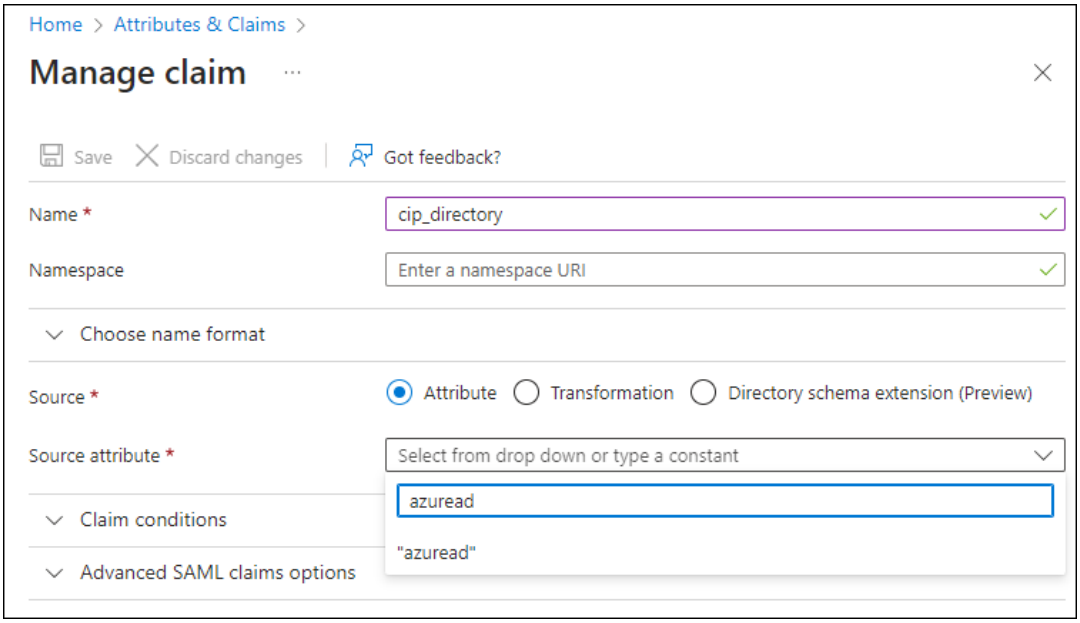
b) From the command bar, select **Add new claim**.

c) In **Name**, enter **cip_directory**.

d) In **Source**, leave **Attribute** selected.

e) In **Source attribute**, enter **azuread**. This value appears in quotation marks after you enter it.

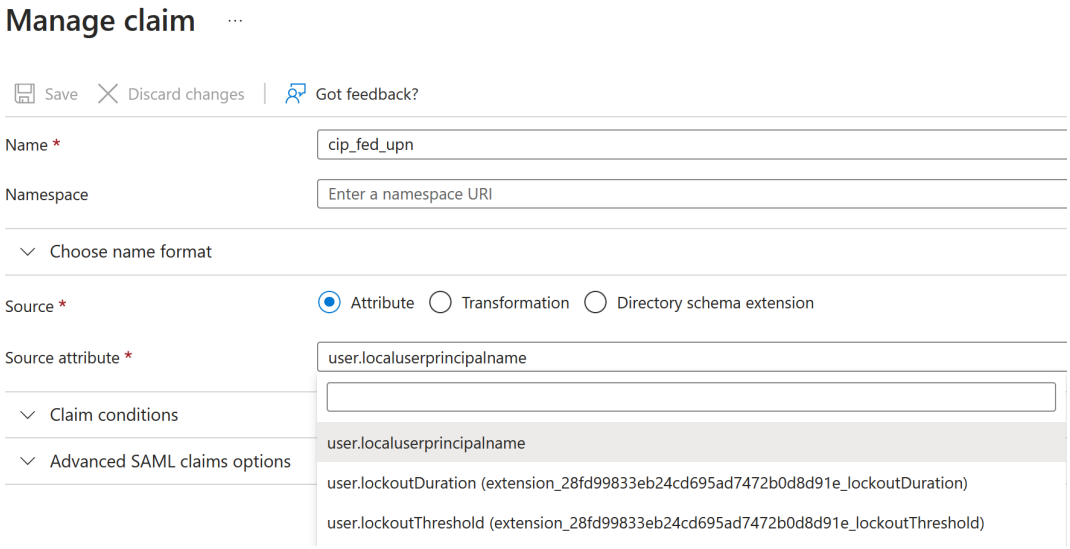
© 1997–2026 Citrix Systems, Inc. All rights reserved.



f) From the command bar, select **Save**.

g) Create additional claims with the following values in the **Name** and **Source attribute** fields:

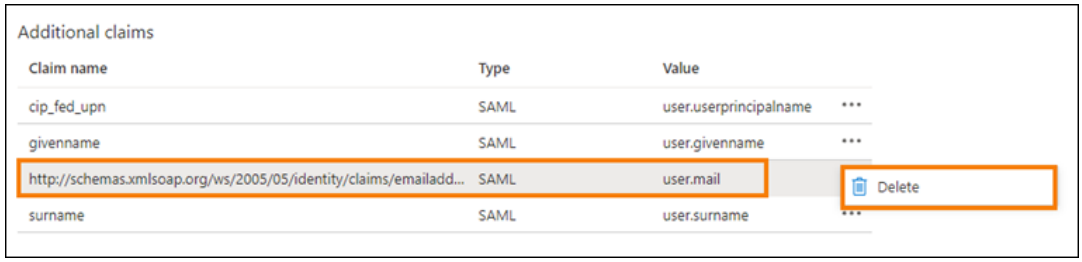
Name	Source attribute
cip_fed_upn	user.localuserprincipalname
displayName	user.displayname
givenName	user.givenname
familyName	user.surname



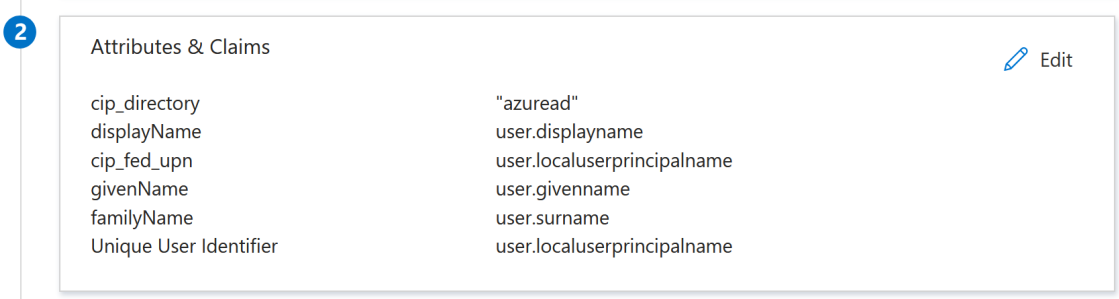
© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> You can create these additional claims by either repeating Steps b-f for each claim or by modifying the default claims in the **Additional claims** section that already have the source attributes listed in the table above. The default claims include the namespace `http://schemas.xmlsoap.org/ws/2005/05/identity/claims`.
>
> If you modify the default claims, you must remove the namespace from each claim. If you create new claims, you must delete the claims that include the namespace. If claims with this namespace are included in the resulting SAML assertion, the assertion will be invalid and will include incorrect SAML attribute names.

h) In the **Additional claims** section, for any remaining claims with the `http://schemas.xmlsoap.org/ws/2005/05/identity/claims` namespace, click the ellipsis (…) button and click **Delete**.

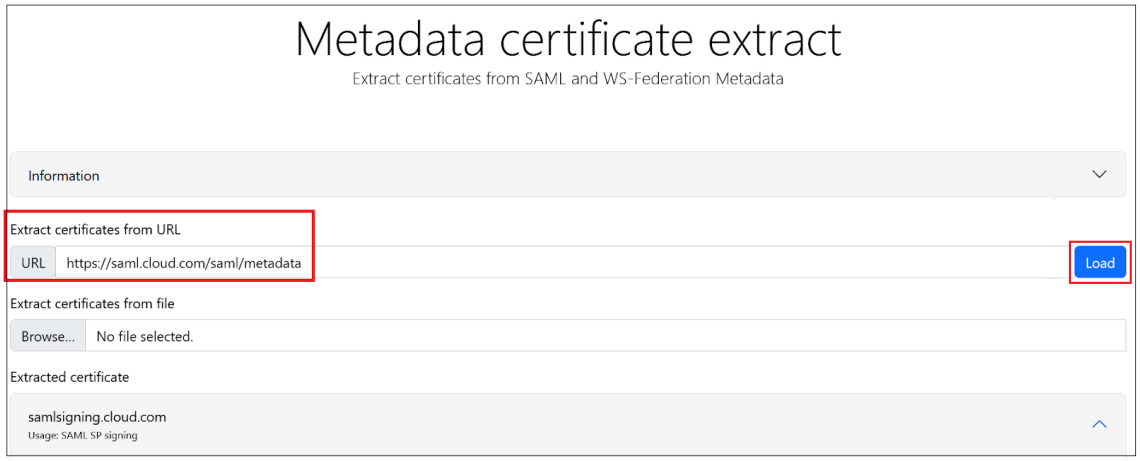


When finished, the **Attributes & Claims** section appears as illustrated below:

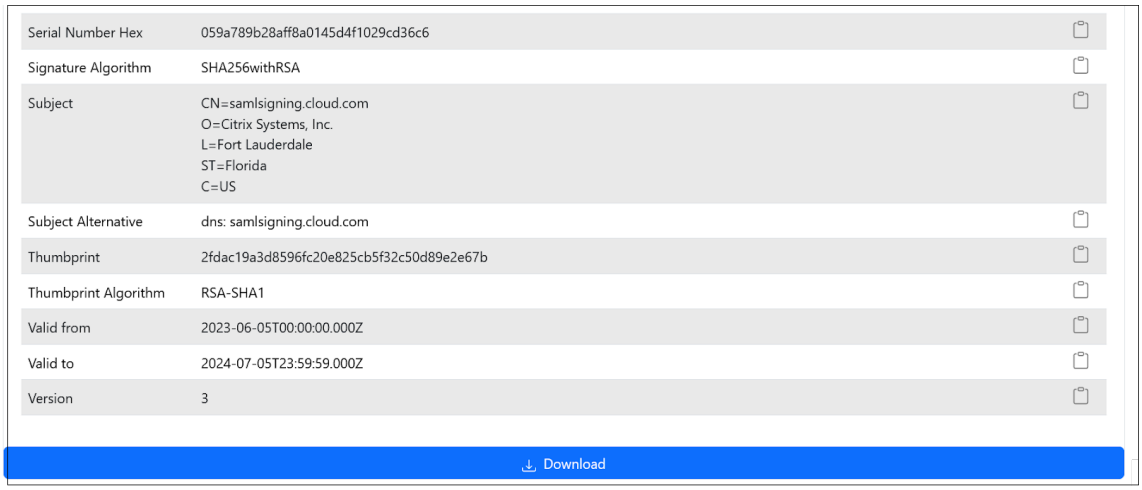


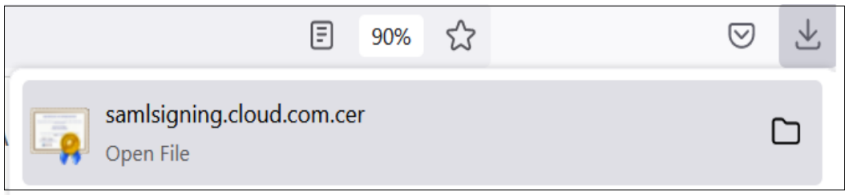
10. Obtain a copy of the Citrix Cloud SAML signing certificate using this third party online tool.
11. Enter https://saml.cloud.com/saml/metadata into the URL field and click **Load**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



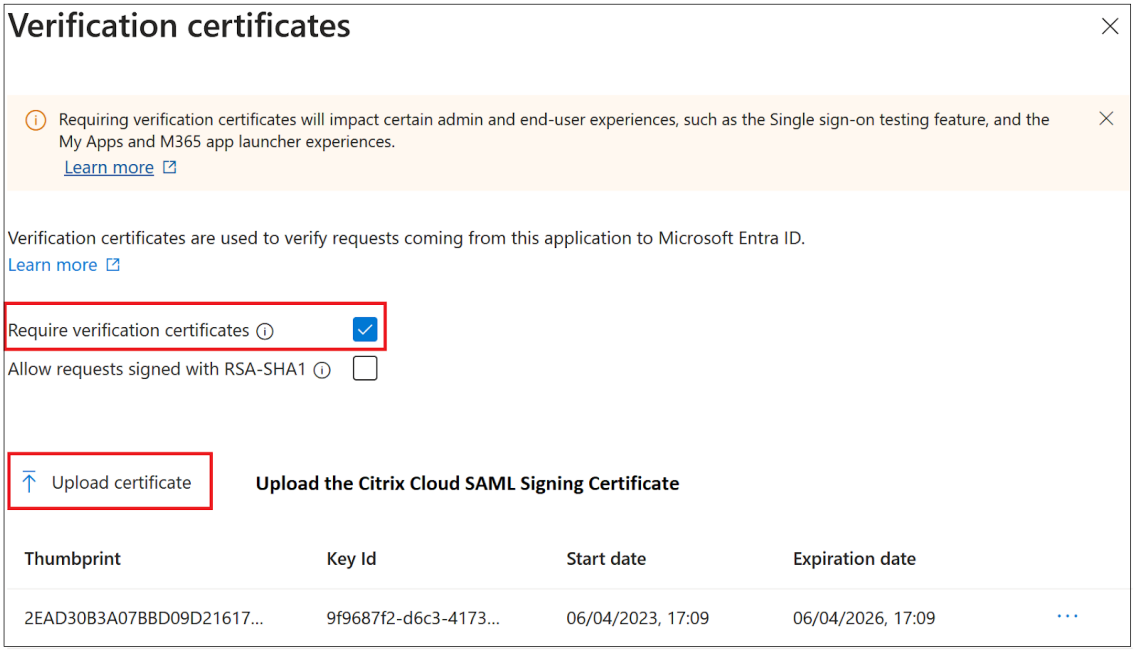
12. Scroll to the bottom of the page and click **Download**.

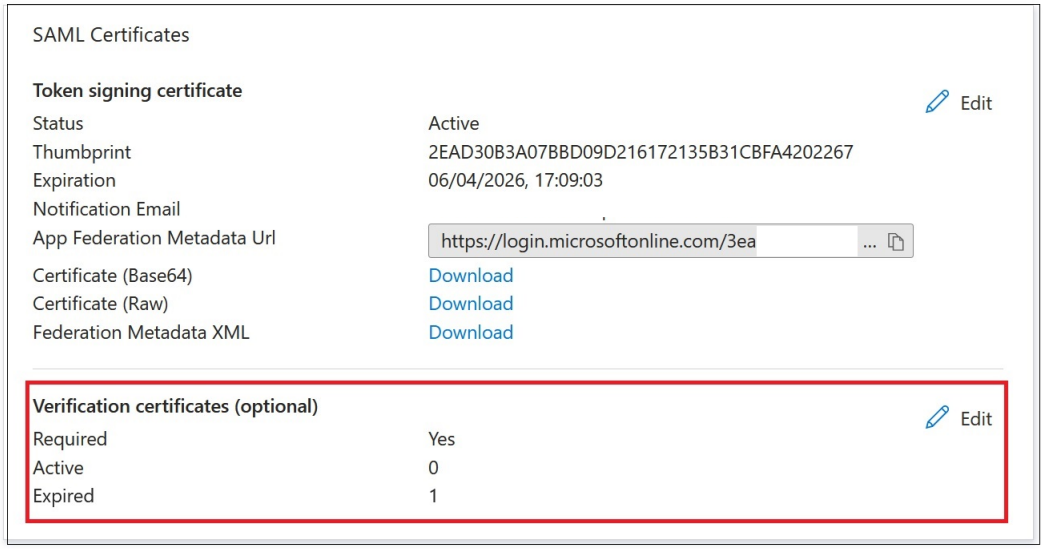




13. Configure the Entra ID SAML application Signing Settings.
14. Upload the production SAML signing certificate obtained in step 10 within the Entra ID SAML application.
    - Enable **Require verification certificates**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.





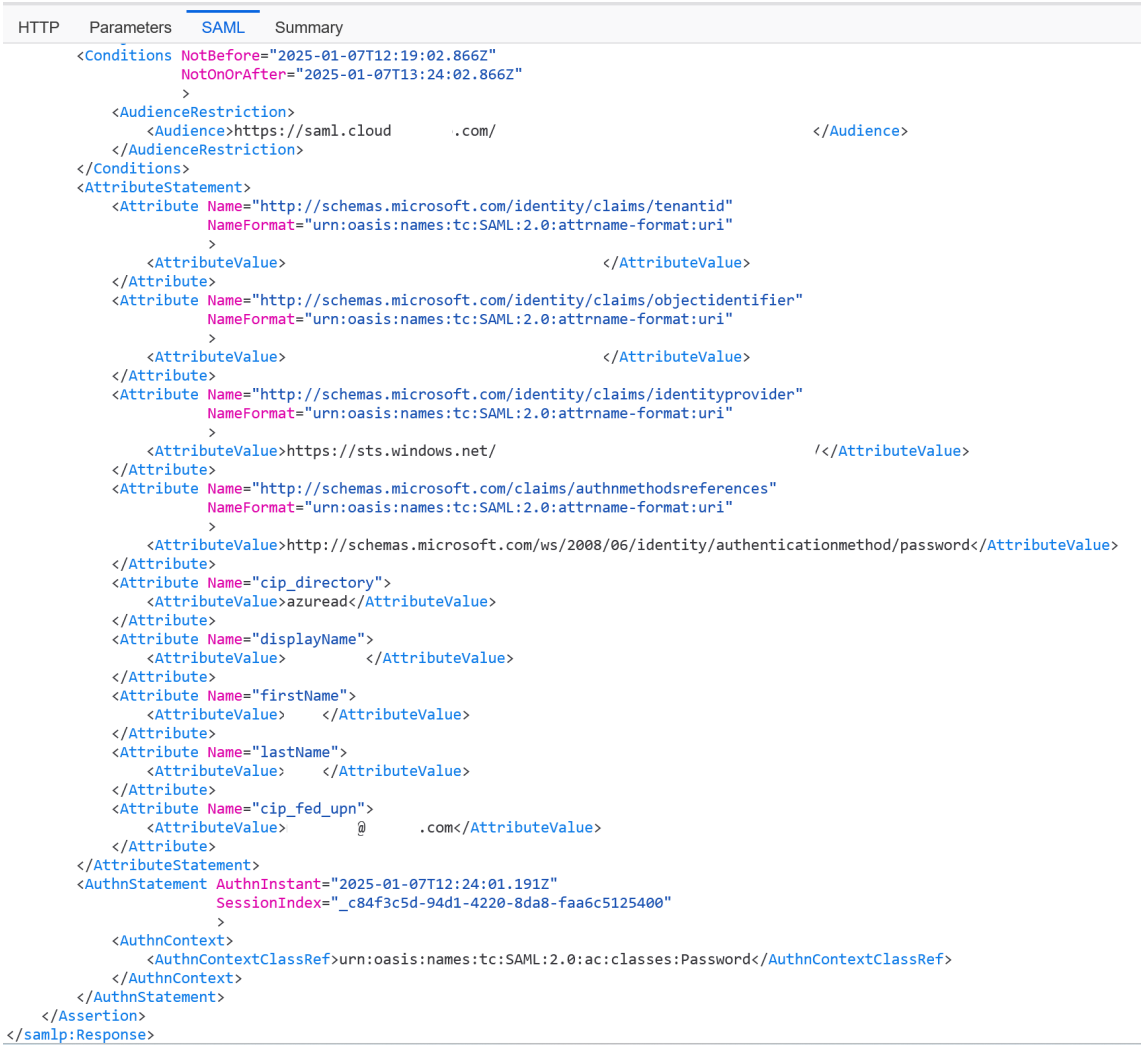
Troubleshooting

1. Verify your SAML assertions contain the correct user attributes using a SAML networking tool, such as the SAML-tracer browser extension.
2. Locate the SAML response shown in yellow and compare to this example:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Click on the **SAML** tab in the bottom pane to decode the SAML response and view as XML.
4. Scroll to the bottom of the response and verify that the SAML assertion contains the correct SAML attributes and user values.



If your end users still can't sign in to their store, contact Citrix Support and provide the following information:

- SAML-tracer capture
- Date and time the sign-in to the store failed
- The affected user name
- The caller IP address of the client computer that you used to sign in to the store. You can use a tool like https://whatismyip.com to get this IP address.

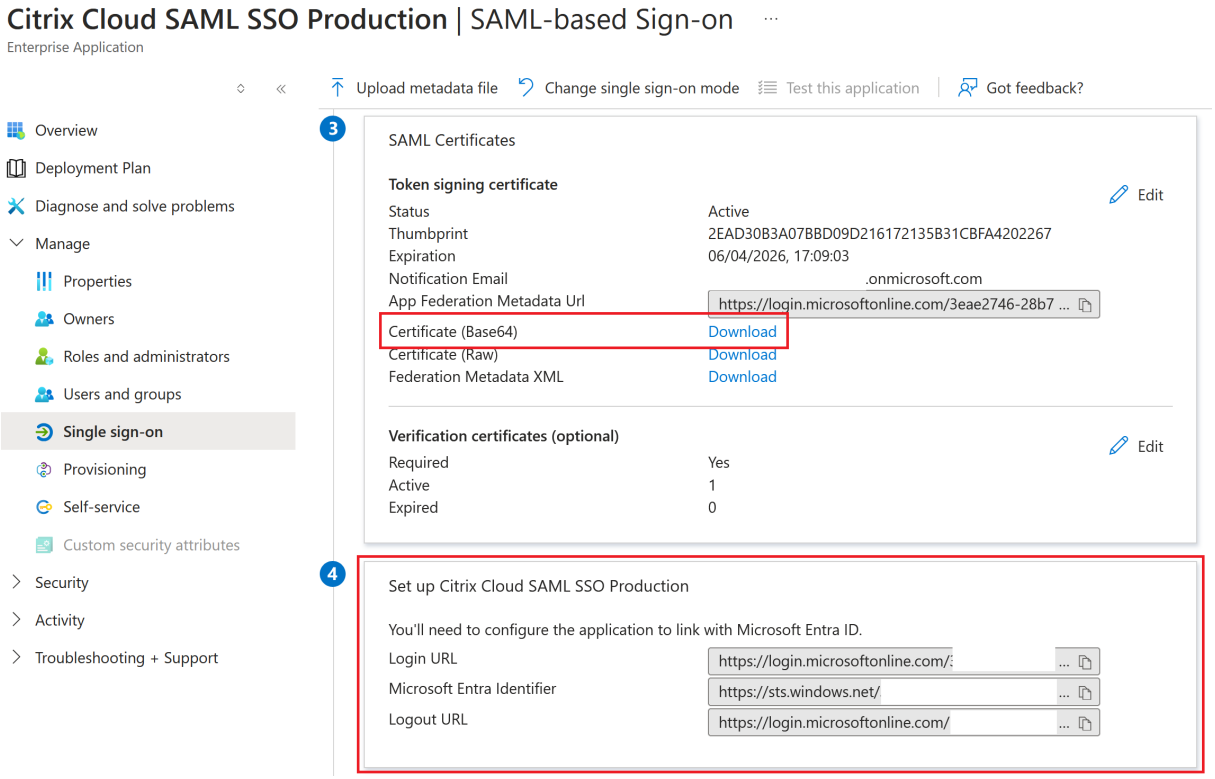
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure the Citrix Cloud SAML connection

All Citrix logon flows need to be Service Provider initiated using either a store URL or a Citrix Cloud GO URL.

Use the default recommended values for the SAML connection within **Identity and Access Management > Authentication > Add an identity provider > SAML**.

Obtain the Entra ID SAML application SAML endpoints from your Entra ID portal to enter into Citrix Cloud.



Entra ID SAML endpoint examples to be used within the Citrix Cloud SAML connection

> **Important:**
>
> EntraID SSO and Logout SAML endpoints are the same URL.

In this field in Citrix Cloud	Enter this value
Entity ID	`https://sts.windows.net/<yourEntraIDTenantID>`
Sign Authentication Request	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In this field in Citrix Cloud	Enter this value
SSO Service URL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`
SSO Binding Mechanism	HTTP Post
SAML Response	Sign Either Response Or Assertion
Authentication Context	Unspecified, Exact
Logout URL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`
Sign Logout Request	Yes
SLO Binding Mechanism	HTTP Post

SAML using Entra ID for Guest and B2B identities for store authentication

June 22, 2026

Author:
Mark Dear, Javier Lopez Santacruz

It is essential you understand whether B2B SAML is appropriate for your authentication use case before following this article. Read the use case descriptions and FAQ thoroughly before deciding to implement this particular special case SAML solution. Before proceeding, make sure you fully understand the scenarios where B2B SAML is appropriate and which types of identities you need to use.

Prerequisites

- A SAML application specifically configured for use with B2B SAML that only sends **cip_upn** for authentication within the SAML assertion.
- FrontEnd users within your SAML provider.
- A resource location containing a pair of Citrix Cloud™ connectors joined to the AD forest and domain where the AD shadow accounts are created.
- Either use the implicit UPN or add an alternative UPN suffix added to the backend AD forest where the AD shadow accounts are created.
- Backend AD shadow accounts with matching UPNs.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- DaaS or CVAD resources mapped to the AD shadow account users.
- One or more FAS servers linked to the same resource location.

FAQ

Why should I use B2B SAML?

It is very common for large organisations to invite contractors and temporary employees into their identity platform. The goal is to grant the contractor temporary access to a store using the user's existing identity such as a contractor email address, or an email address outside of your organisation. B2B SAML allows the use of native or guest frontend identities that do not exist inside the AD domain where DaaS resources are published.

What is B2B SAML?

AD Attribute	Default Attribute Name in the SAML Assertion
userPrincipalName	cip_upn
Mail	cip_email
objectSID	cip_sid
objectGUID	cip_oid

The other three AD user attributes objectSID, objectGUID, and mail required for authentication are obtained using the Citrix Cloud connectors joined to the AD domain where the AD shadow account exists. They no longer need to be included in the SAML assertion during a SAML sign-in flow for store or Citrix Cloud.

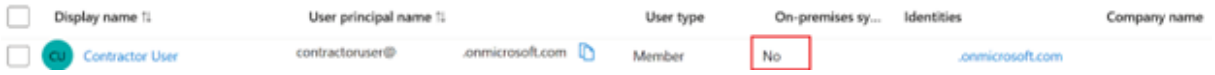
AD Attribute	Default Attribute Name in the SAML Assertion
userPrincipalName	cip_upn

> **Important:**
>
> It is still necessary to send the **displayName** for all SAML flows including B2B SAML. The **displayName** is required by the store UI to correctly show the store user's full name.

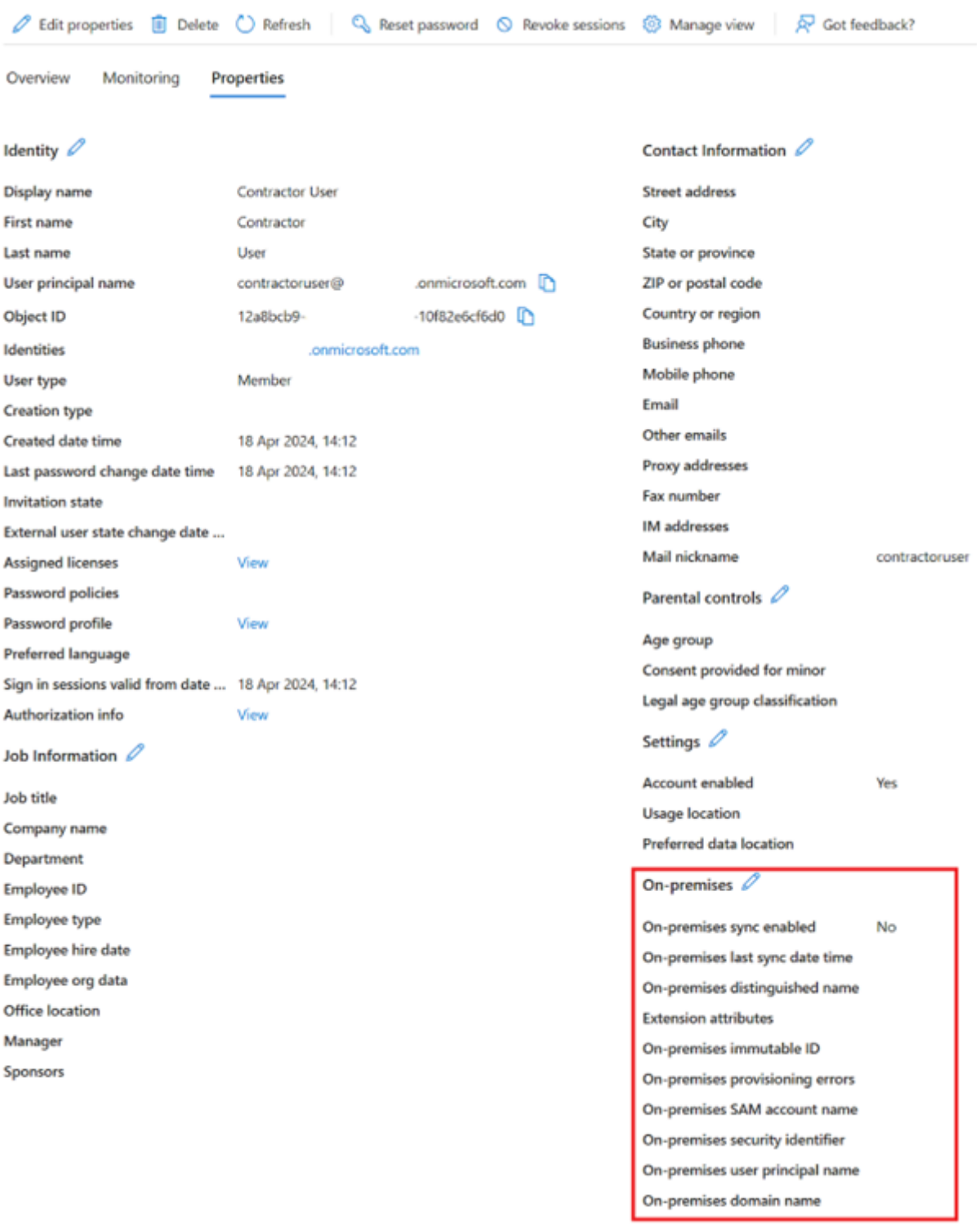
© 1997–2026 Citrix Systems, Inc. All rights reserved.

What is a native SAML user identity?

A native SAML user is a user identity that only exists within your SAML provider directory, e.g. Entra ID or Okta. These identities do not contain on-prem user attributes as they are not created via AD synching tools like Entra ID Connect. They require matching AD backend shadow accounts to be able to enumerate and launch DaaS resources, the native SAML user must be mapped to a corresponding account within Active Directory.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

What is a B2B user imported from another Entra ID tenant?

A B2B user is an Entra ID user which exists as a member inside Entra ID tenant 1 and is invited to other Entra ID tenants such as Entra ID tenant 2 as a guest user. The B2B SAML app is configured inside Entra ID tenant 2 and is connected to Citrix Cloud as a SAML IdP. B2B users require matching AD backend shadow accounts to be able to enumerate and launch DaaS resources. The B2B user must be mapped to a corresponding shadow account within Active Directory.

Refer to Microsoft documentation for details of B2B users and how to invite member users from other Entra ID tenants into your Entra ID tenant as guest users.

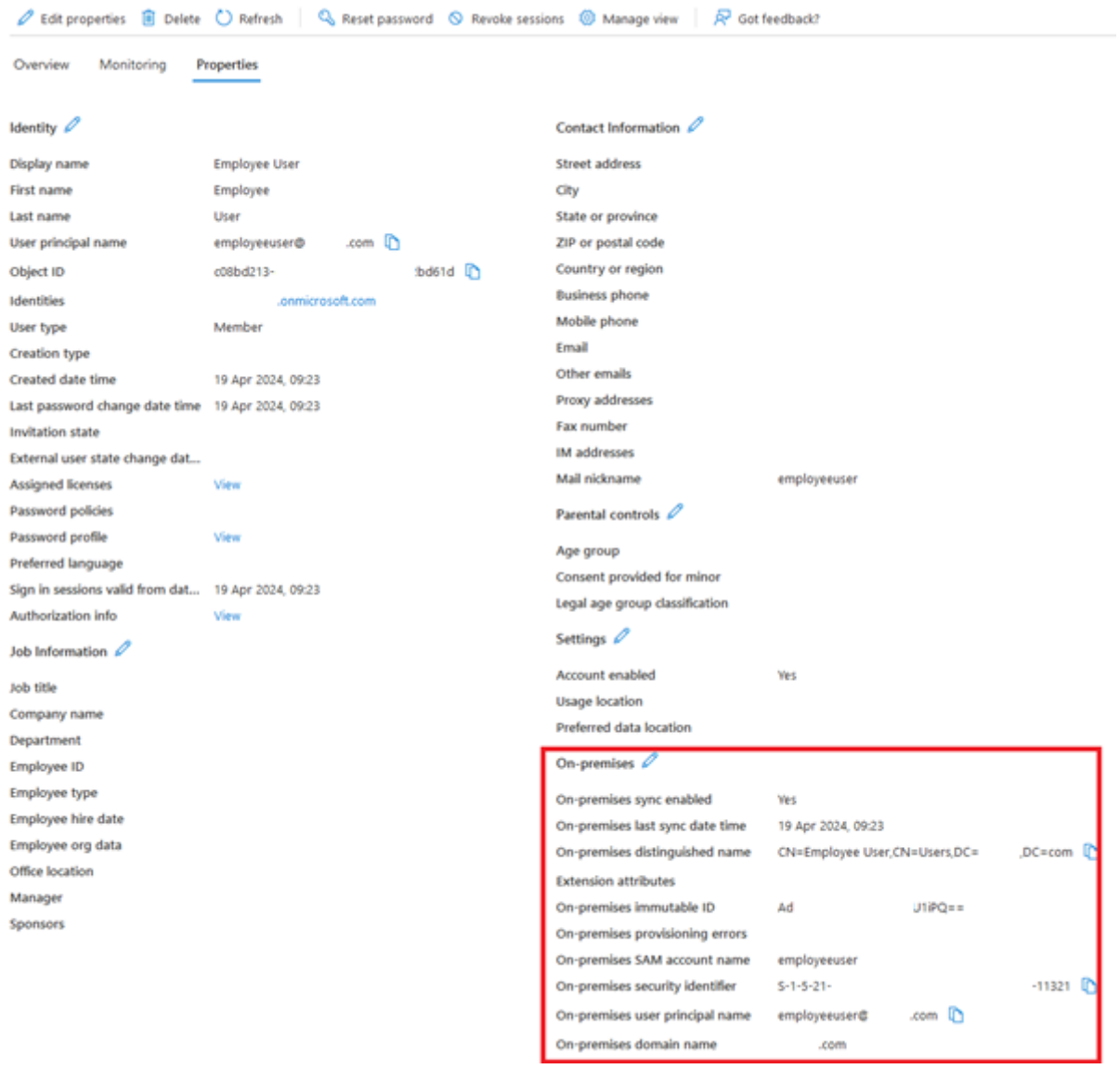
Overview: B2B collaboration with external guests for your workforce
Properties of a Microsoft Entra B2B collaboration user

What is an AD backed SAML user identity?

An AD backed SAML user is a user identity that exists within your SAML provider directory like Entra ID or Okta and also within your on premise AD forest. These identities contain on-prem user attributes as they are created via AD synching tools like Entra ID Connect. AD backend shadow accounts are not required for these users as they contain on premise SIDs and OIDs and so can enumerate and launch DaaS resources published using AD domain joined VDAs.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



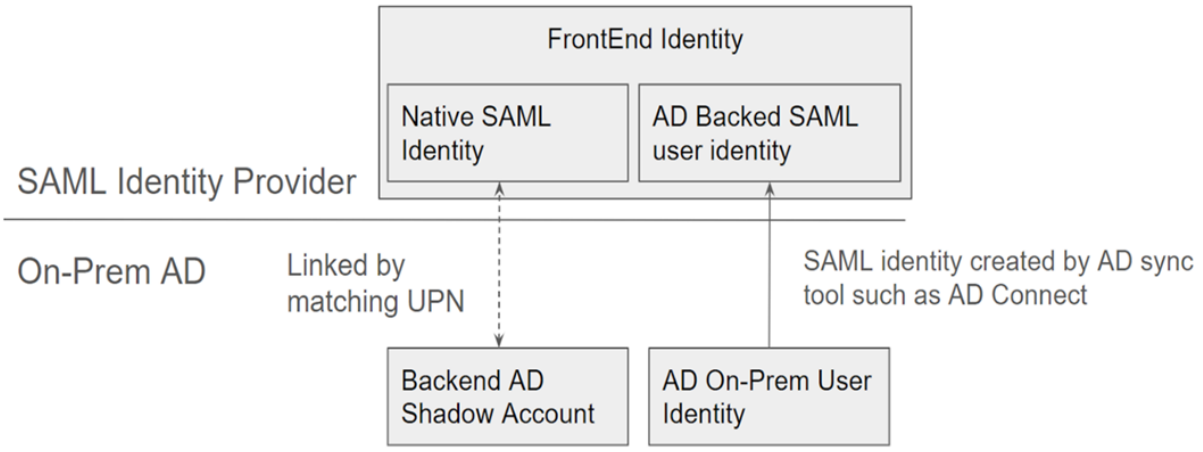
What is a FrontEnd Identity?

A frontend identity is the identity used to sign-in to both the SAML provider and store. Frontend identities have different user attributes depending on how they were created within the SAML provider.

1. Native SAML user identity
2. AD backed SAML user identity

Your SAML provider may have a mixture of these two types of identities. For example, if you have both contractors and permanent employees within your identity platform, the B2B SAML will work for both types of Frontend identities but is only mandatory if you have some accounts that are of type native SAML user identity.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



What is a Backend AD shadow account?

A backend AD shadow account is an AD account used by DaaS, which is mapped to a corresponding frontend identity within your SAML provider.

Why are Backend AD shadow accounts needed?

In order to enumerate DaaS or CVAD resources published using AD domain joined VDAs, AD accounts within the Active Directory forest that the VDAs are joined to are required. Map resources within your DaaS delivery group to shadow account users, and to AD groups containing shadow accounts within the AD domain which you joined your VDAs to.

> **Important:**
>
> Only native SAML users with no AD Domain attributes require matching AD shadow accounts. If your FrontEnd Identities are imported from Active Directory then you do not need to use B2B SAML, and do not need to create Backend AD shadow accounts.

How do we link the FrontEnd Identity to the corresponding Backend AD shadow account?

The method used to link the FrontEnd identity and the Backend identity is by using matching UPNs. The two linked identities should have identical UPNs so that store can tell that they represent the same end user that needs to sign in to store, and to enumerate and launch DaaS resources.

> **Important**
>
> A single frontend identity can only be mapped to a single backend identity in one AD forest/domain. Enumeration of DaaS resources will occur using just one SID value obtained from the AD shadow account lookup performed by the correct Citrix Cloud connectors. You cannot create a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> one to many relationship using a single frontend user which matches multiple AD shadow accounts with the same UPN suffix. The backend AD shadow account should exist only within a single AD forest/domain.
>
> Supported using unambiguous UPN matching between Frontend and Backend identities
> FrontEnd User (user@yourforest.com) > Backend User in AD Forest 1 (UPN user@yourforest.com)
>
> Unsupported as there is UPN ambiguity when attempting to match one Frontend to one Backend identity
> FrontEnd User (user@yourforest1.com) > Backend User in AD Forest 1 (UPN user@yourforest1.com) > Backend User in AD Forest 2 (UPN user@yourforest1.com)

Is Citrix FAS needed for B2B SAML?

Yes. FAS is required for SSON to the VDA during launch when using any federated authentication method to sign in to store.

What is the "SID mismatch problem"and when can it occur?

The "SID mismatch problem"is caused when the SAML assertion contains a SID for a FrontEnd user, which does not match the SID of the AD Shadow Account user. This can happen when the account signing into your SAML provider has an on premise SID, which is not the same as the shadow account user's SID. This can only occur when the Frontend identity is provisioned by AD synchronisation tools like Entra ID Connect and from a different AD Forest than where the shadow account was created.

`B2B SAML` prevents the "SID mismatch problem"from occurring. The correct SID is always fetched for the shadow account user via the Citrix Cloud connectors joined to the backend AD domain. The shadow account user lookup is performed using the UPN of the FrontEnd user, which is then matched to its corresponding backend shadow account user.

Example of the SID Mismatch Problem:
FrontEnd user was created by Entra ID Connect and is synced from **AD forest 1**.
`S-1-5-21-000000000-0000000000-0000000001-0001`

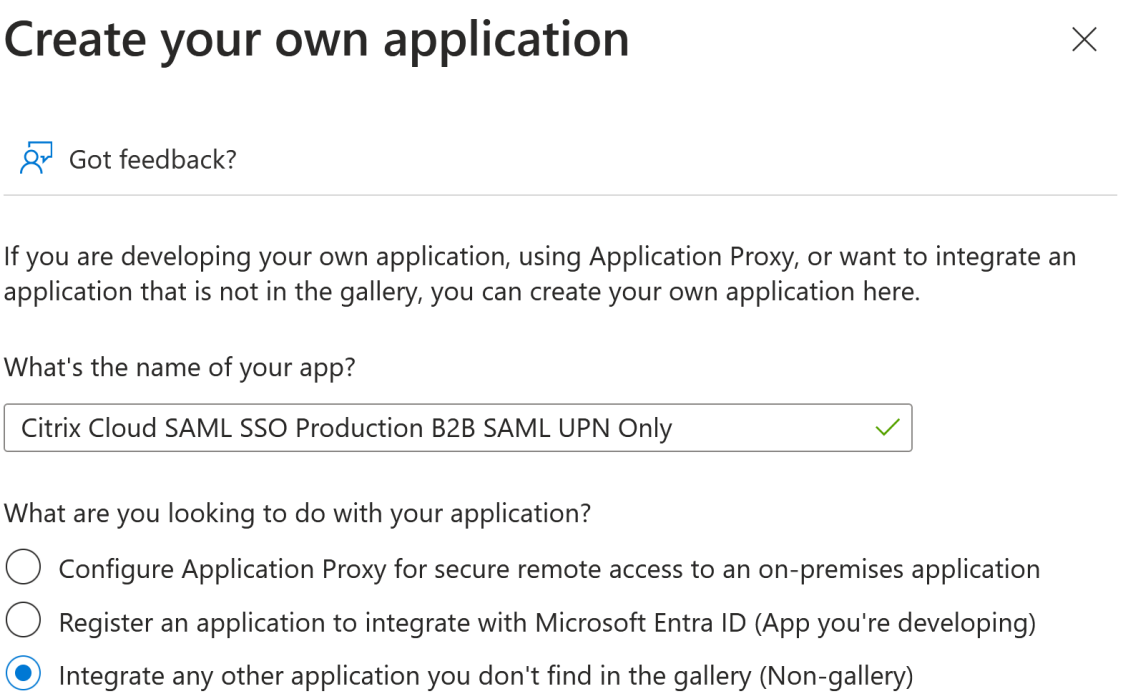
Backend shadow account user was created within **AD forest 2** and mapped to DaaS resources
`S-1-5-21-000000000-0000000000-0000000002-0002`

The SAML assertion contains all four cip_* attributes and **cip_sid** contains the value `S-1-5-21-000000000-000` , which does not match the shadow account's SID and triggers an error.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure the B2B SAML Application within Entra ID for external guest accounts

1. Sign-in to the Azure portal.
2. From the portal menu, select **Entra ID**.
3. From the left pane, under **Manage**, select **Enterprise Applications**.
4. Select **Create your own application**.
5. Enter a suitable name for the SAML application such as `Citrix Cloud SAML SSO Production B2B SAML UPN Only`.



6. From the left navigation pane, select **Single sign-on** and from the working pane, click **SAML**.
7. In the **Basic SAML Configuration** section, click **Edit** and configure the following settings:

   a) In the **Identifier (Entity ID)** section, select **Add identifier** and then enter the value associated with the region in which your Citrix Cloud tenant is located:

   - For Europe, United States, and Asia-Pacific South regions, enter `https://saml.cloud.com`.
   - For the Japan region, enter `https://saml.citrixcloud.jp`.
   - For the Citrix Cloud Government region, enter `https://saml.cloud.us`.

   b) In the **Reply URL (Assertion Consumer Service URL)** section, select **Add reply URL** and then enter the value associated with the region in which your Citrix Cloud tenant is located:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

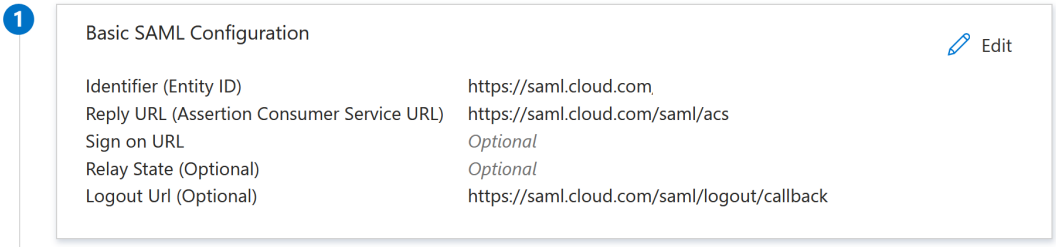
- For Europe, United States, and Asia-Pacific South regions, enter `https://saml.cloud.com/saml/acs`.
- For the Japan region, enter `https://saml.citrixcloud.jp/saml/acs`.
- For the Citrix Cloud Government region, enter `https://saml.cloud.us/saml/acs`.

c) In the **Sign on URL** section, enter your store URL.

d) In the **Logout URL (Optional)** section, enter the value associated with the region in which your Citrix Cloud tenant is located:

- For Europe, United States, and Asia-Pacific South regions, enter `https://saml.cloud.com/saml/logout/callback`.
- For the Japan region, enter `https://saml.citrixcloud.jp/saml/logout/callback`.
- For the Citrix Cloud Government region, enter `https://saml.cloud.us/saml/logout/callback`.

e) From the command bar, click **Save**. The **Basic SAML Configuration** section appears as follows:



8. In the **Attributes & Claims** section, click **Edit** to configure the following claims. After SAML app creation, configure the following attributes.

a) For the Unique User Identifier (Name ID) claim, set the Name Identifier Format to be unspecified and its source attribute as `user.localuserprincipalname`.

b) For **cip_upn** claim, leave the default value of `user.localuserprincipalname`.

c) For **displayName**, leave the default value of `user.displayname`.

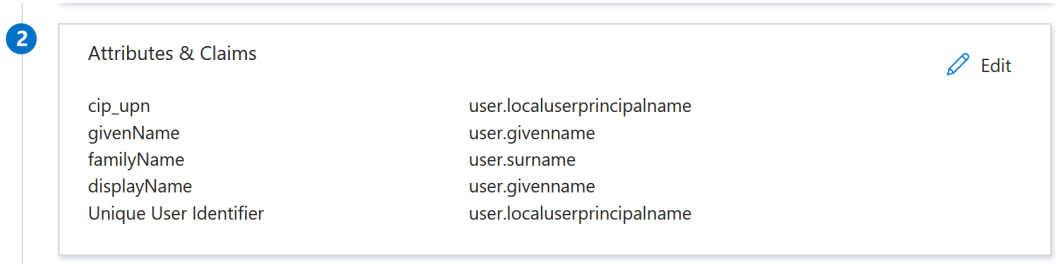
d) For **givenName** claim, update the default value to be `user.givenname`.

e) For **familyName** claim, update the default value to be `user.surname`.

f) In the **Additional claims** section, for any remaining claims with the `http://schemas.xmlsoap.org/ws/2005/05/identity/claims` namespace, click the ellipsis (...) button and click **Delete**. No need to include these claims as they are duplicates of the above user attributes.

When finished, the **Attributes & Claims** section appears as illustrated below:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

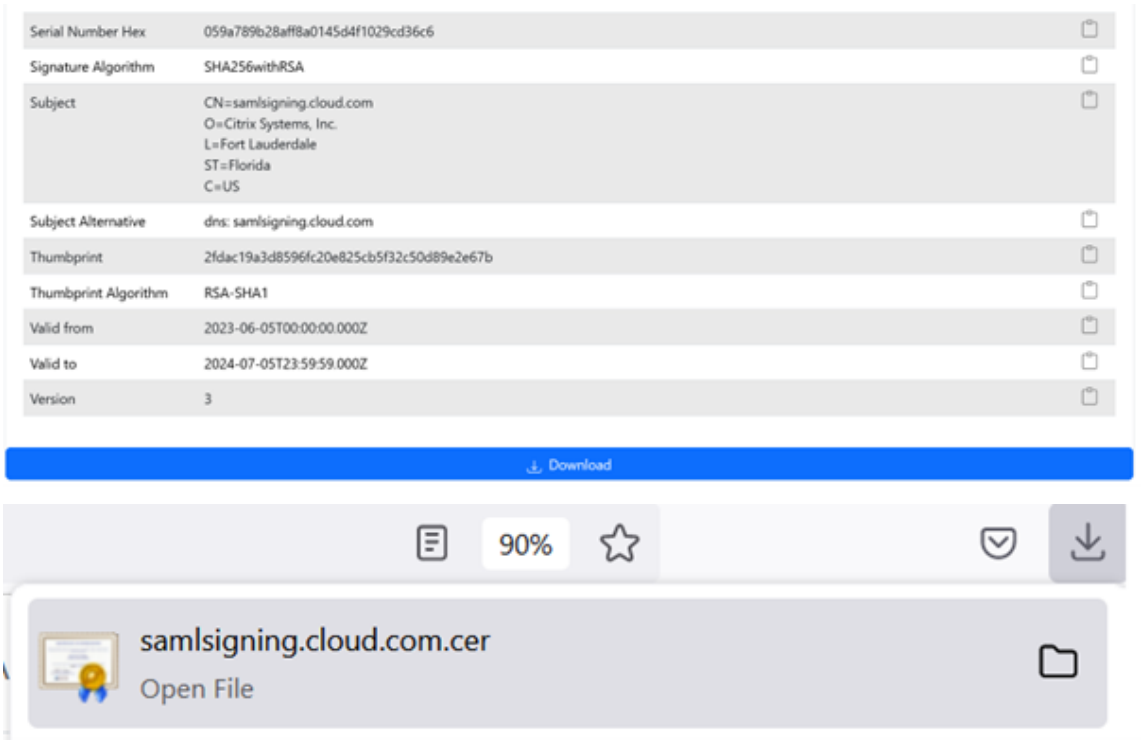


g) Obtain a copy of the Citrix Cloud SAML signing certificate using this third party online tool.

h) Enter `https://saml.cloud.com/saml/metadata` in the URL field and click **Load**.



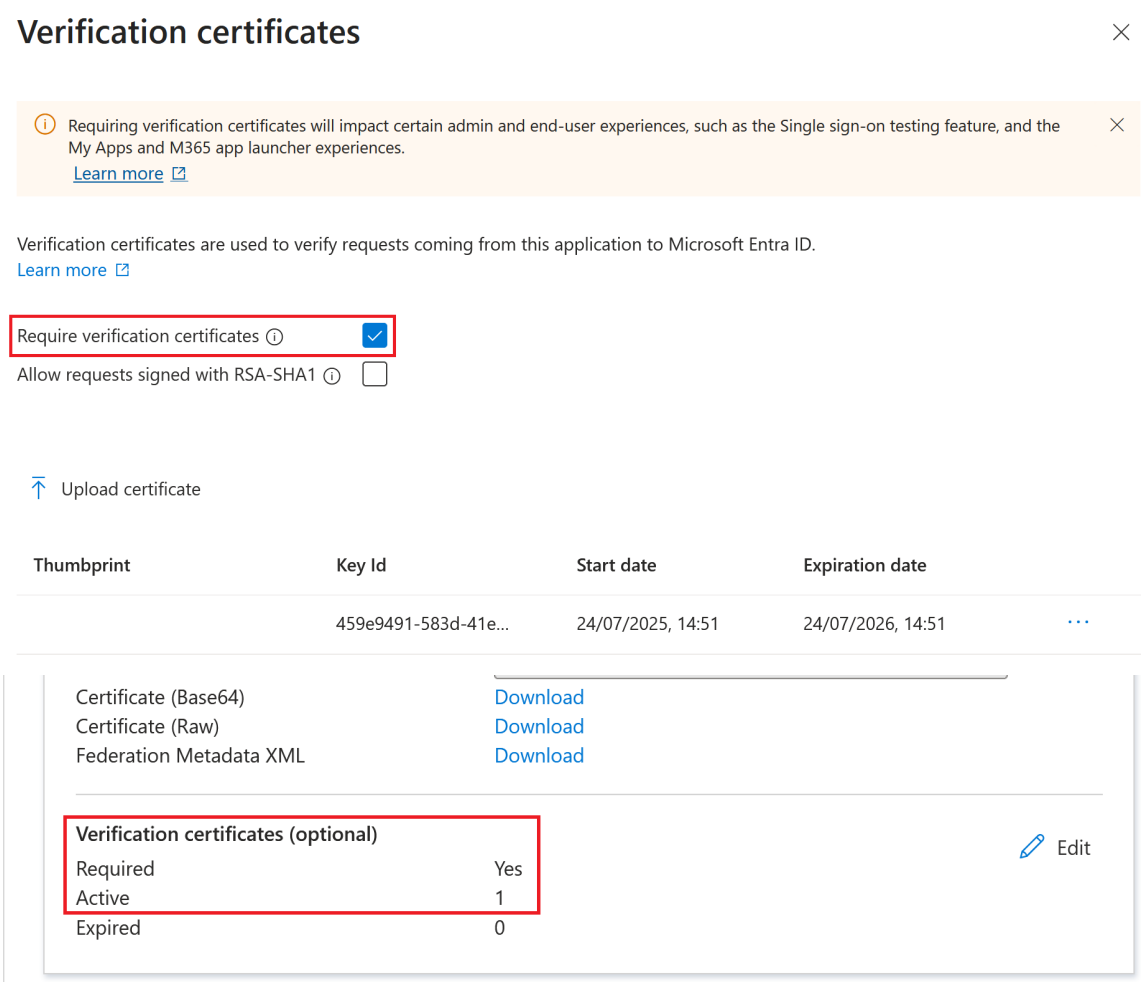
9. Scroll to the bottom of the page and click **Download**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

10. Configure the Entra ID SAML application Signing Settings.
11. Upload the production SAML signing certificate obtained in step 10 within the Entra ID SAML application

    a) Enable **Require verification certificates**.



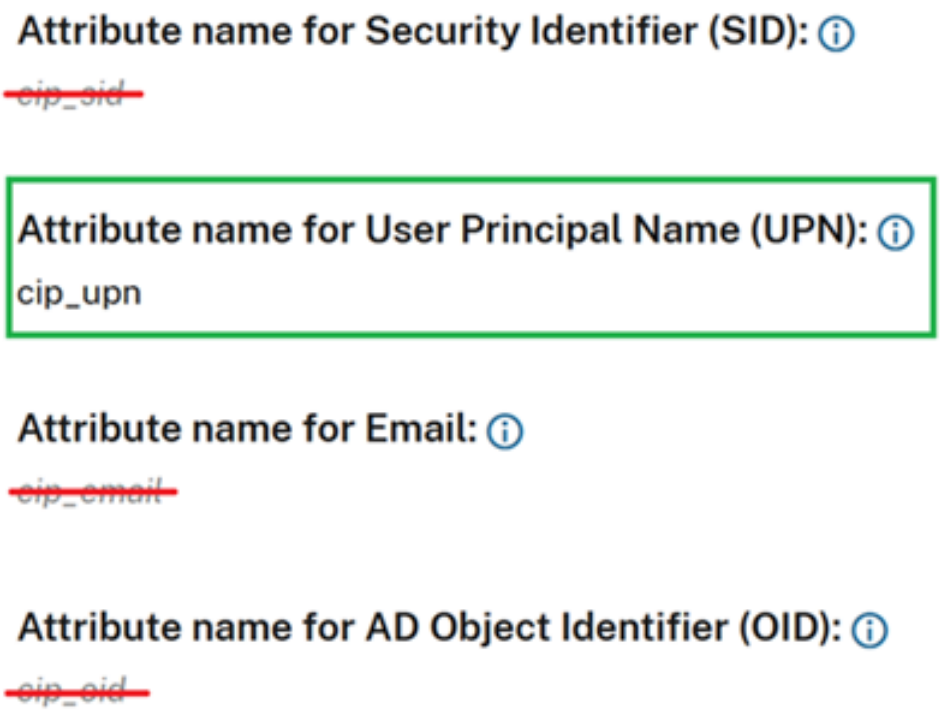
Configure the Citrix Cloud B2B SAML Connection

By default, Citrix Cloud will expect cip_upn, cip_email, cip_sid and cip_oid to be present in the SAML assertion and will fail the SAML sign-in if these attributes are not sent. To prevent this, remove the checks for these attributes when you create your new SAML connection.

1. Create a new SAML connection using the default settings.
2. Navigate to the **SAML Attribute Mappings Configuration** section at the bottom and make changes before saving the new SAML configuration.
3. Remove the SAML attribute name from each of the **cip_email**, **cip_sid**, and **cip_oid** fields.
4. Do not remove **cip_upn** from its field.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Do not remove any other attributes from their respective fields. The **displayName** is still needed by the store UI and should not be changed.



Configure your AD Shadow Account Resource Location and Connectors

A resource location and connector pair within the backend shadow account AD forest are required. Citrix Cloud requires connectors within this AD forest to look up shadow account user identities and attributes such as cip_email, cip_sid, and cip_oid when only cip_upn is provided directly within the SAML assertion.

1. Create a new **Resource Location** which will contain Citrix Cloud connectors joined to the back-end shadow account AD forest.



2. Name the Resource Location to match the AD forest, which contains the backend AD shadow accounts you wish to use.
3. Configure a pair of Citrix Cloud connectors within the newly created resource location.

For example

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ccconnector1.shadowaccountforest.com
ccconnector2.shadowaccountforest.com

Configure FAS within the Backend AD Forest

Contractor Frontend users will definitely require FAS. During DaaS launches contractor users will not be able to manually enter windows credentials to complete the launch as they will likely not know the AD shadow account password.

1. Configure one or more FAS servers within the backend AD forest where your shadow accounts were created.
2. Link the FAS servers to the same Resource Location that contains a pair of Citrix Cloud connectors joined to the backend AD forest where your shadow accounts were created.



Configure alternative UPN Suffixes within your AD Domain

> **Important:**
>
> A UPN is not the same as the users email address. In many cases they are the same value for ease of use, but UPN and email can often have different values and are defined in different active directory attributes and within different Entra ID user attributes. This solution depends on UPN matching between frontend and backend identities and not email matching.

You can use the implicit UPN suffix for your domain if it is publicly routable in DNS or add a matching alternative UPN suffix for every external FrontEnd user you wish to invite into your Okta or Entra ID tenants. If AD uses yourdomain.local as the implicit UPN you will have to choose an alternative UPN suffix like yourdomain.com. Entra ID will not allow you to add yourdomain.local within Custom Domain Names.

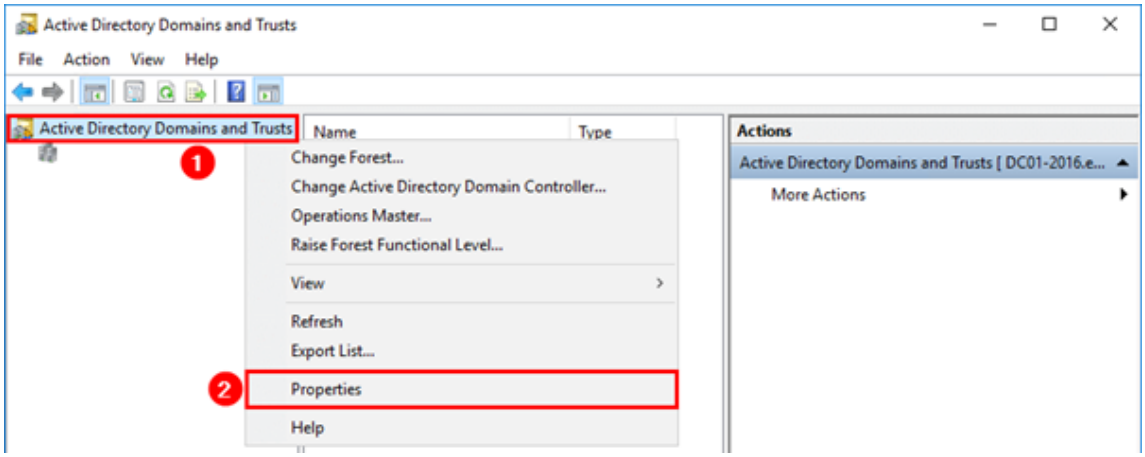
For example, if you invite an external user contractoruser@hotmail.co.uk and you wish to associate this with a backend AD shadow account contractoruser@yourforest.com then add yourforest.com as an ALT UPN Suffix within your AD forest.

Add Alternative UPN Suffixes in Active Directory using Active Directory Domains and Trusts UI

1. Sign in to a domain controller within your backend AD forest.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Open the **Run dialog**, and then type in `domain.msc`, and then click **OK**.
3. On the Active Directory Domains and Trusts window, right-click **Active Directory Domains and Trusts**, and then select **Properties**.
4. On the **UPN Suffixes** tab, in the Alternative UPN Suffixes box, add an alternative UPN suffix, and then select **Add**.



5. Click **OK**.

Manage your Backend AD Forest's UPN Suffixes using PowerShell

You may need to add a large number of new UPN suffixes to your backend AD forest in order to create the necessary shadow account UPNs. The number of alternative UPN suffixes you will be required to add to your backend AD forest will depend on how many different external users you choose to invite into your SAML Provider tenant.

Here is some PowerShell to achieve this if a large number of new alternative UPN suffixes need to be created.

```
# Get the list of existing ALT UPN suffixes within your AD Forest
(Get-ADForest).UPNSuffixes

# Add or remove ALT UPN Suffixes
$NewUPNSuffixes = @("yourforest.com","externalusers.com")

# Set action to "add" or "remove" depending on the operation you wish
   to perform.
$Action = "add"
foreach($NewUPNSuffix in $NewUPNSuffixes)
{

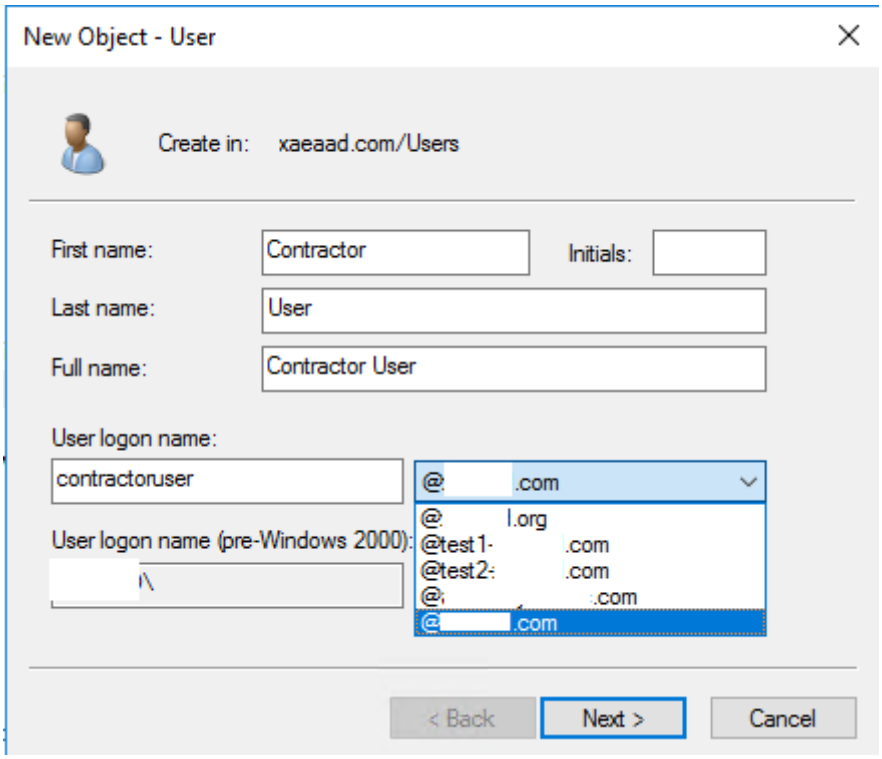
    Get-ADForest | Set-ADForest -UPNSuffixes @{
  $Action=$NewUPNSuffix  }

 }
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure an AD Shadow Account within your Backend AD Forest

1. Create a new AD shadow account user.
2. The AD forest implicit UPN such as `yourforest.local` is selected by default for new AD users. Select the appropriate alternative UPN suffix you created earlier. For example, select `yourforest.com` as the shadow account user's UPN Suffix.



The shadow account user's UPN can also be updated through PowerShell.

```
Set-ADUser "contractoruser" -UserPrincipalName "
    contractoruser@yourforest.com"
```

> **Important**
>
> Windows AD PowerShell will allow you to create shadow account users with any UPN suffix you specify even if that UPN suffix does not exist inside your AD forest. The alternative UPN Suffix you wish to use must exist within the AD forest as the Citrix Cloud connectors depend on this list to lookup the backend shadow account users. If the alternative UPN suffix does not appear in the AD forest as per the screen shot above then Citrix Cloud will not be able to match your frontend identity to an appropriate backend AD shadow account.

3. The shadow account user's UPN should exactly match the external FrontEnd identity user's UPN.
4. Test the FrontEnd user's sign in to store.

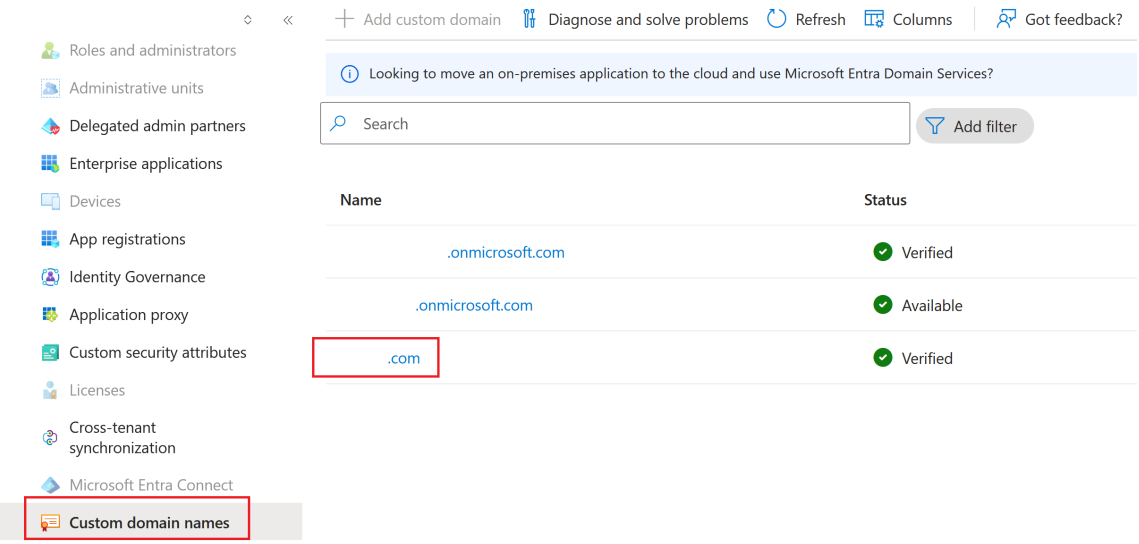
© 1997–2026 Citrix Systems, Inc. All rights reserved.

5. Verify all expected resources are enumerated in store after the sign-in has succeeded. Resources mapped to the AD shadow account should appear.

Configure the Guest Entra ID User UPN to match the AD Shadow Account UPN

When external guest users are invited to an Entra ID tenant, an auto generated UPN is created indicating that the user is external. The external Entra ID user will be automatically assigned the @Entra IDtenant.onmicrosoft.com UPN suffix, which is unsuitable for use with B2B SAML and will not match your AD shadow account. This will need to be updated to match an imported DNS domain within Entra ID and the alternative UPN suffix you created within your AD forest.

1. Import a Custom Domain into Entra ID that matches the alternative UPN suffix you added to your AD forest.

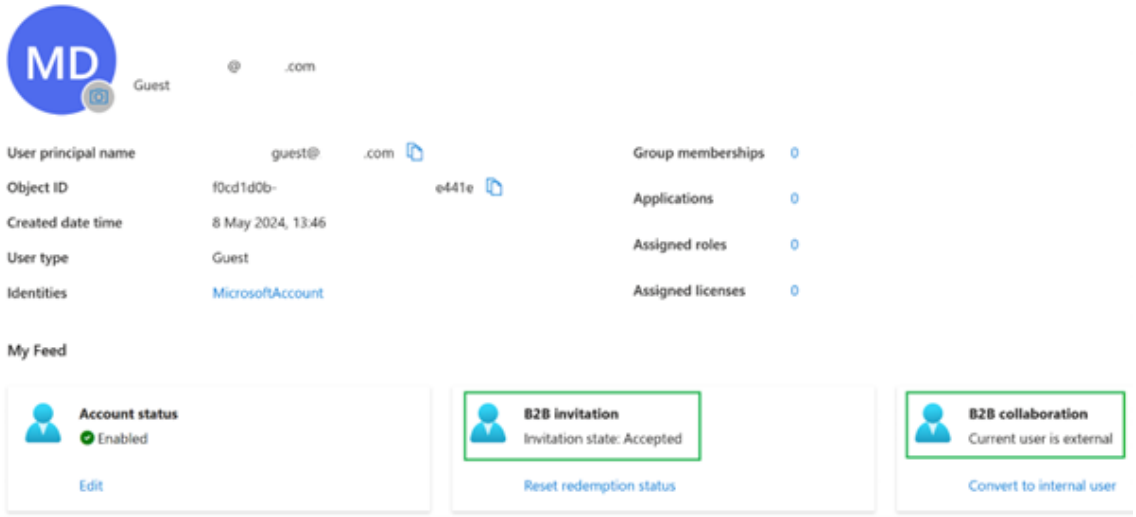


2. Invite a guest user such as `contractoruser@hotmail.co.uk` and ensure the invited gues user accepts the Microsoft invitation to the Entra ID tenant.

   Example external guest user UPN format generated by Microsoft. `contractoruser_hotmail.co.uk#EXT#@yourEntra IDtenant.onmicrosoft.com`



© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Important:**
>
> Citrix Cloud and store cannot use UPNs containing the # character for SAML authentication.

3. Install the necessary Azure PowerShell Graph modules to allow you to manage Entra ID users.

```
Install-Module -Name "Microsoft.Graph" -Force
Get-InstalledModule -Name  "Microsoft.Graph"
```

4. Sign in to your Entra ID tenant using a global admin account and with the `Directory.AccessAsUser.All` scope.

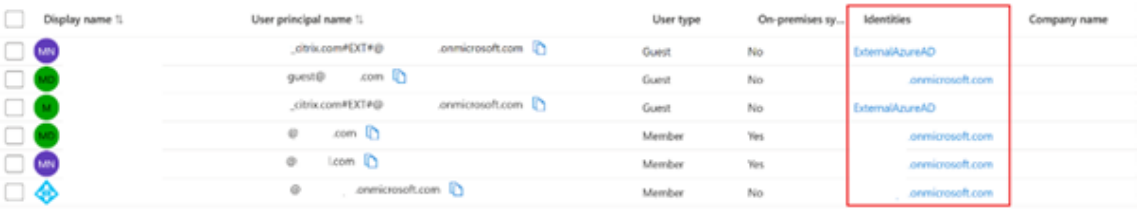
> **Important:**
>
> If you use a less privileged account or do not specify the `Directory.AccessAsUser.All` scope you will not be able to complete Step 4 and update the Guest user's UPN.

```
Connect-MgGraph -Scopes Directory.AccessAsUser.All
```

5. Update the Entra ID user with a UPN that matches the UPN you configured for your AD shadow account.

```
$GuestUserId = (Get-MgUser -UserId "contractoruser_hotmail.co.uk#
    EXT#@yourentraidtenant.onmicrosoft.com").Id
Update-MgUser -UserId $GuestUserId -UserPrincipalName "
    contractoruser@your.com"
```

6. Get the entire list of external guest users within your Entra ID tenant (optional).



© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-MgUser -filter "userType eq 'Guest'" | Select Id,DisplayName,
    UserPrincipalName,Mail
```

7. Get the Guest user identity that needs its UPN updated and then update its UPN suffix.

```
$GuestUserId = (Get-MgUser -UserId "contractoruser_hotmail.co.uk#
    EXT#@yourEntra IDtenant.onmicrosoft.com").Id

Update-MgUser -UserId $GuestUserId -UserPrincipalName "
    contractoruser@yourforest.com"
```

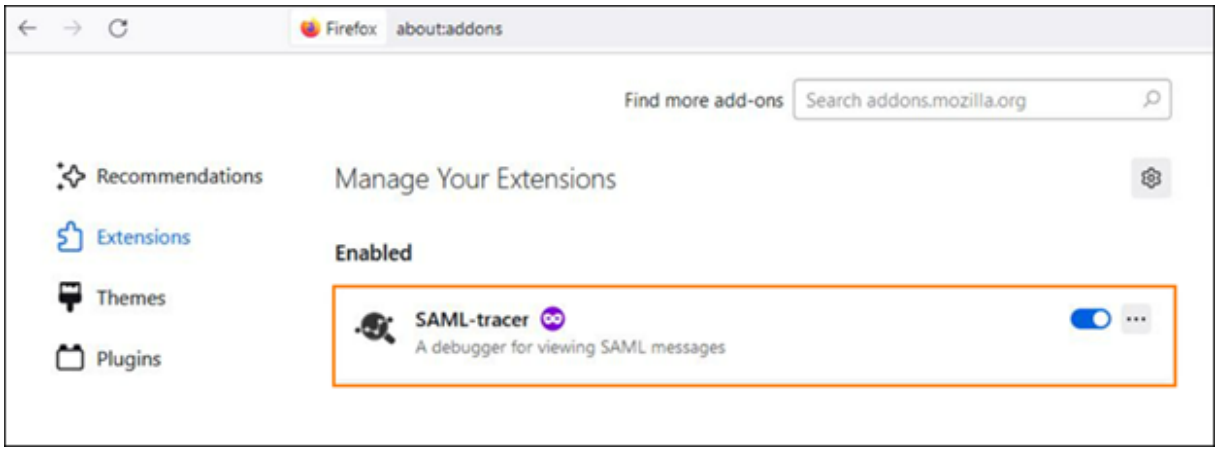
8. Check the Guest user identity can be found using its newly updated UPN.

```
Get-MgUser -UserId "contractoruser@yourforest.com"
```

Testing the B2B SAML Solution

Once all documented steps have been completed in AD, Citrix Cloud and your SAML provider then you need to test the sign-in and verify that the correct list of resources are shown for the guest user within store.

Citrix recommends the use of the SAML-tracer browser extension for all SAML debugging. This extension is available for most common web browsers. The extension decodes Base64-encoded requests and responses into SAML XML, which renders them human-readable.



Example of a B2B SAML assertion using just cip_upn for authentication captured using SAML tracer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<AttributeStatement>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/tenantid">
        <AttributeValue>                                    </AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/objectidentifier">
        <AttributeValue>                                    </AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/identity/claims/identityprovider">
        <AttributeValue>https://sts.windows.net/                                    /</AttributeValue>
    </Attribute>
    <Attribute Name="http://schemas.microsoft.com/claims/authnmethodsreferences">
        <AttributeValue>http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/        </AttributeValue>
    </Attribute>
    <Attribute Name="cip_upn">
        <AttributeValue>                    </AttributeValue>
    </Attribute>
    <Attribute Name="lastName">
        <AttributeValue>    </AttributeValue>
    </Attribute>
    <Attribute Name="firstName">
        <AttributeValue>    </AttributeValue>
    </Attribute>
    <Attribute Name="displayName">
        <AttributeValue>          </AttributeValue>
    </Attribute>
</AttributeStatement>
```

FrontEnd Identity Type	Synched from AD	Has Connectors in AD	Needs AD Shadow Account	Login using Attribute
Internal AD Backed User in Shadow Account Forest	Yes	Yes	No	UPN
Internal AD Backed User in Different Forest	Yes	No	Yes	UPN
Internal Native User	No	Not applicable	Yes	UPN
External Guest User	No	Not applicable	Yes	Email

1. Map the correct DaaS resources to AD backed and shadow account users or groups that contain them.
2. Start the SAML tracer browser extension and capture the entire logon and logoff flow.
3. Log into store using the attribute specified in the table for the frontend user type you wish to test.

   Guest Entra ID user logon: The contractor user you invited to your Entra ID tenant as a guest user has the email address `contractoruser@hotmail.co.uk`.

   Enter the guest user's **email address** when prompted by Entra ID.

   OR

   AD backed Entra ID user/Native Entra ID user logon: These Entra ID users will have UPNs in the format of `adbackeduser@yourforest.com` or `nativeuser@yourforest.com`.

   Enter the user's **UPN** when prompted by Entra ID.
4. Check the assertion only contains the **cip_upn** attribute for authentication and that it also contains the **displayName** attribute required by the store UI.
5. Check the user can see the required DaaS resources in the UI.

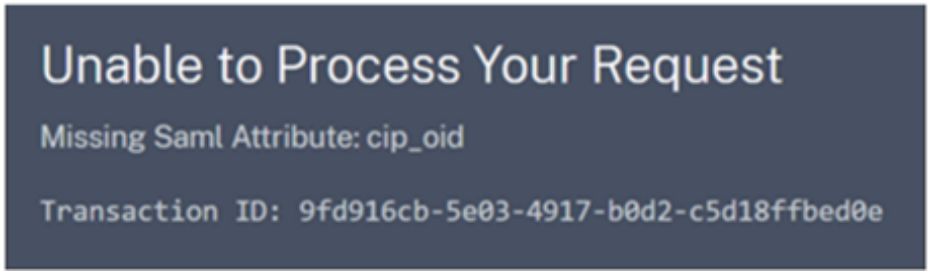
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting the B2B SAML Solution

Wrong UPN being sent within the SAML assertion

Cause: This can only occur for **B2B** accounts imported from Entra ID tenant 1 into Entra ID tenant 2. The wrong UPN can be sent within the SAML assertion when using **B2B** users imported from other Entra ID tenants. If `user.userprincipalname` is used and the end user logs in with a B2B user imported from another Entra ID tenant then the wrong value for **cip_upn** will be sent in the SAML assertion. The value for **cip_upn** used in the SAML assertion will be from the source Entra ID tenant which contains the B2B user as a **member**. Using `user.localuserprincipalname` ensures that the value for **cip_upn** is taken from the Entra ID tenant with the B2B user invited as a **guest**.

Missing cip_* Attribute Errors



Cause 1: The SAML attribute is not present in the SAML assertion but Citrix Cloud is configured to expect to receive it. You have failed to remove the unnecessary cip_* attributes from the Citrix Cloud SAML connection within the SAML Attributes section. Disconnect and reconnect SAML to remove references to the unnecessary cip_* attributes.

Cause 2: This error can also occur if there is no corresponding AD shadow account for the Citrix Cloud connectors to look up in your backend AD forest. You may have correctly configured the frontend identity but the backend AD shadow account identity with a matching UPN does not exist or cannot be found.

Logon succeeds but no DaaS resources are shown after the user has logged into store

Cause: This is most likely caused by incorrect frontend to backend identity UPN mappings.

Ensure the 2 UPNs for the frontend and backend identities exactly match and represent the same end user that is logging into store. Check that the DaaS delivery group contains mappings to the correct AD shadow account users or AD groups that contain them.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

During Launch of DaaS Resources FAS SSON to the AD domain joined VDAs is failing

When attempting to launch DaaS resources the store end user is prompted to enter their windows credentials within the GINA. Also Event ID 103 is appearing within the windows event logs on your FAS servers.

[S103] Server [CC:FASServer] requested UPN [frontenduser@yourforest.com] `SID S-1-5-21-000000000-00` , but lookup returned `SID S-1-5-21-000000000-0000000000-0000000001-0002`. [correlation: cc#967472c8-4342-489b-9589-044a24ca57d1]

Cause: Your B2B SAML deployment is suffering from the "SID mismatch problem". You have frontend identities which contain SIDs from an AD forest which is different from the backend shadow account AD forest.
Do not send **cip_sid** in the SAML assertion.

Logon fails for AD Backed Users when the same UPN suffix exists in multiple connected AD forests

Citrix Cloud has multiple resource locations and connectors joined to different AD forests. Logon fails when AD backed users imported into Entra ID from a different AD forest than the shadow accountAD forest are used.

AD Forest 1 is synched to Entra ID to create frontend users with UPNs such as `frontenduser@yourforest.com`.

AD Forest 2 contains the backend shadow accounts with UPNs such as `frontenduser@yourforest.com`.

Cause: Your B2B SAML deployment is suffering from the "UPN ambiguity problem". Citrix Cloud cannot determine which connectors to use to look up the user's backend identity.

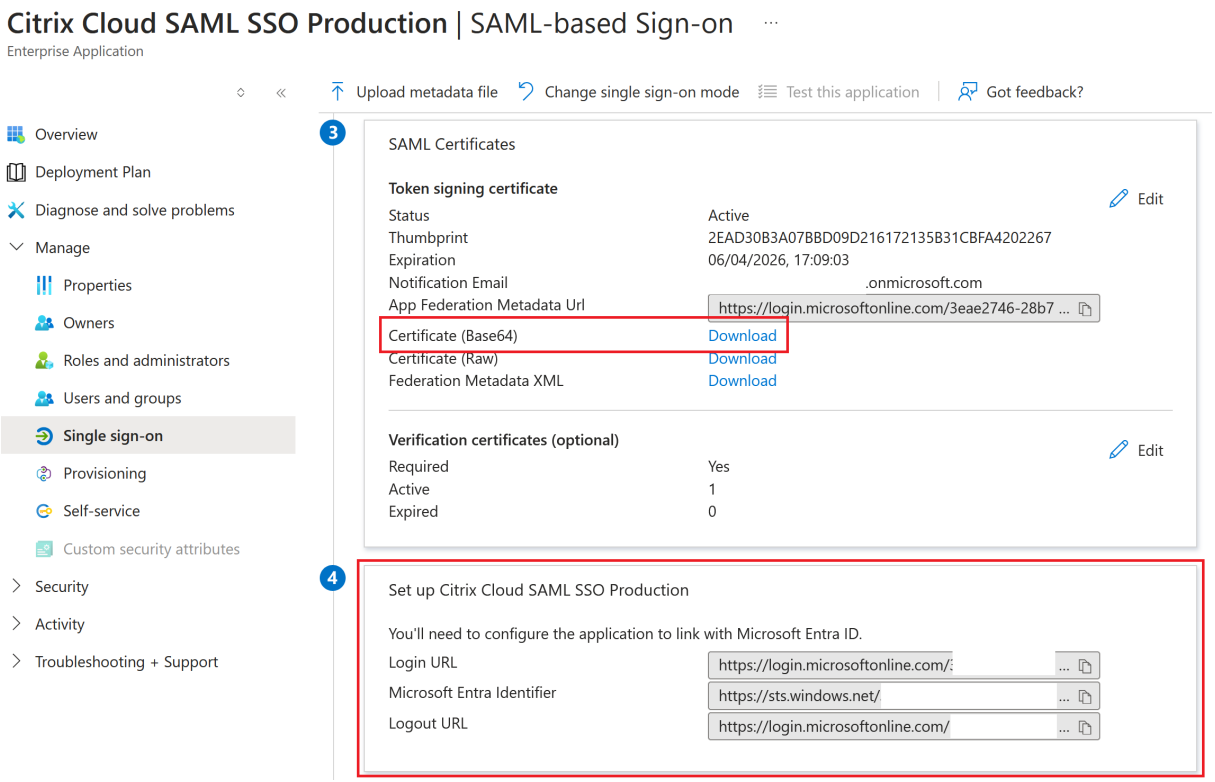
Do not send **cip_sid** in the SAML assertion.
Your user's UPN exists in more than one AD forest connected to Citrix Cloud.

Configure the Citrix Cloud SAML connection

All Citrix logon flows need to be Service Provider initiated using either a store URL or a Citrix Cloud GO URL.

Obtain the Entra ID SAML application SAML endpoints from your Entra ID portal to enter into Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Entra ID SAML endpoint examples to be used within the Citrix Cloud SAML connection

Use the default recommended values for the SAML connection within **Identity and Access Management > Authentication > Add an identity provider > SAML**.

> **Important:**
>
> EntraID SSO and Logout SAML endpoints are the same URL.

In this field in Citrix Cloud	Enter this value
Entity ID	`https://sts.windows.net/<yourEntraIDTenantID>`
Sign Authentication Request	Yes
SSO Service URL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`
SSO Binding Mechanism	HTTP Post
SAML Response	Sign Either Response Or Assertion
Authentication Context	Unspecified, Exact

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In this field in Citrix Cloud	Enter this value
Logout URL	`https://login.microsoftonline.com/<yourEntraIDTenantID>/saml2`
Sign Logout Request	Yes
SLO Binding Mechanism	HTTP Post

Configure Okta as a SAML provider for store authentication

June 22, 2026

Author:
Mark Dear

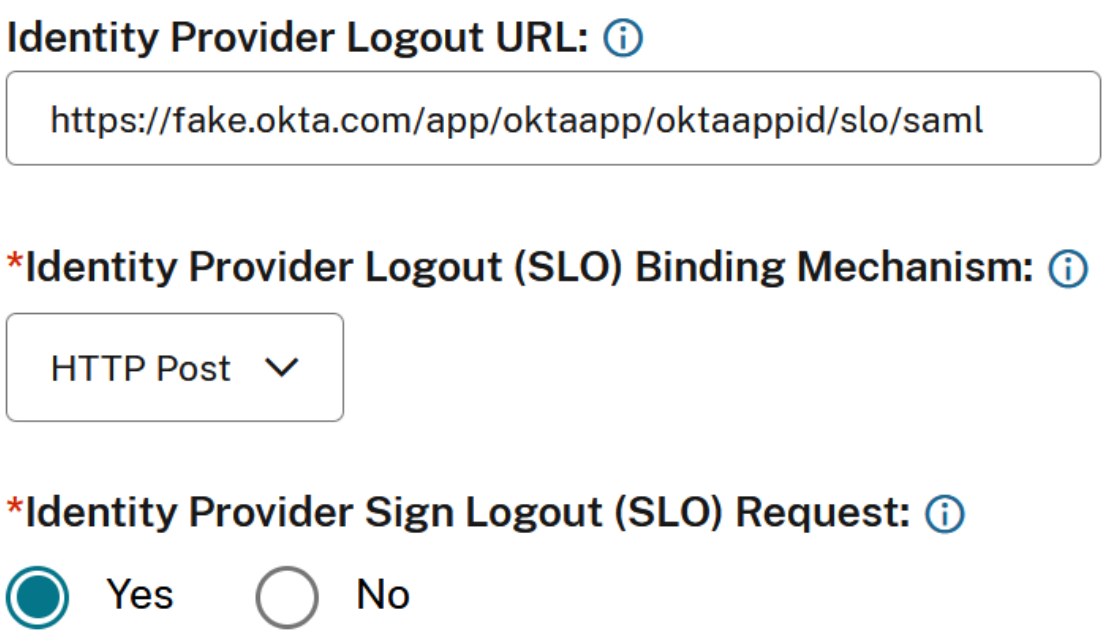
This article describes the required steps for configuring an Okta SAML application and the connection between Citrix Cloud™ and your SAML provider. Some of these steps describe actions that you perform in your SAML provider's administration console.

Prerequisites

Before you complete the tasks in this article, ensure that you've met the following prerequisites:

- Citrix Support has enabled the **SendNameIDPolicyInSAMLRequest** feature in Citrix Cloud. This feature is enabled upon request. For more information about these features, see Required cloud features for SAML using Okta.
- You have an Okta organization that uses one of the following Okta domains:
  - okta.com
  - okta-eu.com
  - oktapreview.com
- You have synchronized your Active Directory (AD) with your Okta organization.
- **Sign Authentication Requests** is enabled in your Okta organization.
- **Identity Provider Single Logout (SLO)** is configured within both Citrix Cloud and Okta SAML applications. When SLO is configured, and the end user signs out of their store, they also sign out of Okta and all other service providers that share the Okta SAML application.
- **Identity Provider Sign Logout (SLO) Requests** is enabled within Citrix Cloud.
- **Identity Provider Logout Binding (SLO)** is HTTPPost within Citrix Cloud.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Required cloud features for SAML using Okta

Before you complete the tasks in this article, you must contact Citrix Support to enable the **SendNameIDPolicyInSAMLRequest** feature. This feature enables Citrix Cloud to supply the **NameID** policy as **Unspecified** in the SAML request to your SAML provider. This feature is enabled for use with Okta only.

You can request these features by signing in to your Citrix account and opening a ticket through the Citrix Support web site.

Requirements

This article includes a task in which you create a SAML application in the Okta Admin console. This application requires a SAML signing certificate for your Citrix Cloud region.

You can extract this certificate from the Citrix Cloud SAML metadata for your region using an extraction tool such as the one located at https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract. Citrix recommends acquiring the Citrix Cloud SAML certificate beforehand so you can supply it when needed.

The steps in this section describe how to acquire the signing certificate using the extraction tool at https://www.rcfed.com/SAMLWSFed/MetadataCertificateExtract.

To acquire the Citrix Cloud metadata for your region:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In the extraction tool of your choice, enter the metadata URL for your Citrix Cloud region:
   - For European Union, United States, and Asia Pacific-South regions, enter `https://saml.cloud.com/saml/metadata`.
   - For the Japan region, enter `https://saml.citrixcloud.jp/saml/metadata`.
   - For the Citrix Cloud Government region, enter `https://saml.cloud.us/saml/metadata`.
2. Click **Load**. The extracted certificate appears below the URL that you entered.
3. Click **Download** to download the certificate in PEM format.

Sync accounts with the Okta AD agent

To use Okta as a SAML provider, you must first integrate your on-premises AD with Okta. To do this, you install the Okta AD agent in your domain and add your AD to your Okta organization. For guidance for deploying the Okta AD agent, see Get started with Active Directory integration on the Okta web site.

Afterward, you import your AD users and groups to Okta. When importing, include the following values associated with your AD accounts:

- Email
- SID
- UPN
- OID

To synchronize your AD users and groups with your Okta organization:

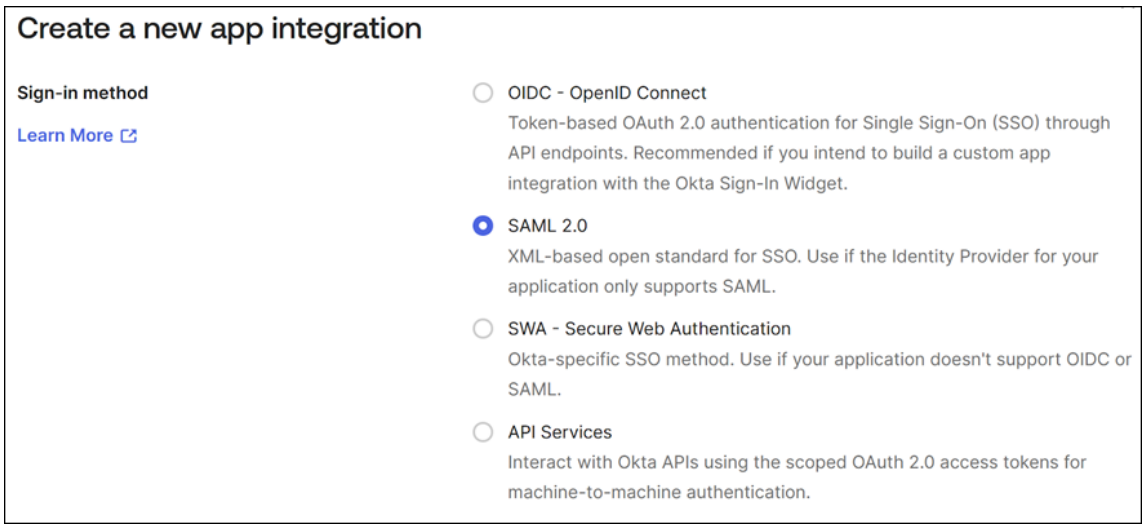
1. Install and configure the Okta AD agent. For complete instructions, refer to the following articles on the Okta website:
   - Install the Okta Active Directory agent
   - Configure Active Directory import and account settings
   - Configure Active Directory provisioning settings
2. Add your AD users and groups to Okta by performing a manual import or an automated import. For more information about Okta import methods and instructions, refer to Manage Active Directory users and groups on the Okta website.

Configure an Okta SAML application for store authentication

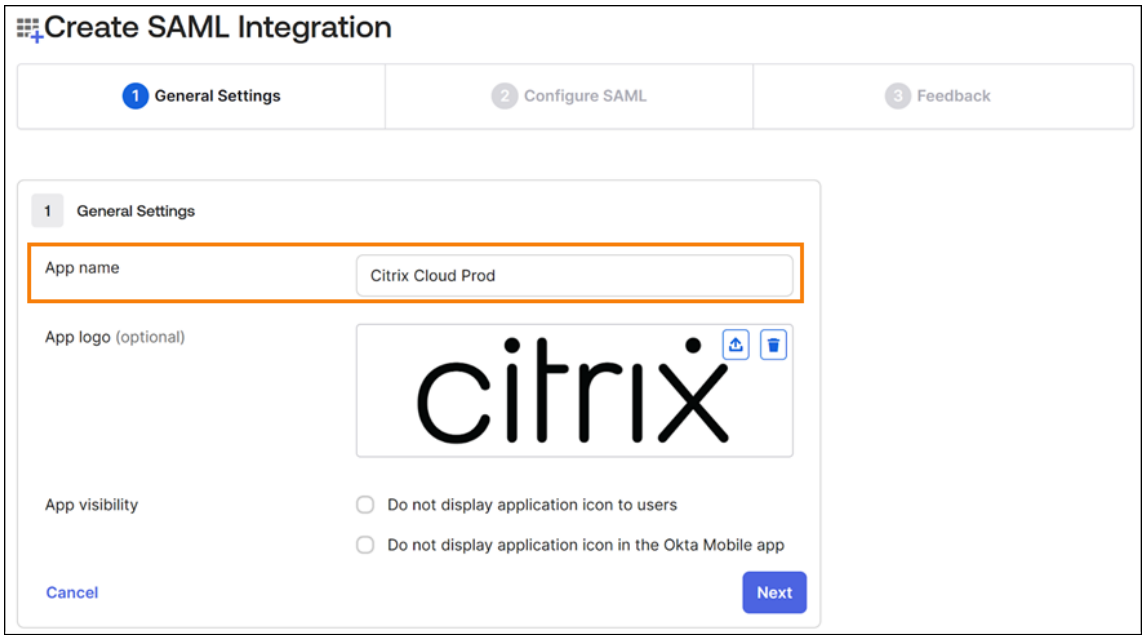
1. Sign in to your Okta organization using an administrator account with permissions to add and configure SAML applications.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. In the Admin console, select **Applications > Applications > Create App Integration** and then select **SAML 2.0**. Select **Next**.



3. In **App Name**, enter a friendly name for the application. Select **Next**.



4. In the **SAML Settings** section, configure the Citrix Cloud Service Provider (SP) connection:

   a) In **Single sign-on URL**, enter the URL that corresponds to the Citrix Cloud region for your Citrix Cloud customer:

   - If your customer ID is in the European Union, United States, or Asia Pacific-South regions, enter `https://saml.cloud.com/saml/acs`.
   - If your customer ID is in the Japan region, enter `https://saml.citrixcloud.jp/saml/acs`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If your customer ID is in the Citrix Cloud Government region, enter `https://saml.cloud.us/saml/acs`.

b) Select **Use this for Recipient and Destination URL**.

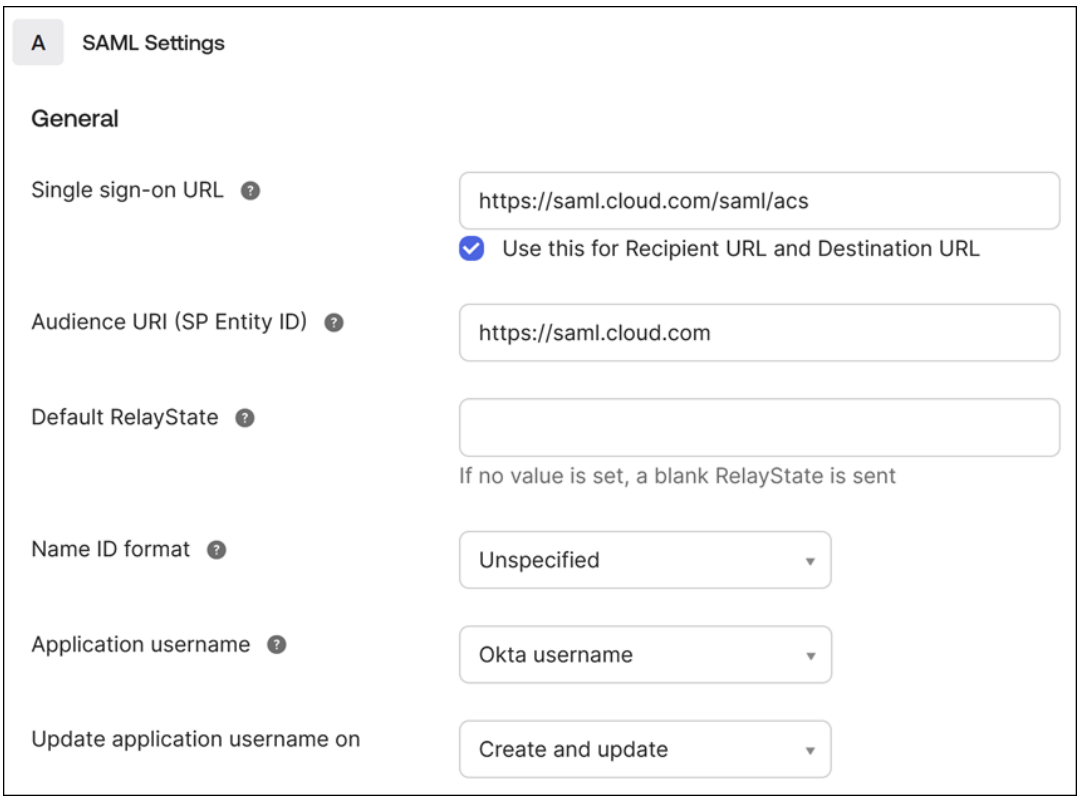
c) In **Audience URI (SP Entity ID)**, enter the URL that corresponds to the Citrix Cloud region for your Citrix Cloud customer:

- If your customer ID is in the European Union, United States, or Asia Pacific-South regions, enter `https://saml.cloud.com`.
- If your customer ID is in the Japan region, enter `https://saml.citrixcloud.jp`.
- If your customer ID is in the Citrix Cloud Government region, enter `https://saml.cloud.us`.

d) In **Name ID Format**, select **Unspecified**. The NameID policy that Citrix Cloud sends within the SAML request must match the NameID format specified within the Okta SAML application. If these items don't match, enabling **Sign Authentication Request** results in an error from Okta.

e) In **Application username**, select **Okta username**.

As an example of this configuration, the following image illustrates the correct configuration for US, EU, and Asia Pacific-South regions:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> The **Name ID** setting must be configured as **Unspecified**. Using a different value for this setting causes the SAML sign-in to fail.

f) Click **Show Advanced Settings** and configure the following settings:

- In **Response**, select **Signed**.
- In **Assertion Signature**, select **Signed**.
- In **Signature Algorithm**, select **RSA-SHA256**.
- In **Assertion Encryption**, select **Unencrypted**.

g) In **Signature Certificate**, upload the SAML signing certificate for your Citrix Cloud region in PEM format. For instructions for acquiring the SAML signing certificate, see Requirements in this article.

h) In **Enable Single Logout**, select **Allow application to initiate Single Logout**.

i) In **Single Logout URL**, enter the URL that corresponds to your Citrix Cloud region:

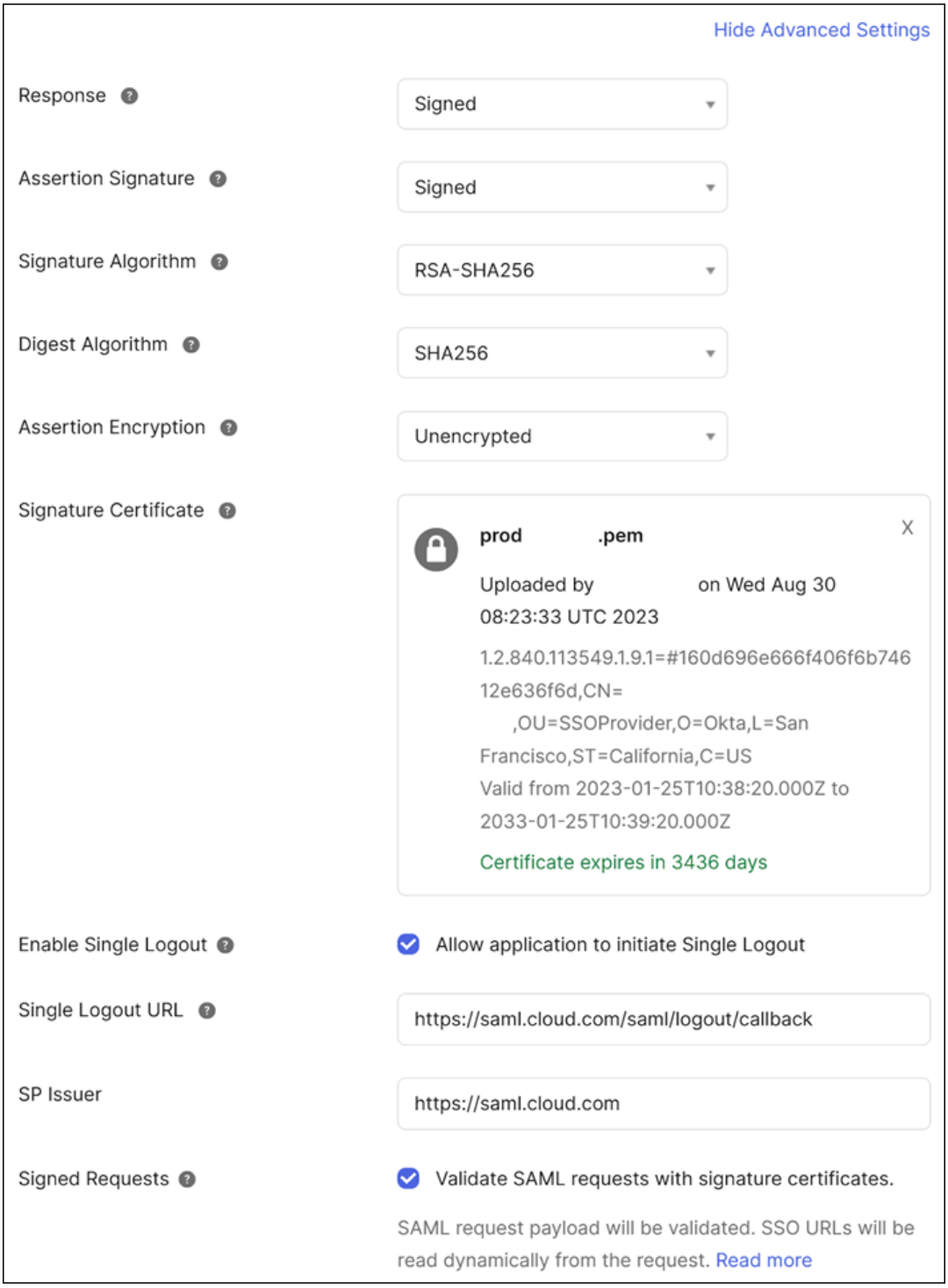
- For European Union, United States, and Asia Pacific-South regions, enter `https://saml.cloud.com/saml/logout/callback`.
- For the Japan region, enter `https://saml.citrixcloud.jp/saml/saml/logout/callback`.
- For Citrix Cloud Government, enter `https://saml.cloud.us/saml/logout/callback`.

j) In **SP Issuer**, enter the value that you entered earlier in **Audience URI (SP Entity ID)** (Step 4c of this task).

k) In **Signed Requests**, select **Validate SAML requests with signature certificates**.

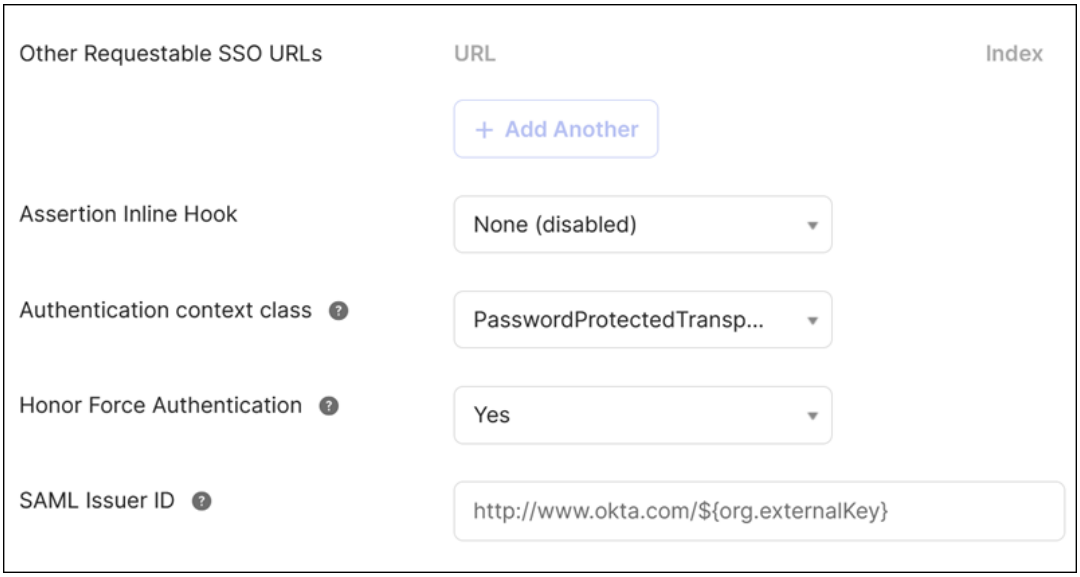
The following image illustrates the correct configuration for US, EU, and Asia Pacific-South regions:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



l) For all remaining advanced settings, accept the default values.

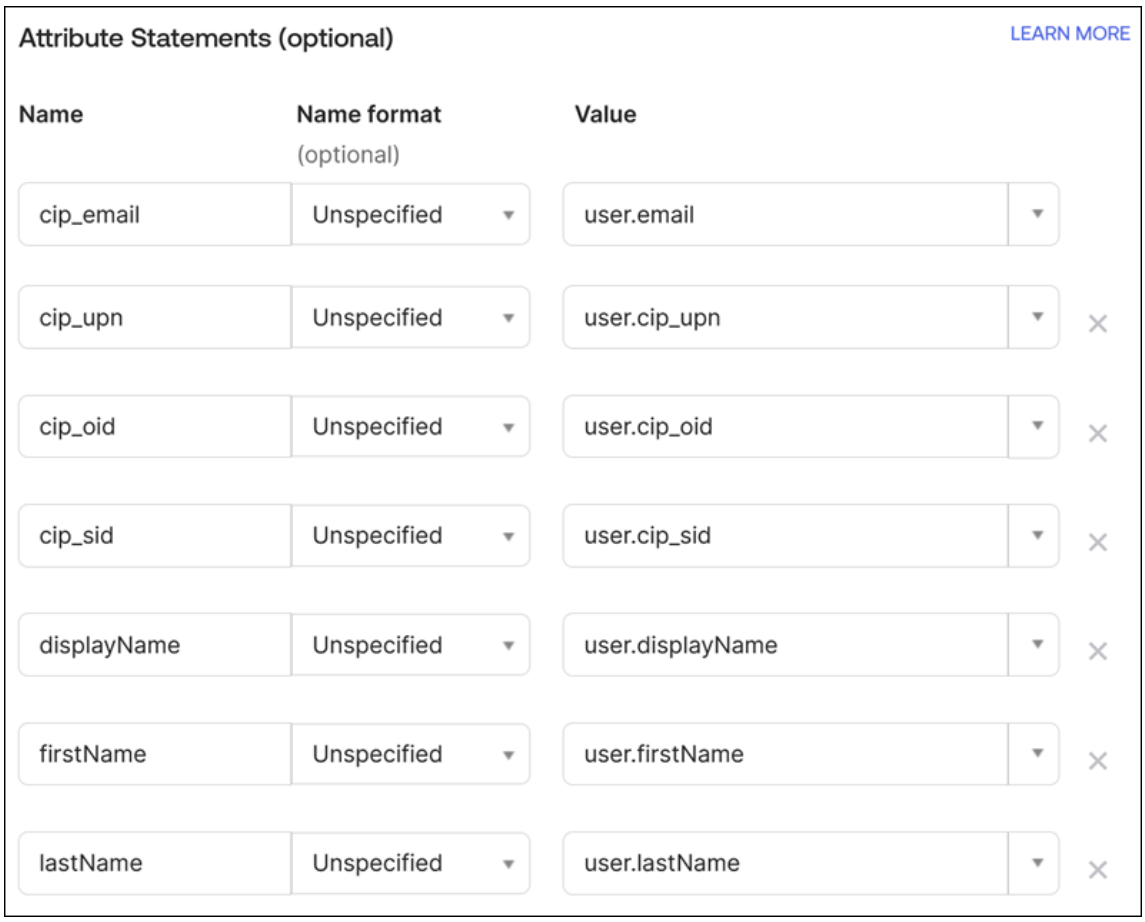
© 1997–2026 Citrix Systems, Inc. All rights reserved.



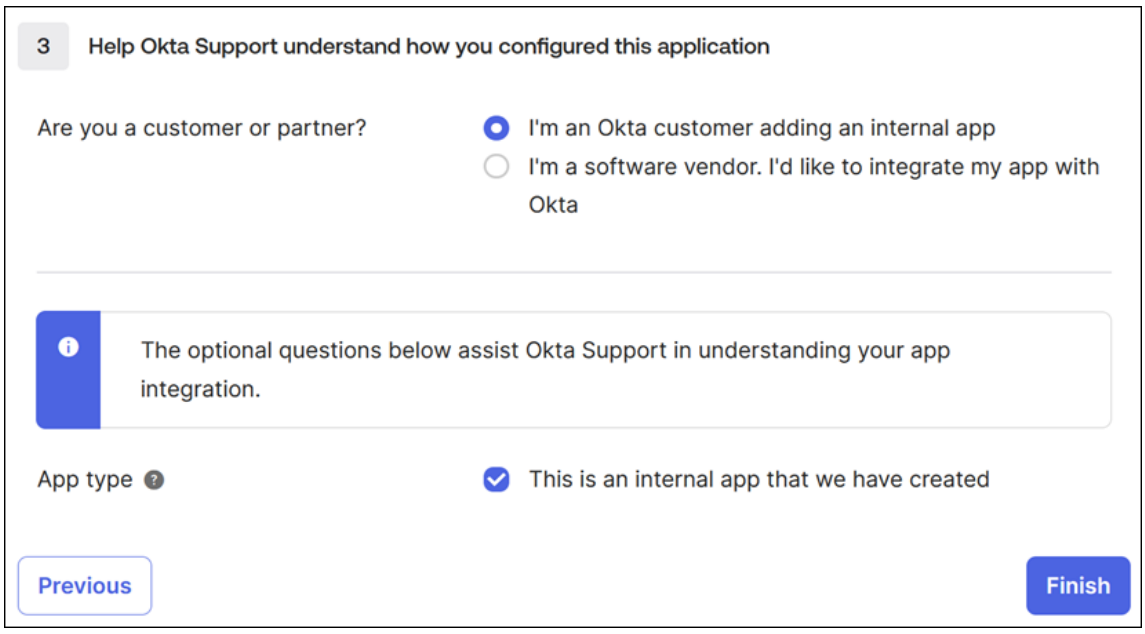
5. Under **Attribute Statements (optional)**, enter the values for **Name**, **Name format**, and **Value** as shown in the following table:

Name	Name format	Value
cip_upn	Unspecified	user.cip_upn
displayName	Unspecified	user.displayName
firstName	Unspecified	user.givenName
lastName	Unspecified	user.familyName

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. Select **Next**. The Okta configuration statement appears.



7. In **Are you a customer or partner?**, select **I'm an Okta customer adding an internal app**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

8. In **App type**, select **This is an internal app that we have created**.
9. Select **Finish** to save your configuration. The profile page for your SAML application appears and displays the contents of the **Sign On** tab.

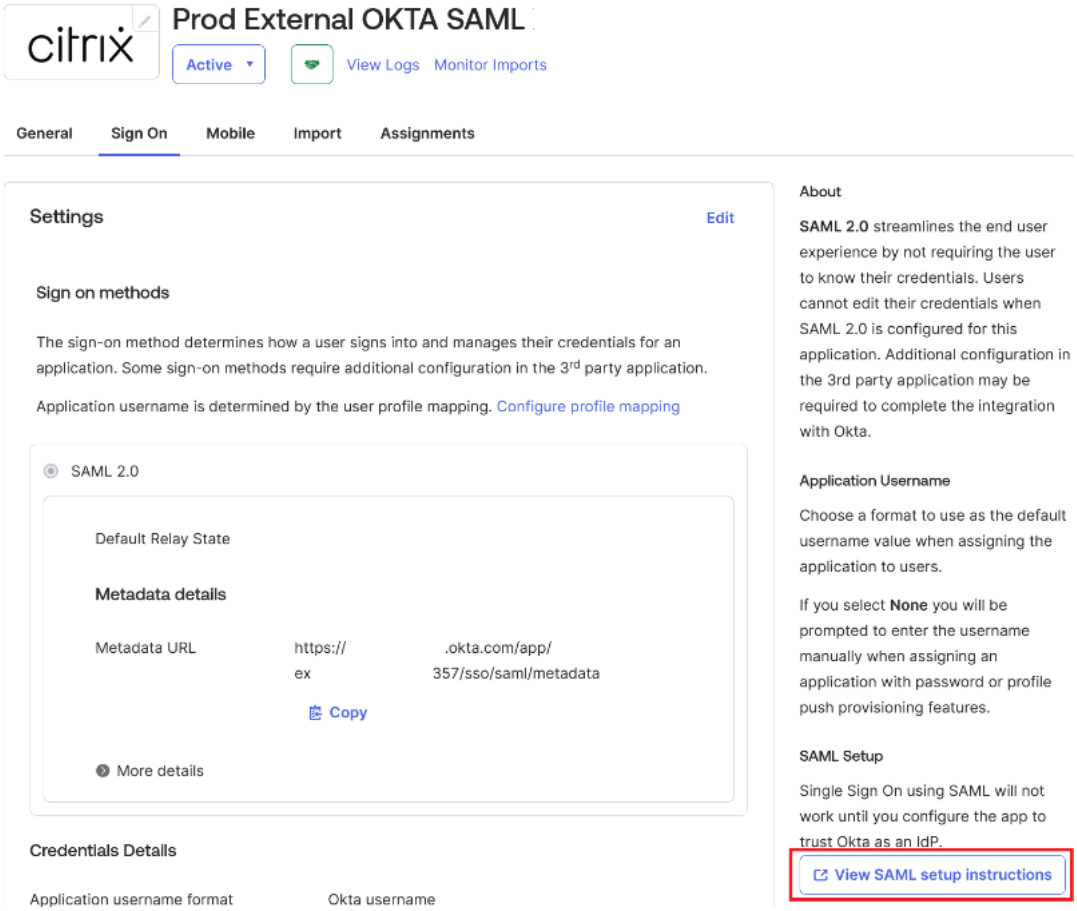
After configuration, select the **Assignments** tab and assign users and groups to the SAML application.

Configure the Citrix Cloud SAML connection

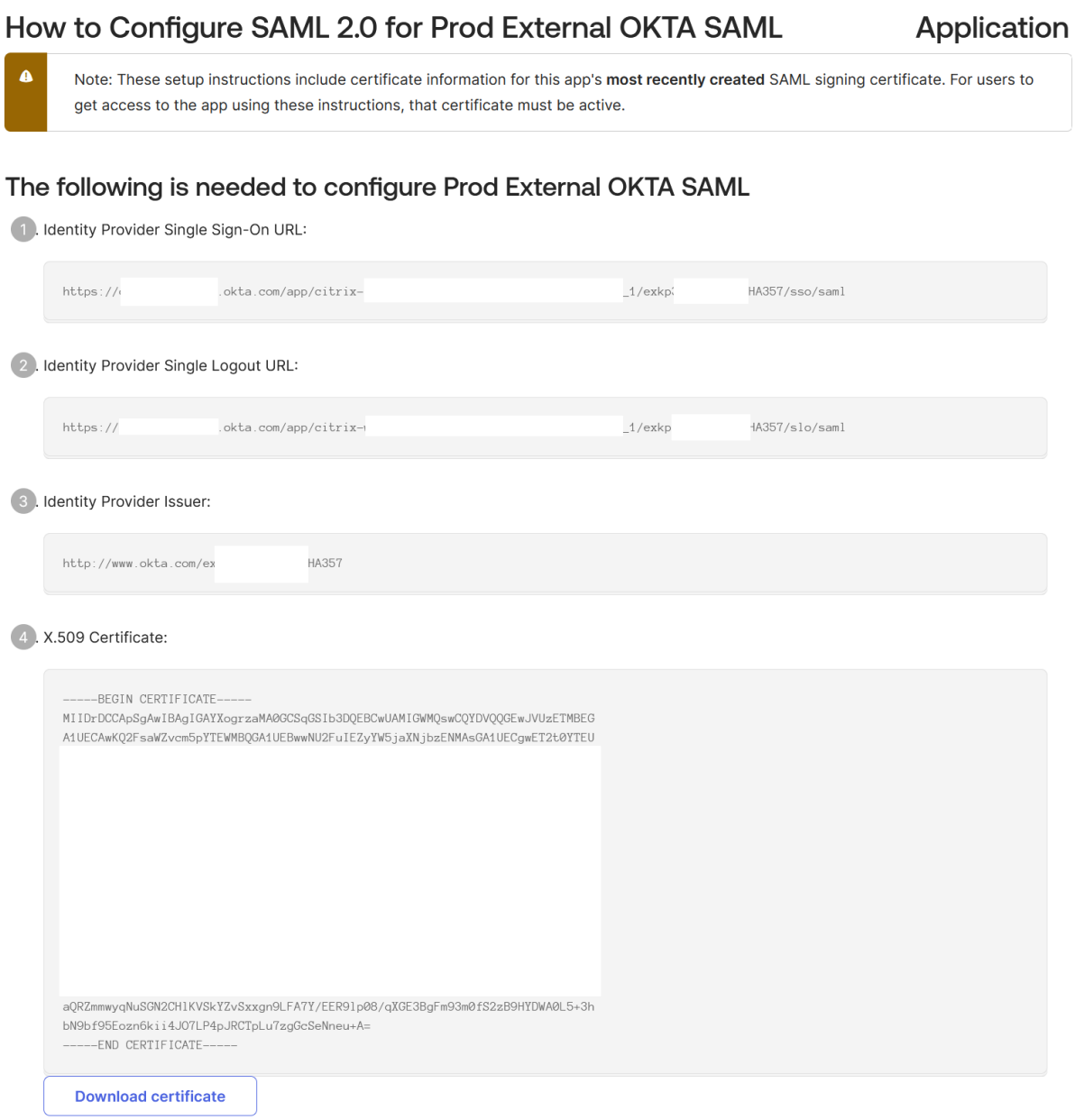
All Citrix logon flows need to be Service Provider initiated using either a store URL or a Citrix Cloud GO URL.

Use the default recommended values for the SAML connection within **Identity and Access Management → Authentication →Add an identity provider → SAML**.

Obtain the Okta SAML application SAML endpoints to enter into Citrix Cloud from your Okta portal.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



How to Configure SAML 2.0 for Prod External OKTA SAML Application

Note: These setup instructions include certificate information for this app's **most recently created** SAML signing certificate. For users to get access to the app using these instructions, that certificate must be active.

The following is needed to configure Prod External OKTA SAML

1. Identity Provider Single Sign-On URL:

https://[redacted].okta.com/app/citrix-[redacted]_1/exkp[redacted]HA357/sso/saml

2. Identity Provider Single Logout URL:

https://[redacted].okta.com/app/citrix-[redacted]_1/exkp[redacted]HA357/slo/saml

3. Identity Provider Issuer:

http://www.okta.com/ex[redacted]HA357

4. X.509 Certificate:

-----BEGIN CERTIFICATE-----
MIIDrDCCApSgAwIBAgIGAYXogrzaMA0GCSqGSIb3DQEBCwUAMIGWMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
[redacted]
aQRZmmwyqNuSGN2CHlKVSkYZvSxxgn9LFA7Y/EER9lp08/qXGE3BgFm93m0fS2zB9HYDWA0L5+3h
bN9bf95Eozn6kii4JO7LP4pJRCTpLu7zgGcSeNneu+A=
-----END CERTIFICATE-----

Download certificate

> **Important:**
>
> Okta does not require a scoped entity ID. This document assumes Scoped Entity ID is disabled. See Citrix documentation on scoped entity ID for an explanation as to what a scoped entity ID is and when it is required. Use the default Citrix Cloud SAML connection settings and leave **Scoped Entity ID** disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SAML Identity Provider Configuration

SAML Application Scoped Entity ID



In this field in Citrix Cloud	Enter this value
Entity ID	`http://www.okta.com/<oktaSAMLappID>`
Sign Authentication Request	Yes
SSO Service URL	`https://<youroktatenant>.okta.com/app/<oktatenantname>_<samlappname>/<samlappID>/sso/saml`
SSO Binding Mechanism	HTTP Post
SAML Response	Sign Either Response Or Assertion
Authentication Context	Unspecified, Exact
Logout URL	`https://<youroktatenant>.okta.com/app/<oktatenantname>_<samlappname>/<samlappID>/slo/saml`
Sign Logout Request	Yes
SLO Binding Mechanism	HTTP Post

Configure an On-Premise PingFederate Server as the SAML Provider for stores and Citrix Cloud™

August 11, 2026

Author:
Mark Dear

This article was written by collaboration between both Citrix® and Ping engineers and has been reviewed by both parties to ensure technical accuracy at the time of writing. Refer to Ping documentation for instructions on how to provision, configure and licence an on premise PingFederate server for use as a SAML provider as this is beyond the scope of this article.

This document was written using PingFederate versions 11.3 and 12.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites

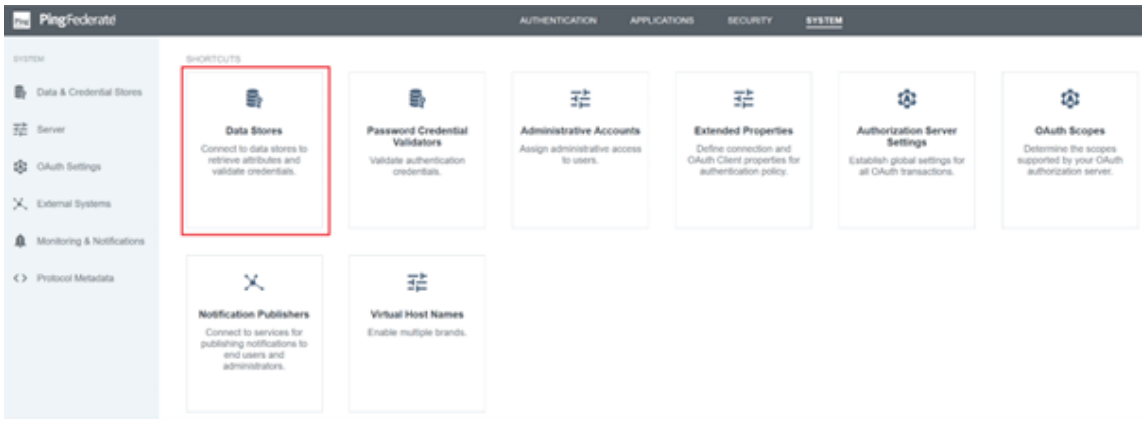
This article specifically addresses SAML configuration and ensure that the following conditions are fulfilled.

- You have already provisioned an on-premise PingFederate server within your organization and obtained the necessary license. For more information, see PingFederate Installation.
- You need to have installed a supported version of Java on to the PingFederate server. Refer to Ping Identity documentation for the supported Java versions. For more information, see Java PingFederate Requirement.
- You have configured the required networking and firewall rules to allow Citrix Cloud to redirect to the on premise PingFederate server during the store/Citrix Cloud admin console SAML logon process. For more information, see PingFederate Network Requirements.
- You have imported a publicly signed x509 certificate onto your PingFederate server that can act as server certificate for the PingFederate server.
- You have imported a publicly signed x509 certificate onto your PingFederate server that can act as a SAML signing certificate for the IdP. This certificate must be uploaded to Citrix Cloud during the SAML connection process.
- You have connected your on-premise Active Directory to PingFederate. For more information, see PingFederate LDAP Datastore

> **Note:**
>
> While configuring PingFederate for use with Citrix Cloud and store, refer to PingFederate documentation to understand what individual SAML settings do and to help supplement the instructions provided here.

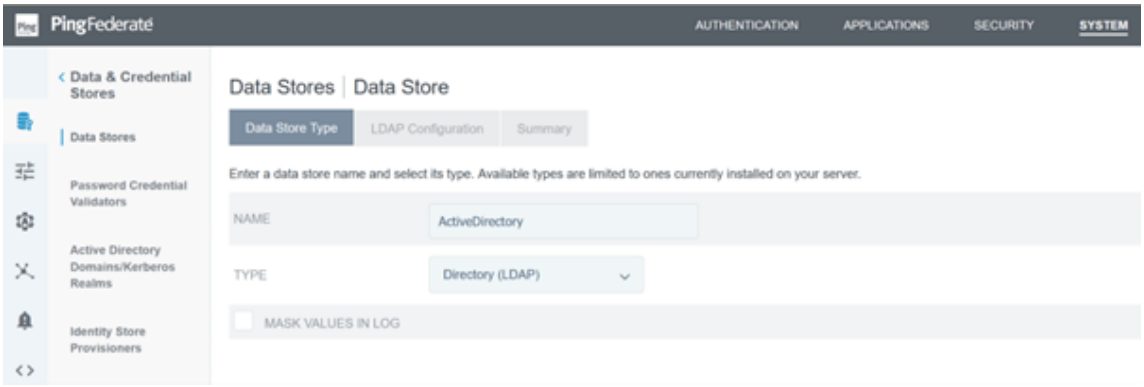
Configure an Active Directory Connection to your AD domain using a DataStore within PingFederate

1. Configure an Active Directory connection within Data Stores.

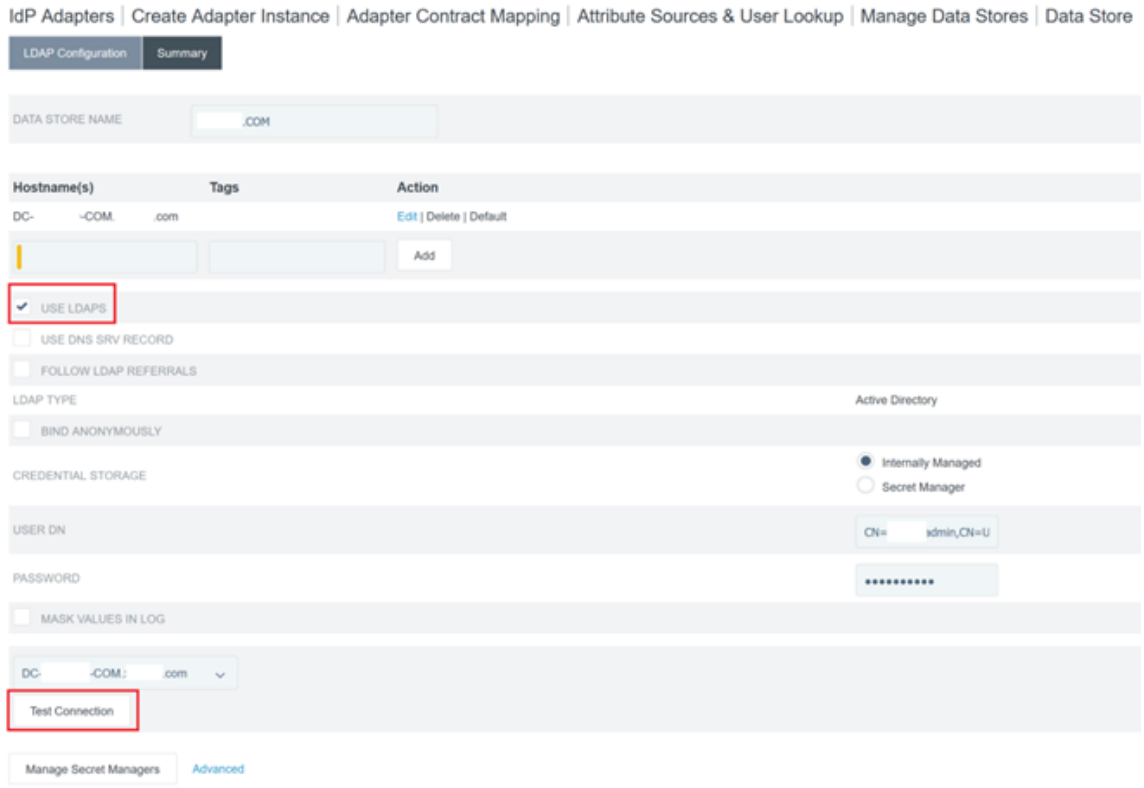


© 1997–2026 Citrix Systems, Inc. All rights reserved.

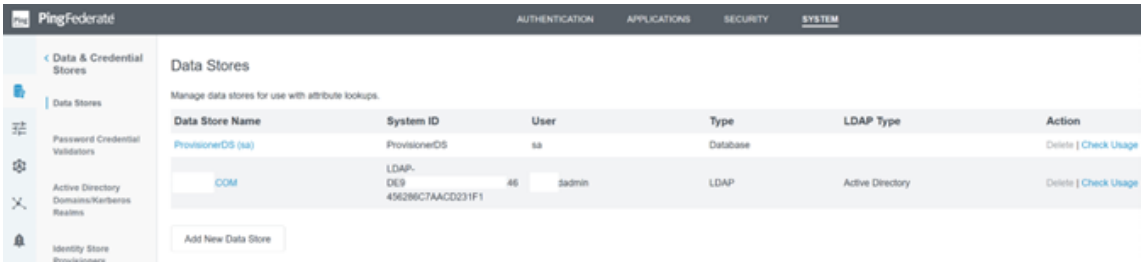
2. Select Type as **Directory (LDAP)**.



3. Configure your domain controllers for LDAPS connections and add your list of domain controller FQDNs within the hostnames field. Then click **Test Connection**.



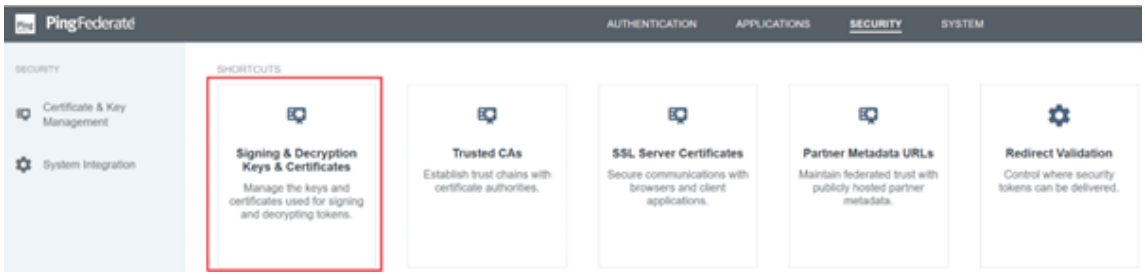
4. Once configured, the Active Directory Connection should resemble the following example:



© 1997–2026 Citrix Systems, Inc. All rights reserved.

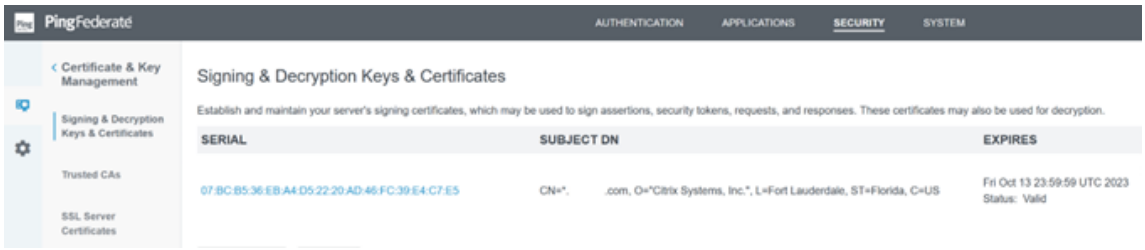
Upload the Citrix Cloud SAML Signing Certificate

1. Click the **Security** tab
2. Upload the SAML signing certificate you wish PingFederate to use within **Signing & Decryption Keys and Certificates**.

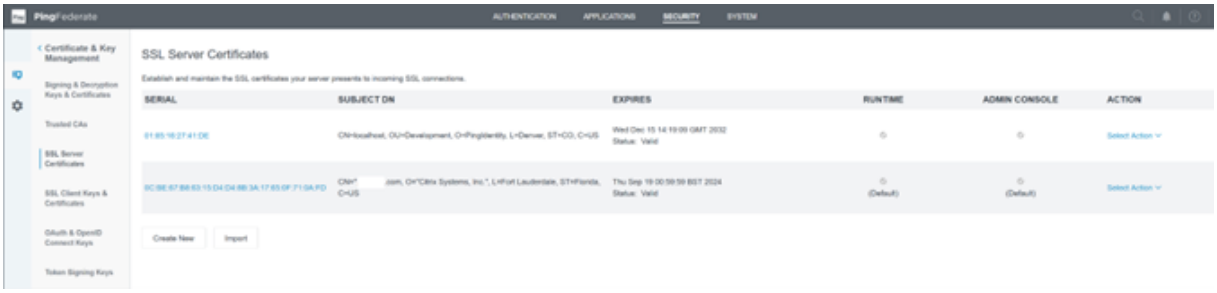


> **Note:**
>
> The certificate used is a publicly signed Digicert `pingfederateserver.domain.com` certificate in this example.

3. Upload any CA certificates used to sign your PingFederate server SAML signing certificate.



> **Note:**
>
> The PingFederate server certificate and SAML signing certificate can be the same SSL cert or you can use different SSL certs. You need to provide a copy of the SAML signing certificate to Citrix Cloud when you configure the SAML connection.

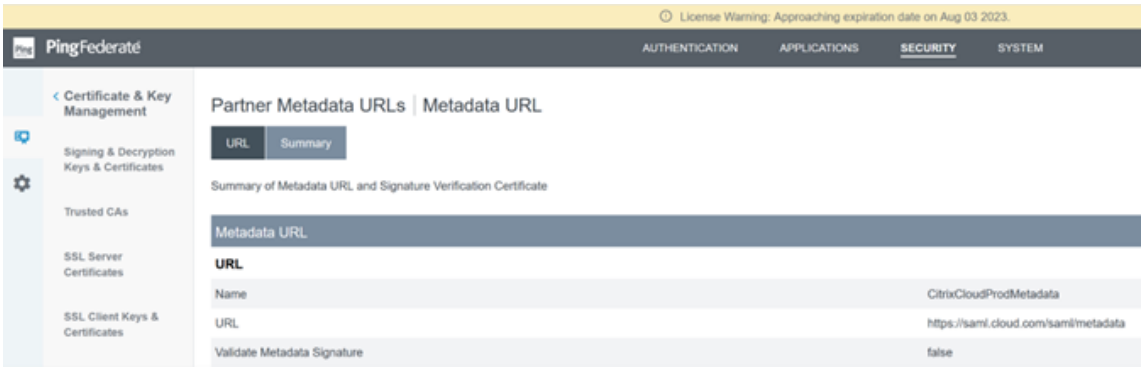


© 1997–2026 Citrix Systems, Inc. All rights reserved.

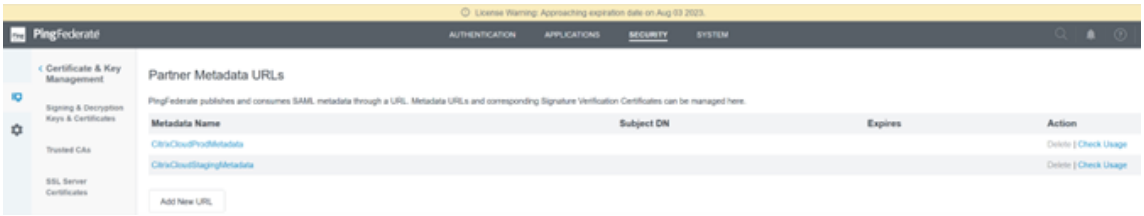
Upload the Citrix Cloud Metadata

1. Provide a name for the Citrix Cloud metadata and enter the metadata URL corresponding to the Citrix Cloud region where your Citrix Cloud tenant is located.

   - https://saml.cloud.com/saml/metadata - Commercial EU, US and APS
   - https://saml.citrixcloud.jp/saml/metadata - Japan
   - https://saml.cloud.us/saml/metadata - Governement



2. Once configured, the Citrix Cloud metadata configuration should resemble the following example.

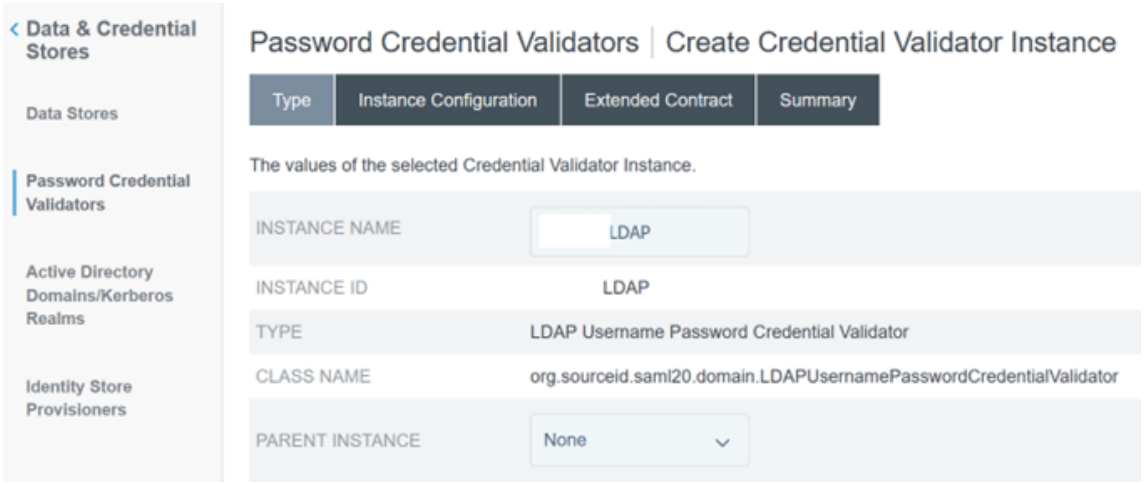


Configure a password credential validator within PingFederate

For more information, see PingFederate Password Credential validator

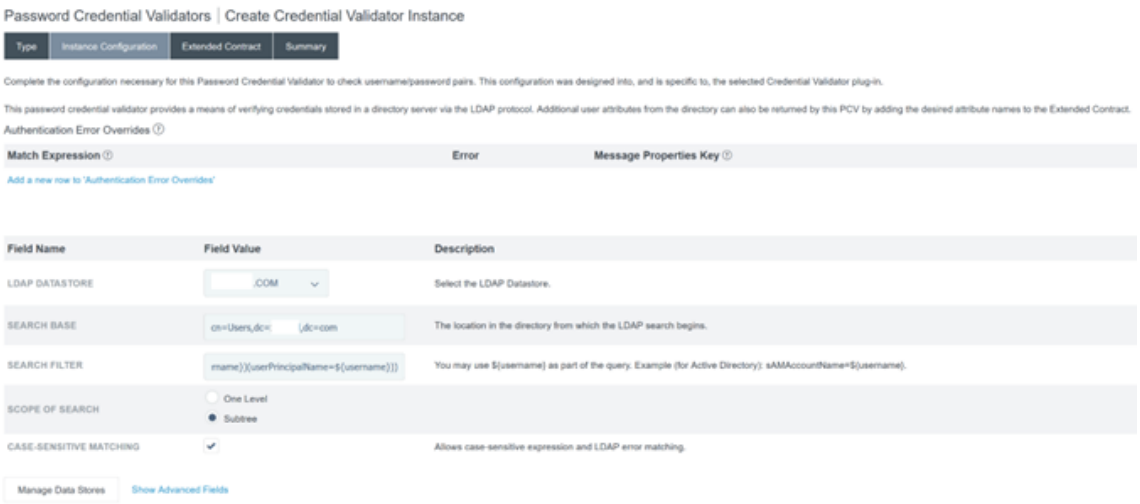
1. Configure the password credential validator type as LDAP username and password.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Configure the **Instance Configuration**. Select the AD domain connection and data store that you configured earlier Configure an Active Directory Connection to your AD domain using a DataStore within PingFederate. Enter a suitable LDAP filter as shown in the example.

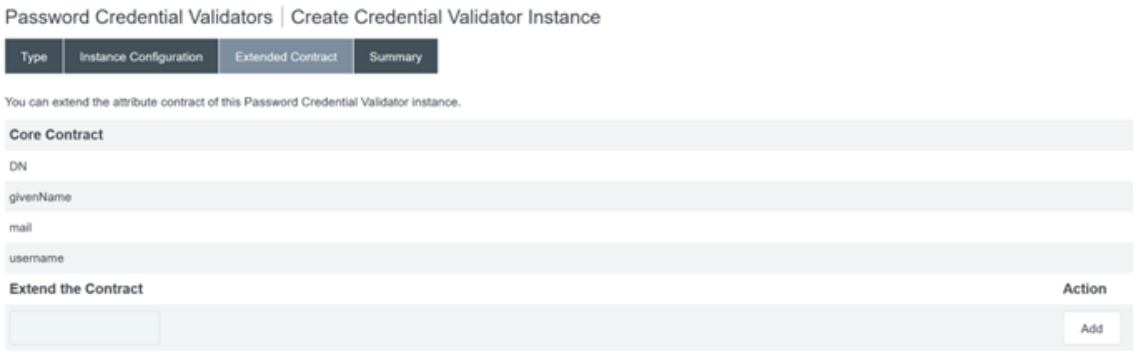
```
(((sAMAccountName=${ username } )(userPrincipalName=${ username } ))
```



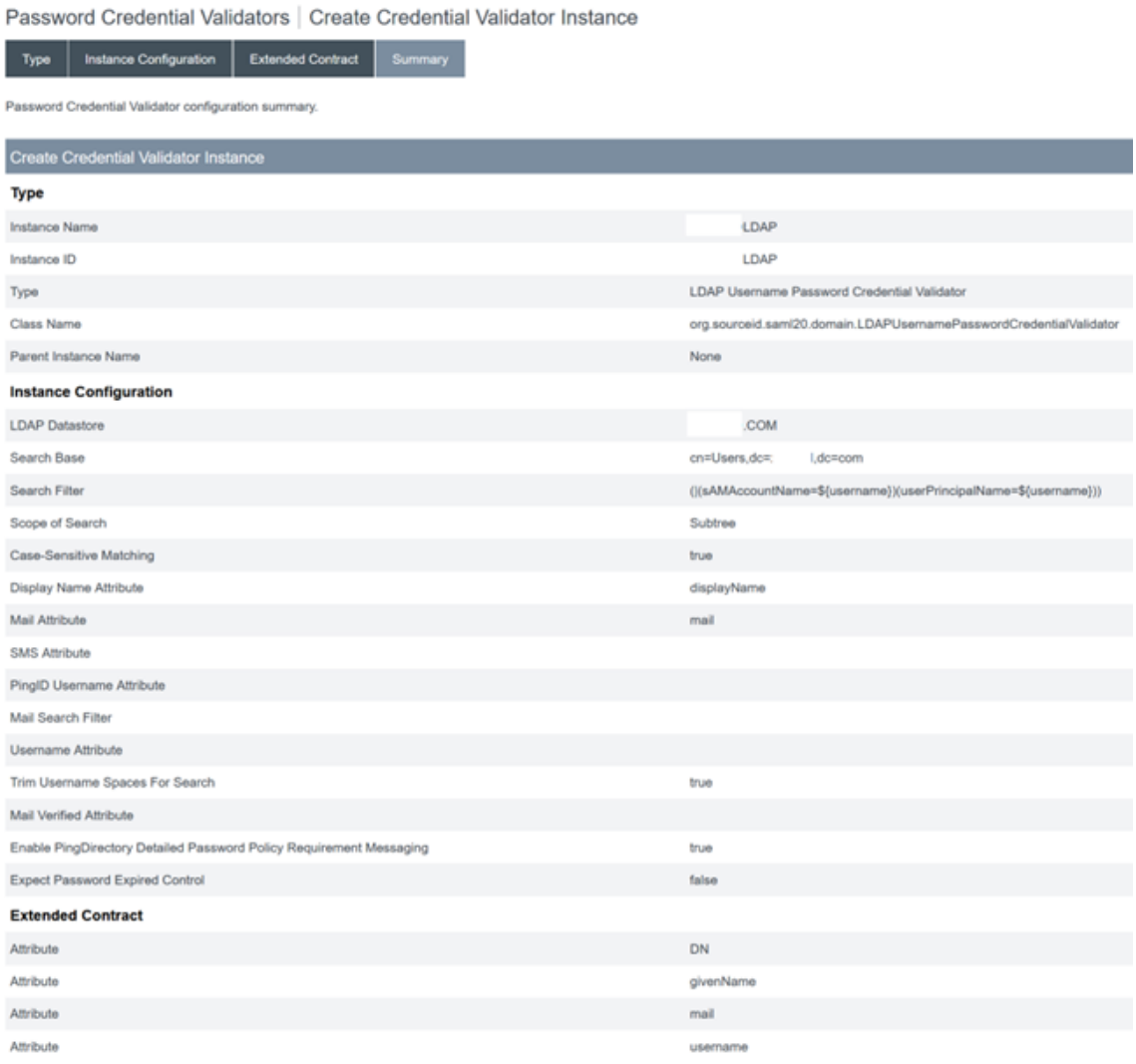
> **Note:**
>
> The example filter accommodates both sAMAccountName and userPrincipalName AD username formats, enabling end users to sign in to store or Citrix Cloud using either of these formats.

3. Configure the **Extended Contract**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. The **Password Credential Validator** summary should resemble this example.

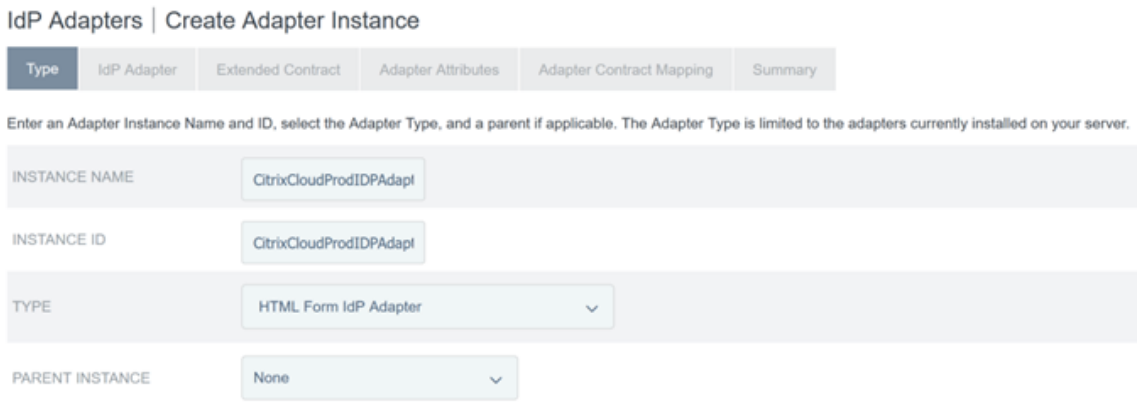


Configure the IDP Adapter within PingFederate

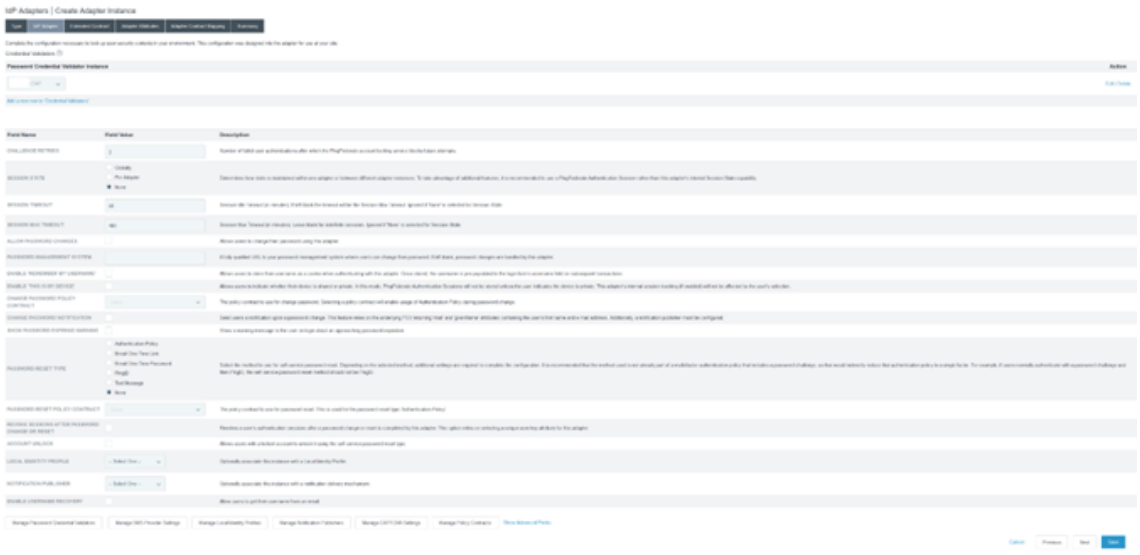
For more information, see PingFederate HTML form adapter

© 1997–2026 Citrix Systems, Inc. All rights reserved.

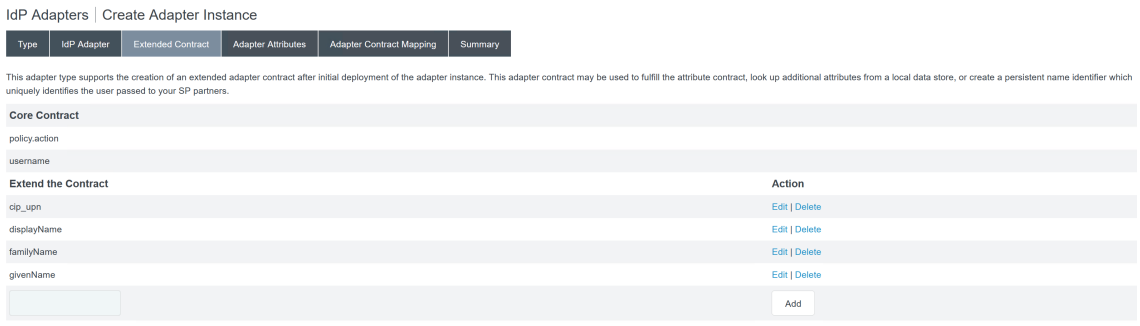
1. Create a new IDP adapter of type HTML Form IdP Adapter.



2. Select the existing **Password Credential Validator** you configured earlier and configure the IDP Adapter. For more information, see Configure a password credential validator within PingFederate.

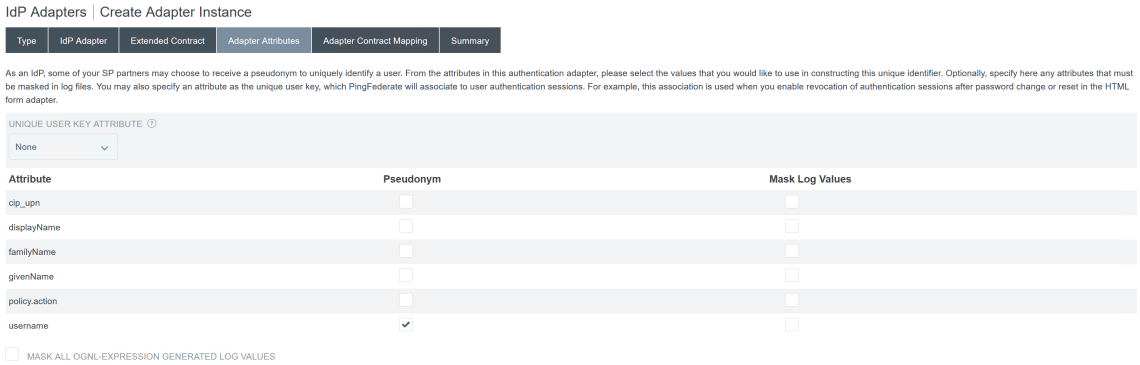


3. Configure the **Extended Contract** with SAML attributes that are passed to Citrix Cloud or stores during SAML logon.



4. Configure the **Adapter Attributes**.

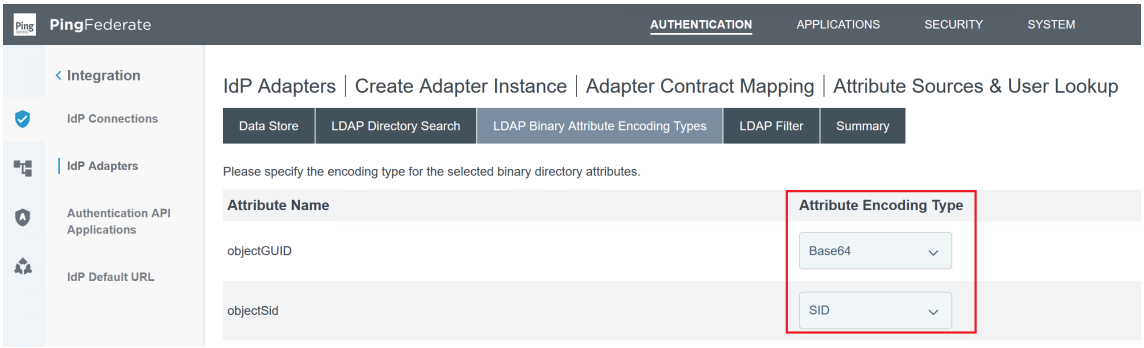
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Configure the **Adapter Contract Mapping** where SAML attributes are mapped to LDAP user attributes from AD identities. Click **Configure the adapter contract**.

   Set the encoding of the 2 binary attributes.

   - objectGUID = base64 (encoded)
   - objectSid = SID (unencoded)

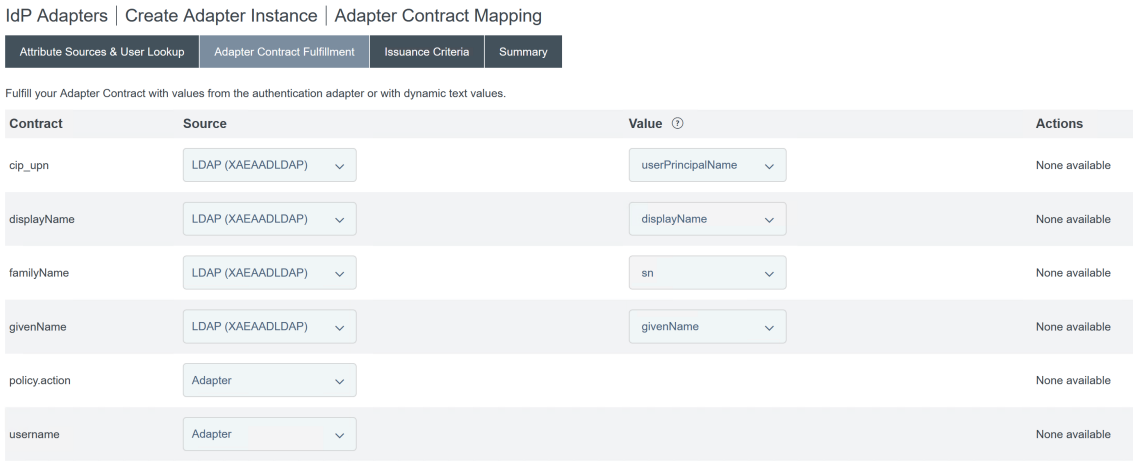


6. Configure **Attribute Sources & User Lookup**.

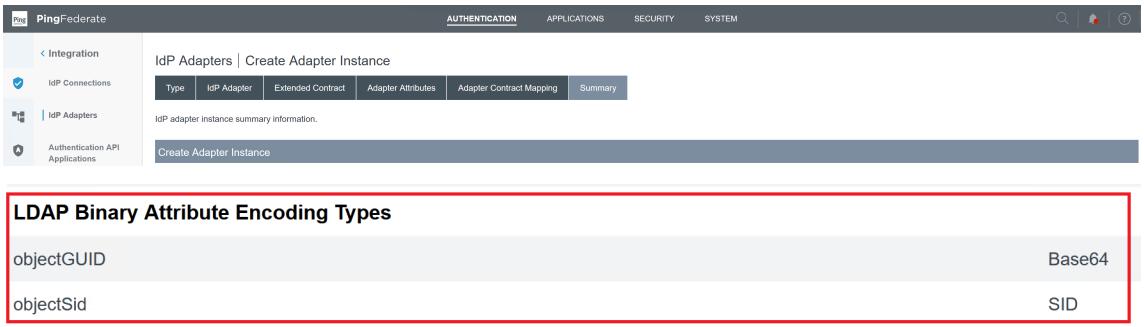


7. Configure **Adapter Contract Fulfilment**. Select **LDAP** and the name of your active directory data store as the source of the user attribute data. Value is the active directory attribute for the user such as `objectGUID` or `objectSid`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. The binary attribute encoding should appear as shown in the below screenshots in the **HTML form adapter** summary.

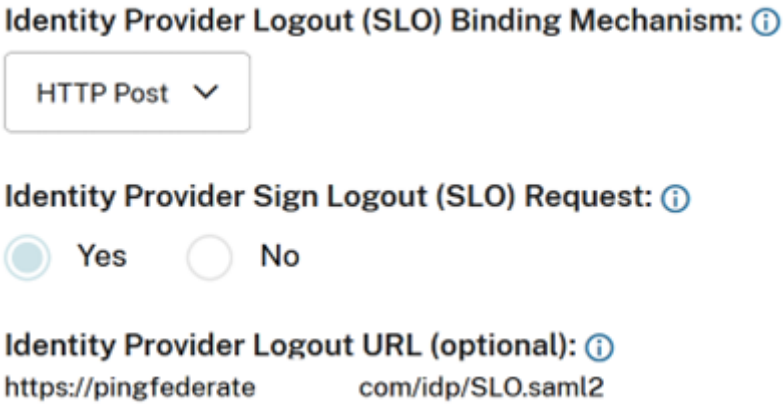


Configuring the Service Provider Connection (SAML application) for Citrix Cloud or Workspaces

The sample PingFederate configuration provided below assumes the following SAML authentication requirements within your organisation.

- SAML authentication requests sent from store/Citrix Cloud admin console MUST be signed.
- SAML HTTP POST bindings will be used for both SSO and SLO requests.
- Single Logout (SLO) is a requirement within your organisation. When an end user signs out of store or the Citrix Cloud admin console, a SAML SLO request is sent from Citrix Cloud to the SAML provider (IdP) to sign out the user.
- PingFederate requires signed HTTP POST requests to initiate sign out. SAML provider requires Signed SLO requests.

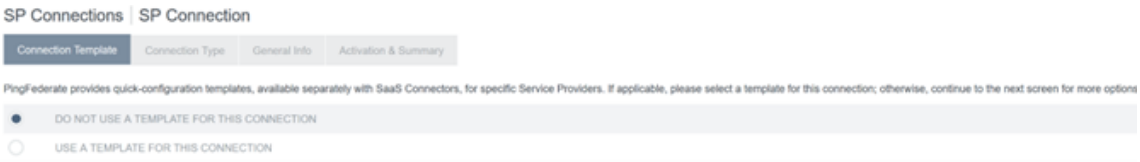
© 1997–2026 Citrix Systems, Inc. All rights reserved.



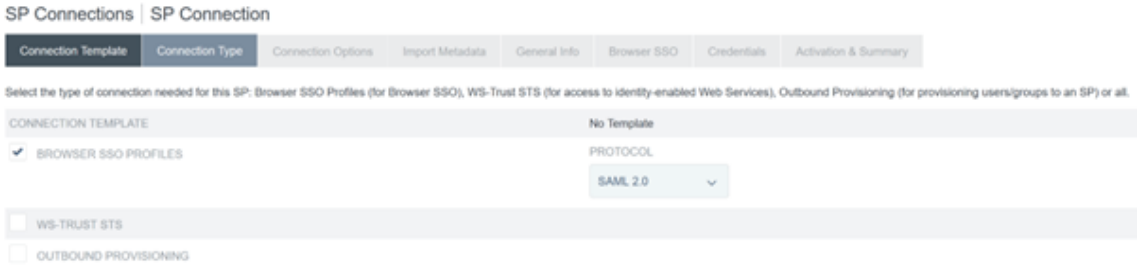
For more information, see PingFederate SP Management

Procedure

1. Configure the **Connection Template**.



2. Configure the **Connection Type** and select **Browser SSO profiles and SAML 2.0**.

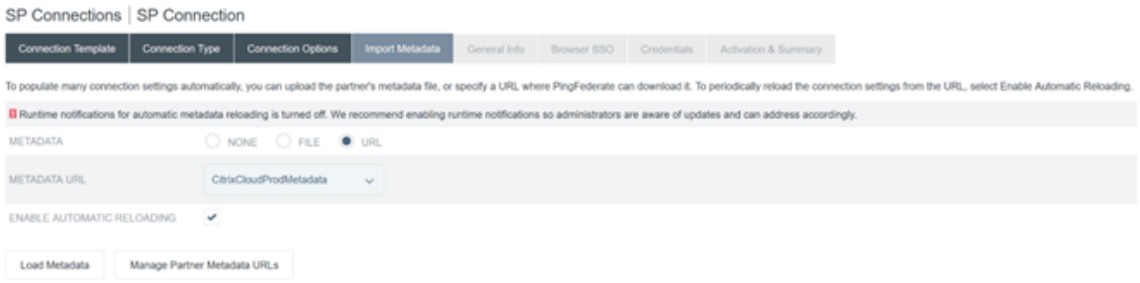


3. Configure the **Connection Options**.



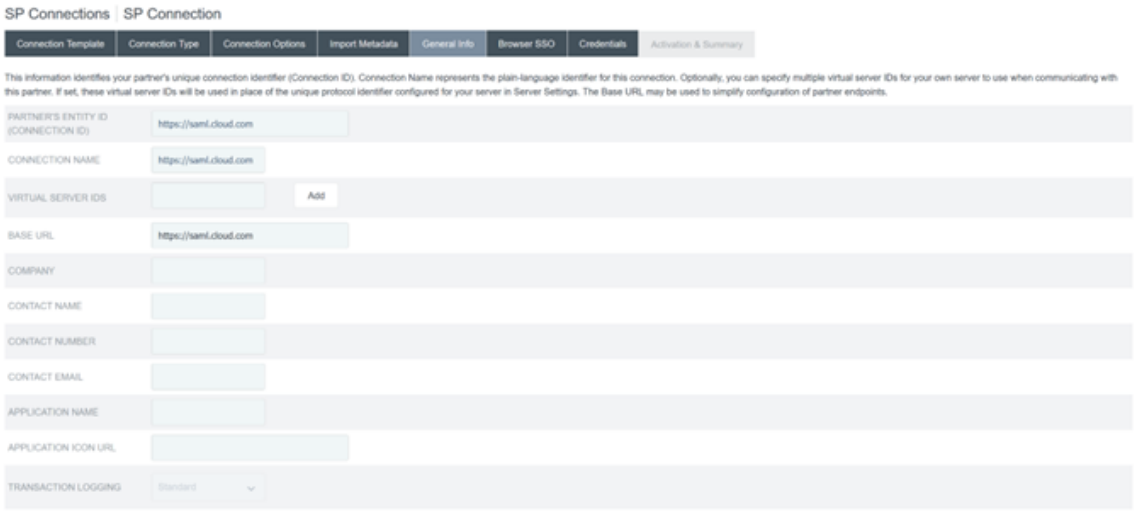
4. Import the Citrix Cloud Metadata. Select URL and the `CitrixCloudProdMetadata` URL you created earlier and click **Load Metadata**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

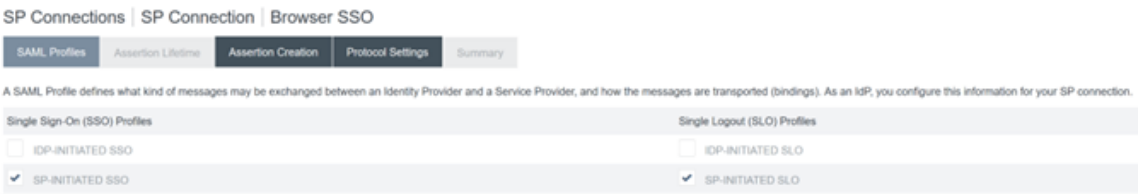


5. Configure **General Info**. Set the Service Provider Connection Entity ID, Base URL and Connection Name to the Citrix Cloud SAML endpoint for your Citrix Cloud customer region.

    - https://saml.cloud.com - Commercial EU, US and APS
    - https://saml.citrixcloud.jp - Japan
    - https://saml.cloud.us - Gov



6. Configure **Protocol Settings**.



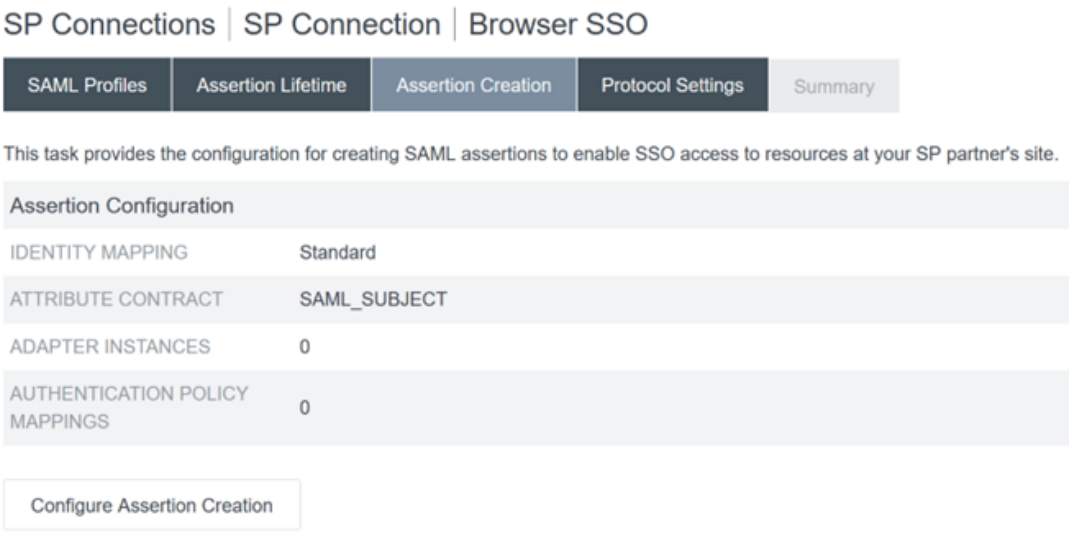
7. Use the default **Assertion Lifetime** settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

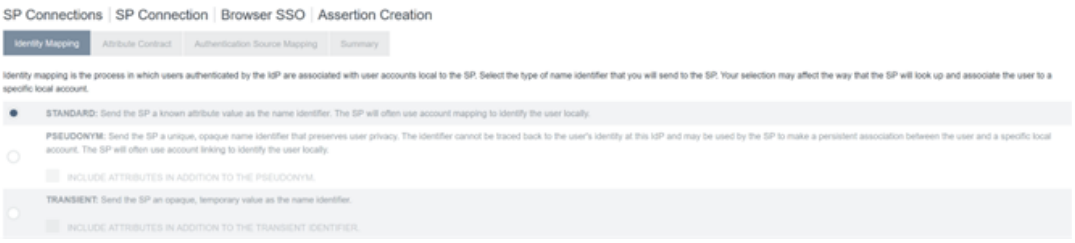


8. Configure SAML Assertion Creation.

   a) Click **Configure Assertion Creation**

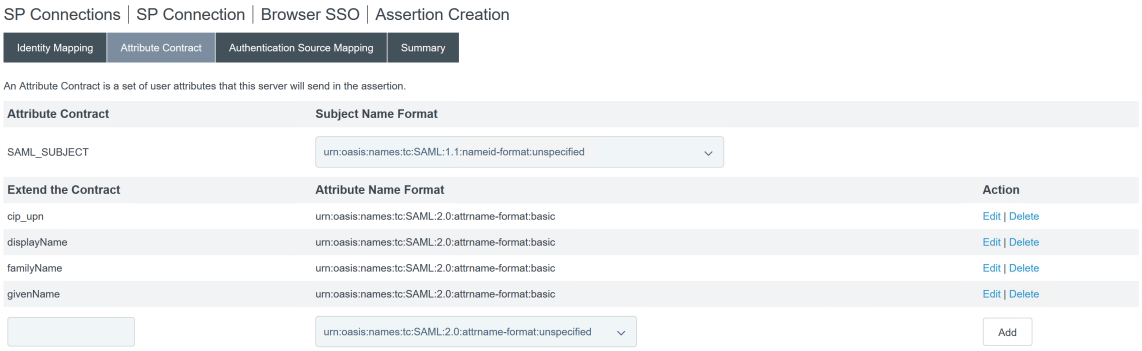


   b) Select **Standard**.



9. Configure **Attribute Contract**.

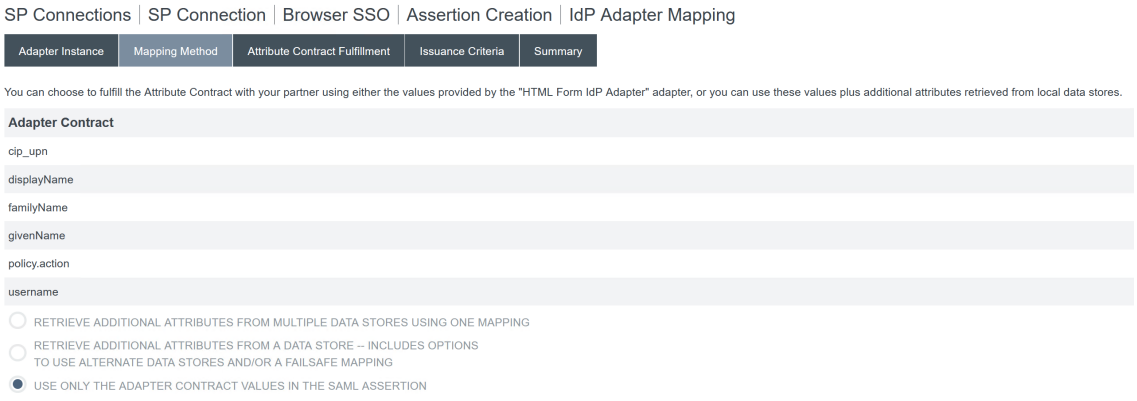
© 1997–2026 Citrix Systems, Inc. All rights reserved.



10. Configure **Adapter Instance**.

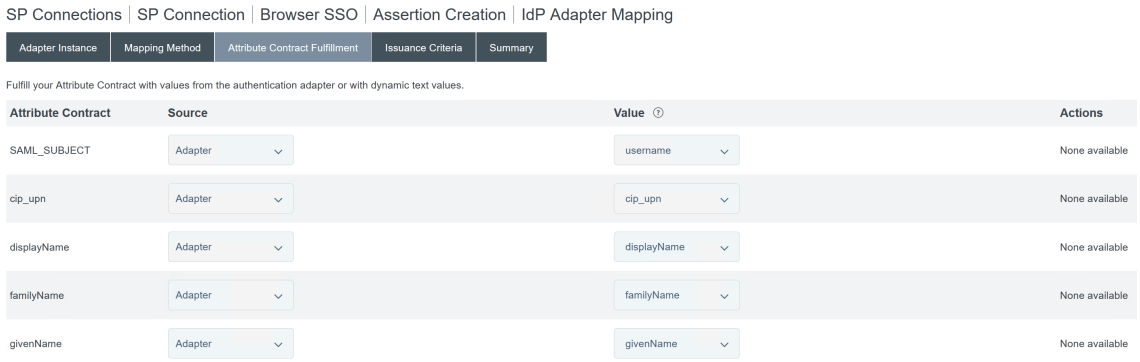


11. Configure **Mapping Method**.



12. Configure **Attribute Contract Fulfilment**.

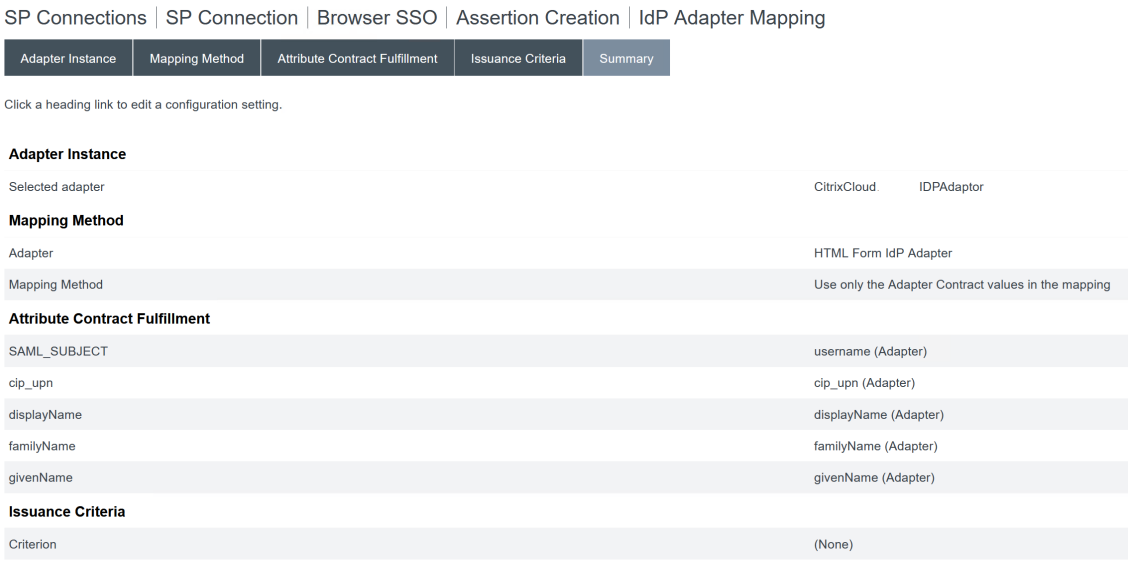
© 1997–2026 Citrix Systems, Inc. All rights reserved.



13. Configure **Issuance Criteria** as the defaults with no conditions.



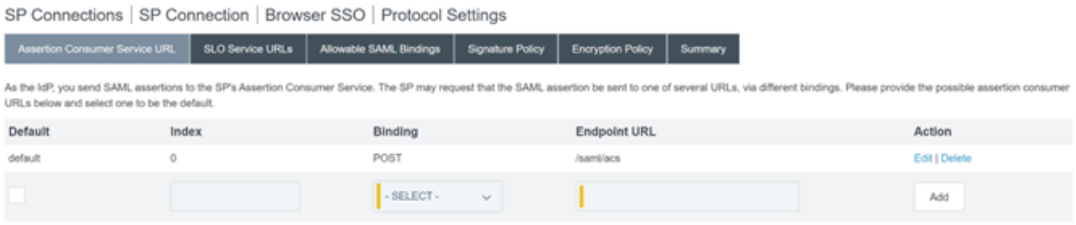
14. The completed **IDP Adapter Mapping** appears as follows:



15. Configure **Protocol Settings**. SAML paths required by Citrix Cloud will be appended to your PingFederate server base URL. It is possible to override the base URL by entering a full path within the endpoint URL field but this is usually unnecessary and undesirable.
    Base URL - https://youpingfederateserver.domain.com

    a) Configure the Assertion Consumer Service URL which appends the SAML path to the PingFederate server base URL. EndpointURL - `/saml/acs`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

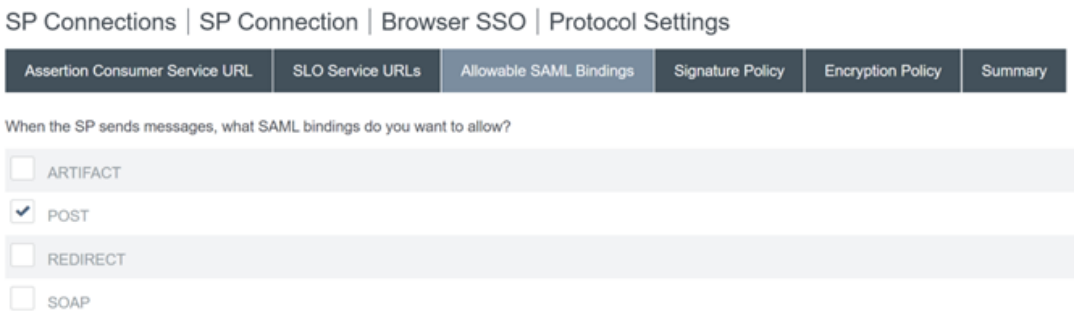


b) Configure **SLO Service URL**. EndpointURL - `/saml/logout/callback`



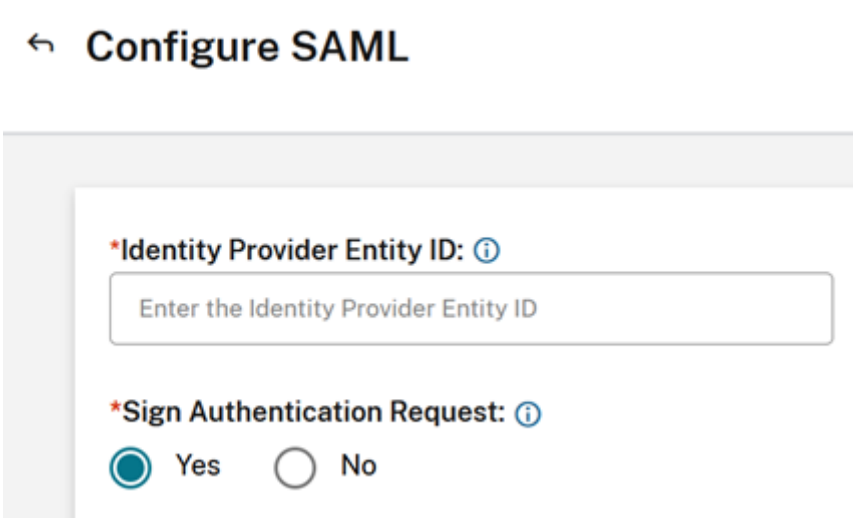
> **Important:**
>
> The Citrix Cloud SAML connection requires a PingFederate Logout URL to be configured to match this if you wish to perform SLO when signing out of store or Citrix Cloud. Failing to configure the Logout URL within your SAML connection will cause end users to just sign out of store but not PingFederate.

a) Configure **Allowable SAML Bindings**.



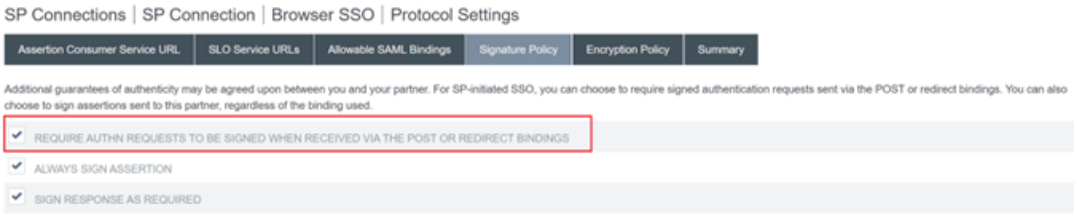
b) Configure **Signature Policy**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

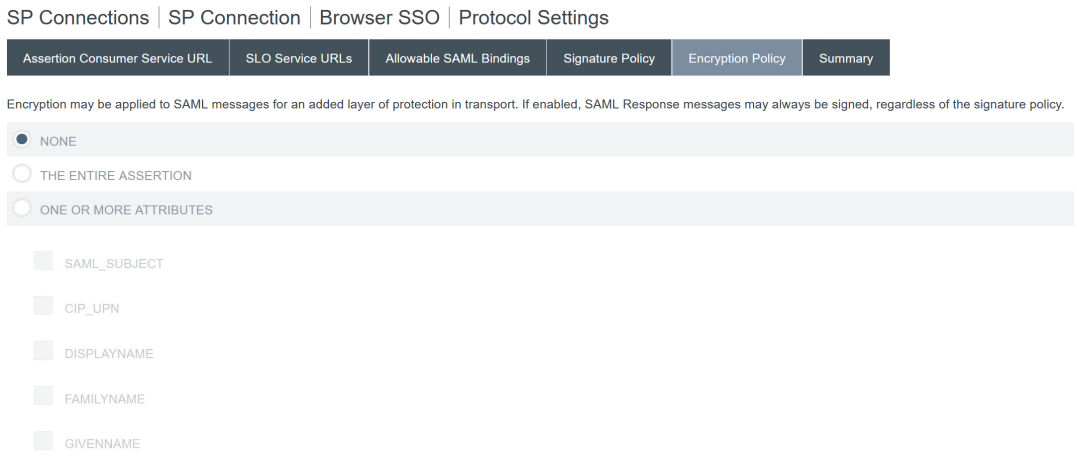


> **Important:**
>
> SAML signing settings must be configured consistently on both sides of the SAML connection. store or Citrix Cloud (SP) must be configured to send signed SSO and SLO requests.

a) PingFederate (IDP) must be configured to perform enforcement of signed requests using the Citrix Cloud SAML signing verification certificate.



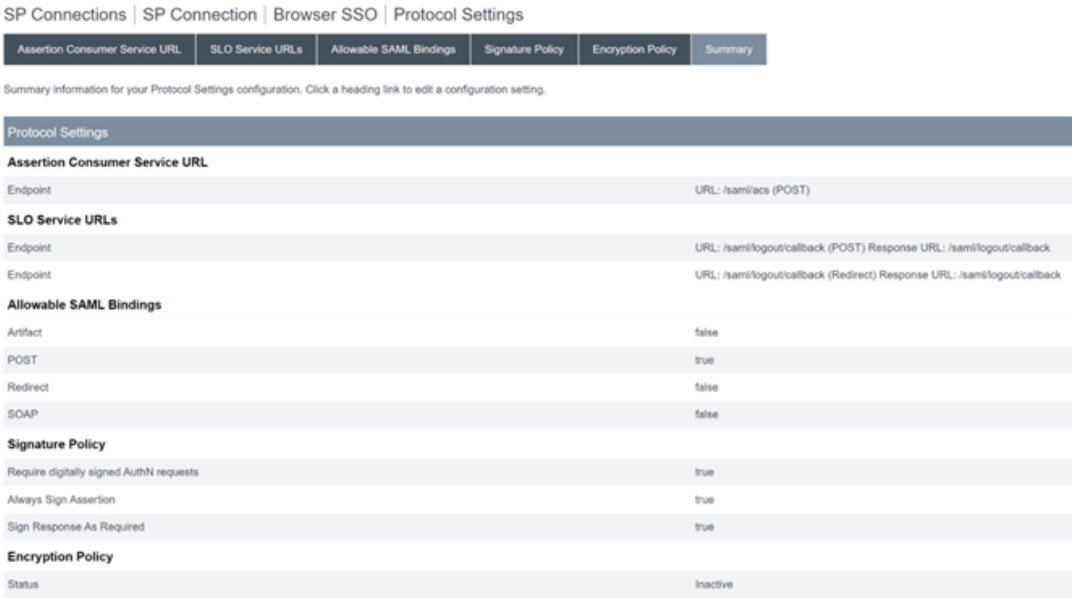
b) Configure the **Encryption Policy**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

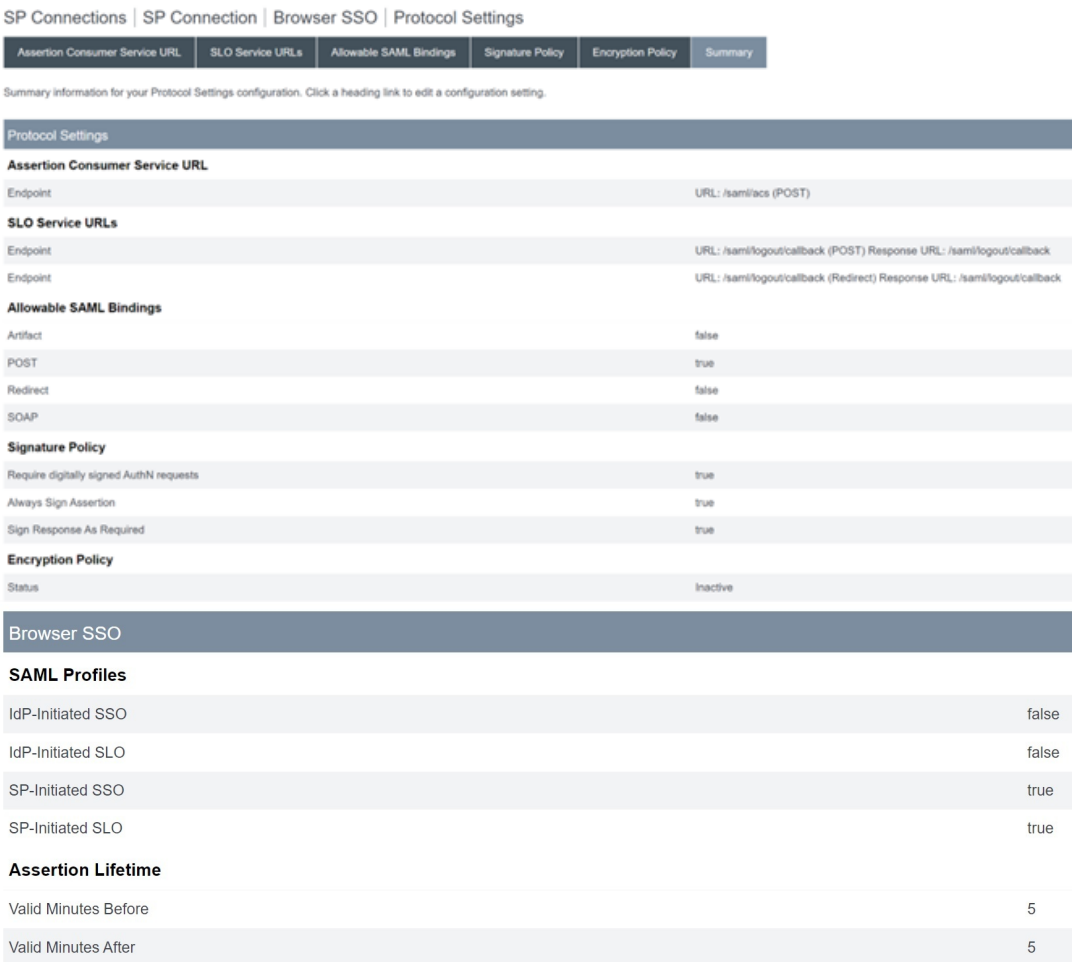
> **Note:**
>
> It is recommended to set Encryption to **NONE** during initial setup and testing so you can debug any issues with missing or incorrect SAML attributes in the assertion. If you require encrypted assertions, it is recommended that you enable encryption after proving that the logon to store or Citrix Cloud is successful and all resources have been successfully enumerated and can be launched. Debugging issues with SAML whilst encryption is enabled will be impossible if you cannot view the plaintext contents of the SAML assertion.

c) Review the **Summary** tab.



d) Review the **Citrix Cloud Service Provider (SP) Connection**. Once the **Citrix Cloud SP connection** is configured it should look like this example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



SP Connections | SP Connection | Browser SSO | Protocol Settings

Assertion Consumer Service URL | SLO Service URLs | Allowable SAML Bindings | Signature Policy | Encryption Policy | Summary

Summary information for your Protocol Settings configuration. Click a heading link to edit a configuration setting.

Protocol Settings

Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST) Response URL: /saml/logout/callback
Endpoint	URL: /saml/logout/callback (Redirect) Response URL: /saml/logout/callback
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	false
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	true
Always Sign Assertion	true
Sign Response As Required	true
Encryption Policy	
Status	Inactive

Browser SSO

SAML Profiles	
IdP-Initiated SSO	false
IdP-Initiated SLO	false
SP-Initiated SSO	true
SP-Initiated SLO	true
Assertion Lifetime	
Valid Minutes Before	5
Valid Minutes After	5

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Assertion Creation	
Identity Mapping	
Enable Standard Identifier	true
Attribute Contract	
Attribute	SAML_SUBJECT
Subject Name Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Attribute	cip_upn
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	displayName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	familyName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Attribute	givenName
Attribute Name Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Authentication Source Mapping	
Adapter instance name	CitrixCloudStagingIDPAdaptor
Adapter Instance	
Selected adapter	CitrixCloudStagingIDPAdaptor
Mapping Method	
Adapter	HTML Form IdP Adapter
Mapping Method	Use only the Adapter Contract values in the mapping
Attribute Contract Fulfillment	
SAML_SUBJECT	username (Adapter)
cip_upn	cip_upn (Adapter)
displayName	displayName (Adapter)
familyName	familyName (Adapter)
givenName	givenName (Adapter)

Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST) Response URL: /saml/logout/callback
Endpoint	URL: /saml/logout/callback (Redirect) Response URL: /saml/logout/callback
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	false
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	true
Always Sign Assertion	true
Sign Response As Required	true
Encryption Policy	
Status	Inactive

Credentials	
Digital Signature Settings	
Selected Certificate	CN=*. .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (0C:BE:67:B8:63:15:D4:D4:8B:3A:17:65:0F:71:0A:FD | Exp: Sep 19, 2024)
Include Certificate in KeyInfo	false
Selected Signing Algorithm	RSA SHA256

Signature Verification	
Trust Model	
Trust Model	Unanchored
Signature Verification Certificate	
Active Certificate 1	CN=samlsigning.cloud .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (03:48:4A:61:BF:59:EB:13:9C:20:FE:F1:5B:3A:83:29 | Exp: May 11, 2024)
Active Certificate 2	CN=samlsigning.cloud .com, O="Citrix Systems, Inc.", L=Fort Lauderdale, ST=Florida, C=US (0B:5F:B5:43:89:16:B0:2F:98:45:58:D1:DA:D1:B1:1D | Exp: Mar 11, 2025)

> **Userful tip:**
>
> Use the SP Connection Activation and Summary page to review your SAML application and for debugging purposes as it allows quick and easy configuration changes to be made. The SP Connection Activation and Summary page allows you to navigate to any of the SAML configuration sub sections by clicking on the title of that section. Click on any of the titles highlighted in red to update these settings.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Protocol Settings	
Assertion Consumer Service URL	
Endpoint	URL: /saml/acs (POST)
SLO Service URLs	
Endpoint	URL: /saml/logout/callback (POST)
Allowable SAML Bindings	
Artifact	false
POST	true
Redirect	true
SOAP	false
Signature Policy	
Require digitally signed AuthN requests	false
Always Sign Assertion	true
Sign Response As Required	true

16. The completed **Citrix Cloud SP connection** should appear in the list like this.



17. It is possible to export the SP connection in the form of an XML file. Citrix recommends taking a backup of your SP connection once you have tested it with Citrix Cloud and store.



Configure the Citrix Cloud SAML connection

All Citrix logon flows need to be Service Provider initiated using either a store URL or a Citrix Cloud GO URL.

Use the default recommended values for the SAML connection within **Identity and Access Management → Authentication →Add an identity provider → SAML**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

In this field in Citrix Cloud	Enter this value
Entity ID	`https://yourpingfedbaseurl.domain.com`, where `yourpingfedbaseurl.domain.com` is your PingFederate server domain.
Sign Authentication Request	Yes
SSO Service URL	`https://yourpingfedbaseurl.domain.com/idp/SSO.saml2` where `yourpingfedbaseurl.domain.com` is your PingFederate server domain.
SSO Binding Mechanism	HTTP Post
SAML Response	Sign Either Response Or Assertion
Authentication Context	Unspecified, Exact
Logout URL	`https://yourpingfedbaseurl.domain.com/idp/SLO.saml2` where `yourpingfedbaseurl.domain.com` is your PingFederate server domain.
Sign Logout Request	Yes
SLO Binding Mechanism	HTTP Post

Important:

- The use of the incorrect PingFederate IDP-initiated SSO endpoint `https://yourpingfederateserv.domain.com/idp/startSSO.ping?PartnerSpId=https://saml.cloud.com` is not supported. Citrix Cloud and store do not support IDP-initiated SSO.
- The following extract is taken from PingFederate documentation:
  This is the path used to initiate an unsolicited IdP-initiated single sign-on (SSO) transaction during which a SAML response containing an assertion is sent to a service provider (SP).
- The use of the incorrect SAML endpoint is known to cause SAML logon failures and the following error within Citrix Cloud's authentication platform.
  `ExceptionMessage=An IdP-initiated SAML response from YourSAMLApp was received unexpectedly.`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

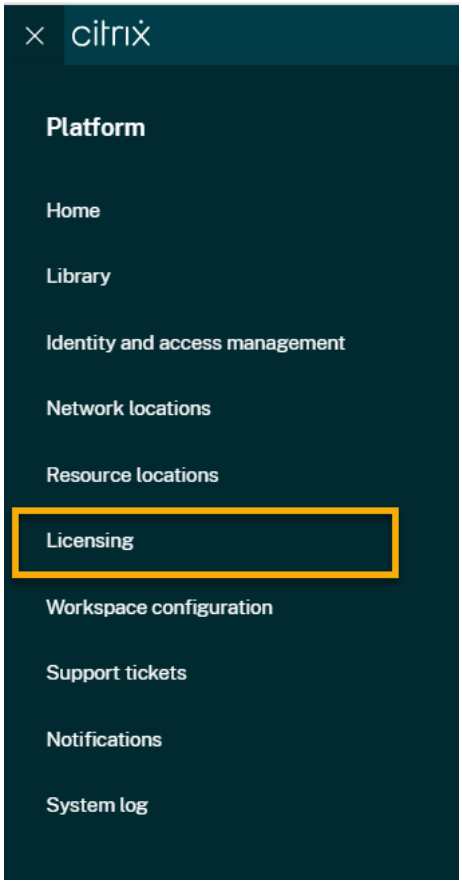
Licensing for Citrix Cloud™

September 6, 2025

Citrix Cloud provides license and usage monitoring for certain cloud services. As well, license and usage monitoring is available for on-premises deployments where Citrix License Server is registered with Citrix Cloud.

Licensing for enterprise customers

Enterprise customers can monitor license assignments and usage for supported cloud services by selecting **Licensing** from the Citrix Cloud menu.



For more information about enterprise license and usage monitoring for cloud services, see Monitor licenses and active usage for cloud services.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Licensing for on-premises deployments

Enterprise customers with an on-premises deployment of Citrix Virtual Apps and Desktops can use Citrix Cloud to stay abreast of licenses and usage for both User/Device and Concurrent licensing models. By registering Citrix License Server with Citrix Cloud, customers can use the **Licensed Deployments** page in Citrix Cloud for the following tasks:

- Monitor the reporting status of registered license servers
- View license assignments and usage trends for deployments that use the User/Device licensing model.
- View peak license usage trends for deployments that use the Concurrent licensing model.

For more information about license and usage monitoring for on-premises Virtual Apps and Desktops deployments, see Monitor licenses and usage for on-premises deployments.

Licensing for Citrix Service Providers (CSP)

Citrix Service Providers can use the following tools to understand and report on product licenses and usage:

- License Usage Insights is a free service in Citrix Cloud that collects and aggregates product usage information across single-tenant and multitenant customers. For more information, see Licensing for Citrix Service Providers.
- The Licensing feature in Citrix Cloud enables customers of CSPs to monitor their licenses and usage for supported Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) products. CSPs can sign in under their customer's Citrix Cloud account to view and export this information as well. For more information, see the following articles:
  - Customer license and usage monitoring for Citrix DaaS

Monitor licenses and active usage for cloud services

September 6, 2025

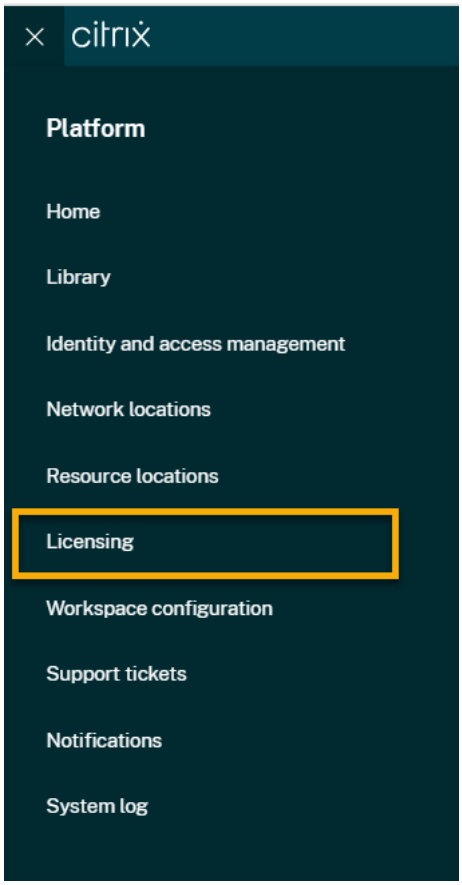
Licensing in Citrix Cloud™ enables you to stay on top of license consumption for the cloud services you have purchased. Using the summary and detail reports, you can:

- View license availability and assignments at a glance
- View daily and monthly active usage trends for applicable cloud services
- Drill down to see individual license assignment details and usage trends

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Export license usage data to CSV

To view licensing data for your cloud services, select **Licensing** from the console menu.



> **Note:**
>
> This article covers Licensing features that are common to all supported Citrix Cloud services. Some aspects of Licensing might be different, depending on the service (for example, license assignment). For more information about licenses and usage for each service, see the following articles:
>
> - Monitor licenses and active usage for Citrix DaaS (User/Device)
> - Monitor licenses and peak usage for Citrix DaaS and Citrix DaaS Standard for Azure (Concurrent)
> - Monitor licenses and active usage for Citrix DaaS Standard for Azure (User/Device only)
> - Monitor licenses and active usage for Endpoint Management service
> - Monitor bandwidth usage for Gateway service
> - Monitor licenses and usage for Secure Private Access

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Supported regions and cloud services

Licensing is available for supported services in the US, EU, and Asia Pacific South regions only.

Licensing is supported for the following cloud services:

- Citrix DaaS (User/Device and Concurrent licensing models) - formerly Citrix Virtual Apps and Desktops service
- Citrix DaaS Standard for Azure (User/Device licensing model) - formerly Citrix Virtual Apps and Desktops Standard for Azure
- Endpoint Management
- Gateway
- Secure Private Access (formerly Secure Workspace Access)

Multi-type licensing for Citrix DaaS™

Licensing in Citrix Cloud supports multi-type licensing for Citrix DaaS. If both User/Device and Concurrent licensing models are introduced into a single Citrix Cloud account, Citrix Cloud shows license usage under each licensing mode in the Licensing console page.

Citrix recommends setting up multi-type licensing at the site and delivery group levels before reviewing the Licensing page. Otherwise, the correct information might not appear. For instructions, see Multi-type licensing in the Citrix DaaS documentation.

If the Licensing console page doesn't display the correct multi-type license usage after successfully using the Web Studio or PowerShell setup methods, you have the following options:

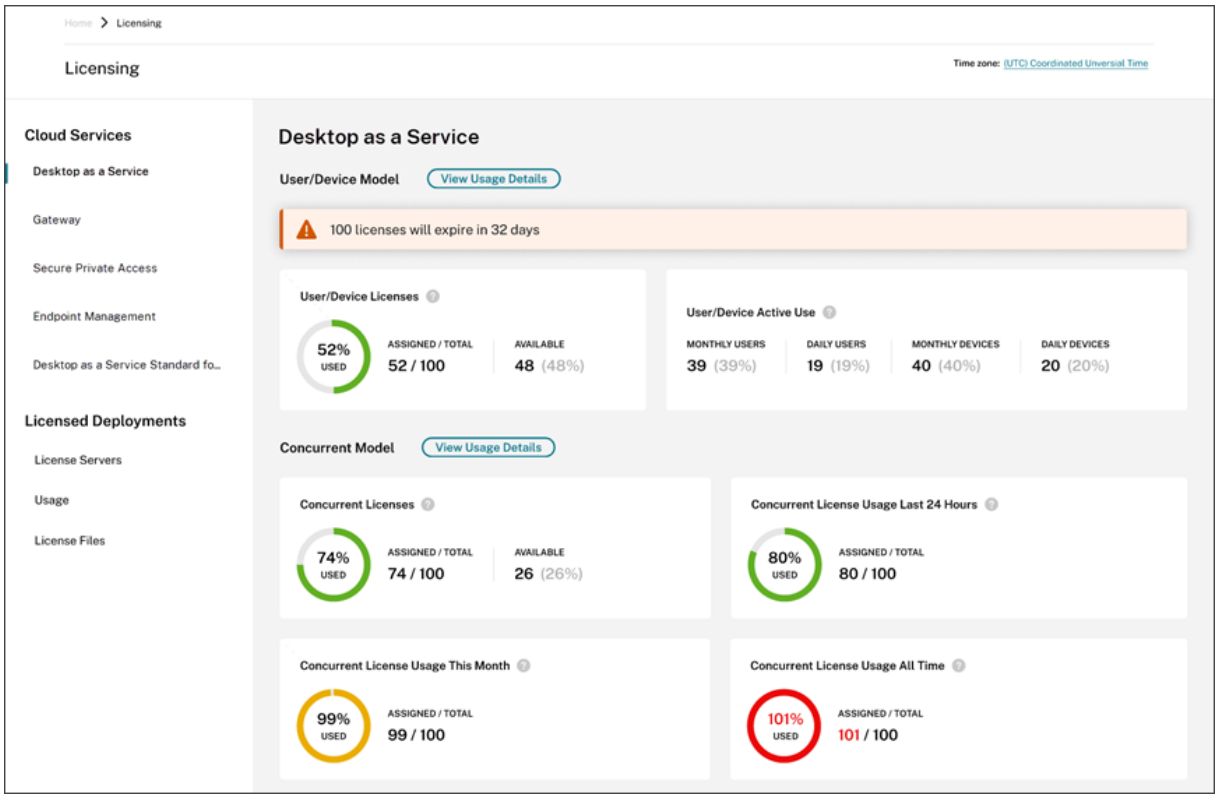
- Wait 30 days and release any unused licenses.
- Contact Citrix Customer Service.

License assignment

In general, users are assigned a license upon first use of the cloud service. Some services might assign licenses differently based on the licensing model they use. For more information about how licenses are assigned for each service, see the Licensing articles referenced at the top of this article.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Licensing summary and details



The Licensing summary provides an at-a-glance view of the following information for each supported service:

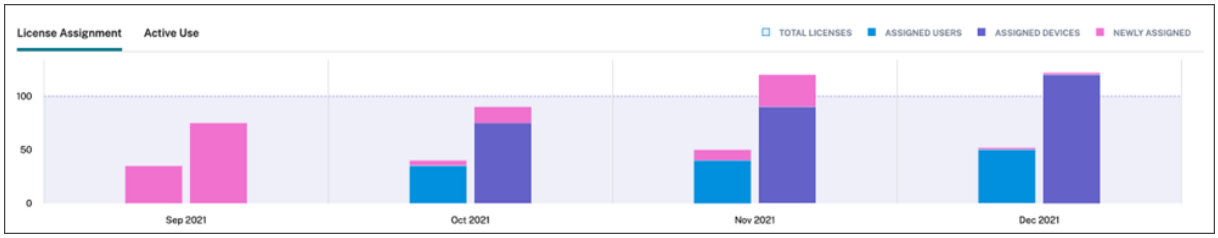
- Percentage of total purchased licenses assigned. As the percentage approaches 100%, the percentage goes from green to yellow. If the percentage exceeds 100%, the percentage turns red.
- The ratio of assigned licenses to purchased licenses and the number of available licenses remaining.
- The time remaining before the cloud service subscription expires. If the subscription expires within the next 90 days, a warning message appears.

For some services, this summary might include additional information such as active use. For more information about service-specific details, see the Licensing articles referenced at the top of this article.

Usage trends and license activity

For a detailed view of your cloud service licenses, click **View Usage Details**. You can then see a breakdown of usage trends and consumers of cloud service licenses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



This breakdown includes varying information, depending on the cloud service. For more information about service-specific usage trends and license activity, see the Licensing articles referenced at the top of this article.

Release assigned licenses

In general, an assigned license is eligible for release if the consumer hasn't used the cloud service for 30 consecutive days. When a license is released, the number of remaining licenses increases and the number of assigned licenses decreases accordingly.

For some services, releasing licenses might be different, depending on the licensing model used. For more information about releasing licenses for a specific service, see the Licensing articles referenced at the top of this article.

FAQ

- **Does Citrix® prevent cloud service usage if assigned licenses exceed purchased licenses?** No, Citrix does not prevent any service launches if you overuse your cloud license amount. License Usage provides information for understanding your cloud license usage, so Citrix expects that you will monitor your license assignments and stay within your purchased license amount. If, at any point, you believe that you are going to overuse your service, Citrix encourages you to contact your sales representative to discuss your licensing requirements.
- **What licensing information is being captured?** Currently, only license information associated with user logins is captured.
- **Is multi-type licensing supported with Citrix DaaS (for example, using both User/Device and Concurrent User models)?** Yes. See Multi-type licensing in this article for additional information.
- **Is multi-edition licensing supported for Citrix DaaS? For example, can I use both Premium and Advanced editions on the same Citrix Cloud account?** No, this use case is not supported. A Citrix DaaS site can be licensed for only one edition. If you want to use multiple Citrix DaaS instances on the same Citrix Cloud account, they must be the same edition.
- **What is the difference between Monitor reporting (in Director) vs Concurrent licensing insights?** The Monitor report and explanation of concurrent sessions provides a different interpretation and metric than a measure of concurrent licenses in use. In most cases, using the

© 1997–2026 Citrix Systems, Inc. All rights reserved.

number of concurrent sessions within Director as a representation or forecast of peak concurrent licenses in use greatly overstates the number of concurrent licenses needed. Do not use the Monitor report in Director as a substitute for a report on concurrent license usage. The two main differences between the reporting tools are:

- **Sampling Time Length:** Licensing has a five-minute sampling period. Every five minutes, Citrix Cloud counts the unique devices currently connected to the service. All the five-minute sampling periods are aggregated to determine peak usage in a 24-hour, monthly, and contract length period. The Monitor report in Director can show intervals of up to two hours depending on how the report is run.
- **Uniqueness:** Licensing looks for uniqueness amongst devices when sessions are launched. The Monitor report does not account for unique devices.

- **After migrating users to a new instance of a cloud service (for example, I changed the domain name for my organization), why are my licenses in-use counted twice for the same users?-* Citrix Cloud uses the User Principle Name (UPN) to count unique users. If a user accessed the cloud service before and after the migration occurred, Citrix Cloud captures two unique UPNs for the user, each with a different domain name. Therefore, Citrix Cloud counts the same user twice. You can release the older license assignment after 30 days, assuming the user doesn't access the service under the old domain name. Citrix does not prevent any service launches if you overuse your cloud license amount.
- **Why am I seeing duplicate licenses for the same user or device?-* This is by design of the Workspace app for HTML5 and locally-installed Workspace app. Launches through Workspace app for HTML5 consume a User/Device license. As well, launches through locally-installed Workspace app consume a User/Device license. So, if a user launches apps through Workspace app for HTML5 and then launches through a locally-installed version of Workspace app later, Citrix Cloud shows that the user consumed two licenses. This behavior doesn't affect user connectivity, but can result in inflated device license usage reports in the Licensing console. Citrix does not prevent any service launches if you overuse your cloud license amount.

Monitor licenses and active usage for Citrix DaaS (User/Device)

September 6, 2025

This article describes how you can manage cloud service license assignments and monitor active usage using the Licensing console in Citrix Cloud.

If you purchased Citrix Azure Consumption Fund to use with your service deployment, see Monitor Citrix Managed Azure resource consumption for Citrix DaaS for more information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

License assignment

Citrix Cloud assigns a license when a unique user or unique device launches an app or desktop for the first time.

Domain name truncation

If you host multiple domains and have users with similar accounts in those domains (for example, `johnsmith@company.com` and `johnsmith@mycompany.com`), you can allow Citrix Cloud to ignore the account domain and consider only the user name of the account (for example, johnsmith). This process is known as *domain name truncation*. By default, domain name truncation is disabled.

When domain name truncation is enabled, Citrix Cloud's calculation of unique users changes. Instead of counting `johnsmith@company.com` and `johnsmith@mycompany.com` as two unique users, Citrix Cloud counts only johnsmith as a unique user. This calculation change affects the following Licensing data:

- License assignment
- Active use
- License usage trends over time
- Licenses eligible for release

These changes in licensing data are also reflected when you export data to a CSV file from the Licensing console.

> **Note:**
>
> If you host multiple domains with similar accounts where the user name is slightly different (for example, an individual user has the accounts `johnsmith@company.com` and `jsmith@newcompany.com`), domain name truncation has no effect on Citrix Cloud's calculations. Citrix Cloud still counts johnsmith and jsmith as unique users even if they belong to the same individual.

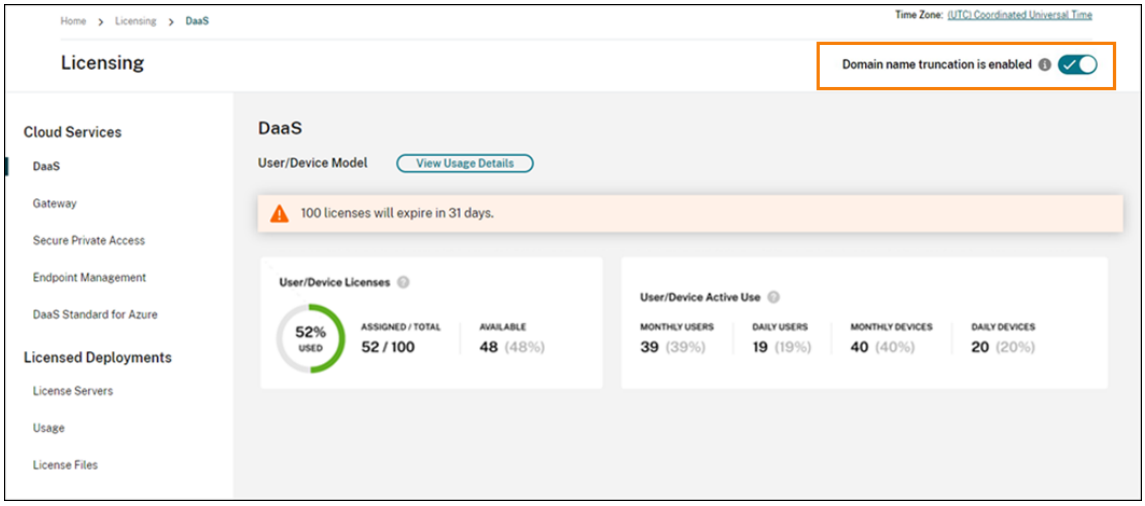
Enable or disable domain name truncation

By default, domain name truncation is disabled. Domain name truncation has an effect on your User/Device usage data from the moment you enable or disable the feature. For example, if you enable domain name truncation in a given month, the data that Citrix Cloud records in that month is affected. However, historical data for previous months, when the feature was disabled, remains unaffected. Likewise, if you disable domain name truncation in a given month, the data that Citrix Cloud records in that month is affected. However, historical data for the months when the feature was enabled remains intact.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

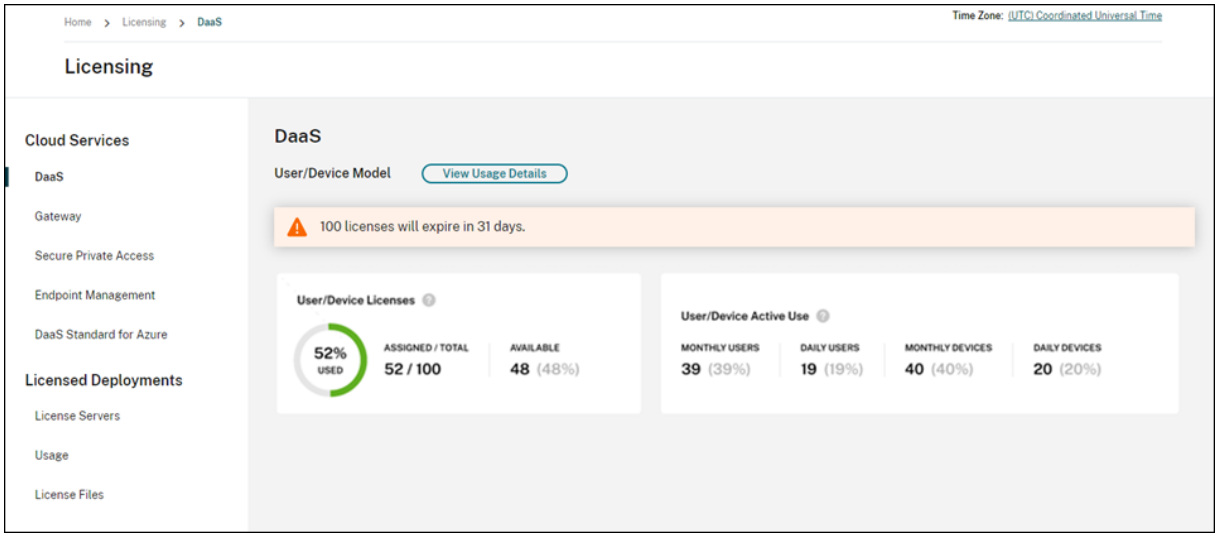
To enable or disable domain name truncation:

1. Click the toggle near the top-right of the Licensing console.



2. When prompted to confirm your action, select **Yes, I understand**.

Licensing summary



The Licensing summary provides an at-a-glance view of the following information:

- Percentage of total purchased licenses that have been assigned. As the percentage approaches 100%, the percentage goes from green to yellow. If the percentage exceeds 100%, the percentage turns red.

  The quantity of total purchased licenses is the sum of licenses that have been purchased for Citrix DaaS editions that use the User/Device licensing model.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The ratio of assigned licenses to purchased licenses and the number of available licenses remaining.
- Active usage statistics on a monthly and daily basis:
    - Monthly active use refers to the number of unique users or devices that have used the service in the last 30 days.
    - Daily active use refers to the number of unique users or devices that have used the service in the last 24 hours.
- The time remaining before the cloud service subscription expires. If the subscription expires within the next 90 days, a warning message appears.

Calculating assigned licenses and active use

To accurately reflect the User/Device licensing model for Citrix DaaS, Citrix Cloud counts the number of unique users and unique devices that have used the service. To measure assigned licenses, Citrix Cloud uses the lesser of these counts. To measure active use, Citrix Cloud uses each count as the quantity of active users and active devices in a given period.

Example of calculating assigned licenses

If 100 unique users and 50 unique devices have used the service, Citrix Cloud uses the lesser number (50) to determine the number of assigned licenses. The percentage of licenses used and the number of available licenses are based on these 50 assigned licenses.

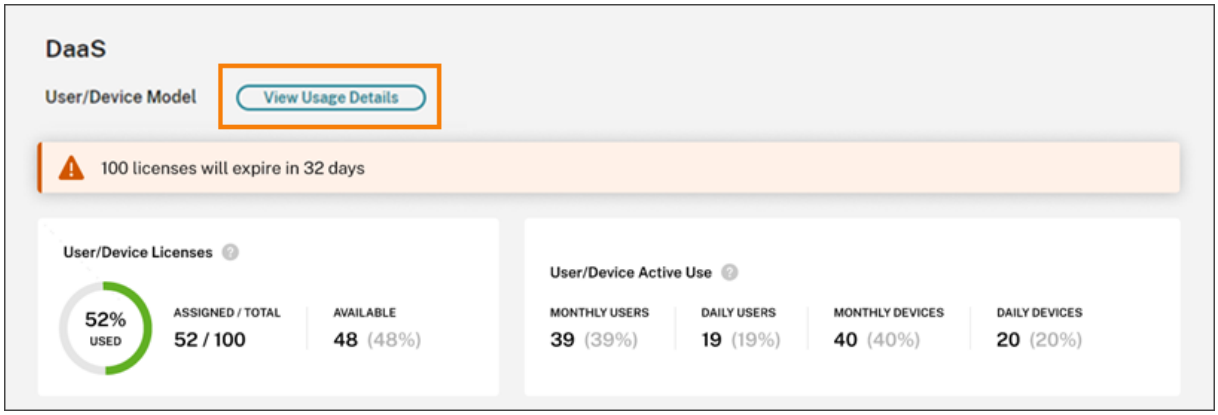
Example of calculating active use

If 10 unique users and 20 unique devices used the service in the last 30 days, Citrix Cloud determines that monthly active use consists of 10 active users and 20 active devices. Likewise, if 30 unique users and 15 unique devices were counted in the last 24 hours, Citrix Cloud determines that daily active use consists of 30 active users and 15 active devices.

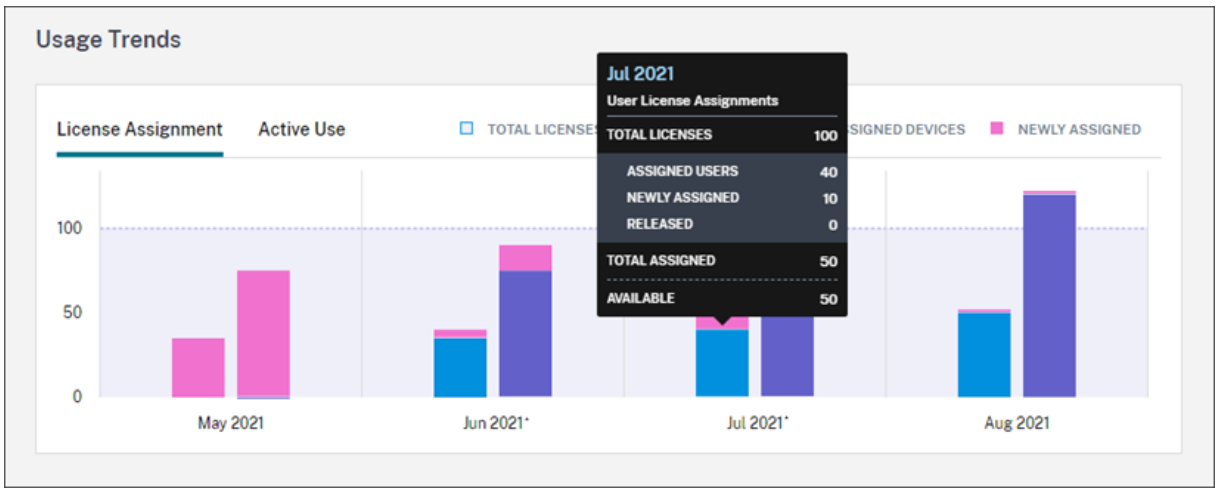
Usage trends

For a detailed view of your licenses, click **View Usage Details** at the far right of summary. You can then see a breakdown of usage trends and individual users and devices that are consuming cloud service licenses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Usage Trends** section displays this breakdown as a graph.

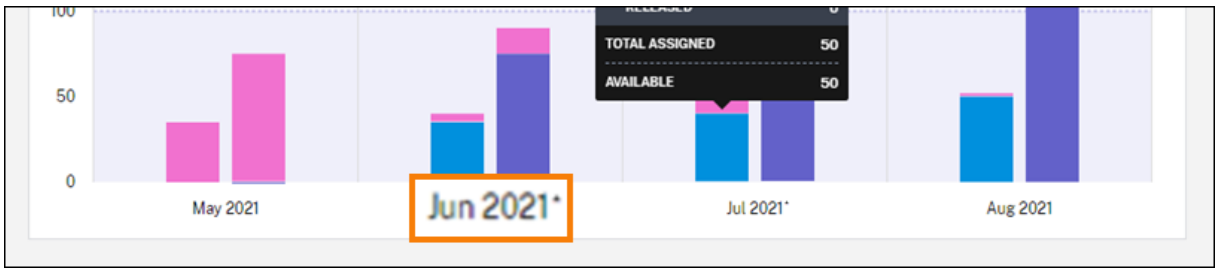


On the **License Assignment** graph, pointing to a bar for a specific month or day shows you the following information:

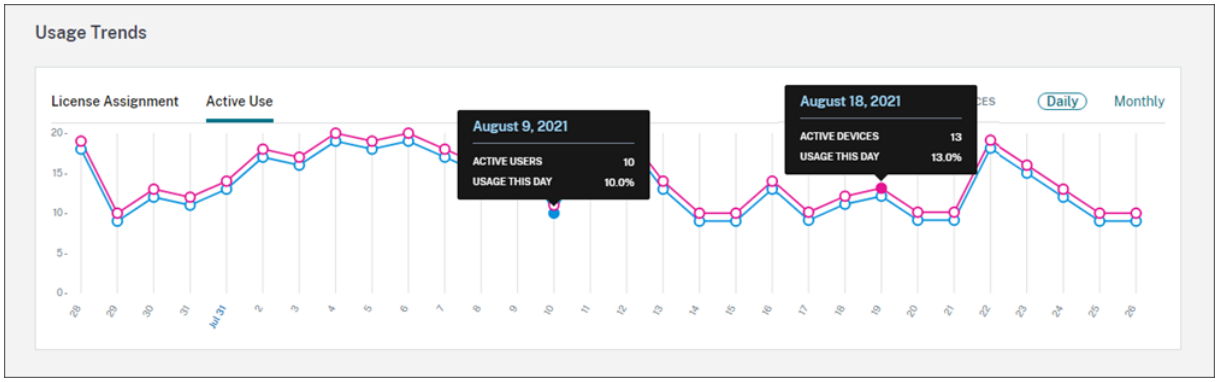
- **Total Licenses:** Your total purchased licenses for the cloud service across all entitlements.
- **Assigned Users:** The cumulative number of licenses assigned to users up to the current month.
- **Assigned Devices:** The cumulative number of licenses assigned to devices up to the current month. If this number seems particularly high for a given month, this could be the result of app or desktop launches occurring through a web browser. To lower this number, Citrix® recommends using a locally-installed Workspace app.
- **Newly Assigned:** The number of new licenses that were assigned for each month. For example, a user accesses the cloud service for the first time in July and is assigned a license. This license is counted as "Newly Assigned"for the month of July.
- **Released:** The number of eligible licenses that were released during each month. For example, if 20 licenses were eligible for release and you released 10 of them in July, the number of released licenses shown for July is 10.

Intervals of time in which domain truncation is enabled are marked with an asterisk.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



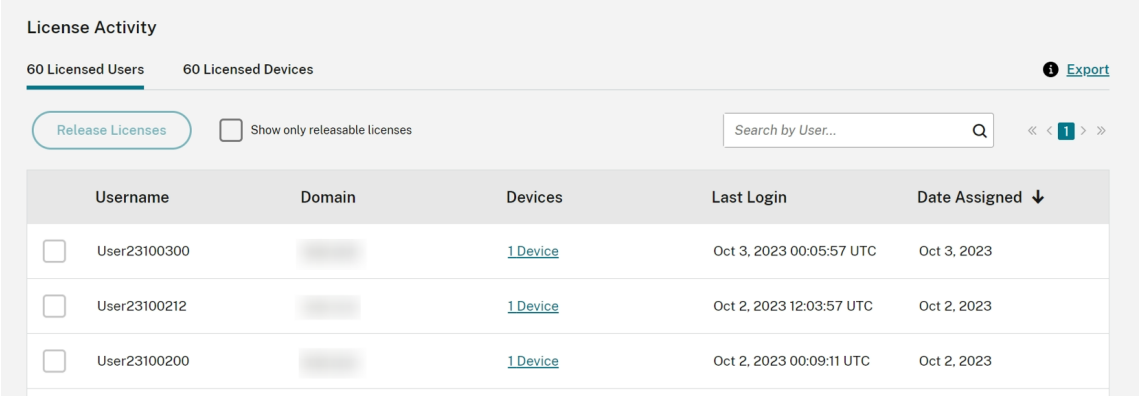
On the **Active Use** graph, you can view active users and devices over the previous calendar month and calendar year, respectively. Pointing to a specific interval on the graph reveals the number of active users or devices and the usage percentage.



License Activity

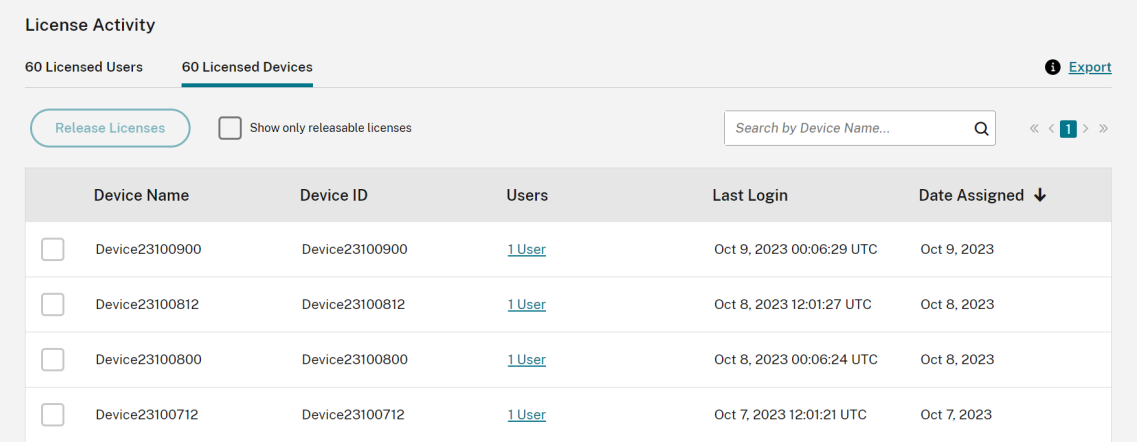
The **License Activity** section displays the following information:

- A list of the individual users who have assigned licenses, including associated devices.



- A list of the devices that have assigned licenses, including associated users.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- The date when a license was assigned to the user or device.

You can also filter the list to show only licenses that are eligible for release. See To release assigned licenses in this article.

Release assigned licenses

When a license is assigned, the assignment period is 90 days and the connection to the service is established. If a user or device hasn't launched an app or desktop for 90 days, these licenses are considered as unused licenses and they are released by Citrix Cloud after 90 days. This process is automated with no actions required by the administrator.

After the assignment period (90 days), the administrator is allowed to release the licenses manually in the following scenarios only:

- The user is no longer associated with the company.
- The user is on an extended leave of absence.

The administrators can release the licenses for devices only when the devices are out of service.

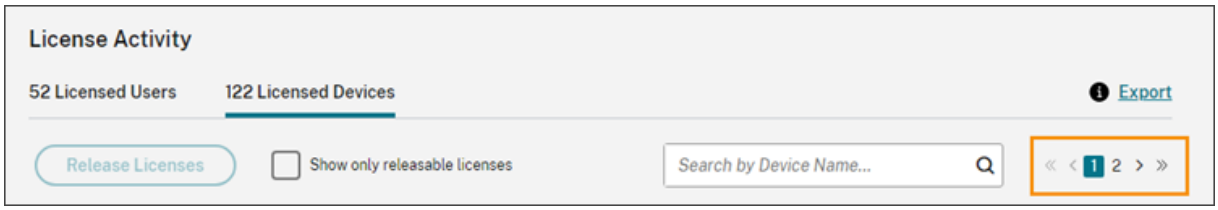
> **Note:**
>
> - It is recommended to follow the automated process of releasing the Licenses. However if the administrator intends to release the licenses before the 90-day period apart from the above mentioned reasons, this might violate the Citrix EULA. Before performing this action, contact Citrix.
> - The administrator can manually release a single license through the UI. Alternatively, the administrator can choose to release licenses using the cloud licensing API. For more information see, APIs to manage Citrix cloud licensing.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

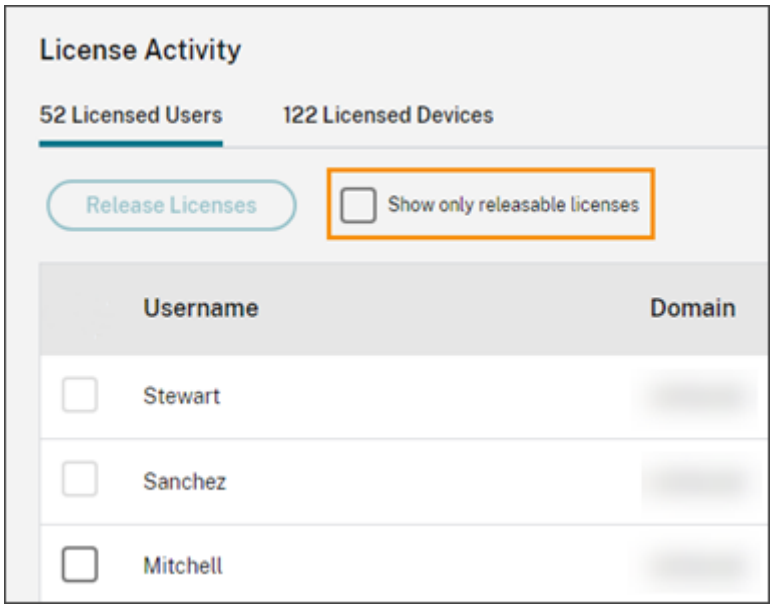
Find releasable licenses

If the user or device hasn't launched an app or desktop for 30 days, Citrix Cloud places the license in releasable state. Releasable licenses appear in the Licensed Users or Licensed Devices list with a dark gray checkbox that can be selected. Licenses that aren't releasable displays a light gray checkbox indicating that license cannot be selected.

The list that appears in the **License Activity** section displays up to 100 assigned licenses at a time. If you have more than 100 licenses, use the page controls to move through the list.



To locate releasable licenses quickly, click **Show only releasable licenses**, next to the **Release Licenses** button. This action hides assigned licenses that aren't yet allowed to be released.



Select releasable licenses

Select the dark gray checkbox next to each license to select it for release. When you select a license from the list, the **Release Licenses** button becomes active.

You can select all releasable licenses one-by-one and click **Release Licenses**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To release assigned licenses

1. Under **License Activity**, click the **Licensed Users** or **Licensed Devices** tab.
2. If needed, click **Show releasable licenses** to display only the users with licenses that are allowed to be released.
3. Select the users or devices you want to manage and then click **Release Licenses**.
4. Review the users or devices you've selected and then click **Release Licenses**.

Automatic switchover of license

If the active User/Device license expires and the Concurrent license is the only active license type for the tenant, the site license automatically switches to the active Concurrent license. This prevents any outage due to lack of active license on the site.

Monitor licenses and peak usage for Citrix DaaS™ (Concurrent User)

August 21, 2026

This article describes the experience for managing Concurrent User licenses for **Citrix DaaS** only.

For information about User/Device licensing for Citrix DaaS, see Monitor licenses and active use for Citrix DaaS (User/Device).

For information about User/Device and Concurrent User licensing for Citrix DaaS Standard for Azure, see Monitor licenses and usage for Citrix DaaS Standard for Azure.

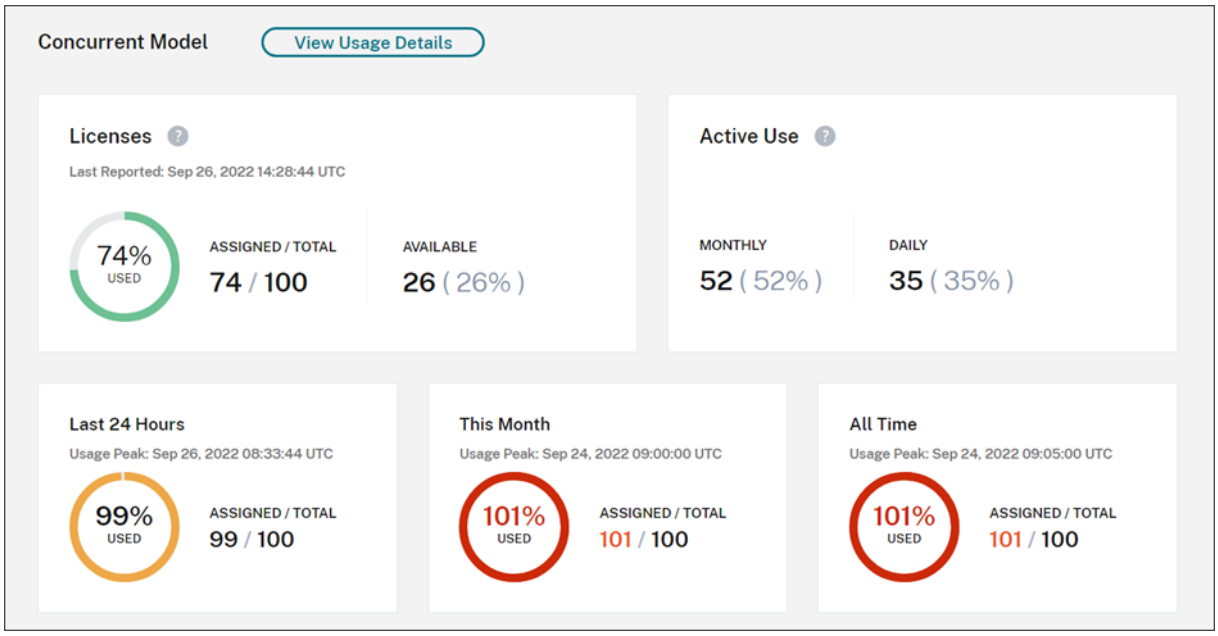
License assignment

Citrix Cloud™ assigns a license when a user launches an app or desktop on their device. When the user logs off or disconnects from the session, the license is no longer assigned. Because license assignment can change depending on the number of devices accessing apps or desktops at any given time.

For more information about the Concurrent User licensing model, see Concurrent license in the Licensing product documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Licensing summary



The Licensing summary provides an at-a-glance view of the following information:

- Percentage of total purchased licenses currently in use when Citrix Cloud last evaluated the licenses in use. The quantity of total purchased licenses is the sum of licenses that have been purchased for Citrix DaaS editions that use the Concurrent User licensing model.
- The ratio of currently assigned licenses to total purchased licenses and the number of available licenses remaining. The **Total** figure shown in this ratio represents the total number of licenses that are currently owned (as of the "Last Reported"date and time).
- Peak usage statistics. In calculating peak licenses in use, Citrix Cloud retrieves the the maximum number of licenses used in the following time periods:
  - **Last 24 hours:** The maximum number of licenses used at one time during the last 24-hour period.
  - **This Month:** The maximum number of licenses used at one time from the start of the current calendar month.
  - **All Time:** The maximum number of licenses used at one time from the start of the subscription.

  The **Total** figure shown for these peak usage periods represents the total number of licenses that were owned at that point in time. If the total number of owned licenses increases or decreases, and there's a corresponding increase in assigned licenses, the **Total** figure changes to reflect the new number of owned licenses for that point in time. However, if there is no corresponding usage peak, the **Total** figure does not change.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Active use statistics. Citrix Cloud displays the total number of unique connections for the following periods:
  - **Monthly:** Monthly active use refers to the number of unique users or devices that have used the service in the last 30 days.
  - **Daily:** Daily active use refers to the number of unique users or devices that have used the service in the last 24 hours. These figures are also represented as percentages of the total number of licenses owned during these periods.

Calculating peak licenses in use

To accurately reflect the Concurrent User licensing model, Citrix Cloud counts the number of unique devices accessing the service simultaneously. If the count is greater than the current peak usage displayed, Citrix Cloud displays the new peak usage with the date and time that it was reached. If the count is less than the current peak usage, the current peak usage doesn't change.

> **Important:**
>
> If you use Monitor in Director for information about concurrent sessions, be aware that the Monitor report provides a different interpretation of concurrent sessions and does not accurately reflect the number of Concurrent User licenses in use. For more information about the differences between Monitor reports and Licensing reports, see the FAQ.

Calculating monthly active use

At the beginning of each month, Citrix Cloud takes a snapshot of the last 30 days. Citrix Cloud displays the total number of unique connections that occurred during that calendar month.

Calculating daily active use

At the same time each day, Citrix Cloud takes a snapshot of the last 24 hours. Citrix Cloud displays the total number of unique connections that occurred during that 24-hour period.

Usage trends and license activity

For a historical view of your licenses, click **View Usage Details**.

The **Usage Trends** section shows you the following information:

- **License Assignment** displays a chart of the following information:
  - **Total Licenses:** Your total purchased Concurrent User licenses.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

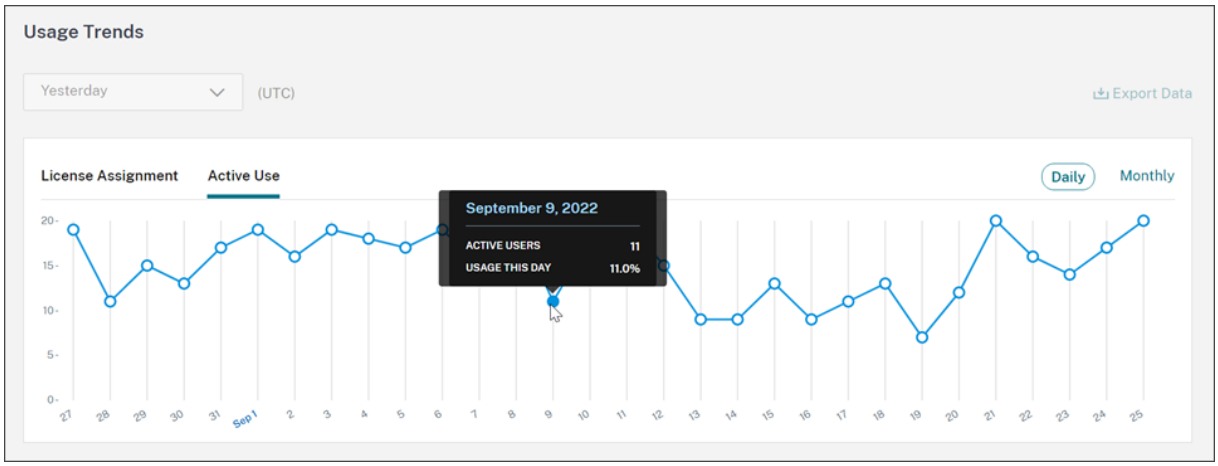
- **Peak Licenses In Use:** The maximum number of licenses assigned for the date range that you select. By default, Citrix Cloud displays peak usage for each month in the current calendar year. To drill down to monthly or hourly peak usage, select the calendar month or day you want to view from the drop-down menu.

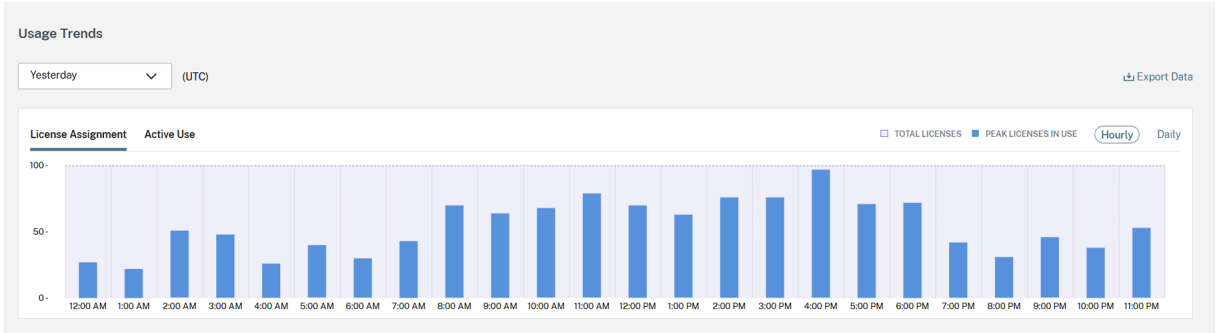
  If the date range you select isn't yet finished, Citrix Cloud displays the current peak usage for the latest interval of time. For example, if you drill down to view a calendar day that's still in progress, the maximum number of licenses is displayed for each hour up to the current moment in time. If the maximum number of licenses increases at the next counting interval, Citrix Cloud updates the peak usage for the current hour.

- **Active Use** displays a chart of the following information:

  - **Daily:** The total number of connections for each day during the previous 30 days.
  - **Monthly:** The total number of connections for each month during the previous calendar year.

Pointing to an interval on the **License Assignment** or **Active Use** charts reveals the details for that interval.

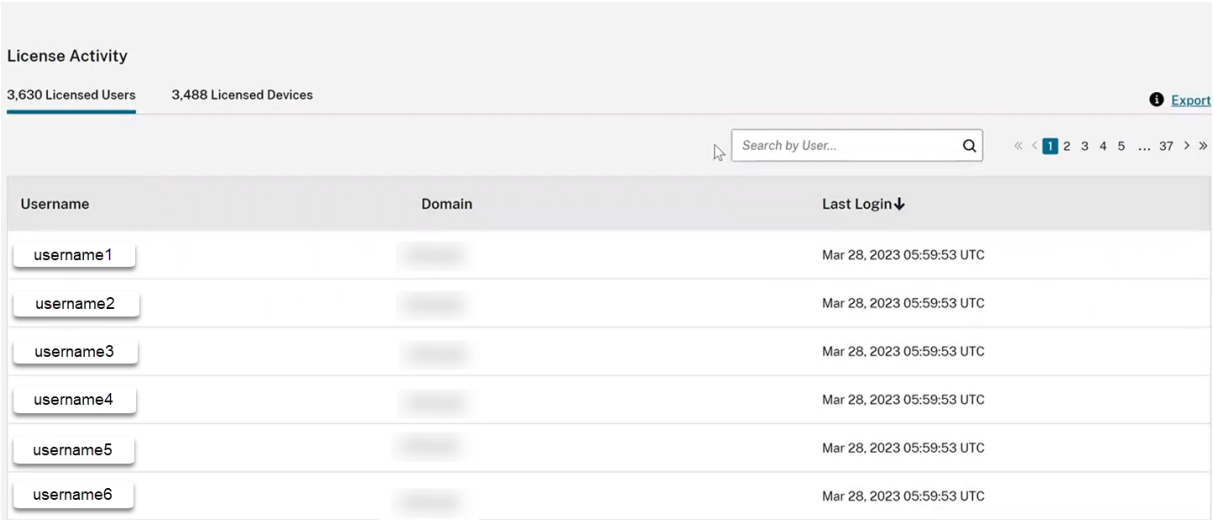




© 1997–2026 Citrix Systems, Inc. All rights reserved.

License activity for users and devices

For user or device licenses, the **License Activity** section displays a list of individual users who have assigned licenses, and the date when a license was assigned to the user.



Release licenses

Concurrent User licenses are released automatically when users sign out or disconnect from their session. You don't need to release these licenses manually.

Monitor licenses and usage for Citrix DaaS Standard for Azure

August 21, 2026

This article describes the experience for managing license assignments for both User/Device and Concurrent User licensing models.

Citrix Azure Consumption Fund (User/Device only)

If you purchased Citrix Azure Consumption Fund to use with your service deployment, see Monitor Citrix Managed Azure resource consumption for Citrix DaaS for more information about consumption reporting for Citrix-managed resources.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

License assignment

User/Device licensing model: Citrix Cloud assigns a license when a unique user or unique device launches a desktop for the first time.

Concurrent User licensing model: Citrix Cloud™ assigns a license when a user launches a desktop on their device. When the user logs off or disconnects from the session, the license is no longer assigned. Because license assignment can change depending on the number of devices accessing desktops at any given time, Citrix Cloud evaluates the number of licenses in use every five minutes.

For more information about the Concurrent licensing model, see Concurrent licenses in the Licensing product documentation.

Calculating peak licenses in use

To accurately reflect the Concurrent licensing model, Citrix Cloud counts the number of unique devices accessing the service simultaneously every five minutes. If the count is greater than the current peak usage displayed, Citrix Cloud displays the new peak usage with the date and time that it was reached. If the count is less than the current peak usage, the current peak usage doesn't change.

Domain name truncation

This feature is supported for the **User/Device** licensing model only.

If you host multiple domains and have users with similar accounts in those domains (for example, `johnsmith@company.com` and `johnsmith@mycompany.com`), you can allow Citrix Cloud to ignore the account domain and consider only the user name of the account (for example, johnsmith). This process is known as *domain name truncation*. By default, domain name truncation is disabled.

When domain name truncation is enabled, Citrix Cloud's calculation of unique users changes. Instead of counting `johnsmith@company.com` and `johnsmith@mycompany.com` as two unique users, Citrix Cloud counts only johnsmith as a unique user. This calculation change affects the following Licensing data:

- License assignment
- Active use
- License usage trends over time
- Licenses eligible for release

These changes in licensing data are also reflected when you export data to a CSV file from the Licensing console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

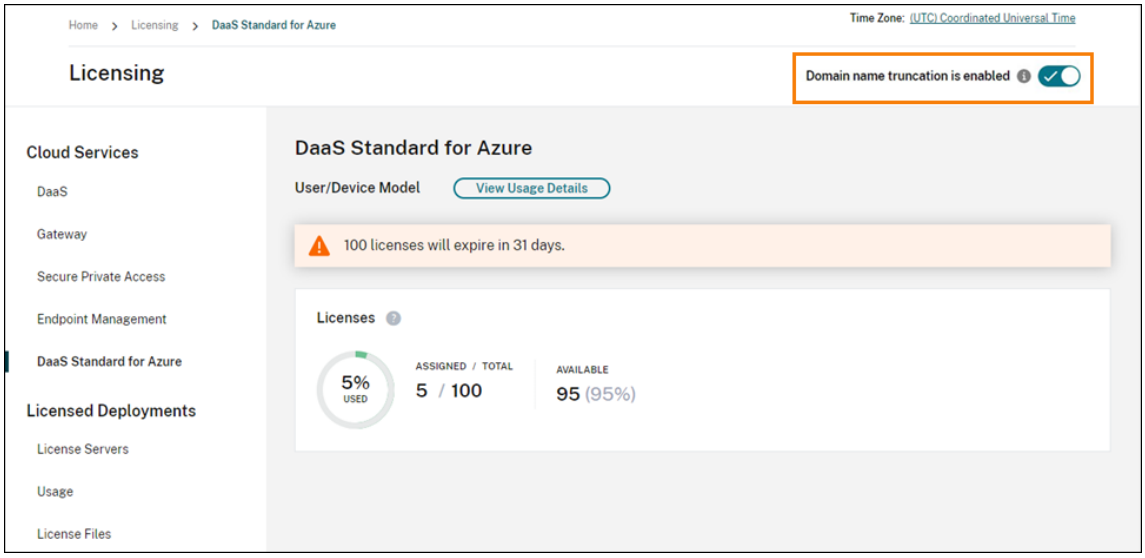
> **Note:**
>
> If you host multiple domains with similar accounts where the user name is slightly different (for example, an individual user has the accounts `johnsmith@company.com` and `jsmith@newcompany.com`), domain name truncation has no effect on Citrix Cloud's calculations. Citrix Cloud still counts johnsmith and jsmith as unique users even if they belong to the same individual.

Enable or disable domain name truncation

By default, domain name truncation is disabled. Domain name truncation has an effect on your User/Device usage data from the moment you enable or disable the feature. For example, if you enable domain name truncation in a given month, the data that Citrix Cloud records in that month is affected. However, historical data for previous months, when the feature was disabled, remains unaffected. Likewise, if you disable domain name truncation in a given month, the data that Citrix Cloud records in that month is affected. However, historical data for the months when the feature was enabled remains intact.

To enable or disable domain name truncation:

1. Click the toggle near the top-right of the Licensing console.



2. When prompted to confirm your action, select **Yes, I understand**.

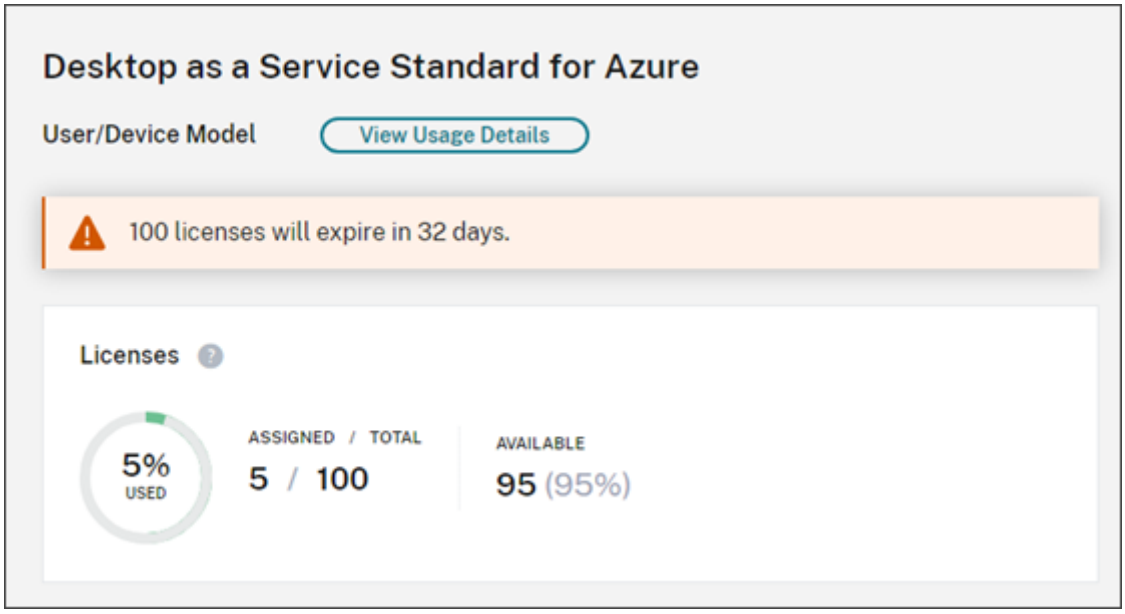
Licensing summary

Citrix Cloud displays summary views of licenses in use under the User/Device and Concurrent User licensing models.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Summary for users and devices

For the User/Device model, the licensing summary shows the licenses that are in use relative to the total number of licenses that you own.



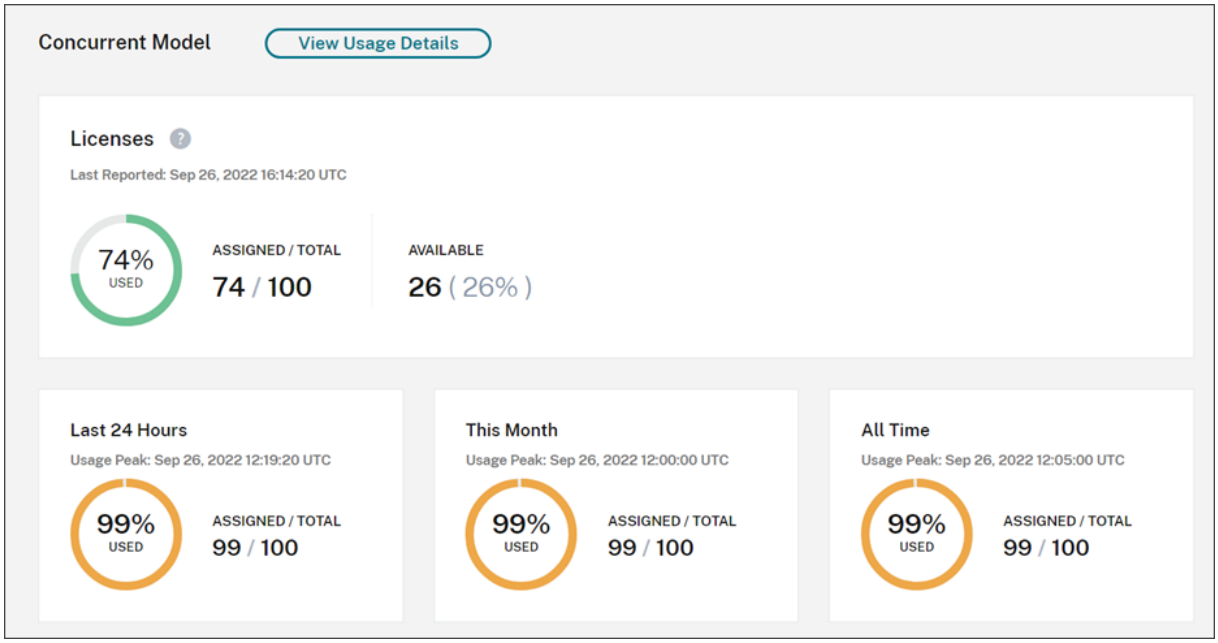
As the percentage approaches 100%, the percentage goes from green to yellow. If the percentage exceeds 100%, the percentage turns red.

Citrix Cloud also displays the ratio of assigned licenses to purchased licenses and the number of remaining available licenses.

Summary for concurrent users

For the Concurrent model, the licensing summary provides an at-a-glance view of the following information:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



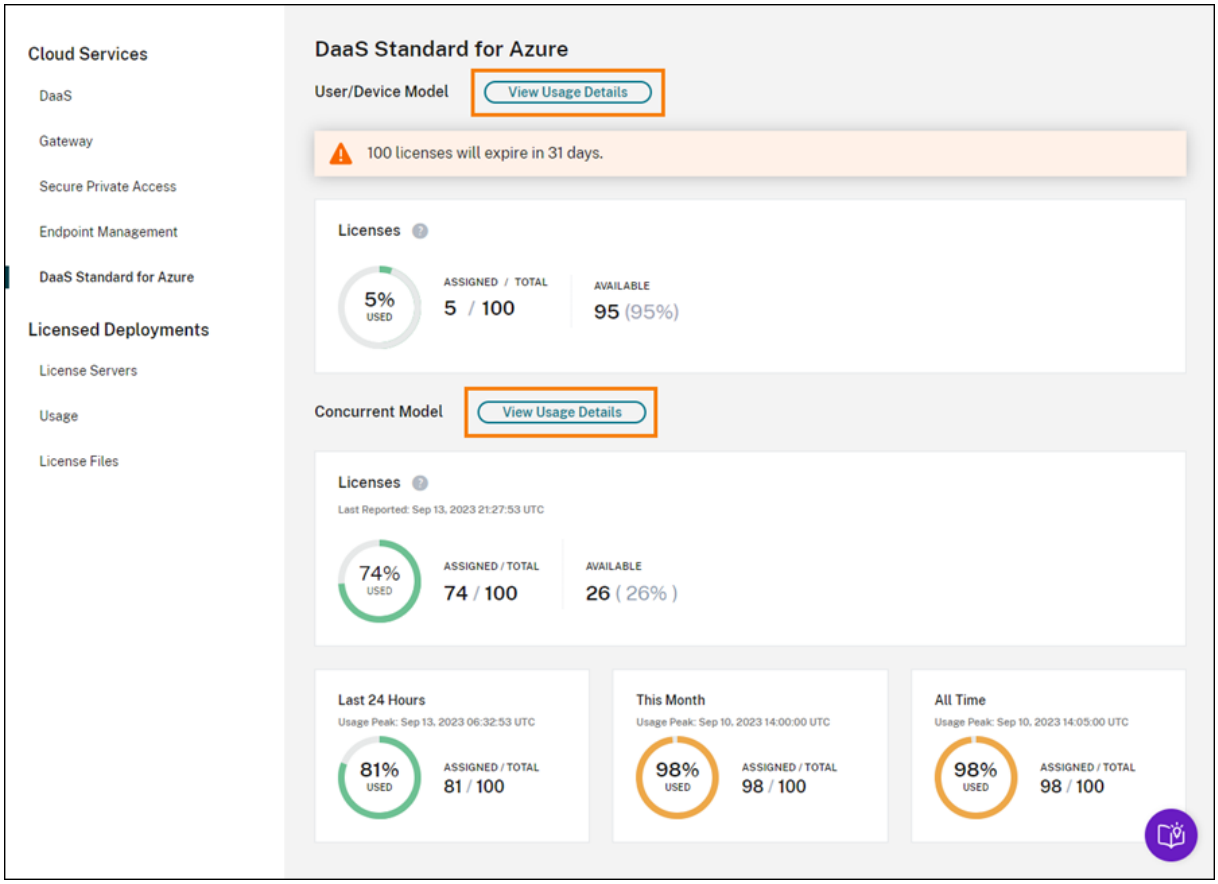
- Percentage of total purchased licenses currently in use when Citrix Cloud last evaluated the licenses in use. Citrix Cloud calculates this percentage every five minutes based on unique devices with active connections to the service. The quantity of total purchased licenses is the sum of licenses that have been purchased for Citrix DaaS Standard for Azure that use the Concurrent licensing model.
- The ratio of currently assigned licenses to total purchased licenses and the number of available licenses remaining. The **Total** figure shown in this ratio represents the total number of licenses that are currently owned (as of the "Last Reported"date and time).
- Peak usage statistics. In calculating peak licenses in use, Citrix Cloud retrieves the the maximum number of licenses used in the following time periods:
  - **Last 24 hours:** The maximum number of licenses used at one time during the last 24-hour period.
  - **This Month:** The maximum number of licenses used at one time from the start of the current calendar month.
  - **All Time:** The maximum number of licenses used at one time from the start of the subscription.

  The **Total** figure shown for these peak usage periods represents the total number of licenses that were owned at that point in time. If the total number of owned licenses increases or decreases, and there's a corresponding increase in assigned licenses, the **Total** figure changes to reflect the new number of owned licenses for that point in time. However, if there is no corresponding usage peak, the **Total** figure does not change.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

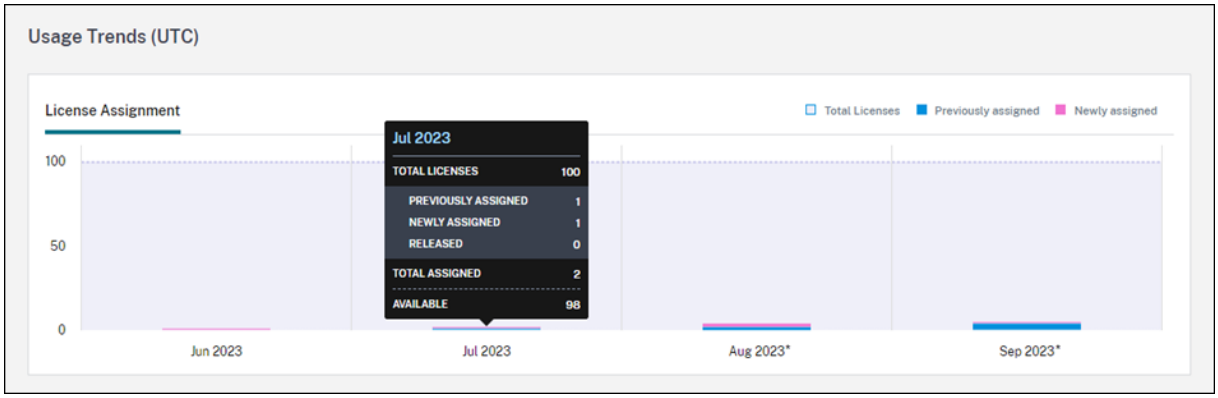
Usage trends

Citrix Cloud displays a breakdown of usage trends for either User/Device or Concurrent User licenses. To view this breakdown, select **View Usage Details** from the licensing summary page.



Trends for users and devices

For User/Devices licenses, the **Usage Trends** section shows you a breakdown of assigned licenses as a chart.

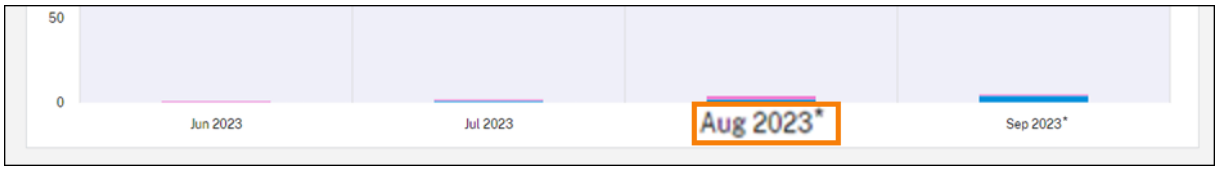


© 1997–2026 Citrix Systems, Inc. All rights reserved.

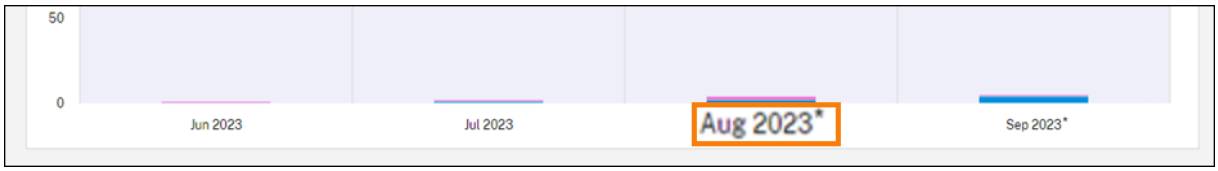
Pointing to an interval on the chart shows you the following information:

- **Total Licenses:** Your total purchased licenses for the cloud service across all entitlements.
- **Previously Assigned:** The number of licenses that were assigned in the previous month. For example, a user accesses the cloud service for the first time in July and is assigned a license. This license is counted as "Newly Assigned"for the month of July. For the month of August, this license is counted as "Previously Assigned."
- **Newly Assigned:** The number of new licenses that were assigned for each month. For example, a user accesses the cloud service for the first time in July and is assigned a license. This license is counted as "Newly Assigned"for the month of July.

Intervals of time in which domain truncation is enabled are marked with an asterisk.



Intervals of time in which domain truncation is enabled are marked with an asterisk.



Trends for concurrent users

For Concurrent User licenses, the **Usage Trends** section shows you the following information:

- **Total Licenses:** Your total purchased Concurrent licenses.
- **Peak Licenses In Use:** The maximum number of licenses assigned for the date range that you select. By default, Citrix Cloud displays peak usage for each month in the current calendar year. To drill down to monthly or hourly peak usage, select the calendar month or day you want to view from the drop-down menu.

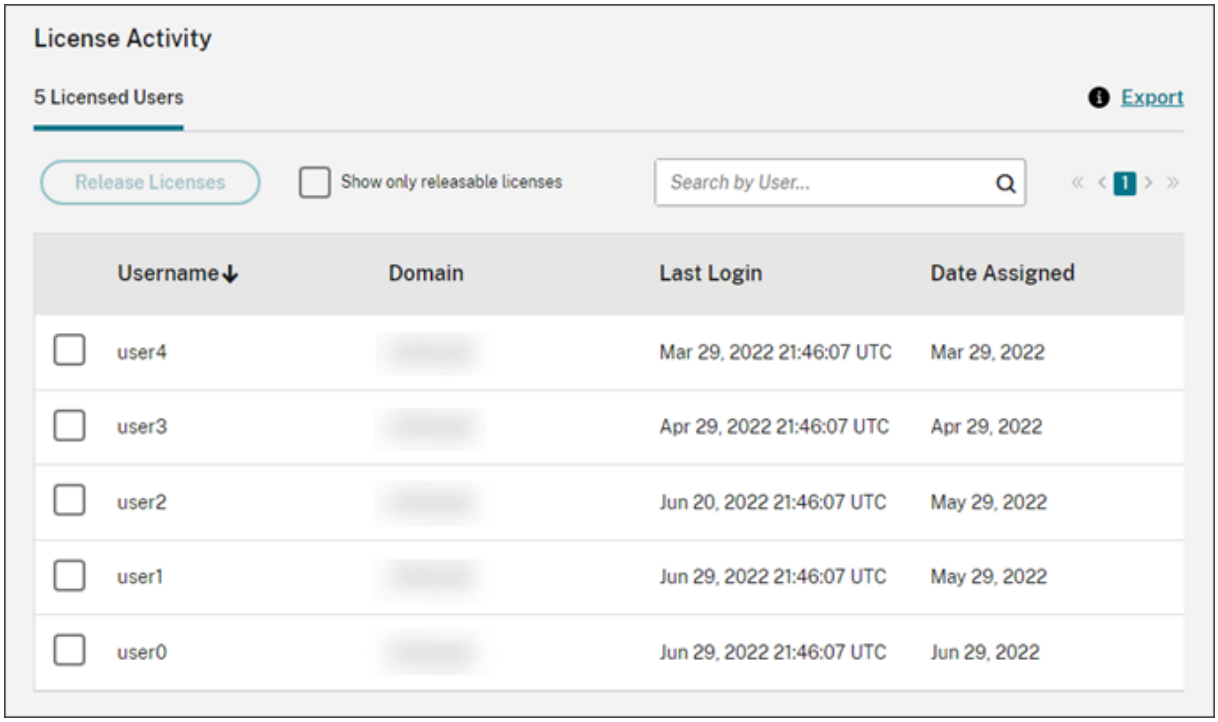
  If the date range you select isn't yet finished, Citrix Cloud displays the current peak usage for the latest interval of time. For example, if you drill down to view a calendar day that's still in progress, the maximum number of licenses is displayed for each hour up to the current moment in time. If the maximum number of licenses increases at the next five-minute counting interval, Citrix Cloud updates the peak usage for the current hour.

Pointing to an interval on the chart reveals the total licenses and peak licenses in use for that interval.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

License activity for users and devices

For User/Device licenses, the **License Activity** section displays a list of individual users who have assigned licenses, and the date when a license was assigned to the user. This section is not available for Concurrent licenses.



You can also filter the list to show only licenses that are eligible for release. See Release assigned licenses in this article.

Release User/Device licenses

Releasing eligible User/Device licenses varies depending on the service subscription type.

- **Yearly service subscriptions:** If you have a yearly subscription, you can release licenses for users that haven't launched an app or a desktop in the last 30 days. You can release multiple licenses in bulk or individually.
- **Monthly service subscriptions:** If you have a monthly subscription, you can release licenses on the first day of each month, regardless of the inactivity period.

When a license is assigned, the assignment period is 90 days and the connection to the service is established. If a user or device hasn't launched an app or desktop for 90 days, these licenses are considered as unused licenses and they are released by Citrix Cloud after 90 days. This process is automated with no actions required by the administrator.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

After the assignment period (90 days), the administrator is allowed to release the licenses manually in the following scenarios only:

- The user is no longer associated with the company.
- The user is on an extended leave of absence.

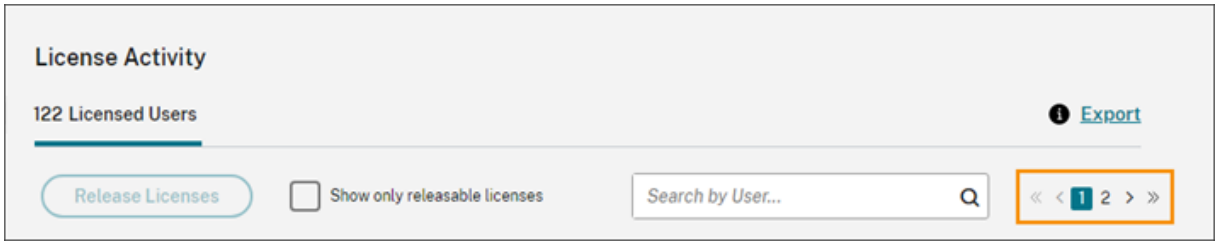
The administrators can release the licenses for devices only when the devices are out of service.

> **Note:**
>
> - It is recommended to follow the automated process of releasing the Licenses. However if the administrator intends to release the licenses before the 90-day period apart from the above mentioned reasons, this might violate the Citrix EULA. Before performing this action, contact Citrix.
> - The administrator can manually release a single license through the UI. Alternatively, the administrator can choose to release licenses using the cloud licensing API. For more information see, APIs to manage Citrix cloud licensing.

Find eligible licenses

If the user or device hasn't launched an app or desktop for 30 days, Citrix Cloud places the license in releasable state. Releasable licenses appear in the Licensed Users or Licensed Devices list with a dark gray checkbox that can be selected. Licenses that aren't releasable displays a light gray checkbox indicating that license cannot be selected.

The list that appears in the **License Activity** section displays up to 100 assigned licenses at a time. If you have more than 100 licenses, use the page controls to move through the list.



To locate eligible licenses quickly, select **Show only releasable licenses**, next to the **Release Licenses** button. This action hides assigned licenses that aren't yet eligible for release.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Select eligible licenses

Select the dark gray checkbox next to each license to select it for release. When you select a license, the **Release Licenses** button becomes active.

You can select all releasable licenses one-by-one and click **Release Licenses**.

Release assigned licenses

1. If needed, click **Show releasable licenses** to display only the users with licenses that are allowed to be released.
2. Select the users you want to manage and then click **Release Licenses**.
3. Review the users you've selected and then click **Release Licenses**.

Release Concurrent User licenses

Concurrent User licenses are released automatically when users sign out or disconnect from their session. You don't need to release these licenses manually.

Monitor licenses and active usage for Endpoint Management

October 26, 2023

License assignment

In general, users are assigned a license upon first use of the cloud service. For Endpoint Management, a license is assigned when a user enrolls a device. After a device is enrolled, the device periodically

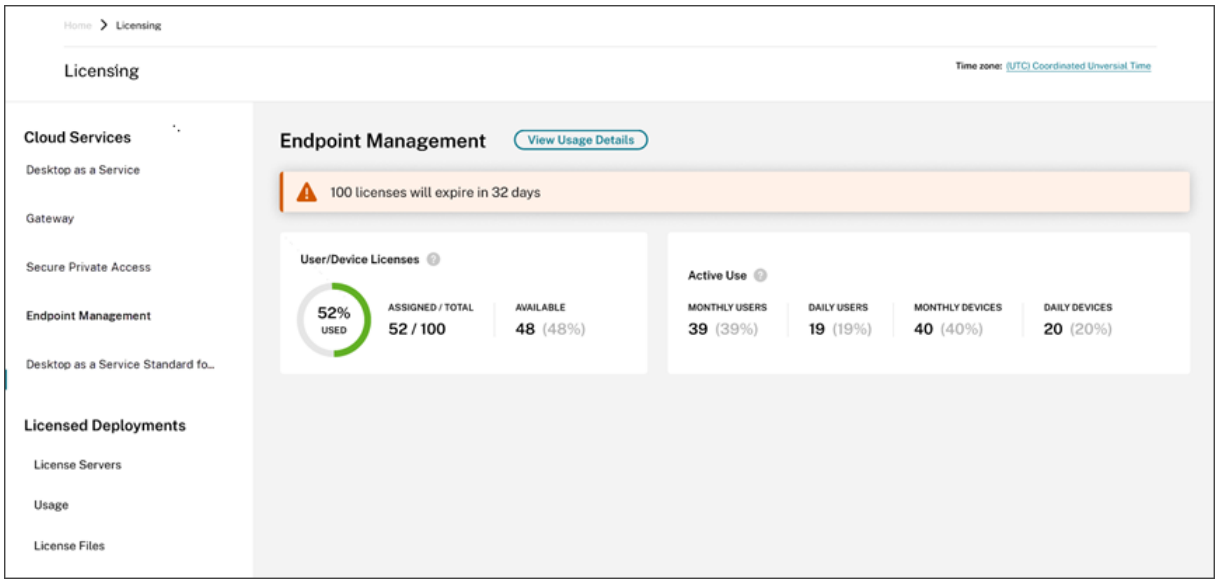
© 1997–2026 Citrix Systems, Inc. All rights reserved.

checks in with Citrix Cloud. Citrix Cloud then uses this "check-in pulse" to calculate monthly usage and helps administrators to remain aware of users' most recent service usage.

First-time use occurs the first time a user enrolls a device or the first time a "check-in pulse" occurs for the device.

Licenses are assigned on a per-user basis. So, if two users enroll and use the same device, two licenses are assigned.

Licensing summary and details



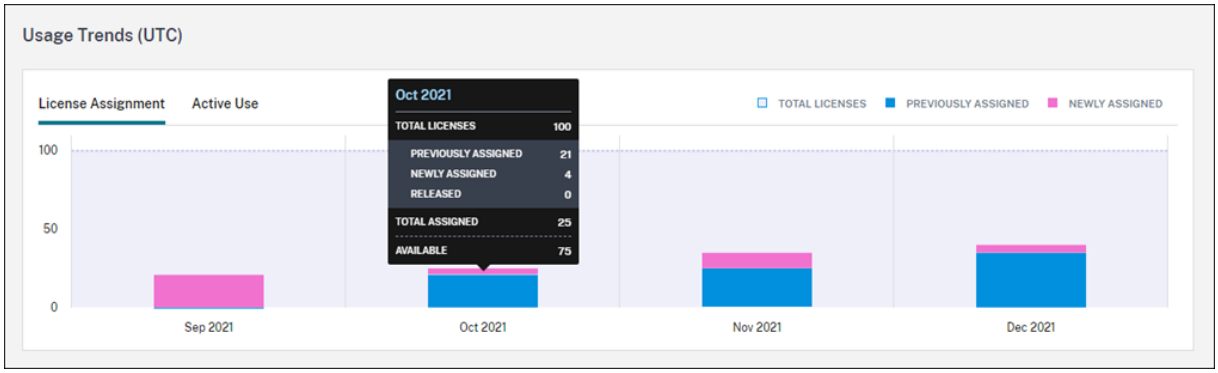
The Licensing summary provides an at-a-glance view of the following information for each supported service:

- Percentage of total purchased licenses assigned. As the percentage approaches 100%, the percentage goes from green to yellow. If the percentage exceeds 100%, the percentage turns red.
- The ratio of assigned licenses to purchased licenses and the number of available licenses remaining.
- Active usage statistics on a monthly and daily basis:
  - Monthly active use refers to the number of unique users that have used the service in the last 30 days.
  - Daily active use refers to the number of unique users that have used the service in the last 24 hours.
- The time remaining before the cloud service subscription expires. If the subscription expires within the next 90 days, a warning message appears.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

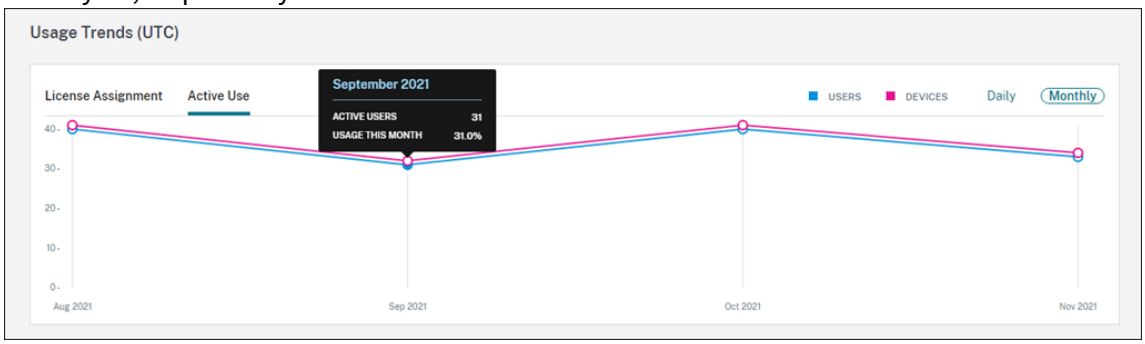
Usage trends

For a detailed view of your licenses, click **View Usage Details**. You can then see a breakdown of usage trends and individual users and devices that are consuming cloud service licenses.



This breakdown shows you the following information:

- **Total Licenses:** Your total purchased licenses for the cloud service across all entitlements.
- **Previously Assigned:** The cloud service licenses that were already assigned at the beginning of each month. For example, if a user is assigned a license in July, that assignment is counted in the Previously Assigned number for August.
- **Newly Assigned:** The number of cloud service licenses that were assigned during each month. For example, a user who accesses the cloud service for the first time in July is assigned a license. This license is counted in the Newly Assigned number for July.
- **Active Use:** Daily and monthly active usage trends over the previous calendar month and calendar year, respectively.

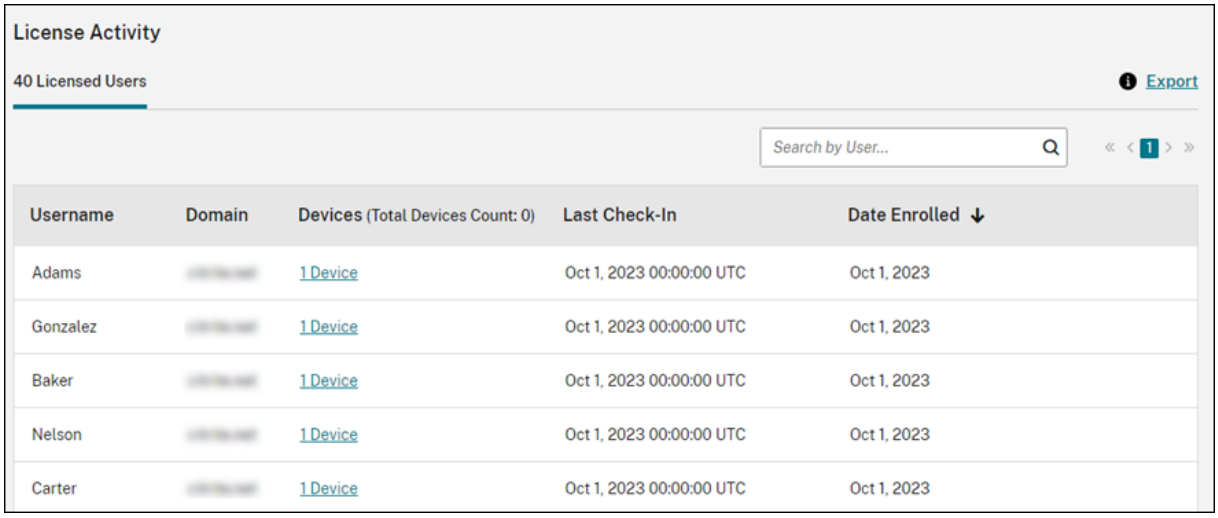


License Activity

The **License Activity** section displays a list with the following information:

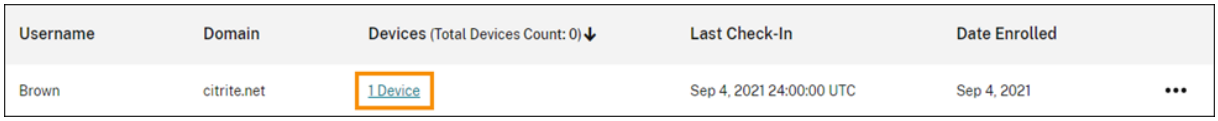
- The individual consumers who have assigned licenses
- The date when licenses were assigned
- The number of enrolled devices and the date of the last check-in for each user

© 1997–2026 Citrix Systems, Inc. All rights reserved.

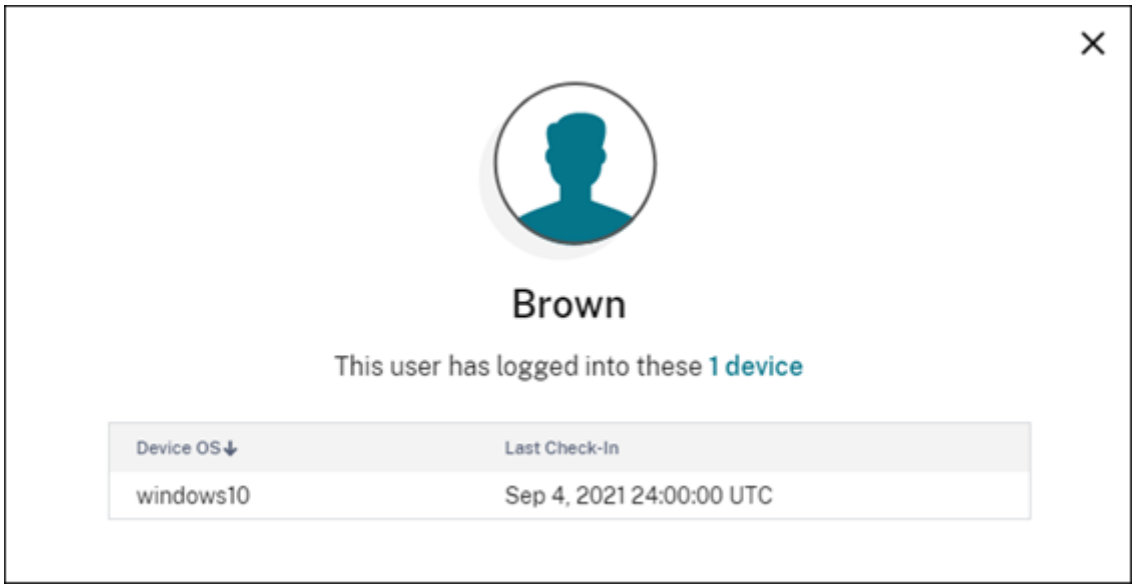


View enrolled devices

To view the number of enrolled devices for a specific user, click the link in the **Devices** column.



Citrix Cloud displays a list of the enrolled devices for the user and the date of the last check-in for each device.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Release assigned licenses automatically

Citrix Cloud automatically releases licenses for users that meet **all** of the following conditions for the last 30 days:

- The user hasn't enrolled a new device.
- The user has an existing device that hasn't checked in with Citrix Cloud.

No other action is required to release eligible licenses.

After eligible licenses are released, users can acquire another license by enrolling a device.

Monitor bandwidth usage for Gateway service

July 17, 2026

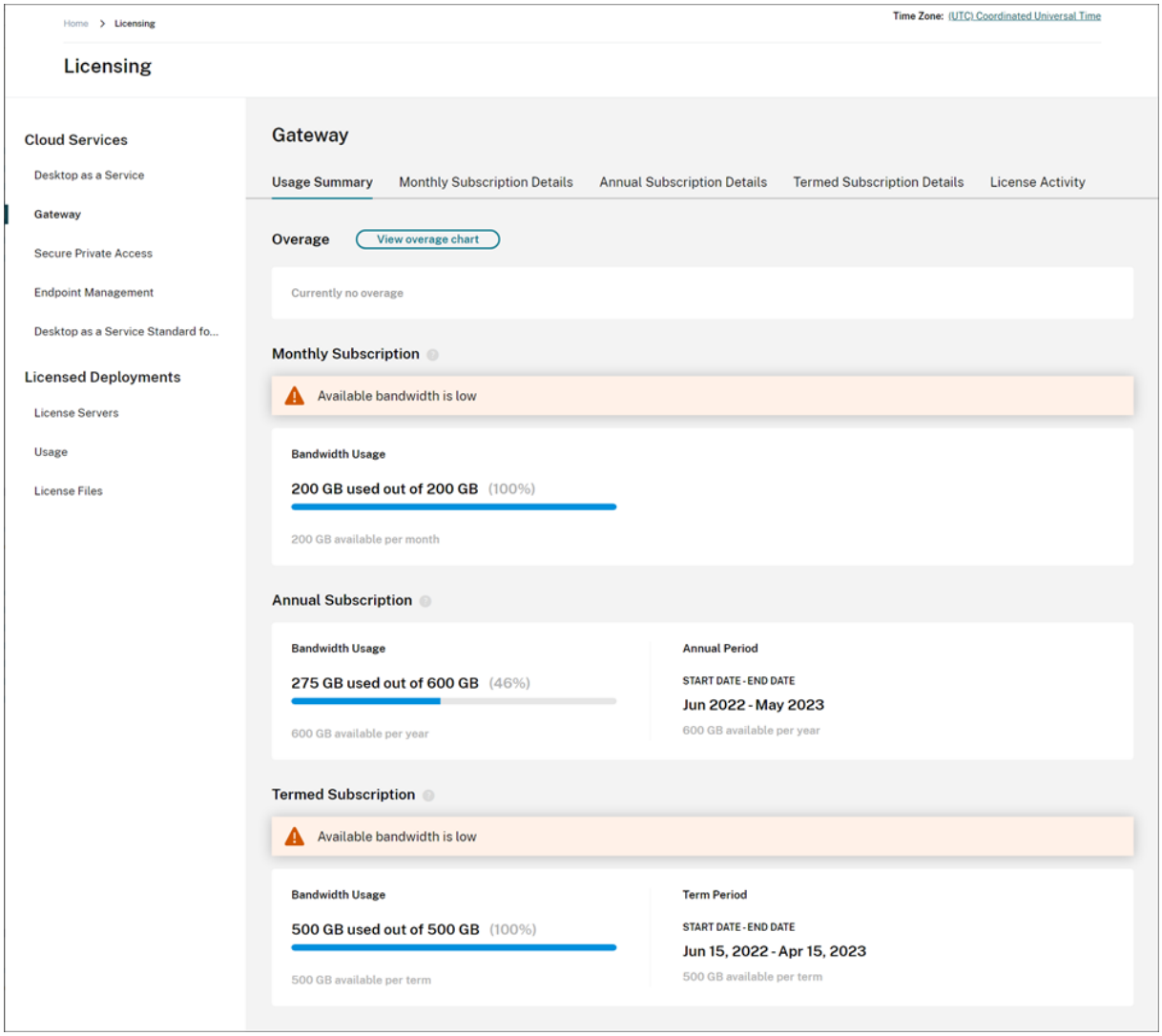
This article describes bandwidth usage through the Gateway service when used with Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service) and Citrix® StoreFront Cloud. Bandwidth consumption for the Gateway service included with the Virtual Apps Essentials service isn't displayed on the **Licensing** page of the Citrix Cloud management console.

> **Note:**
>
> Licensing for the Gateway service helps you understand your bandwidth usage as it relates to using virtual apps and desktops. Citrix® doesn't enforce bandwidth usage allotments in your environment. In the event you overuse your bandwidth allotment, Citrix doesn't interfere with production workloads or the operation of the service. If Citrix changes how the policies for the Gateway service and bandwidth usage are enforced, Citrix notifies you before these changes take effect.

Usage summary

The usage summary provides an at-a-glance view of bandwidth usage for each Gateway service subscription and the total overage across all your subscriptions (monthly, annual, and termed).

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Citrix Cloud™ displays the total amount of bandwidth and the amount of bandwidth consumed for each subscription type.

Depending on the subscription type, Citrix Cloud also displays the billing period for the subscription:

- Monthly subscriptions: Citrix Cloud doesn't display the current billing period. For these subscriptions, the billing period starts on the first day of each month and ends on the last day of that month.
- Annual subscriptions: Citrix Cloud displays the starting and ending dates of the billing period. For these subscriptions, the billing period is one year.
- Termed subscriptions: Citrix Cloud displays the starting and ending dates of the billing period. For these subscriptions, the billing period is the length of time for which the subscription was purchased. For example, if a termed subscription for a period of three years is purchased, the starting and ending dates of the billing period correspond to that three-year interval.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

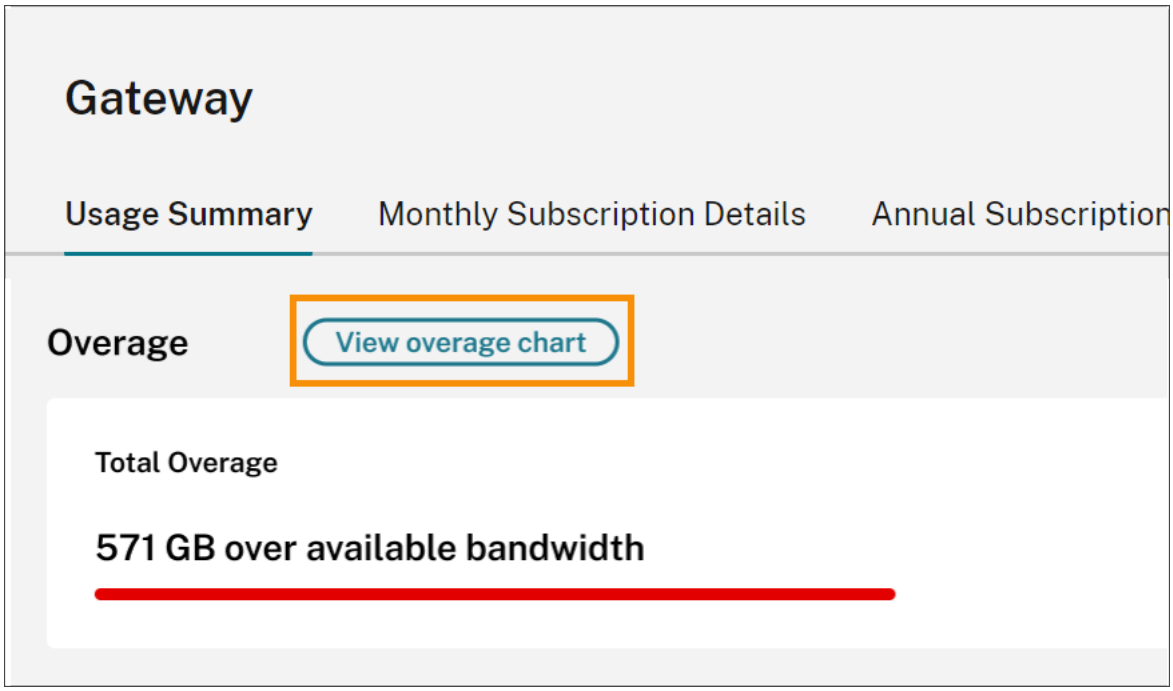
If a subscription expires within 90 days, a warning message appears for that subscription.

Overage

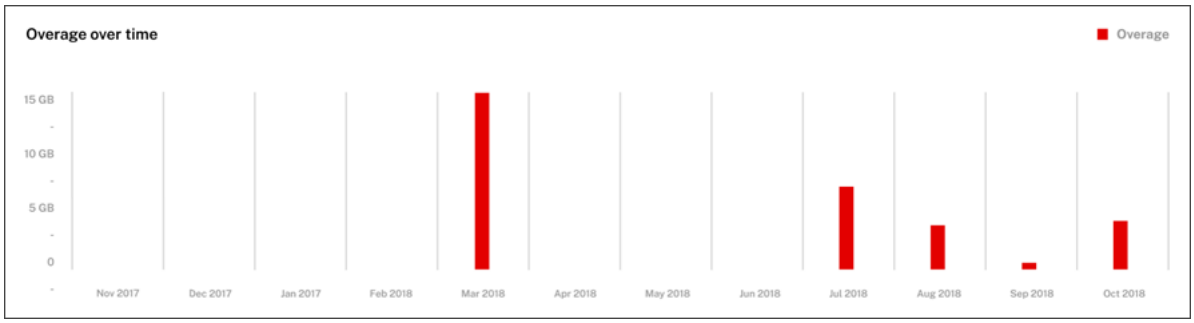
Citrix Cloud calculates overage on a monthly basis across all your subscriptions. If you consume more bandwidth than you've purchased, Citrix Cloud displays the excess bandwidth as overage.

If you have multiple subscriptions, Citrix Cloud measures your bandwidth usage against the subscription that has the earliest ending date first. If you exhaust the bandwidth allotment in that subscription, Citrix Cloud measures your bandwidth usage against the subscription with the next earliest ending date. If you exhaust the bandwidth allotment in all your subscriptions, Citrix Cloud displays excess usage as overage.

The Usage Summary page displays total overage for the current month. To view overage over time, select **View overage chart**.



Citrix Cloud displays a chart of your total overage for the last 12 months.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Overage for the current month doesn't carry over to the next month. When the next month begins, total overage resets to zero.

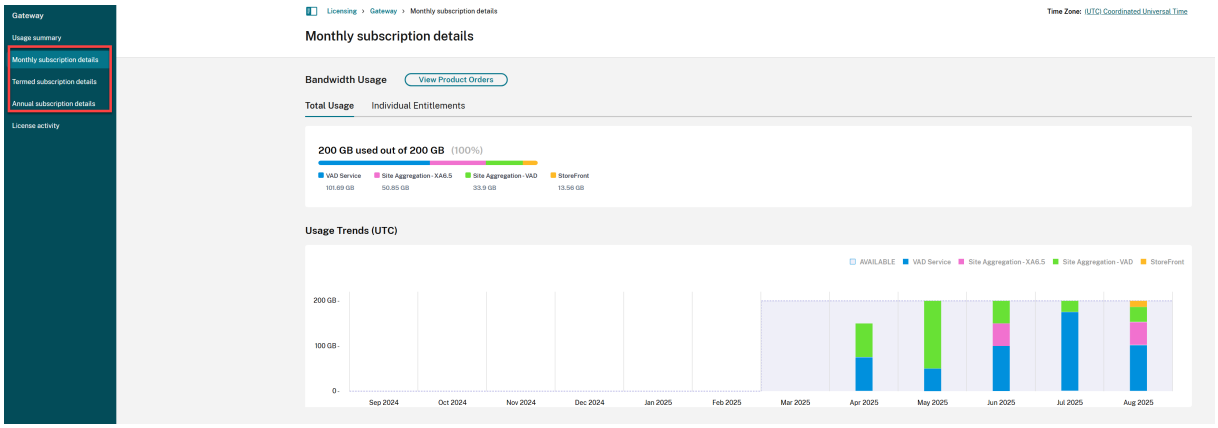
Unused bandwidth

Citrix Cloud automatically resets bandwidth usage for a subscription at the next billing period. If you don't use the full amount of bandwidth during a given subscription period, Citrix Cloud doesn't carry over any unused bandwidth to the next billing period.

For example, if your monthly subscription includes 150 GB of total bandwidth and you use 100 GB of bandwidth in a given month, Citrix Cloud resets usage to zero and displays 150 GB as your total amount of bandwidth at the beginning of the next month. The unused bandwidth isn't added to your total bandwidth allotment.

Usage details

For a detailed view of your subscriptions, select the monthly, annual, or termed subscription details tabs near the top of the console.



For each subscription type, the details tab displays the following information:

- **Total Usage:** The amount of bandwidth consumed out of the total bandwidth available across all subscriptions of a given type. For monthly subscriptions, total usage is shown for the current month. For annual and termed subscriptions, the total usage is cumulative across all of your annual or termed subscriptions.
- **Individual Entitlements:** The total amount of bandwidth consumed for each subscription of a given type. For example, if you have multiple annual subscriptions, this tab shows you the usage breakdown for each annual subscription separately.

The amount of consumed bandwidth is broken down based on access through Citrix DaaS (**VAD Service**) or through your on-premises Virtual Apps and Desktops deployment using site aggregation in

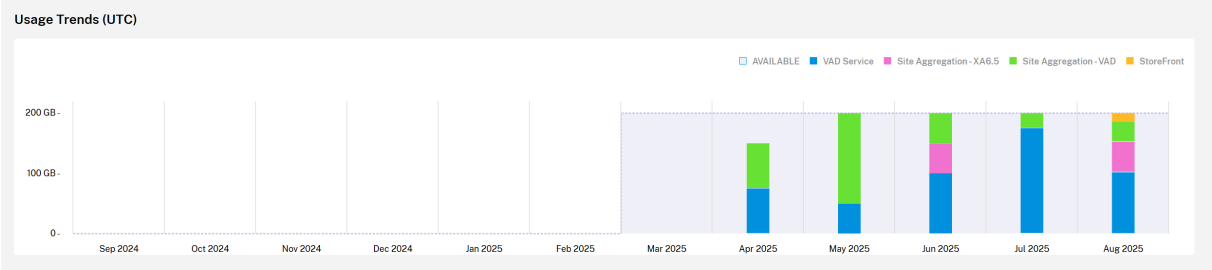
© 1997–2026 Citrix Systems, Inc. All rights reserved.

StoreFront Cloud.

Usage trends

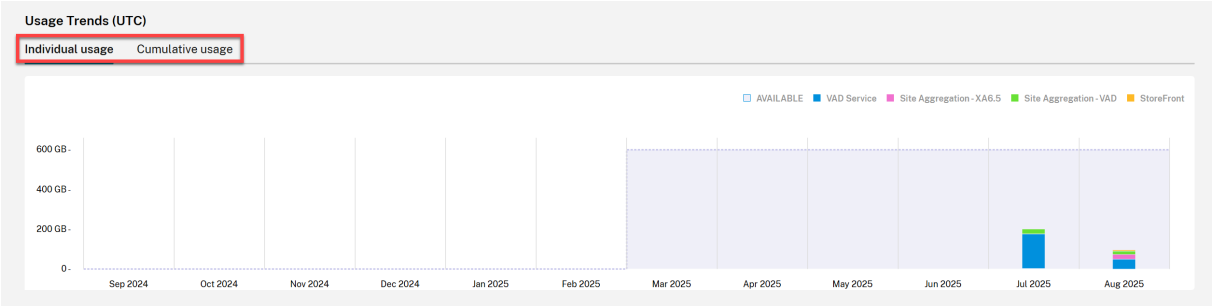
The **Usage Trends** section shows you a breakdown of usage over the last 12 months.

For monthly subscriptions, usage is displayed for each individual month in which it was used.

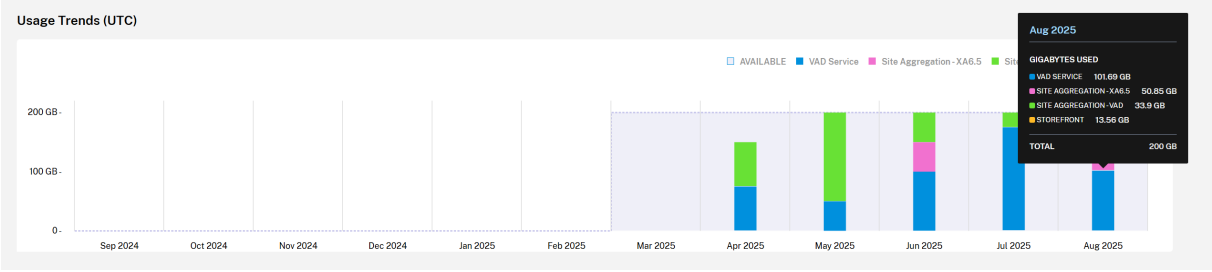


For annual and termed subscriptions, this section includes the following views:

- **Individual usage:** The bandwidth usage that occurred during each individual month of the current billing period.
- **Cumulative usage:** The bandwidth usage that accumulated at each month during the current billing period.



For all subscription types, pointing to a bar in the Usage Trends chart reveals the bandwidth usage for that point in time, broken down by access.

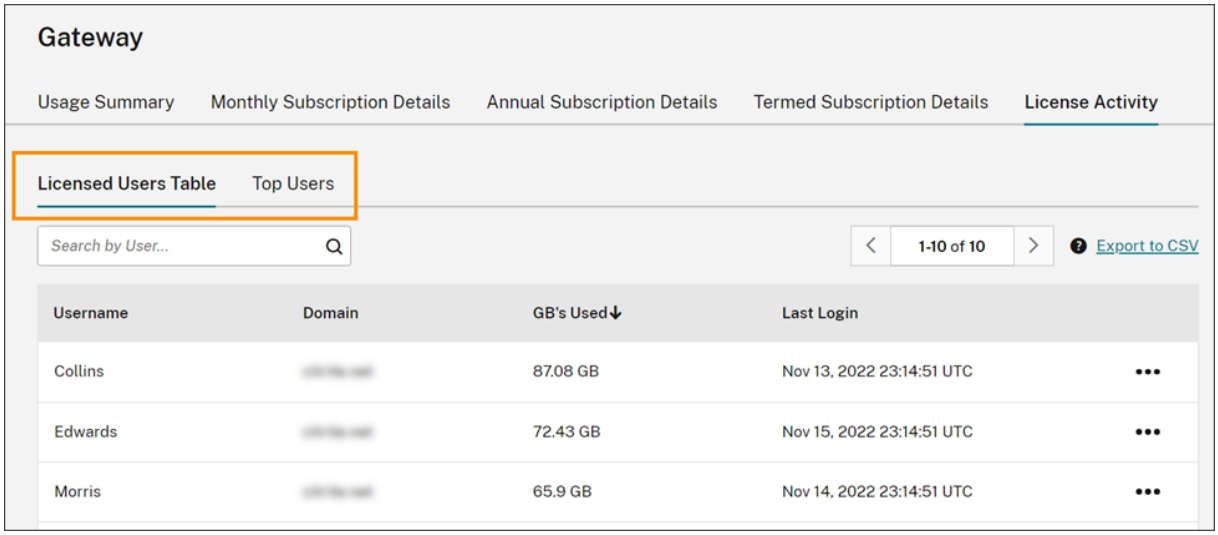


License activity

The **License Activity** section provides views of the following information:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

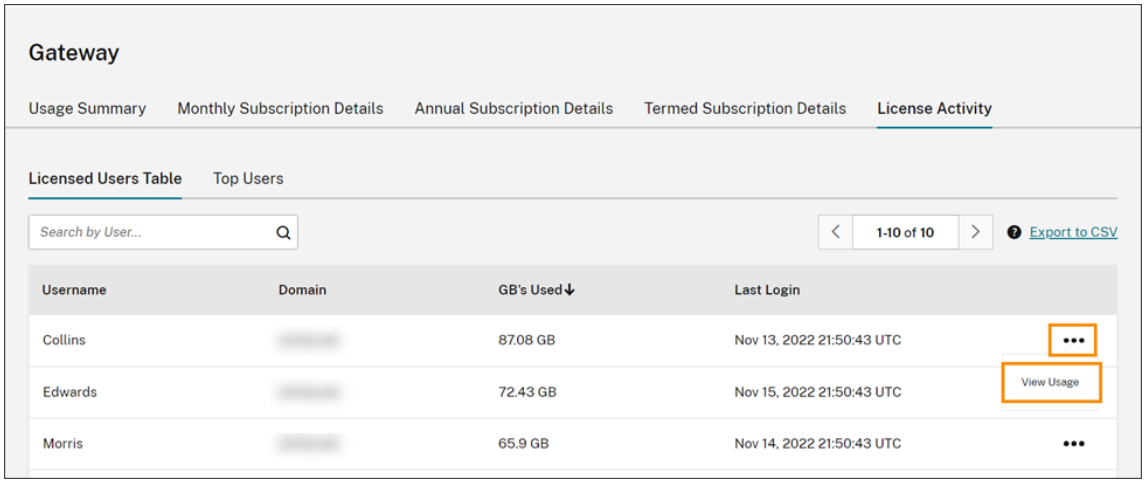
- **Licensed Users:** Displays a list of individual users who have assigned licenses. This list includes the domain to which each user belongs, the amount of bandwidth used over the last 30 days, and the date when the user last used a service that required bandwidth usage.
- **Top Users**: Displays a list of the top 10 users according to bandwidth usage. This list includes a breakdown of usage for each user over the last 30 days according to access type (Citrix DaaS™ or on-premises Virtual Apps and Desktops through site aggregation).



Citrix Cloud displays the bandwidth usage over the last 30 days for a particular user even if they are no longer using a license. When a Gateway service subscription expires, Citrix Cloud still displays the bandwidth that individual users consumed in the 30-day period.

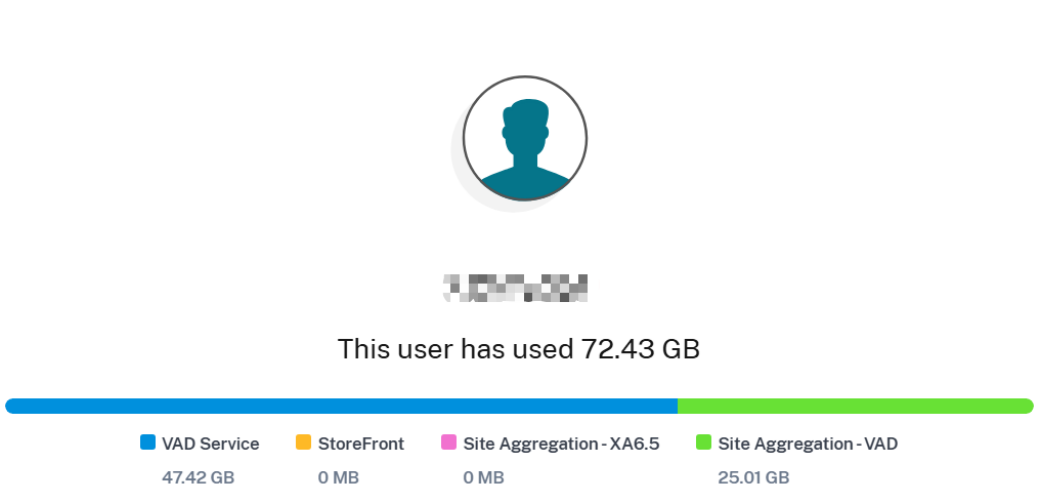
View usage details for a specific user

1. Select **Licensed Users Table** and locate a user in the list that you want to view.
2. Select **View Usage** from the ellipsis menu at the far right of the page.



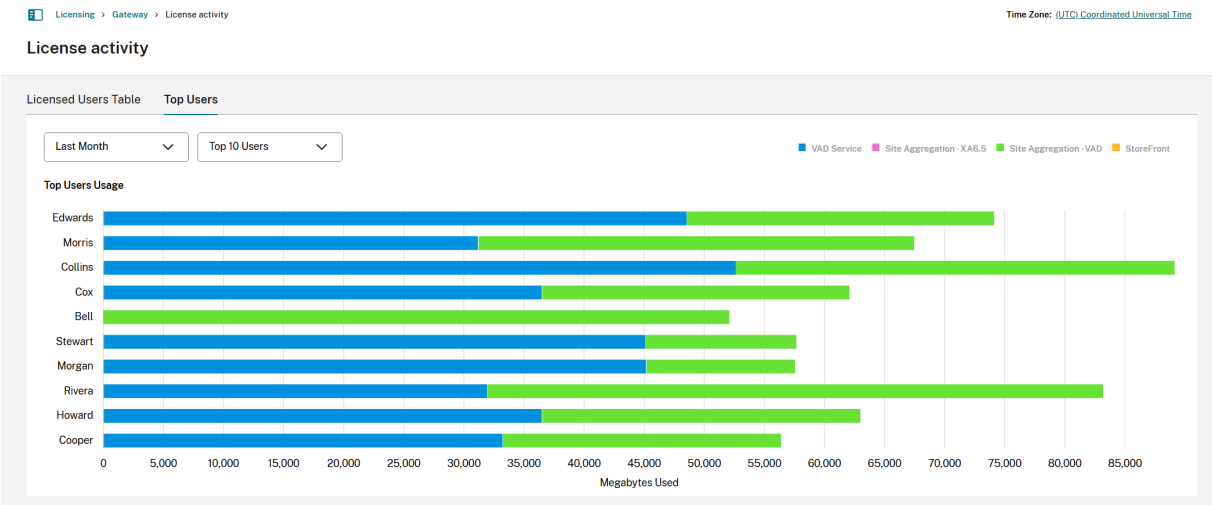
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Cloud displays the user's bandwidth, broken down by access.



View usage details for top users

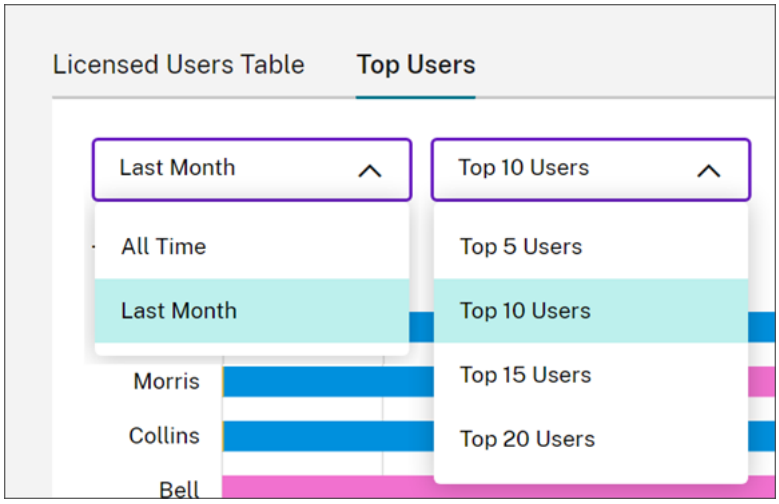
Select **Top Users**.



Citrix Cloud displays a chart of the bandwidth usage for the top users, broken down by access.

By default, the **Top Users** chart displays the top 10 users who have used the most bandwidth during the last 30 days. You can change this view to display the top five, top 15, or top 20 users. You can also change the duration to **All time**, which displays the top users over the life of your subscription. To change this view, select an option from each menu.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



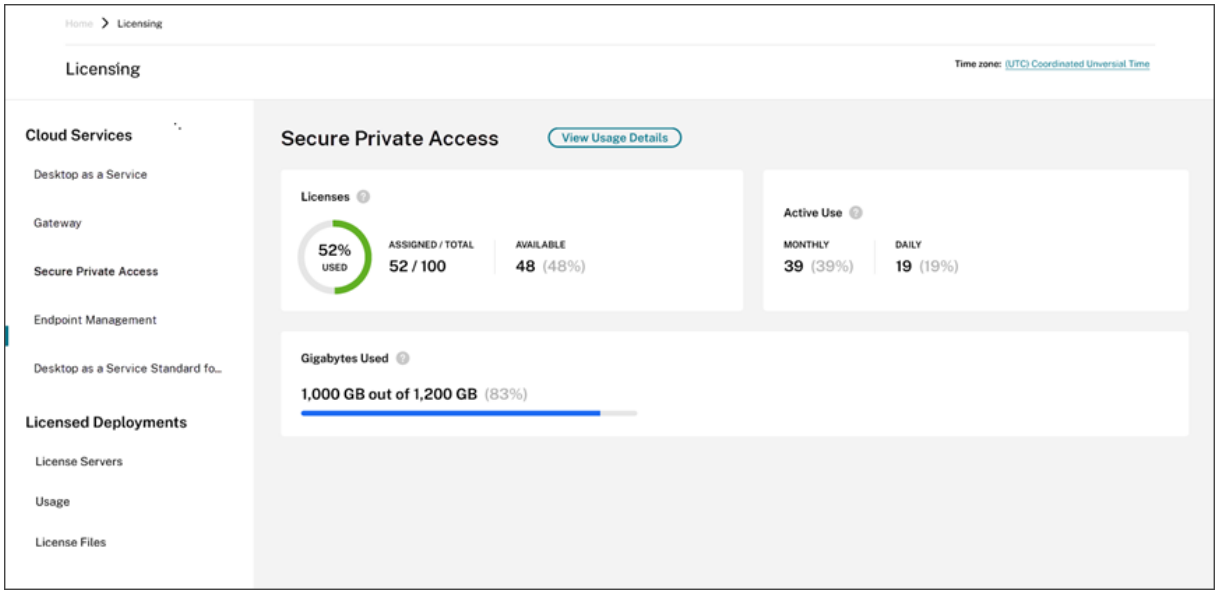
Monitor licenses and usage for Secure Private Access

September 6, 2025

License assignment

A license is assigned when a unique user launches a Web and SaaS apps or TCP and UDP apps for the first time.

Licensing summary



© 1997–2026 Citrix Systems, Inc. All rights reserved.

The Licensing summary shows the following information:

- Percentage of total purchased licenses that are assigned.
    - As the percentage approaches 100%, the percentage goes from green to yellow. If the percentage goes beyond 100%, the percentage turns red.
- The ratio of assigned licenses to purchased licenses and the number of licenses that are available for assignment.
- Active usage statistics on a monthly and daily basis:
    - Monthly active use refers to the number of unique users that have used the service in the last 30 days.
    - Daily active use refers to the number of unique users that have used the service in the last 24 hours.
- The amount of bandwidth consumed out of the total amount of bandwidth for all subscriptions.
- The time remaining before the cloud service subscription expires. If the subscription is about to expire within the next 90 days, a warning message appears.

Licenses and bandwidth used

In Secure Private Access Advanced subscriptions, each user has access to 5 GB of bandwidth per month (60 GB per user, per year). In Secure Private Access Standard subscriptions, each user has access to 1 GB of bandwidth per month (12 GB per user, per year). This bandwidth is pooled across the number of licenses and for the subscription period.

For example, if you buy 100 licenses for three years, you have 18000 GB of total bandwidth (6000 GB per year for three years). This bandwidth is spread across all licensed users for the three-year period. If you buy more subscriptions, Citrix Cloud™ displays the total number of licenses and bandwidth across all your subscriptions.

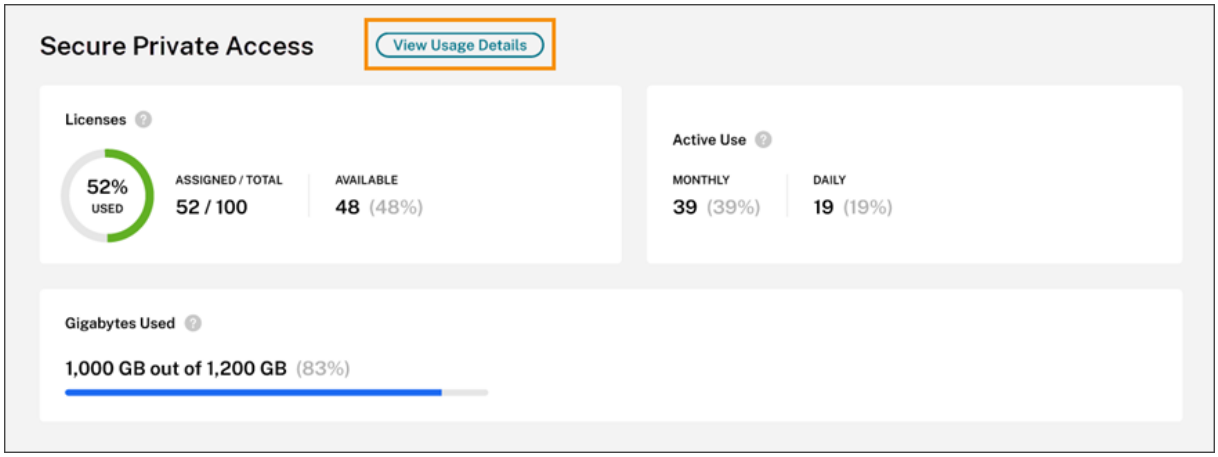
If you don't use the full amount of bandwidth during the subscription period, Citrix Cloud doesn't carry over any unused bandwidth when you renew. When you use more than your purchased bandwidth the subscription expires, the amount of available bandwidth remains at zero when you renew the subscription.

For multiple subscriptions with overlapping terms, the amount of bandwidth associated with each subscription is removed from Licensing when each subscription expires. For example, if you purchased two subscriptions, Citrix Cloud displays the total licenses and total bandwidth across both subscriptions. When the first subscription expires, Citrix Cloud displays only the bandwidth associated with the unexpired subscription.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Usage trends

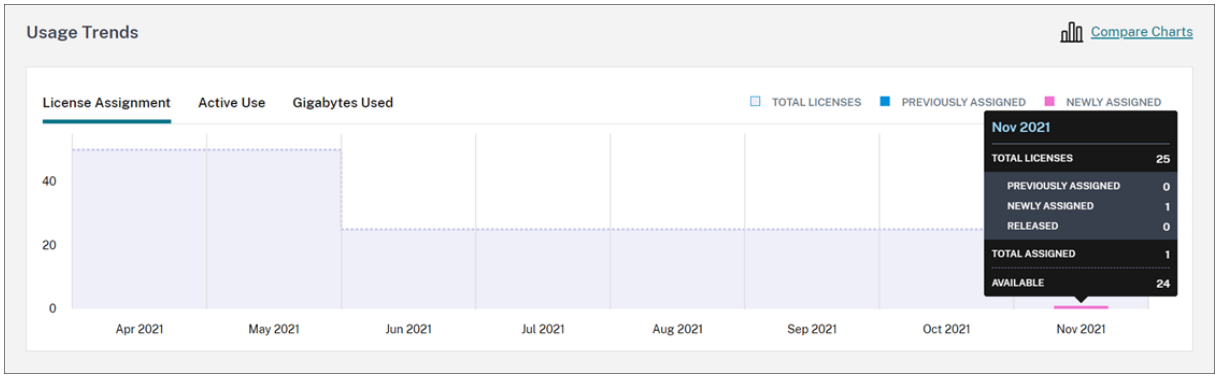
For a detailed view of your bandwidth usage and licenses, click **View Usage Details**.



Citrix Cloud displays a breakdown of bandwidth consumption based on the type of apps that users have access.



You can also see a breakdown of usage trends and individual users who are consuming cloud service licenses and bandwidth.



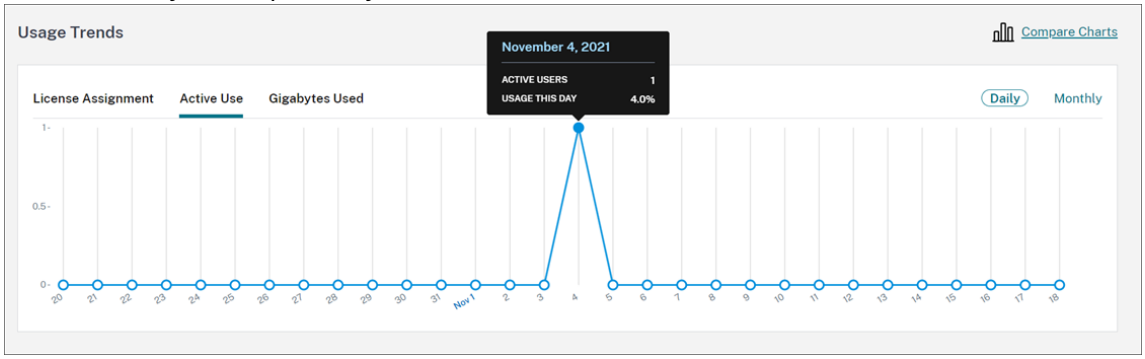
This breakdown, under **Usage Trends**, shows you the following information:

- On the **License Assignment** tab:
  - **Total Licenses:** Your total purchased licenses for the cloud service across all entitlements.

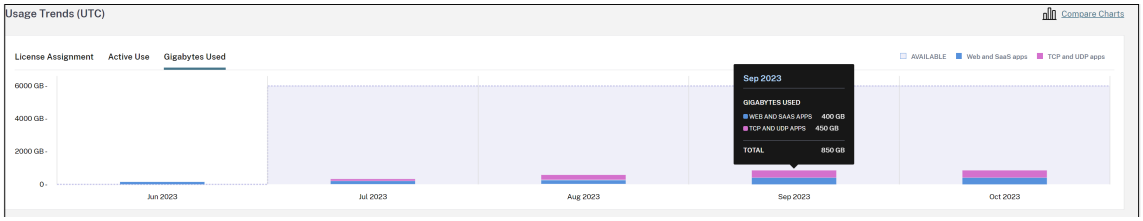
© 1997–2026 Citrix Systems, Inc. All rights reserved.

  - **Previously Assigned:** The cloud service licenses that were already assigned at the beginning of each month. For example, if a user is assigned a license in July, Citrix Cloud counts that assignment in the Previously Assigned number for August.
  - **Newly Assigned:** The number of licenses that were assigned for each month. For example, when you access the cloud service for the first time in July and is assigned a license. Citrix Cloud counts that license in the Newly Assigned number for July.

- On the **Active Use** tab: Daily and monthly active usage trends over the previous calendar month and calendar year, respectively.



- On the **Gigabytes Used** tab: The amount of bandwidth consumed out of the total bandwidth available. It shows per-user usage and per-application information like Web and SaaS apps and TCP and UDP apps.



To compare license assignment, active use, and bandwidth usage trends, select **Compare Charts**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

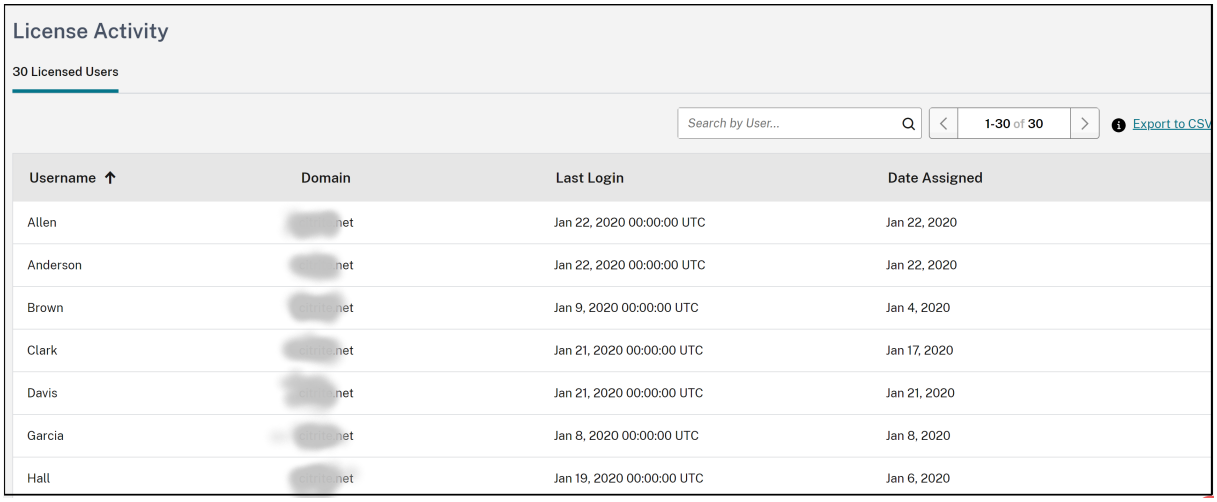


> **Note:**
>
> Usage trends are cumulative for the length of the current subscription term. When you renew the subscription, usage trends are reset at the start of the new subscription term.

License Activity

The **License Activity** section also displays the following information:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- A list of the individual users who have assigned licenses.
- The domain to which the user belongs.
- The date when the user last used the service.
- The date when a license was assigned to the user.

Release assigned licenses

Citrix Cloud automatically releases licenses if you haven't used the service in the last 30 days. No action is required from the Citrix administrator to release the licenses.

When a license is released, the number of remaining licenses increases and the number of assigned licenses decreases accordingly. After a license is released, you can acquire another license by signing in and using the cloud service.

Monitor Citrix Managed Azure resource consumption for Citrix DaaS™

September 6, 2025

When you purchase an entitlement to Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service), you can also purchase the Citrix Azure Consumption Fund that allows you to use resources in a Citrix Managed Azure subscription. You can use these resources for delivering apps and desktops to your users alongside your on-premises VDAs.

When you buy the Citrix Azure Consumption Fund, you can pay for consumption using one of the following methods:

- Pay-as-you-go: For the Citrix Managed Azure resources that you use during a given month, Citrix bills you during the following month. Citrix Cloud™ displays your usage as overage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Prepaid consumption: You can pre-pay for consumption on a monthly or yearly (termed) basis. For any usage that exceeds your pre-paid consumption, Citrix Cloud displays this usage as overage. For any overage in a given month, Citrix bills you during the following month.

Each consumption unit is valued at $1.00 USD. The Licensing console in Citrix Cloud helps you track the units that you use.

To estimate consumption costs, use the Citrix Managed Azure Consumption Calculator. To estimate consumption and licensing costs for Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure), use the Licensing and Consumption Calculator.

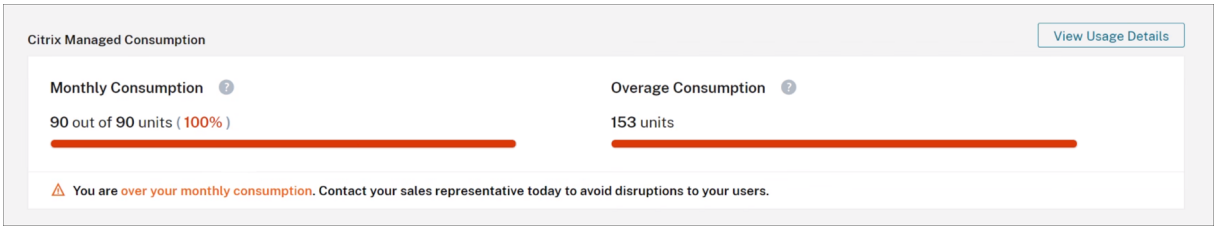
Supported products

Consumption monitoring is available for the following editions of Citrix DaaS:

- Citrix DaaS Advanced (formerly Virtual Apps Advanced)
- Citrix DaaS Premium (formerly Virtual Apps Premium)
- Citrix DaaS Advanced Plus (formerly Virtual Apps and Desktops Advanced)
- Citrix DaaS Premium (formerly Virtual Apps and Desktops Premium)
- Citrix DaaS Standard for Azure (formerly Virtual Apps and Desktops Standard for Azure)

Consumption summary

The Citrix Managed Consumption section displays a summary of the units that you've used in your Consumption Fund.



Monthly Consumption shows the number of consumption units that you've used for the current month out of the total number of monthly Consumption Fund units that you've purchased. Monthly consumption resets each month. Unused consumption units aren't carried over to the next month.

Term Consumption shows the number of consumption units that you've used out of the total number of term Consumption Fund units that you've purchased. As with monthly consumption units, unused term consumption units aren't carried over to the next year.

Overage Consumption shows the number of consumption units that you've used beyond the number of units in your Azure Consumption Fund. If you use Citrix Managed Azure resources on a pay-as-you-go basis, your consumption appears as overage by default.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

How overage is measured

If you use the Azure Consumption Fund on a pay-as-you-go basis, Citrix Cloud displays the number of consumption units that you've used for the current month as overage.

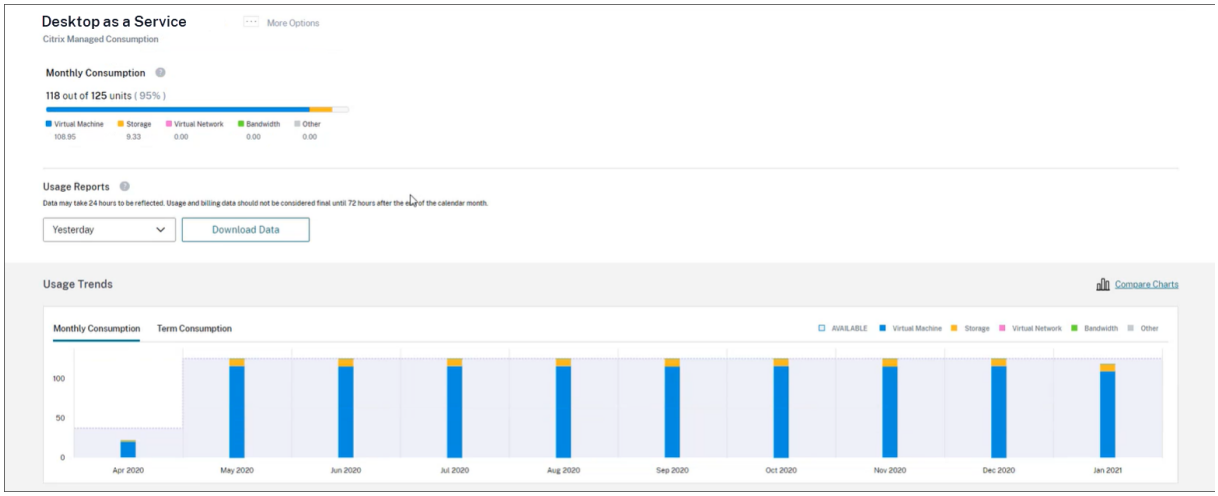
If you prepaid for consumption on either a monthly or yearly basis, Citrix Cloud displays the number of monthly or term consumption units that you've used for the current month or year. If you consume more units than you purchased, Citrix Cloud displays the excess units as overage.

If you prepaid for consumption on both a monthly and a yearly basis, Citrix Cloud measures your consumption against your purchased monthly units first. After those units are consumed, Citrix Cloud measures your consumption against your yearly units. After those units are consumed, Citrix Cloud displays any excess units that you consume as overage.

If you buy additional consumption units and your account has existing overage, the new consumption units are not applied to the overage. The new consumption units are only applied to usage that occurs after those units are purchased.

Consumption details

For a detailed view of your consumption units, click **View Usage Details** at the far right of the summary. The details page displays breakdowns of your consumption and usage trends.



Usage reports

You can download usage information as a CSV file for an interval that you specify. Click **Download Data** to generate and download a CSV file to your local machine.

Data can take up to 72 hours after the end of a day or month to reflect all usage.

The CSV file includes the following sections:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Report summary that shows the consumption units available before and after the report date range, total usage charges, and pending overage.

Data may take 24 hours to be reflected. Usage and billing data should not be considered final until 72 hours after the end of the calendar month.			
Org ID	51938754		
Report Date	12/3/2021		
Date Start	11/1/2021		
Date End	11/30/2021		
Report Summary			
	Credits	Debits	
Monthly Consumption Units Available before 11/01/2021	$0		
Termed Consumption Units Available before 11/01/2021	$0		
Trial Consumption Units Available before 11/01/2021	$0		
Total Usage to Charge		$851.96	
Expired Consumption Commitment		$0.00	
Total	$0.00	$851.96	

Monthly Consumption Units Available after 11/30/2021	$0		
Termed Consumption Units Available after 11/30/2021	$0		
Trial Consumption Units Available after 11/30/2021	$0		
Pending Overage by 11/30/2021	$0.00		

- Daily summary that shows the total usage charge, remaining monthly and term funds, and overage charge for each day of the report date range.

Daily Summary				
Date	Total Usage	Remaining Monthly Funds	Remaining Termed Funds	Overage Amount
11/1/2021	$28.40	$0	$0	$0
11/2/2021	$28.40	$0	$0	$0
11/3/2021	$28.40	$0	$0	$0
11/4/2021	$28.40	$0	$0	$0
11/5/2021	$28.39	$0	$0	$0
11/6/2021	$28.39	$0	$0	$0
11/7/2021	$28.40	$0	$0	$0
11/8/2021	$28.40	$0	$0	$0

- Metered usage of Azure VMs, network connections, Azure storage, and bandwidth for each day of the report date range.

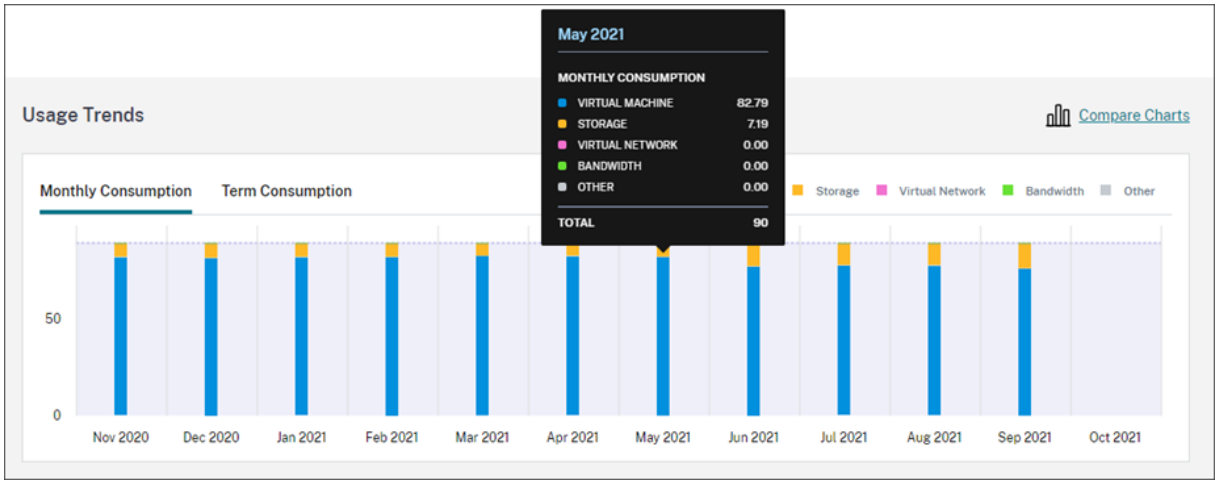
Date	Citrix Meter Name	Citrix Meter Description	Catalog Id	Catalog Name	Citrix Meter Region	Citrix Meter Category	Citrix Meter Sub Category	Citrix Meter Unit	Quantity	SRP	Total	Total Charged
11/1/2021	Bandwidth	Data Transfer Out - Zone 1	07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	Bandwidth		10 GB	0.0000444	$1.13	$0.00	$0.00
11/1/2021	Bandwidth	Data Transfer Out - Zone 1	f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	Bandwidth		10 GB	0.0000018	$1.13	$0.00	$0.00
11/1/2021	Bandwidth	Data Transfer Out - Zone 1	N/A	N/A	None	Bandwidth		10 GB	0.0064263	$1.13	$0.01	$0.01
11/1/2021	Bandwidth	Data Transfer Out - Zone 1	cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	Bandwidth		10 GB	0.0000137	$1.13	$0.00	$0.00
11/1/2021	Bandwidth	Data Transfer Out - Zone 1	6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	Bandwidth		10 GB	0.0000015	$1.13	$0.00	$0.00
11/1/2021	Bandwidth	Data Transfer Out - Zone 1	dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	Bandwidth		10 GB	0.0000073	$1.13	$0.00	$0.00
11/1/2021	Bandwidth	Data Transfer Out - Zone 1	e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	Bandwidth		10 GB	0.0000334	$1.13	$0.00	$0.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Machines Dv3/DSv3 Series - D2 v3/D2s v3 - US East		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	US East	VirtualMachine		10 Hours	2.4	$1.25	$3.00	$3.00
11/1/2021	Virtual Network Peering	Ingress	N/A	N/A	None	VirtualNetwork		100 GB	0.00016714	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering	Egress	f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	VirtualNetwork		100 GB	0.00000034	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering	Ingress	cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	VirtualNetwork		100 GB	0.00000323	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering	Ingress	07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	VirtualNetwork		100 GB	0.00000422	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering	Egress	07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	VirtualNetwork		100 GB	0.00000165	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering	Ingress	dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	VirtualNetwork		100 GB	0.00000307	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering	Egress	e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	VirtualNetwork		100 GB	0.00000129	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering	Egress	cb7516c0-33e7-485a-9eb0-d84b7f2e9c5a	Windows-11-MultiSession	None	VirtualNetwork		100 GB	0.00000148	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering	Egress	dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	None	VirtualNetwork		100 GB	0.00000115	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering	Ingress	e86cee4e-1930-4d87-b2e5-3b189bb3e6e3	Win-11-SS-22	None	VirtualNetwork		100 GB	0.00000342	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering	Egress	N/A	N/A	None	VirtualNetwork		100 GB	0.00012714	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering	Egress	6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	VirtualNetwork		100 GB	0.00000121	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering	Ingress	6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	None	VirtualNetwork		100 GB	0.00000323	$1.30	$0.00	$0.00
11/1/2021	Virtual Network Peering	Ingress	f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	None	VirtualNetwork		100 GB	0.00000094	$1.30	$0.00	$0.00
11/1/2021	General Block Blob - Read Operations		N/A	N/A	None	Storage		100000000	0.00000016	$4.68	$0.00	$0.00
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		N/A	N/A	US East	Storage		1 /Month	0.400032	$7.64	$3.06	
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		dfb04e0a-b08f-4f0a-af95-fff7cdd6cd83	AVD Desktops	US East	Storage		1 /Month	0.033336	$7.64	$0.25	$0.25
11/1/2021	Standard HDD Managed Disks - S10 - Disks - US East		6dbcda61-cdf6-4135-86e0-76e2f5f45204	Windows-11-SingleSession	US East	Storage		1 /Month	0.100008	$7.64	$0.76	$0.76
11/1/2021	Virtual Machines Av2 Series - A2 v2 - US East		N/A	N/A	US East	VirtualMachine		100 Hours	0.48	$11.83	$5.68	$5.68
11/1/2021	Premium SSD Managed Disks - P10 - Disks - US East		f061eeac-2507-459c-ab99-71fde94b318e	Finance desktops	US East	Storage		1 /Month	0.033336	$19.22	$0.64	$0.64
11/2/2021	Bandwidth	Data Transfer Out - Zone 1	07f1d01f-9ffb-472e-93ab-ae2d7393202a	Win-11-MS-2	None	Bandwidth		10 GB	0.0000235	$1.13	$0.00	$0.00

© 1997–2026 Citrix Systems, Inc. All rights reserved.

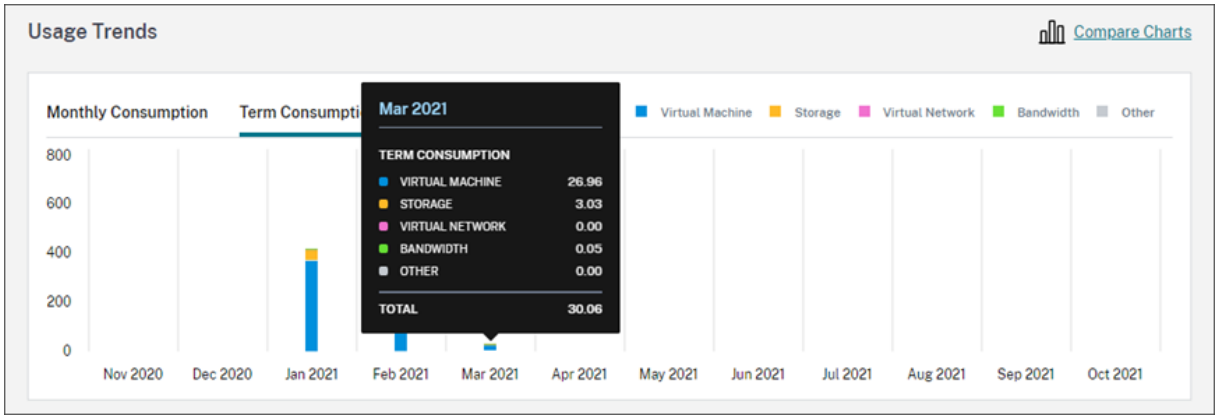
Usage trends and consumption activity

The **Usage Trends** section displays a chart of the Citrix Managed Azure resources that you've used. Pointing to a bar on the chart displays the quantity of resources that you consumed for that month, including virtual machines, storage, virtual network resources, and bandwidth.

Select **Monthly Consumption** to view your monthly consumption for the previous 12 months.

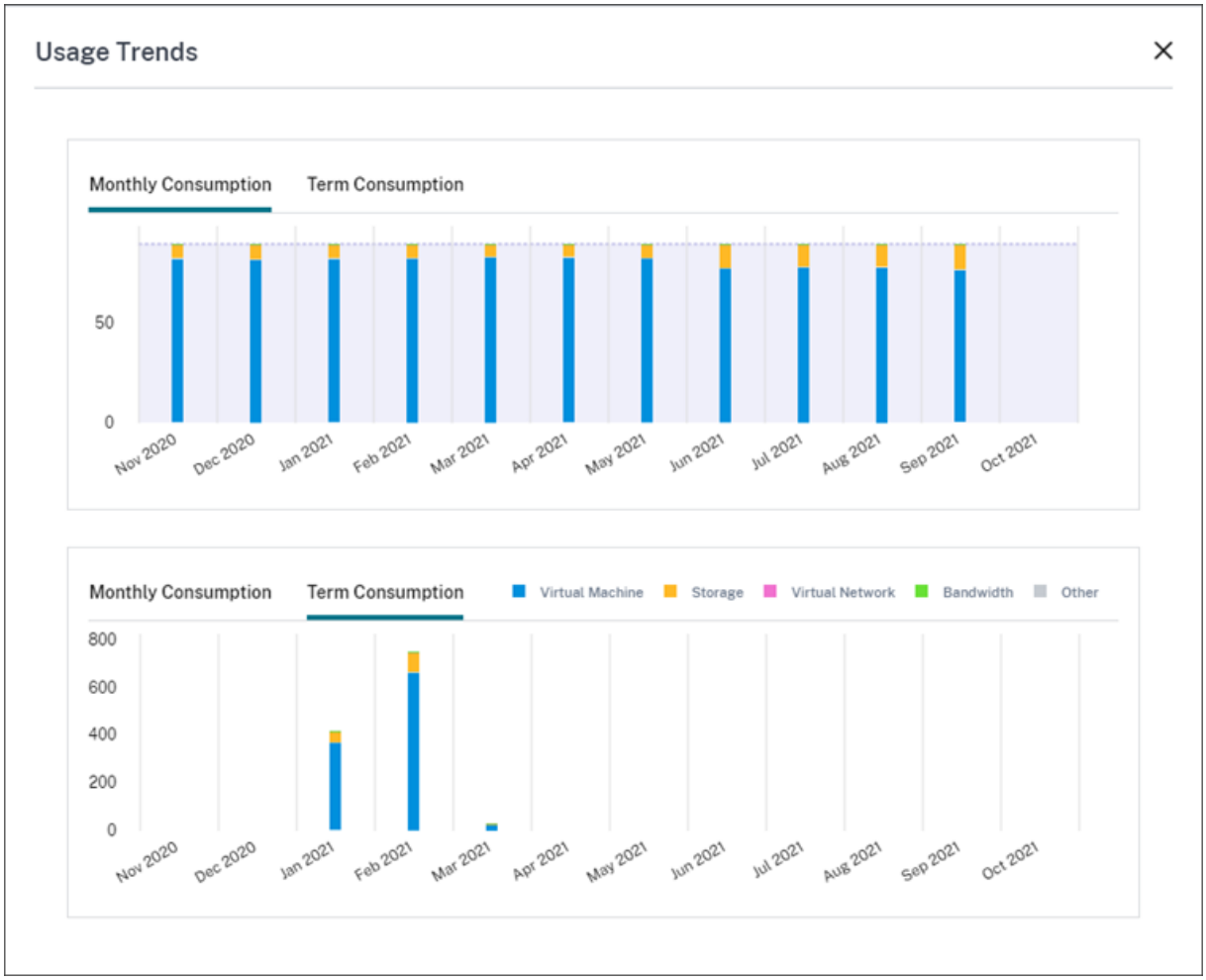


Select **Term Consumption** to view your term consumption for each month during the previous year.

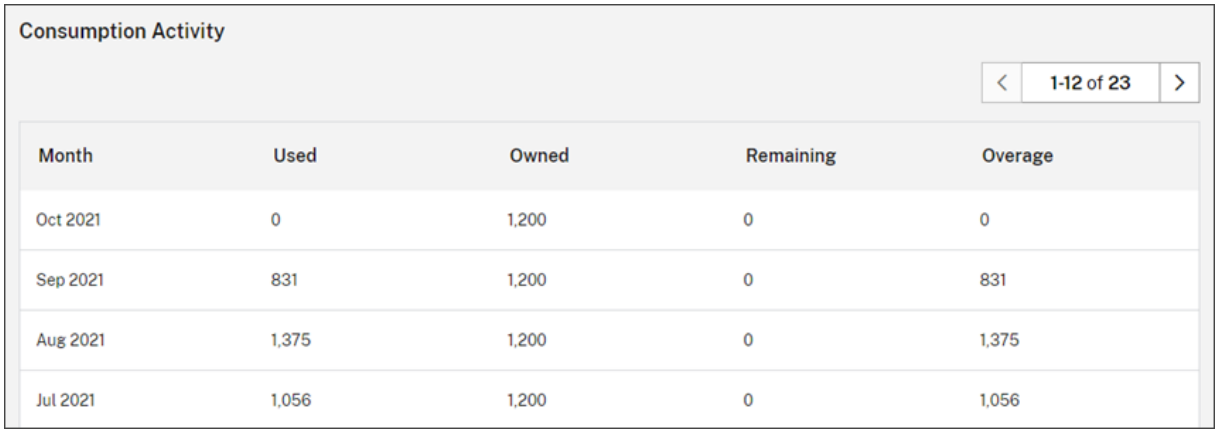


If you purchased both monthly and yearly consumption units, select **Compare Charts** at the far right of the chart to view monthly and term consumption trends in a single view.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Consumption Activity** section also displays a list of your consumption units for each month.



Month	Used	Owned	Remaining	Overage
Oct 2021	0	1,200	0	0
Sep 2021	831	1,200	0	831
Aug 2021	1,375	1,200	0	1,375
Jul 2021	1,056	1,200	0	1,056

Consumption activity includes the following information:

- **Used:** The number of units that were used during each month.
- **Owned:** The total number of purchased units for each month.
- **Remaining:** The number of purchased units that were unused during each month.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Overage:** The number of consumed units that exceeded your purchased units during each month.

Release assigned licenses

The time at which license assignments become eligible for release depends on the Consumption Fund units that you purchased.

You can release inactive licenses after 30 days if:

- You don't use a Citrix Managed Azure subscription with your service deployment.
- You purchased yearly consumption units to use with your service deployment.

You can release inactive licenses during the current month, provided no users or devices launched apps or desktops, if:

- You purchased monthly Consumption Fund units to use with your service deployment.
- You purchased both monthly and yearly Consumption Fund units.

For instructions for releasing eligible licenses, see the following articles:

- Citrix DaaS (User/Device model): Release assigned licenses
- Citrix DaaS Standard for Azure: Release assigned licenses

Monitor licenses and usage for on-premises deployments

March 5, 2026

> **Important:**
>
> Usage insights is applicable only for traditional license files and is not applicable for License Activation Service.

The licensed deployments experience in Citrix Cloud™ consists of the following functions:

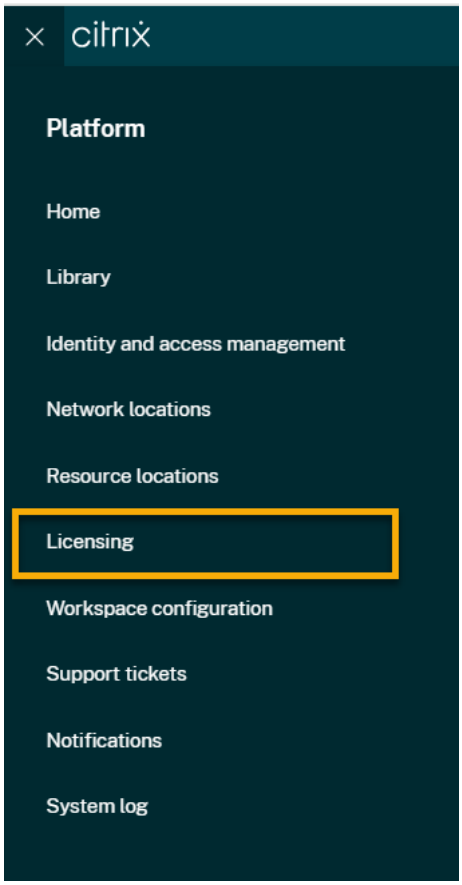
- Product registration: Register your existing Citrix License Servers with Citrix Cloud to get additional usage insights and reporting about your deployments.
- License Server status: View the status of your Citrix License Servers to understand which ones are successfully reporting usage and when they last reported usage to Citrix Cloud.
- Usage insights: View how many licenses are installed and in use across your Citrix License Servers and gain insight into historic license usage trends.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Supported products

Citrix License Server usage insights are available for all Virtual Apps and Desktops editions under the Concurrent and User/Device licensing models.

To view Citrix License Server usage insights, select **Licensing** from the console menu and then select **Licensed Deployments**.



Prerequisites

To use Citrix License Server usage insights, ensure you have the following items:

- A Citrix License Server version 11.15.0.0 or later
- A Citrix Cloud account
- Network access from the Citrix License Server to Citrix Cloud

Connectivity requirements

To register your License Server successfully with Citrix Cloud, ensure that the following addresses are contactable:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- https://las.cloud.com:443
- https://customers.citrixworkspacesapi.net:443
- https://citrix.cloud.com/ (for accessing the admin console to enter the code and view license server status)
- https://trust.citrixnetworkapi.net (for retrieving a code)
- https://trust.citrixworkspacesapi.net/ (for confirming the license server is registered)
- https://cis.citrix.com (for data upload)
- https://core-eastus-release-a.citrixworkspacesapi.net
- https://core.citrixworkspacesapi.net
- ocsp.digicert.com port 80
- crl3.digicert.com port 80
- crl4.digicert.com port 80
- ocsp.entrust.net port 80
- crl.entrust.net port 80

Connect to Citrix Cloud

To enable Citrix License Server usage insights, you perform the following tasks:

1. Enable usage insights for your license servers using the Licensing Manager console. For more information, see Share usage statistics in the Licensing product documentation.
2. Review the connectivity requirements described in Connectivity requirements in this article and ensure the addresses are contactable. If you are using a proxy server with Citrix License Server, ensure that the proxy server is configured as described in Step 5 Configure a proxy server in the Licensing product documentation.
3. Register your license server with Citrix Cloud as described in Register on-premises products with Citrix Cloud.

View on-premises product license usage

Citrix License Server usage insights provides visibility into license usage across your entire Citrix estate. You can access usage reporting that helps you:

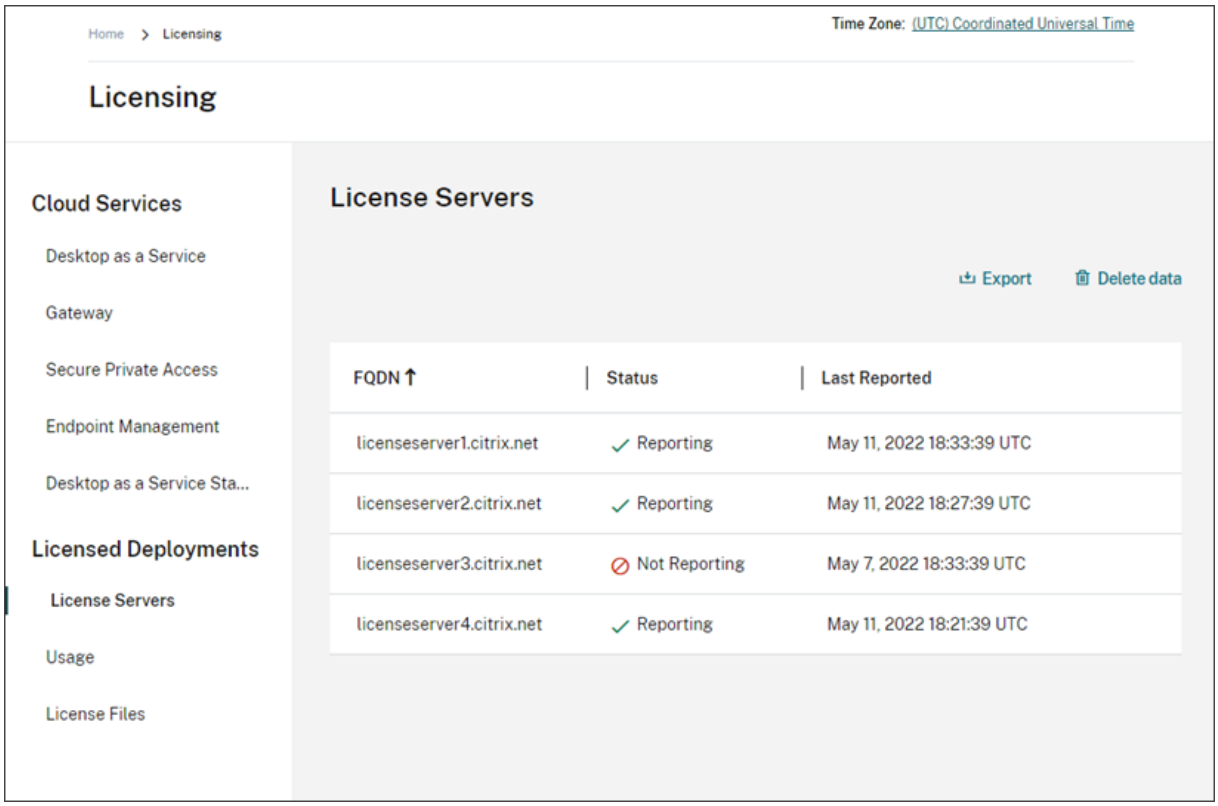
- Understand how many license servers are deployed and registered, and if they are reporting usage information to Citrix Cloud.
- Get visibility into Concurrent and User/Device license usage for Virtual Apps and Desktops.
- Gain insight into aggregate Concurrent and User/Device license usage across multiple deployments.
- Understand historic license usage and monthly license usage trends.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- View the last login time for specific users.
- Compare the number of licenses installed relative to licenses in use across Citrix License Servers.
- Monitor license overdraft.
- View breakdowns of Concurrent and User/Device license usage.

View license server status

The license server status view shows each of the license servers reporting usage to Citrix Cloud.



License servers display the "Reporting"status if they have successfully uploaded usage to Citrix Cloud in the last three days. License servers display the "Not Reporting"status if they previously reported usage in the last 30 days but not reported in the last three days. License servers that haven't reported usage in the last 30 days are removed from the list.

Impact of license server status on license usage views

The reporting status and Last Reported date of a license server dictates whether or not the usage from a particular license server is included in the usage insights views and reports.

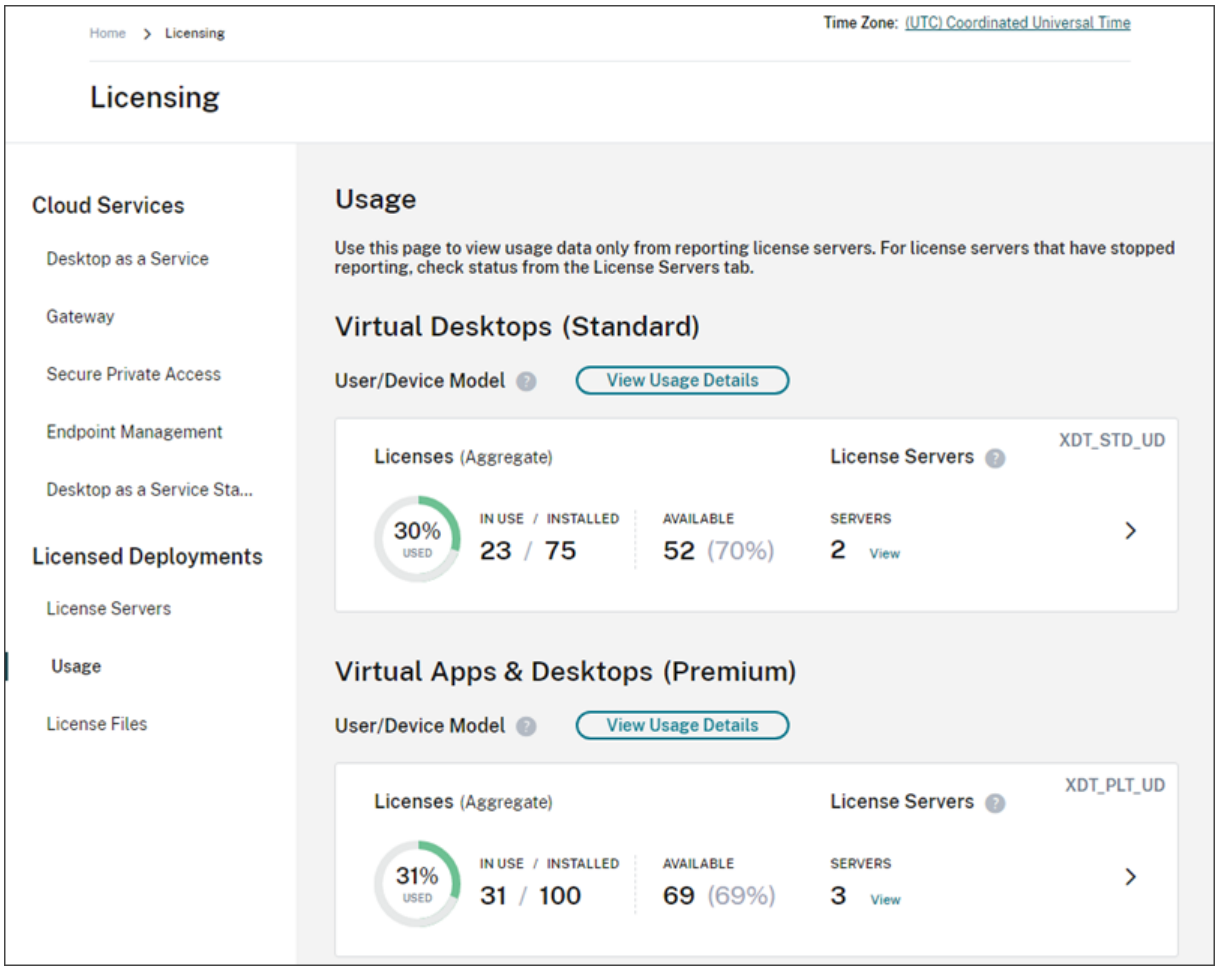
- Current licenses installed and in-use are based exclusively on data from reporting license servers. If a license server is listed as "Not Reporting,"installed and in-use licenses from that license server are not reflected in the usage insights experience.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The Last Reported date for each license server determines how up-to-date the license usage information is in the usage insights experience. The license usage reports shown are only as current as the Last Reported time for each license server.
- Citrix License Servers configured for usage insights and registered with Citrix Cloud update usage once per day. If needed, you can force an update from the Citrix License Manager management console on the license server.

License usage

The Usage tab provides a consolidated view of license usage across your Citrix deployments. Licensing information from each reporting license server is combined into a single view. This view makes it easy to see your complete licensing picture across many different deployments and license servers.



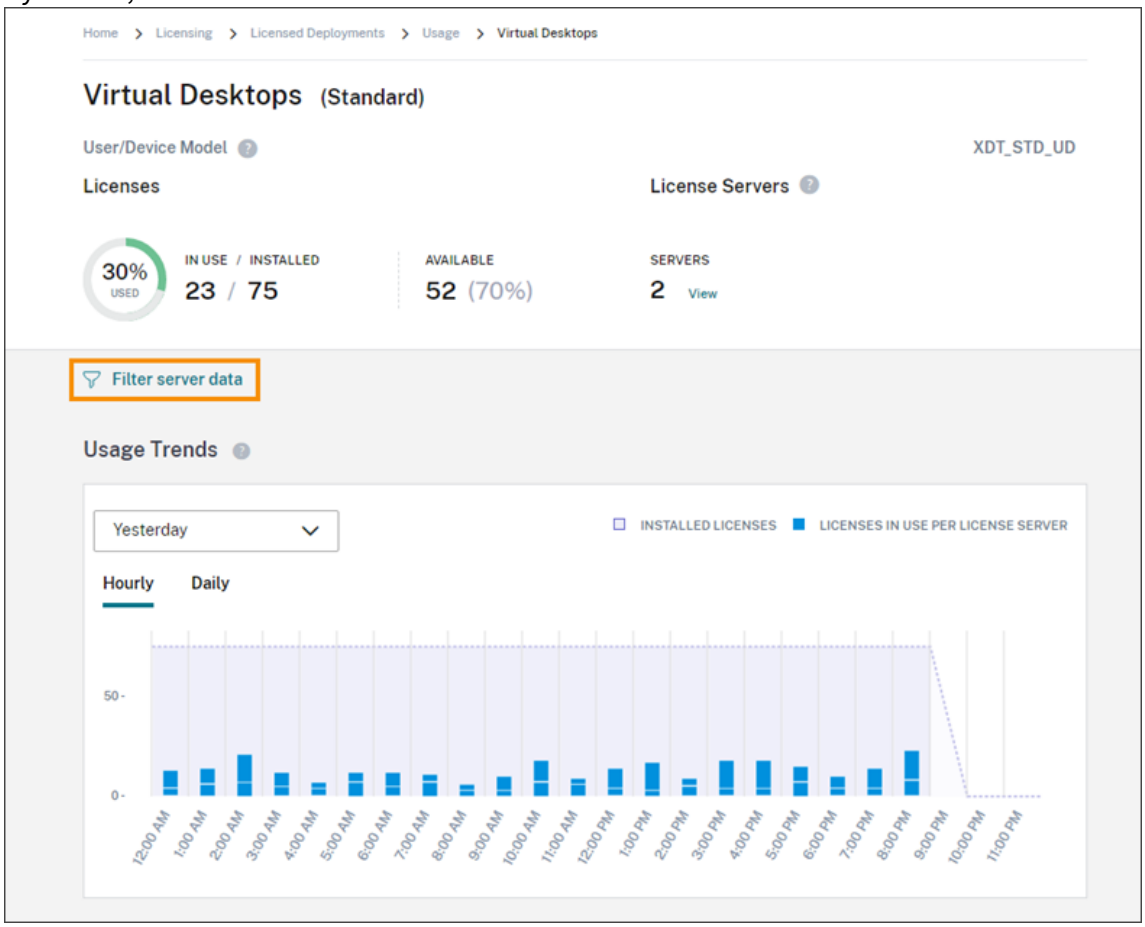
License usage is organized and aggregated across multiple license servers based on product edition and licensing model. A license usage summary card is displayed for each unique license edition found across all reporting license servers. A summary card is displayed for each product edition detected.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Usage per License Server

To view product license usage for each License Server, you can filter the server data.

1. From the **Usage** page, select **View Usage Details** for the product that you want to manage.
2. Click **Filter server data** and then select the License Servers for which you want to view usage. By default, all License Servers are selected.



3. Select **Apply**.

After you apply the filter, Citrix Cloud displays the usage trends, License Server breakdown, and license activity only for the servers you selected.

Peak license usage for the Concurrent licensing model

The reporting experience for Concurrent licenses is organized around the following data points:

- Installed licenses: The number of licenses installed on each license server.
- Peak licenses in-use: The maximum number of licenses that were used in a specific time frame.

In calculating peak licenses in-use, Citrix Cloud retrieves the the maximum number of licenses used in the following time periods:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Last 7 days: The maximum number of licenses used at one time during the last seven days.
- This Month: The maximum number of licenses used at one time in the current calendar month.
- All Time: The maximum number of licenses used at one time since the license server was registered with Citrix Cloud.

> **Important:**
>
> The data for these time periods might not match the number of licenses in use on the license server. The license server reports only the number of licenses in use at any given time. Citrix Cloud receives these individual data points and calculates the peak for these time periods.

Considerations for interpreting license usage

Citrix licensing supports many usage scenarios and includes detailed information. Keep the following considerations in mind when monitoring usage:

- Usage information is based on licenses installed on each of the reporting license servers. If a license server is running out of available licenses, you can allocate and place additional licenses on the license server to increase the number of available licenses.
- The information available in the Citrix License Server usage insights view includes only the information collected and reported by registered and actively reporting Citrix License Servers. The licensed deployments experience does not represent and may not match the total number of licenses you actually own or purchased.
- The percentage of licenses available is computed based on the number of licenses in use relative to the licenses installed on reporting license servers.

Remove License Server registration

Removing License Server registration completely from Citrix Cloud consists of the following tasks:

1. Remove the registered License Server from Citrix Cloud using the Citrix Licensing Manager console. For complete instructions, see Remove registration of your License Server.
2. Remove any usage data that was previously collected.
3. Verify that Citrix Cloud no longer displays the License Server on the Product Registrations page. If the License Server still appears in the list, remove the server as described in Remove a product registration.

Remove usage data

When you remove a registered License Server from Citrix Cloud, usage data that was previously collected is still stored. If you no longer want to keep this data, you can delete it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Important:**
>
> Deleting usage data is permanent and can't be undone. If you delete usage data but don't remove the registration for your License Server, Citrix Cloud continues to collect usage data.

1. From the Citrix Cloud menu, select **Licensing**.
2. On the **License Servers** tab, select **Delete data**.
3. When prompted, select the check boxes to confirm that you understand the impact of the deletion.
4. Select **Delete server data**.

Licensing for Citrix Service Providers

September 6, 2025

The License Usage Insights service in Citrix Cloud™ is a free cloud service that helps **Citrix Service Providers (CSP)** understand and report on product licenses and usage. Only CSP partners have access to License Usage Insights.

> **Note:**
>
> Citrix DaaS was formerly Citrix Virtual Apps and Desktops service. Citrix DaaS Standard for Azure was formerly Citrix Virtual Apps and Desktops Standard for Azure. Some displays might contain the former name.

The License Usage Insights service enables you to:

- Automatically aggregate product usage information from telemetry
- Automatically aggregate cloud licensing usage and consumption for single-tenant and multi-tenant customers
- Easily view which users are accessing your Virtual Apps and Desktops deployments each month
- Create customer breakdowns of licensing usage
- View and understand your historic business with Citrix®
- Export Virtual Apps and Desktops and Citrix DaaS license usage, NetScaler VPX allocations data, and Citrix DaaS Standard for Azure licensing and consumption data to CSV

Additional information

For requirements and setup instructions, see Get started with License Usage Insights.

To view aggregated usage for single tenant and multitenant customers, see Cloud service license usage and reporting for Citrix Service Providers.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To view customers'usage of supported services using the Licensing console, see the following articles:

- Customer license and usage monitoring for Citrix DaaS

Get started with License Usage Insights

September 6, 2025

Supported Citrix® products

The License Usage Insights service provides usage information for the following Citrix products:

- Virtual Apps and Desktops (on-premises) product usage
- Citrix DaaS™ Premium (formerly Virtual Apps Premium and Virtual Apps and Desktops Premium services)
- Citrix DaaS Standard for Azure (formerly Citrix Virtual Apps and Desktops Standard for Azure)
- NetScaler® Console VPX allocations

Requirements

To capture license and usage information for Citrix on-premises products and be compliant, Citrix License Server 11.17.2 build 51000 or later is required. Only Windows-based and VPX-based license servers are supported.

Citrix License Server 11.17.2 build 51000 and later contains key features that are important for Citrix Service Provider (CSP) partners:

- Optimized usage collection: License Server contains new functionality that optimizes licensing behavior and tracking to better support CSPs.
- Call home: License Server includes Call Home features that automate product usage collection for CSP partners. These features are exclusive to CSP partners and will only be activated when a CSP license is detected on the license server.
- To transition to License Activation Service (LAS), support the new event based telemetry and simplify CSP on-prem license distribution between customer sites, the minimum license server version must be 11.17.2 build 51000.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Step 1: Update Citrix License Server

If you're running license servers older than Version 11.17.2 build 51000, you must upgrade your license servers. Upgrading in-place is simple and fast. Complete the following tasks:

1. Download the latest license server. For more information about the latest version of Citrix License Server, refer to the Citrix Licensing documentation.
2. Upgrade your current license server.
3. Repeat the upgrade process for each of your license servers.

Step 2: Sign in to Citrix Cloud™ with My Citrix credentials

Before signing in, you'll need to sign up for a Citrix Cloud account if you do not already have a CSP partner cloud account. Follow the steps described in Sign up for Citrix Cloud.

When creating your account, use the same My Citrix credentials that you use to allocate and download Citrix licenses from citrix.com. Citrix Cloud sends you an email at the address associated with your My Citrix credentials to confirm the account.

When your Citrix Cloud account is ready to use, sign in at https://citrix.cloud.com using your email address and password.

Step 3 (optional): Anonymize usernames through the license server

By default, usernames associated with Virtual Apps and Desktops or Citrix DaaS license checkouts are securely phoned home to Citrix.

Usernames are phoned home so CSP partners can take full advantage of License Usage Insights features and the CSP licensing program.

User information is limited to a single user@domain entry; no additional personal identifiable data is phoned home. Citrix does not share this information.

Partners sensitive to uploading username information can enable username anonymization. When active, username anonymization converts readable usernames into unique strings using a secure and irreversible algorithm prior to upload.

License Usage Insights uses these unique identifiers to track product usage instead of the actual usernames. This approach allows service providers to take advantage of month-to-month insights without visibility into the actual usernames in the cloud service user interface.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To configure username anonymization

1. On the license server, open the configuration file in a text editor. Typically, the configuration file is located at C:\Program Files\Citrix\Licensing\WebServicesForLicensing\SimpleLicenseServiceConfig.xml.
2. In the **Configurations** section, add the **UsageBasedBillingScramble** setting as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<Configurations>
<EncoreConfiguration>
<SamplingPeriod>15</SamplingPeriod>
<RetentionTime>180</RetentionTime>
<Enabled>true</Enabled>
</EncoreConfiguration>
<SARenewalConfigOptions>Notify</SARenewalConfigOptions>
<UsageBasedBillingScramble>1</UsageBasedBillingScramble>
</Configurations>
```

3. Save the file.

Step 4: Use the License Usage Insights service

From the Citrix Cloud console, locate and click the License Usage Insights service tile from the waffle menu. For an overview of the service's key features, see Manage product usage, license servers, and notifications.

Additional details

When using Citrix License Server with License Usage Insights, consider the following items:

- It might take up to 24 hours for a newly updated license server or site to appear in the License Usage Insights management console.
- When usage data is uploaded from a license server, it's processed and stored in a secure fashion so License Usage Insights can access it at a later date. This process might take up to 24 hours to complete.
- By default, usernames associated with Virtual Apps and Desktops or Citrix DaaS license check-outs are securely phoned home to Citrix.
- Usernames are phoned home so CSP partners can take full advantage of License Usage Insights features and the CSP licensing program which supports free users for trial, test, and administrative product use.
- User information is limited to a single user@domain entry; no additional personal identifiable data is phoned home. Citrix will never share this information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Help and support

If you need assistance with License Usage Insights, open a support ticket on the My Support portal. To access My Support from Citrix Cloud:

1. Sign in to Citrix Cloud.
2. Click the **Help** icon near the top-right of the screen.
3. Select **Open a ticket**.
4. Select **Go to My Support** and sign in with your My Citrix credentials.
5. Complete and submit the form.

A member of Citrix Technical Support will follow up and assist you.

Frequently Asked Questions

- **What information is being phoned home? Can I view the information my license servers are sending to Citrix?** Yes, you can view a copy of the information that's phoned home to Citrix. For details, see License server information included in uploads.
- **Is License Usage Insights available to Citrix customers or partners that are not Citrix Service Providers?** No. License Usage Insights is only available to Citrix Service Provider™ partners with an active membership agreement.
- **Can I disable Call Home on the license server?** No. Under the Citrix Service Provider license agreement, all license servers are required to phone home product usage. Partners sensitive to the phone home use case can use the username anonymization feature. For details, see Anonymize usernames through the license server.
- **Will I be billed based on the product usage shown in License Usage Insights?** No. License Usage Insights helps partners understand their product usage so they can audit and bill their customers accurately, and expand the order as needed.

Manage product usage, license servers, and notifications

September 28, 2026

Use License Usage Insights to monitor product usage, track license server status, and manage customer notifications for your Citrix Cloud deployments.

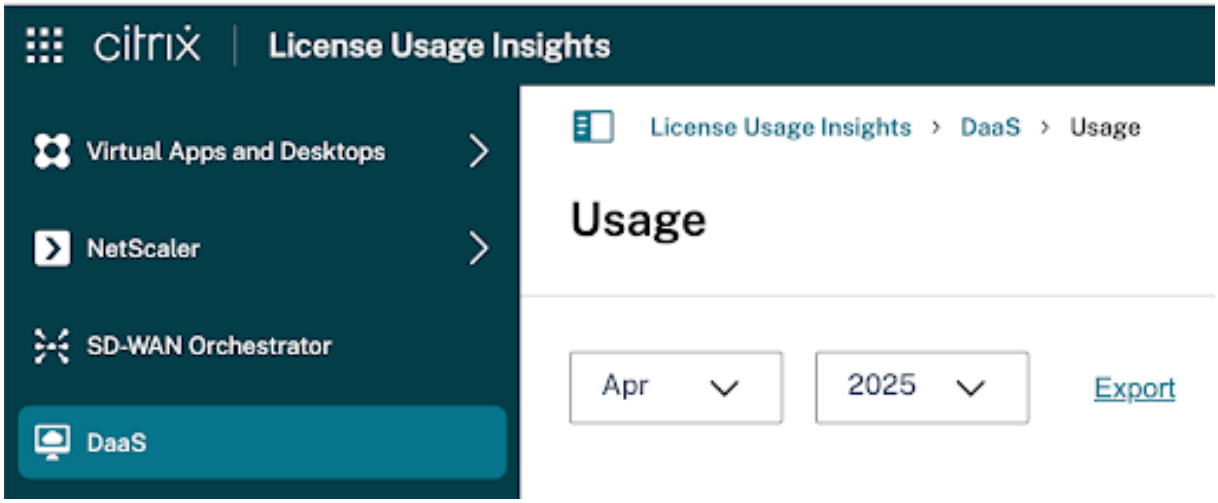
> **Note:**
>
> To display unscrambled user information (such as usernames and domains) and correctly resolve Site and Delivery Group names, upgrade your Citrix Virtual Apps and Desktops™ Delivery

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> Controllers to one of the following minimum supported versions:
>
> - **Current Release:** 2411 or later
> - **LTSR:** 2203 CU7, 2402 CU3, or 2507
>
> Earlier versions display GUIDs instead of field values due to default data scrambling.

Product selection

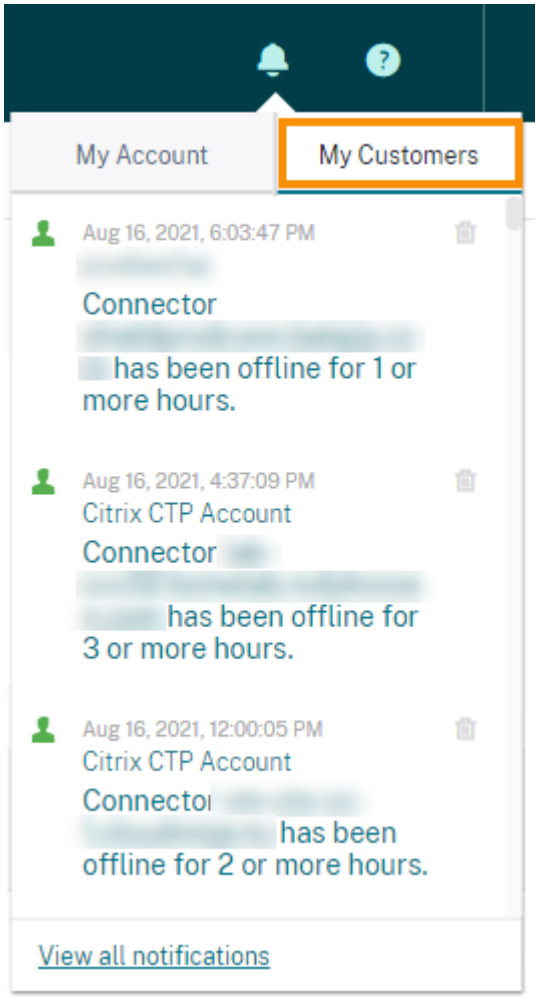
To view licensing details for a different product, click the arrow next to the product name and select the product or service you want to view.



Customer notifications

Monitor solution health across multiple customers without having to visit each deployment individually. The Notifications area in Citrix Cloud aggregates notifications across customers on your dashboard so you can ensure alerts are addressed and services keep running.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



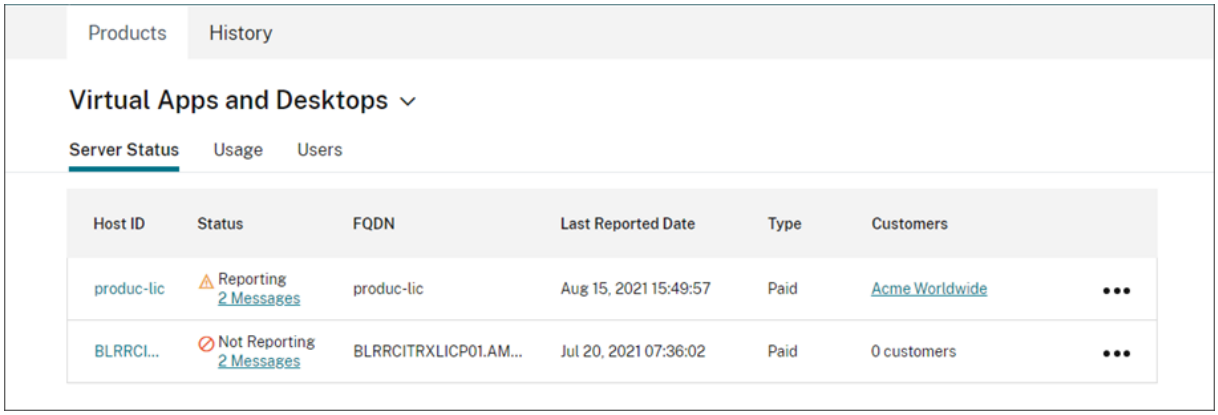
1. From the Citrix Cloud management console, click the **Notifications** icon and then click **My Customers**. A list of the most recent notifications appears.
2. To view a complete list of customer notifications, click **View all notifications**.

License server status

To be compliant with Citrix Service Provider™ license guidelines, all active license servers must be updated and reporting. The license server status shows the license servers you have and whether or not they're updated for use with License Usage Insights.

The service displays a list of active license servers using the traditional license allocation data stored in the Citrix® back office. If the license server is updated and successfully reporting, License Usage Insights displays the "Reporting"status and includes a timestamp of the most recent upload.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



License server information included in uploads

When Call Home is activated on a license server, the following information is uploaded daily:

- License server version
- License file information:
  - License files installed on the server
  - License file expiration dates
  - Product feature and edition entitlement information
  - License quantities
- License usage:
  - Licenses used in the current calendar month
  - Usernames associated with license checkout
  - Product features and editions activated

View a license server upload

CSP partners can inspect the last uploaded payload on their license server to fully understand all of the details that the license server sends to Citrix. A copy of this payload is stored as a .zip file on the license server. By default, this location is C:\Program Files (x86)\Citrix\Licensing\LS\resource\usage\upload_1456166761.z

> **Note:**
>
> Successful uploads are deleted except for the last one. Unsuccessful uploads linger on the disk until a successful upload occurs. When that happens, all but the last upload are deleted.

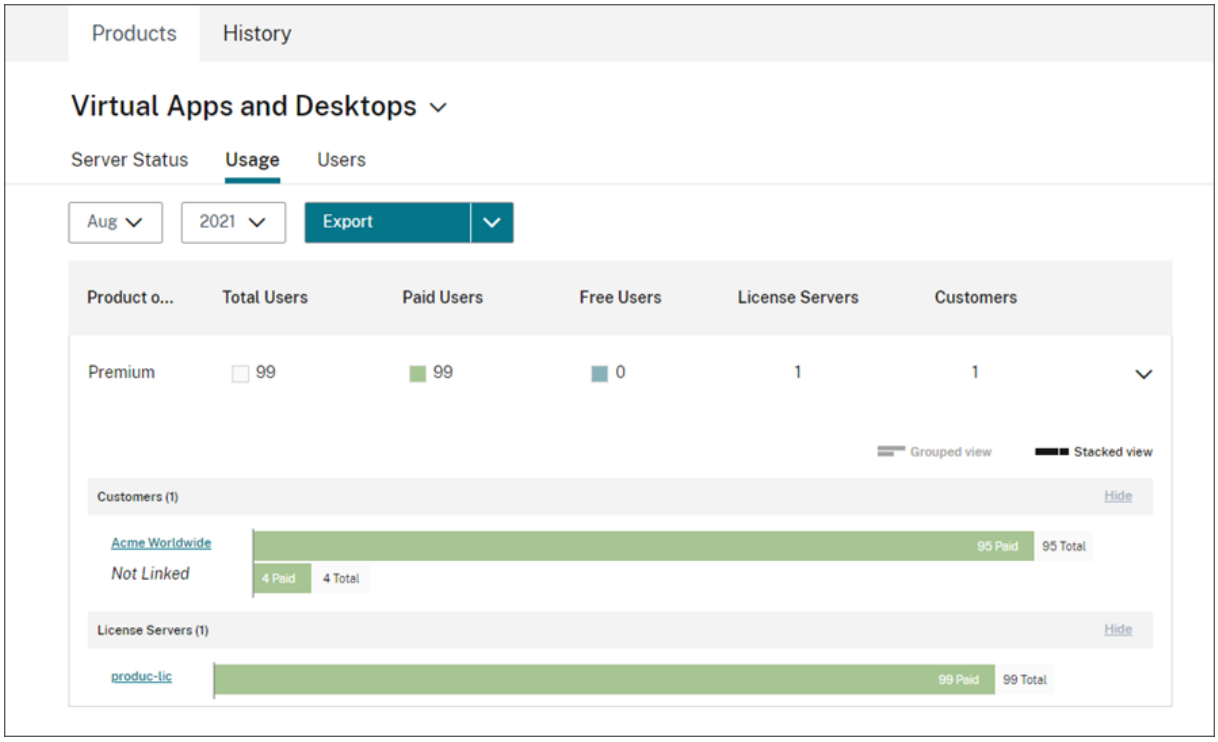
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Usage collection

Usage collection helps you understand product usage through automated data collection and aggregation. There's no need to deploy additional tools.

License Usage Insights automatically aggregates product usage across all Citrix License Servers (for traditional License Server call home) and Sites (for License Activation Service) to provide a complete view of usage across all deployments. You can also create licensing usage breakdowns by associating specific users with the customers or tenants to whom they belong.

The license servers collect and track product license usage and report it back to Citrix using a secure phone home channel. This automated approach provides you with a constant stream of updated usage data, saving time and helping partners better understand usage trends within their deployments.



User Assignment (tagging) for customer breakdown of Virtual Apps and Desktops product usage

This feature provides breakdown of license usage data for each customer, including support for managing and reporting on both single-tenant and multi-tenant site (LAS integrated) or license server (traditional call home) architectures. The objects of License Usage Insights are:

- **License Server**: A 'reporting'or 'not reporting'license server on the list.

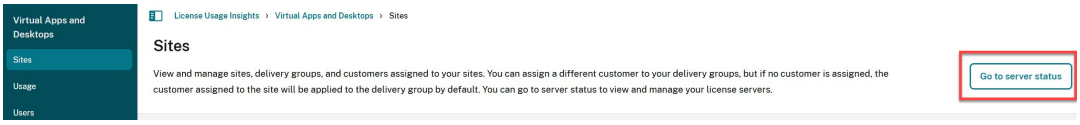
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Site**: A Virtual Apps and Desktops site dedicated to a customer or shared by multiple tenant customers.
- **Delivery Group**: A Virtual Apps and Desktops delivery group normally dedicated to a customer.
- **User**: A single username found in call home usage data.
- **NetScaler**: A single NetScaler VPX™ license allocation (VPX on the VPX List).

> **Note:**
>
> A CSP can update customer tagging for the last monthly and the current month until the 10th of the following month.

To break down licensing usage by customer, you must first associate users with the customers or tenants to whom they belong. If you don't have any customers defined in your Customers dashboard, you can add new ones or you can connect with existing Citrix Cloud customers.

1. If applicable, add customers to the Customers dashboard: From the Citrix Cloud management console waffle menu, click **My Customers**, click **Add or Invite**, and then follow the onscreen instructions.
2. Click the waffle menu and then select **License Usage Insights** tile.
3. With the **Virtual Apps and Desktops** product selected, by default the **Sites** activated via License Activation Service (LAS) will be loaded.
4. To continue assign users from LAS integrated sites:
    a) Click **Users**.
    b) Select the users you want to associate and then click **Bulk Actions > Assign to Customer**.
5. To assign users from the traditional license server call home:
    a) Click **Go to server status** button.



    b) Once the License **Server status** page is loaded (you can also navigate back to LAS integrated Sites by clicking **Go to sites** from this page), select **All users** from the menu option.
    c) Filter and search the users, select the unlinked users and then click **Bulk Actions > Manage Link to Customer**.
6. From the customers list, select the customer with which you want to associate the users.
7. Click **Assign** or **Save**.
8. To view the per-customer breakdown, click the **Usage** view.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

User customer tagging

This feature provides breakdown of license usage data for each customer, including support for managing and reporting on both single-tenant and multi-tenant license server architectures. The objects of License Usage Insights are:

- License Server - A ‘reporting’or ‘not reporting’license server on the list.
- User - A single username found in call home usage data.
- NetScaler® - A single NetScaler VPX license allocation (VPX on the VPX List).

> **Note:**
>
> User customer tagging feature has the same behavior as free user tagging where a CSP can update customer tagging for the current billing cycle until the 10th of the following month.

Server customer tagging

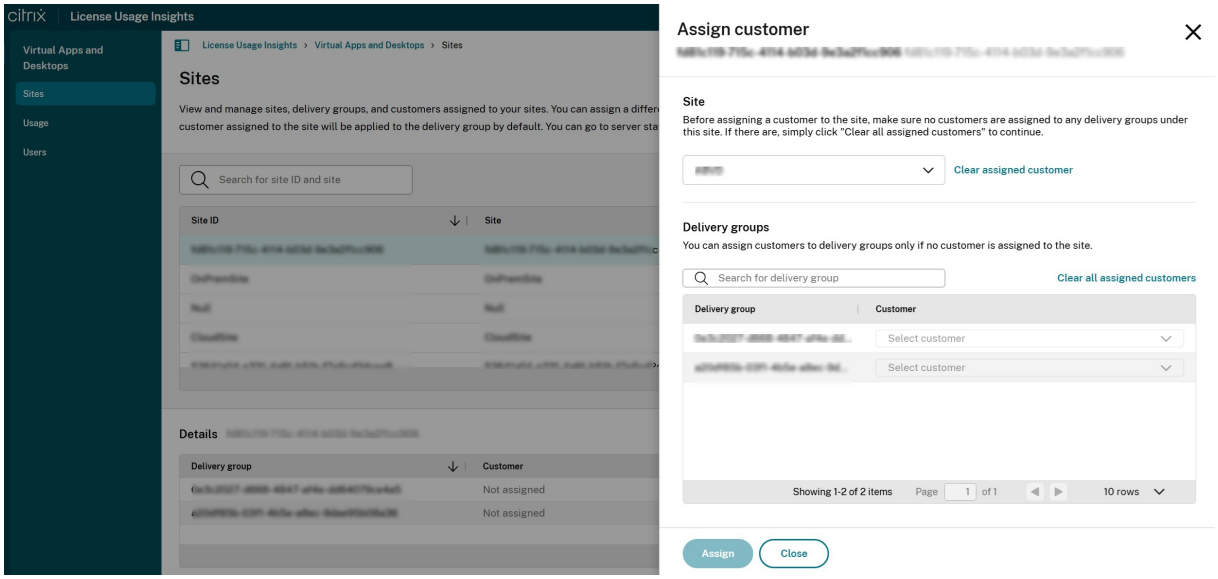
This feature allows license servers used for traditional call home are tagged or assigned to specific customer. By utilizing server customer tagging, any users from that server will automatically be associated with the tagged customer, administrators can easily identify and track resources associated with different customers, facilitating customer billing, reporting and more efficient resource allocation.

Site and Delivery Group customer tagging

Site customer tagging feature is applicable for the Virtual Apps and Desktops sites dedicated to specific customers (a.k.a. single tenant sites), it allows a LAS integrated site to be tagged and assigned to a customer. Once assigned, any users from that site will automatically be associated with the tagged customer in the usage report customer breakdown.

Delivery Group customer tagging feature is applicable for the Virtual Apps and Desktops sites shared by multiple customers (a.k.a. multitenant sites), it allows delivery groups of a LAS integrated site to be tagged to their relevant customers. Once assigned, any users from that delivery group will automatically be associated with the tagged customer in the usage report customer breakdown.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



A site can either be assigned exclusively to a single customer (site tagging), or to multiple customers via delivery group tagging, but cannot be both.

To access site or delivery group tagging, navigate from the waffle menu and select License Usage Insights, from the **Sites** page, select the site in the Sites table, and click **Assign customer**. The same page can also be used for delivery group tagging by selecting a delivery group in the Delivery groups table. If a site has already been exclusively assigned to a customer, then the delivery groups of that site are view-only and cannot be assigned individually to customers until you clear the site customer assignment.

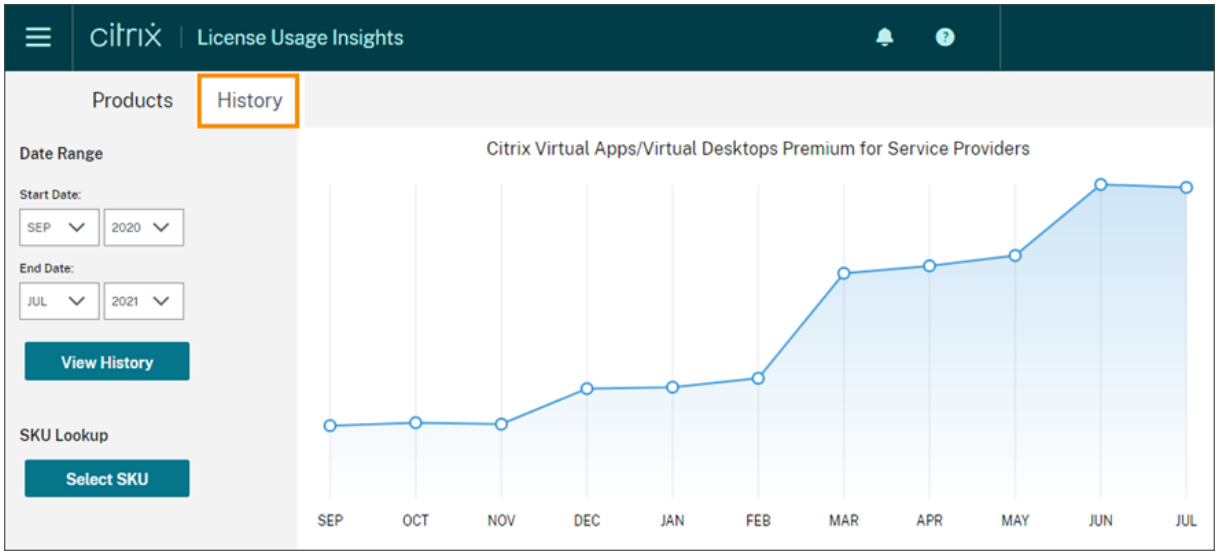
Site and Delivery Group based customer tagging is now in Tech Preview, you can use this form to request to participate in the preview.

Historical trends

You can view a complete historical record of all of your past business with Citrix based on the traditional license server call home. Check the usage you reported last month, last year, or over a configurable time period.

Historical views deliver valuable business insight. As a Citrix Service Provider, you can quickly understand how your business with Citrix is trending and which products are seeing the most growth across your customers and end users.
From the Server status page, click on View product history icon and link.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Export usage and allocations data

You can export the following types of data as a CSV file from License Usage Insights:

- Virtual Apps and Desktops product usage and user list for a specified month
- Current NetScaler VPX allocation details

1. Select **Virtual Apps and Desktops** or **Networking** from the product list.
2. If applicable, select the view you want to export. For example, to export Virtual Apps and Desktops usage details, click the **Usage** view.
3. If applicable, select the month and year you want to export.
4. On the right side of the screen, click **Export**.

Access licensing data with APIs

Citrix provides several APIs that you can use to access your licensing data outside of Citrix Cloud. To learn more about these APIs, see APIs to manage Citrix cloud licensing in the Citrix Developer documentation.

To use these APIs, you must first create a service principal and generate a bearer token. To create a service principal, see Get started with Citrix Cloud APIs.

Distributor access to APIs

You can allow your Citrix distributor or an authorized 3rd party to access your licensing data through Citrix Cloud APIs without granting them full administrator access to your Citrix Cloud account. You might do this so your distributor can validate your usage reports and ensure accurate billing.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To provide distributor access to your licensing data, you can create a service principal with the desired custom access permissions. To create a service principal, see Get started with Citrix Cloud APIs.

For this use case, select **Custom** access and then select **License Usage Insights** > **License Usage Insights: Distributor Access**.

Licensing data available to distributors

This section describes the licensing data and APIs your Citrix distributor can access using the service principal details you provide. Use the links below for more details about each API.

CSP reporting of monthly and historical Virtual Apps and Desktops license usage (License Usage Insights):

- Virtual Apps and Desktops Current Usage
- Virtual Apps and Desktops Historical Usage

CSP reporting of Single-Tenant and Multi-Tenant cloud license usage (License Usage Insights):

- DaaS Current Usage
- DaaS Historical Usage

CSP's cloud license usage (Licensing):

- DaaS Current Usage
- DaaS Historical Usage

Tenant's cloud license usage (Customer Dashboard -> View Licensing)

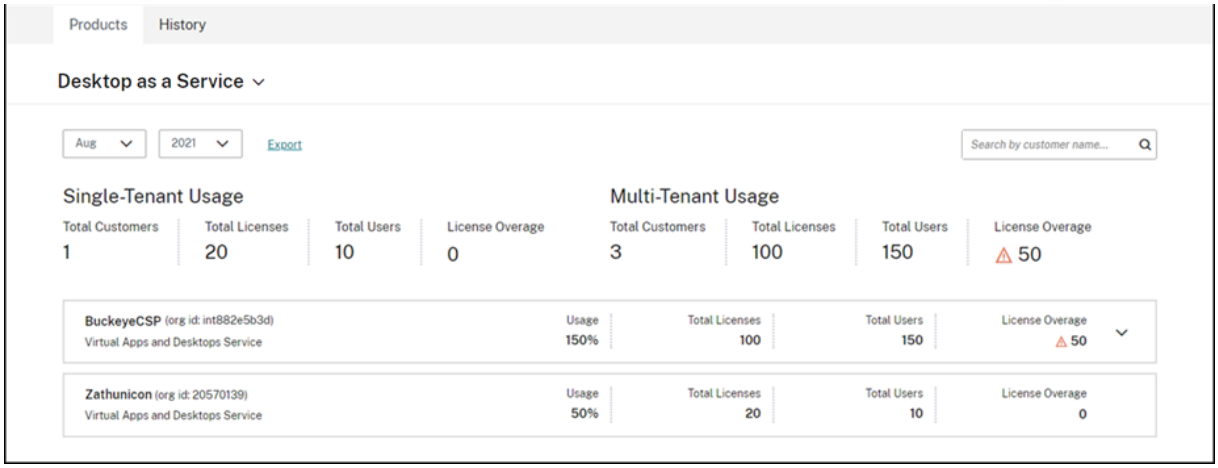
- DaaS CCU Current Usage
- DaaS CCU Historical Usage
- DaaS UD Current Usage
- DaaS UD Historical Usage

Cloud service license usage and reporting for Citrix Service Providers

June 22, 2026

License Usage Insights automatically aggregates cloud service usage to provide a complete view across all single-tenant and multitenant customers. You can also export these details for a given month to a CSV file for further analysis.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Supported services

CSP DaaS license usage is available for Citrix DaaS™ Premium (formerly Virtual Apps and Desktops Premium service) multitenant and single tenant entitlements.

> **Note:**
>
> Mixing CSP DaaS entitlements with other non-CSP DaaS entitlements within the same cloud account is not supported.
> Single tenant CSP DaaS entitlements can only be delivered to a tenant customer account that is linked to a CSP's account on the same Citrix Cloud™ control plane.

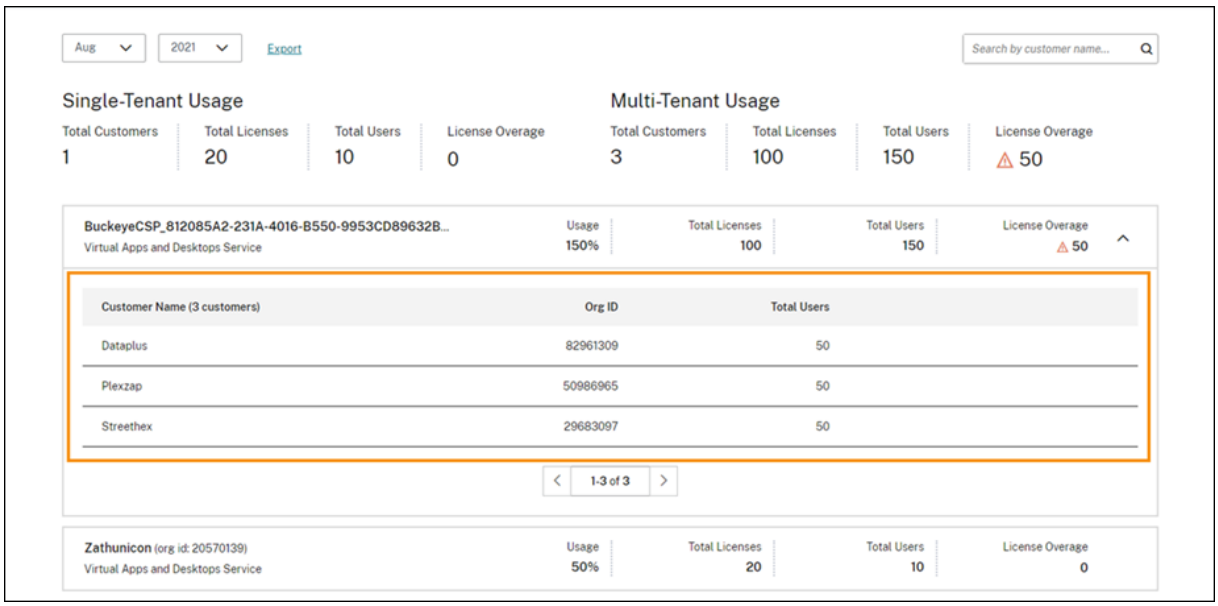
Licensing summaries

License Usage Insights provides the following breakdown for single tenant and multitenant usage for Citrix Service Providers (CSP):

- At-a-glance partner level summary grouped by tenant type that includes the total number of customers and the total number of purchased licenses, users, and overage (overused) licenses across all customers.
- Usage summary for each single tenant customer that includes the percentage of total licenses in use, total purchased licenses, users, and number of overused licenses.

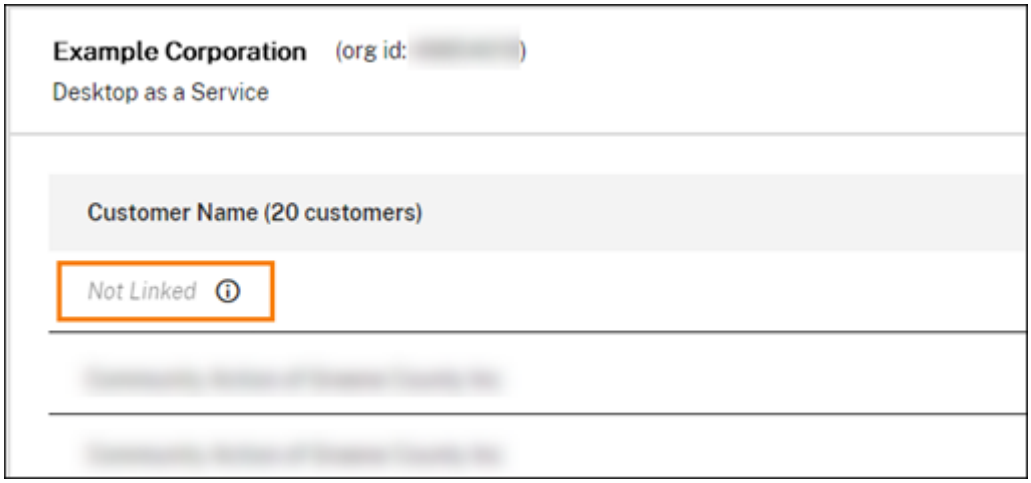
For multitenant services, you can expand the usage summary to view the customers breakdown, account ID, and total users associated with each tenant customer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Tenant customers not linked

In the case that some users of the tenant customers were launching their sessions via the partner's shared store URL rather than the tenant's own store URL, these users might be listed as "Not Linked."



To ensure those unlinked users are properly associated with their relevant tenant customers for accurate billing and reporting while continuing to allow users accessing partner store URL, the service provider (partner) administrator can leverage the below two methods to link the users.

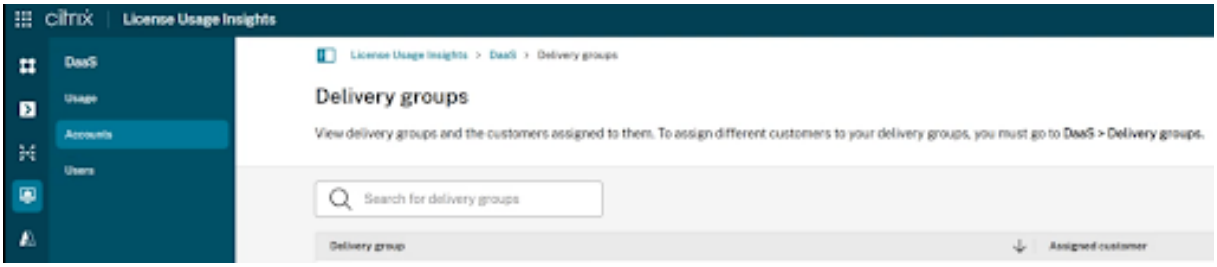
Delivery Group based auto user assignment (tagging)

License Usage Insights (LUI) service can now automatically link the multitenant DaaS users to tenant customers via scoped delivery groups when users launch sessions from those groups, but each of

© 1997–2026 Citrix Systems, Inc. All rights reserved.

those delivery groups must have been assigned with one specific tenant scope. Users launch sessions from unscoped or shared delivery groups cannot be linked. You can view the overall tenant scope assignment (or not assigned) for the multitenant DaaS delivery groups via **License Usage Insights > DaaS > Accounts**.

To assign or update the scope for a delivery group, you need to go to the Studio console for the multi-tenant DaaS.

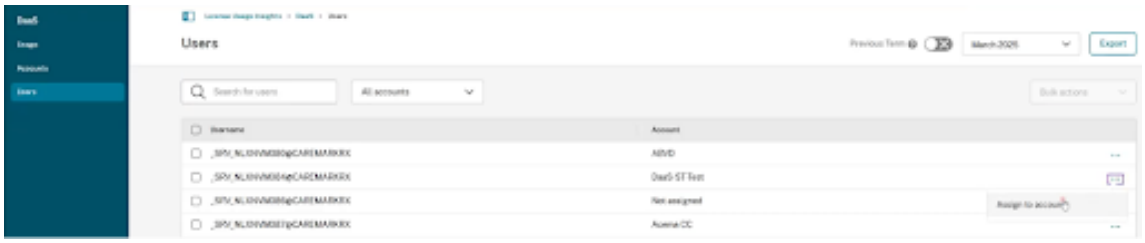


User assignment (tagging) to tenant customer

Tenants should have dedicated delivery groups in a multitenant environment, however under special use cases where a delivery group is shared or some CSP admins belong to multiple delivery groups with different scopes, manual user tagging is needed to assign or un-assign the user to a tenant customer.

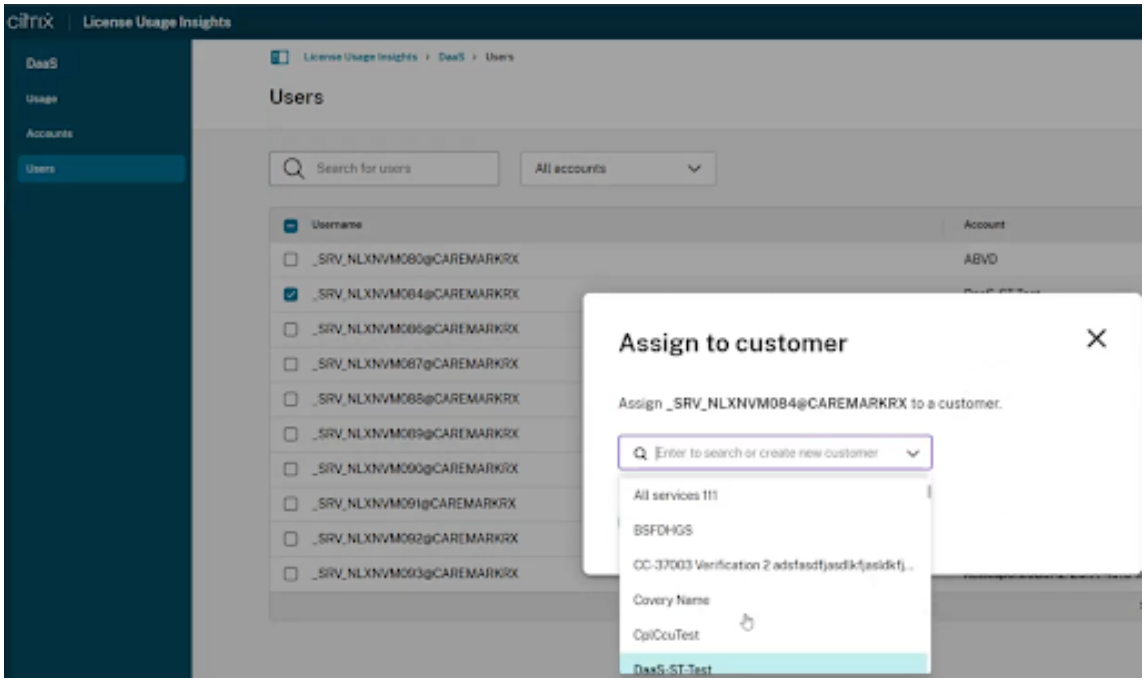
Navigate from the waffle menu > **License Usage Insights > DaaS > Users:**

- To assign an individual user, click on the "…"at the end of the user row, select **Assign to customer**, and choose the tenant customer.



- To assign bulk users, search for users with relevant criteria, check the boxes in the user rows, under **Bulk actions**, click **Assign to customer**, select the tenant customer, and click **Assign**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



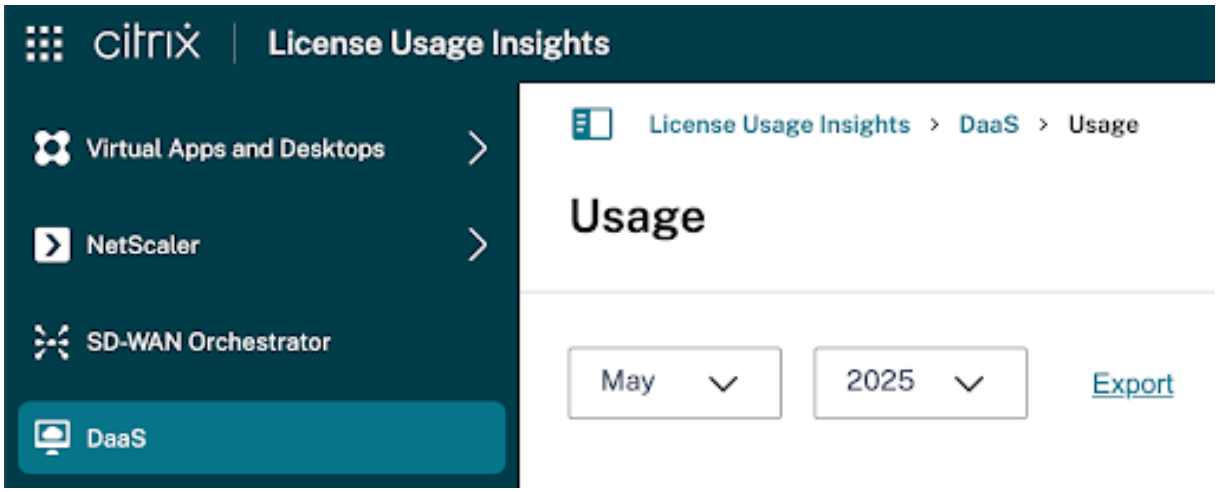
- You can also use the similar process to un-assign a customer.

View and export monthly usage

At any time, you can view license usage from previous months for all customers. You can also export this data to a CSV file for further analysis.

1. From the product menu, select the product you want to view.

For Citrix DaaS, select the month and year you want to view and select **Export**.



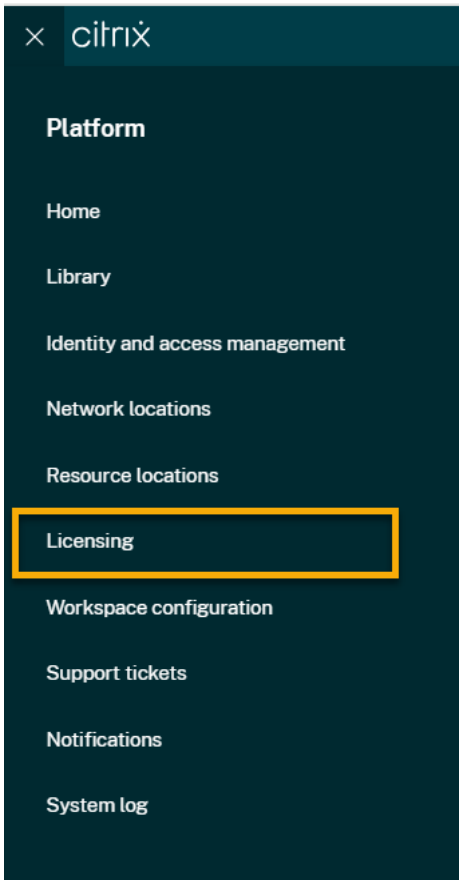
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Customer license and usage monitoring for Citrix DaaS™

September 6, 2025

Customers of **Citrix Service Providers (CSP)** can easily monitor Citrix DaaS licenses for their users in Citrix Cloud. As a CSP, you can access these details by signing in to your customer's account in Citrix Cloud. To view aggregated license usage information across single-tenant and multitenant customers, see Cloud service license usage and reporting for Citrix Service Providers.

Customers can view their licensing data by selecting **Licensing** from the Citrix Cloud™ menu.



License assignment

User/Device licensing model: Citrix Cloud assigns a license when a unique customer user launches an app or desktop for the first time within the current month.

Concurrent User licensing model:

For information about the Concurrent licensing model, see Concurrent licenses in the Licensing product documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Licensing summary

Citrix Cloud displays summary views of licenses in use under the User/Device and Concurrent User licensing models. For the single tenant customers managed by a CSP, mixing CSP licenses and non-CSP licenses (regardless **Concurrent** or **User/Device**) in the same customer account is not supported.

Summary for users and devices

For the User/Device model, the licensing summary provides an at-a-glance view of the licenses that are in use relative to the total number of licenses that you own.

As the percentage approaches 100%, the percentage goes from green to yellow. If the percentage exceeds 100%, the percentage turns red.

Citrix Cloud also displays the ratio of assigned licenses to purchased licenses and the number of remaining available licenses.

Calculating peak licenses in use

To accurately reflect the Concurrent licensing model, Citrix Cloud counts the number of unique devices accessing the service simultaneously every five minutes. If the count is greater than the current peak usage displayed, Citrix Cloud displays the new peak usage with the date and time that it was reached. If the count is less than the current peak usage, the current peak usage doesn't change.

> **Important:**
>
> If you use Monitor in Director for information about concurrent sessions, be aware that the Monitor report provides a different interpretation of concurrent sessions and does not accurately reflect the number of Concurrent User licenses in use. For more information about the differences between Monitor reports and Licensing reports, see the FAQ.

Calculating monthly active use

At the beginning of each month, Citrix Cloud takes a snapshot of the previous calendar month. Citrix Cloud displays the total number of unique connections that occurred during that calendar month.

Calculating daily active use

At the same time each day, Citrix Cloud takes a snapshot of the previous 24 hours. Citrix Cloud displays the total number of unique connections that occurred during that 24-hour period.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Usage trends

Citrix Cloud displays a breakdown of usage trends for either User/Device or Concurrent User licenses. To view this breakdown, select **View Usage Details** from the licensing summary page.

Trends for users and devices

For User/Devices licenses, the **Usage Trends** section shows you a breakdown of assigned licenses as a chart.

Pointing to an interval on the chart shows you the following information:

- **Total Licenses:** Your total purchased licenses for the cloud service across all entitlements.
- **Previously Assigned:** The number of licenses that were assigned in the previous month. For example, a user accesses the cloud service for the first time in July and is assigned a license. This license is counted as "Newly Assigned"for the month of July. For the month of August, this license is counted as "Previously Assigned."
- **Newly Assigned:** The number of new licenses that were assigned for each month. For example, a user accesses the cloud service for the first time in July and is assigned a license. This license is counted as "Newly Assigned"for the month of July.

Licensed users

The **License Activity** section displays a list of the individual customer users who have licenses assigned during the current month. This list also displays the domain to which each user belongs, the date when a license was assigned, and the last time the service was used.

Monthly release of licenses

On the first day of each month, assigned CSP licenses from the previous month are released automatically. When this happens, the number of assigned licenses resets to zero and the list of licensed customer users is cleared. Licenses are re-assigned when users launch apps or desktops for the first time within the new month.

Review monthly license history

On the first day of each month, the list of CSP's licensed customer users from the previous month, under **License Activity**, is cleared when the number of assigned licenses resets to zero. However, you can access user details from previous months at any time and download them as a CSV file, if needed.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. In the **License Activity** section, select **View License History** at the far right of the section.
2. Select the month you want to view. A list of the user details for the selected month appears.
3. To export the list, select **Export to CSV** at the far right of the section and then save the file.

Export license details

At any time, customers can export licensed user details to a CSV file for further analysis. The customer can then use the CSV file as needed to analyze the license details.

To export the current month's details, in the **License Activity** section, select **Export to CSV** at the far right of the section and then save the file.

To export the details for previous months, generate a list for a selected month as described in Review monthly license history. Select **Export to CSV** and save the file.

Licensing for Citrix Platform Flex

August 12, 2026

Citrix Platform Flex is a managed, cloud-delivered platform designed to provide secure, resilient, and flexible delivery of digital workspaces and platform services across clouds.

Citrix Platform Flex shifts customers away from rigid, infrastructure-centric deployment models to a persona-based operating model. Instead of sizing and managing infrastructure manually, customers consume Citrix services that scale based on how work is performed.

At its core, Citrix Platform Flex is built to support:

- Workforce variability (employees, contractors, partners, and temporary users)
- Operational simplicity through Citrix-managed infrastructure
- Predictable and flexible consumption aligned to real usage
- Enterprise-grade resiliency and security across regions

Citrix Platform Flex is designed as a multi-service platform built on Citrix Cloud. Services delivered through the platform share a common operational, security, and economic foundation, allowing customers to adopt additional capabilities over time without re-architecting their environment. Learn more about Citrix Cloud.

Capabilities

Citrix Platform Flex delivers the following platform-level capabilities:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Persona-based computing**: Services are consumed based on worker personas rather than static infrastructure or per-VM licensing using Citrix Flex Credits. Credits are consumed monthly based on the services provided. This enables right-sizing of performance, security, and cost for different types of use cases.
- **Citrix-managed infrastructure**: Citrix owns and operates the underlying cloud infrastructure, including lifecycle management, patching, and resiliency. Customers focus on applications, policies, and user experience, not infrastructure operations.
- **Resiliency**: Platform services are designed for high-availability and business continuity, with support for multi-region deployment patterns and integrated resiliency capabilities.
- **Unified control plane**: Administration, monitoring, access, and policy are delivered through Citrix Cloud, providing consistent management experience across services.

Available services

Citrix Platform Flex delivers services that map to the platform's persona and capability model.

Current services include:

- **Citrix DaaS Flex**: Persona-based virtual app and desktop delivery using Citrix-managed infrastructure on Microsoft Azure. See Citrix DaaS Flex.
- **Citrix SecurSpaces™ Flex**: Persona-based workspaces for developers, data analysts, and AI agents using Citrix-managed infrastructure on Microsoft Azure. See Citrix SecurSpaces Flex.
- **Citrix Experience Insights Flex**: Citrix Experience Insights Flex helps organizations move from workspace telemetry to actionable insight faster across experience, performance, operational resilience, and security use cases. Delivered through a Citrix-managed analytics model and powered by Splunk.

Additional platform services might be delivered through Citrix Platform Flex over time, leveraging the same platform foundations for security, operations, and use.

Concepts and terminology

Flex Credits

Customers purchasing Citrix Platform Flex are licensed for a set number of credits also called **Flex Credits**. Flex Credits are flexible and can be leveraged to consume the available services listed above. See the table below on the credits associated with each persona.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Persona

Citrix Platform Flex leverages a persona-based computing approach to easily define worker profiles. Personas are defined by a virtual app or desktop delivery model and preconfigured based off the Citrix leading practices. Custom personas can be configured to adapt Citrix DaaS Flex to varied user requirements.

Services and personas for Citrix Platform Flex are defined as follows:

Category	Service	Persona	Version	Description	Citrix delivery model
Flex Services	Citrix DaaS Flex	Task worker (light)	v1	Ideal for everyday basic productivity, web browsing, and lightweight cloud-based SaaS applications.	Multi-session virtual applications with 16 users per VDA. 8 vCPU, 32 GB RAM 128 GB Storage. Windows Server OS, RDS
		Task worker (medium)	v1	Aligns with usage for a large percentage of modern corporate workers. Application requirements for modern workers are generally a combination of SaaS and corporate applications.	Multi-session virtual applications with 8 users per VDA. 8 vCPU, 32 GB RAM 128 GB Storage. Windows Server OS, RDS

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Service	Persona	Version	Description	Citrix delivery model
		Task worker (heavy)*	v2	Aligns with users who require frequent access to corporate applications to complete tasks.	Multi-session virtual applications and desktops with 4 users per VDA. 8 vCPU, 32 GB RAM 128 GB Storage (non-persistent). Windows Server OS, RDS
		Knowledge worker (light)	v1	Designed for standard administrative tasks, light multitasking, and core web-based communication tools.	Single-session virtual desktops. 2 vCPU, 8 GB RAM 128 GB Storage. BYOL Windows 11
		Knowledge worker (medium)	v1	Ideal for users who work exclusively within a virtual desktop environment (VDI). Ideal for highly secure use cases, call centers, or organizations looking to adopt thin or zero clients.	Single-session virtual desktops. 4 vCPU, 16 GB RAM 128 GB Storage. BYOL Windows 11

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Service	Persona	Version	Description	Citrix delivery model
		Knowledge worker (heavy)	v1	Built for power users running multiple concurrent business applications, large spreadsheets, and data analytics.	Single-session virtual desktops. 8 vCPU, 32 GB RAM 128 GB Storage. BYOL Windows 11
		Knowledge worker (extra heavy)	v1	Optimized for complex multi-tasking workflows requiring massive memory, large datasets, and heavy local processing.	Single-session virtual desktops. 8 vCPU, 64 GB RAM 128 GB Storage. BYOL Windows 11
		Power worker (GPU)	v1	Ideal for users with demanding graphics requirements, such as those working in artificial intelligence (AI), machine learning, or data visualization.	GPU-enabled single-session virtual desktops. 6 vCPU, 55 GB RAM, 4 GB GPU (A10), 128 GB Storage. BYOL Windows 11

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Service	Persona	Version	Description	Citrix delivery model
		Power worker (non-GPU)	v1	Engineered for CPU-intensive computing, code compilation, and data processing that don't require dedicated graphics rendering.	Single-session virtual desktops. 16 vCPU, 64 GB RAM 128 GB Storage. BYOL Windows 11

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Service	Persona	Version	Description	Citrix delivery model
	Citrix SecurSpaces Flex	Developer (Light)	v1	For lightweight development, scripting, code review, and short-lived workspaces where users need secure access to source code, tools, and dependencies but have modest compute requirements. Well suited for developers, contractors, and technical users working on smaller services, documentation, automation tasks, or occasional development activity.	Linux Container with 2vCPU, 8 GB RAM, and 32 GB Storage

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Service	Persona	Version	Description	Citrix delivery model
		Developer (Medium)	v1	For everyday application development, testing, and debugging where users require a balanced workspace with additional CPU, memory, and storage capacity. Well suited for full-time developers working with standard IDEs, build tools, application runtimes, and moderate-size repositories.	Linux Container with 4vCPU, 16 GB RAM, and 64 GB Storage

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Service	Persona	Version	Description	Citrix delivery model
		Developer (Heavy)	v1	For compute-intensive development, large repositories, complex builds, local test environments, and advanced workloads that require higher performance and more workspace capacity. Well suited for senior developers, platform engineers, data engineers, and teams running demanding development toolchains or frequent build and test cycles.	Linux Container with 8vCPU, 32 GB RAM, and 128 GB Storage

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Category	Service	Persona	Version	Description	Citrix delivery model
	Citrix Experience Insights Flex	All	v1	For actionable insights into end user experience & security across all platforms across enterprise.	Digital employee experience (DEX). Option to add security capabilities for additional credits.
SaaS	Citrix Secure Access with Chrome Enterprise	All	v1	For users that leverage Chrome Enterprise Premium for daily Web or SaaS applications.	CSA with CE capabilities add-on to DaaS Flex or standalone
Software Only	Citrix DaaS (Local/Cloud)	All	v1	Customer self-hosted option.	Customer-defined. Storage not applicable

> **Note:**
>
> - *Citrix will be deprecating the Task worker (heavy) persona in an upcoming release. Please use another available Flex persona for your upcoming machine catalogs.
> - The credits shown are for non-persistent, pooled workloads. Persistent dedicated workloads incur an additional add-on price, outlined in the Additional Options section.

Additional options Citrix Flex provides flexibility to customize workloads to the needs of your end-users. Additional options are defined as optional features or services used in conjunction with Flex Personas.

Citrix DaaS Flex Optional disk sizes and types for each persona are determined by the disk used in the image. Their corresponding Flex credit costs are defined as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Description	Size
Disk cost for single session persistent personas	128 GB Standard SSD Disk 256 GB Standard SSD Disk 512 GB Standard SSD Disk 1024 GB Standard SSD Disk 128 GB Premium SSD Disk 256 GB Premium SSD Disk 512 GB Premium SSD Disk 1024 GB Premium SSD Disk
Disk cost for multi session non-persistent personas	128 GB Premium SSD Disk

Services

See the following Citrix Platform Flex services documents:

- Citrix DaaS Flex
- Citrix SecurSpaces Flex
- Citrix Experience Insights Flex

Platform Flex Credit consumption and reporting

September 4, 2026

Flex Credits are consumed monthly based on the Flex services defined in your Persona section. Other services do not consume Flex Credits. A monthly Flex Credit consumption report is available to help you understand your overall usage patterns.

Consumption calculations by service

- **Citrix DaaS Flex (Managed Capacity Personas)**: This applies to Citrix managed capacity personas (for example, Task worker (heavy, medium), Knowledge worker, Power worker, Custom personas) and associated add-ons, such as Disks for persistent desktops. Consumption is based on the number of configured unique users for each Persona. A configured Persona consumes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Flex Credits even if it is never actively used. Catalog creations and capacity increases are prorated for the month, while capacity reductions and deletions are not. Flex Credits are not consumed if a catalog creation fails.

Example: 100 Task worker users × the Task worker Flex Credit value = total Flex Credits deducted monthly.

> **Note:**
>
> To maintain efficiency, these instances might hibernate during periods of inactivity. Typical resume time in Azure is less than five minutes.

- **Citrix SecurSpaces™ Flex (Managed Capacity Personas)**: This applies to Citrix managed capacity personas (for example, Developer (light, medium, heavy)). Consumption is based on the number of configured unique workspaces for each Persona. A configured Persona consumes Flex Credits even if it is never actively used. Citrix SecurSpaces workspace creations and capacity increases are prorated for the month. Flex Credits are not consumed if a SecurSpaces workspace creation fails.

  Example: 100 Developer (Medium) users × the Developer (Medium) Flex Credit value = total Flex Credits deducted monthly.

- **Citrix Experience Insights Flex**: Consumption is based on the number of unique users. Each specified user count consumes Flex Credits even if users are not actively onboarded. User additions are prorated for the month.

  Examples:

  - 10,000 users for User Experience × User Experience Credits = Total Flex Credits deducted monthly.
  - 10,000 users for User Experience + Security × User Experience + Security Credits = Total Flex Credits deducted monthly.

- **Citrix DaaS Cloud/Local (Bring Your Own Infrastructure)**: This applies to customers using Citrix Virtual Apps and Desktops or Citrix DaaS with a bring-your-own-infrastructure deployment model. Consumption is calculated per unique user, regardless of how many services they access. Even if a single user uses both Citrix Virtual Apps and Desktops and Citrix DaaS, they only count as one user. There is no proration for partial use in a month.

  Example: 1,000 Users × the per-user Flex Credit value = total Flex Credits deducted monthly.

- **Citrix Secure Access with Chrome Enterprise (CSA with CE)**: Consumption is calculated strictly per unique user. There is no proration for partial use in a month.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Flex Credits are deducted monthly from your total aggregate licensed units, which is referred to as the **Flex Credit Allotment** in the Business Unit Terms and Conditions.

Additional terms

- **Adjustments**: If you believe that a Flex Credit adjustment is required, you must submit a support ticket. Citrix will investigate and determine the appropriate next steps.
- **Suspension**: You cannot utilize Flex Credit-based services if you have consumed your total licensed amount, or if your remaining Flex Credit balance is inadequate to cover your desired usage.
- **Expiration**: Any Flex Credits that remain unconsumed during the Subscription Term expires on the Term End Date specified on your Order.

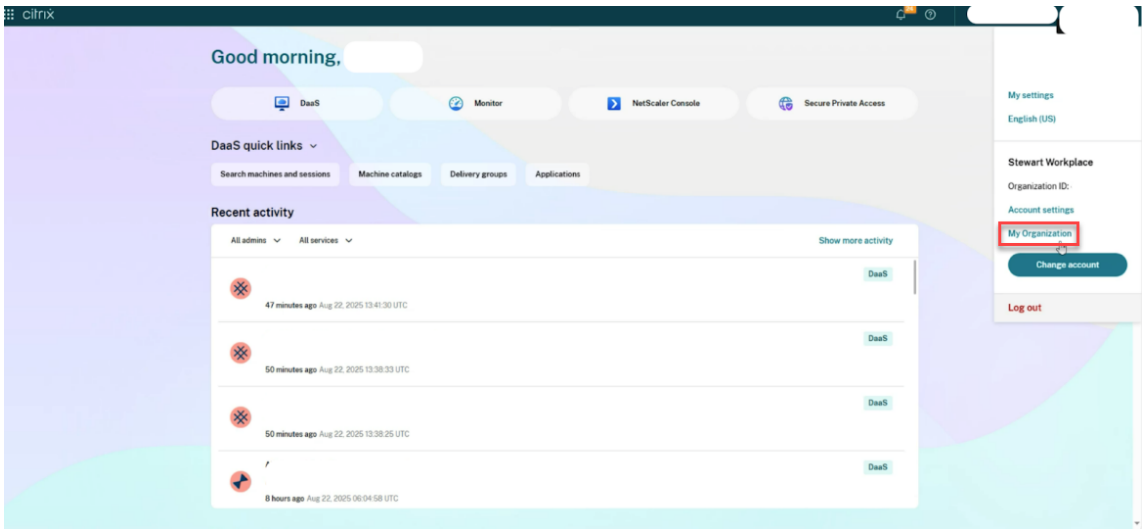
Citrix Cloud™ account management

February 6, 2026

This article walks you through the process of onboarding a Citrix Cloud Account and managing licenses for an account.

Create a Citrix Cloud account

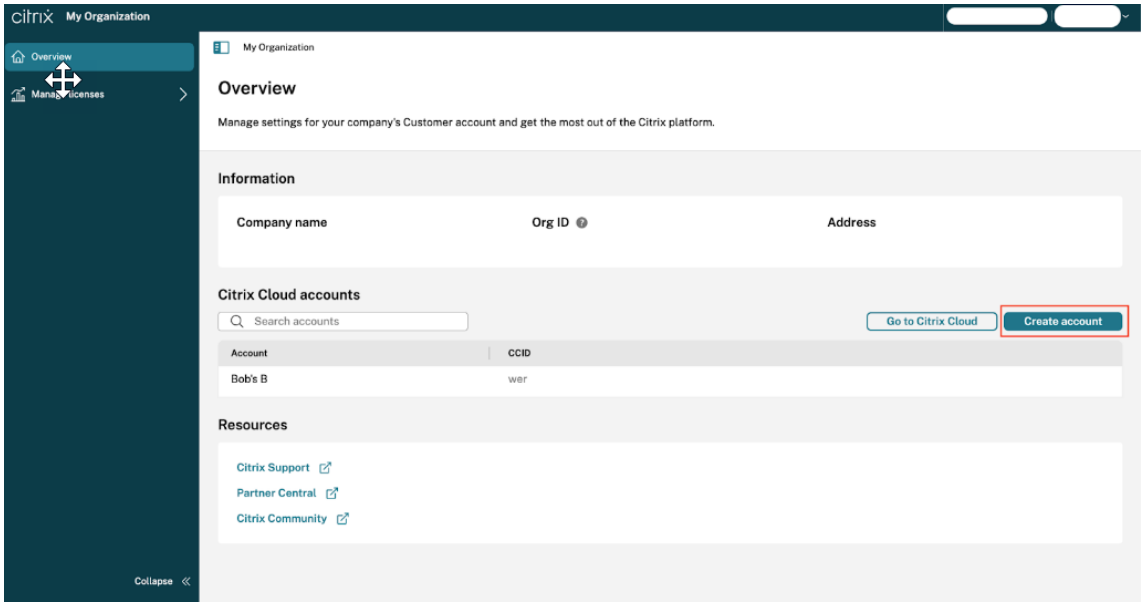
1. From the Citrix **Cloud** console, In the **profile menu**, click My Organization to begin.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

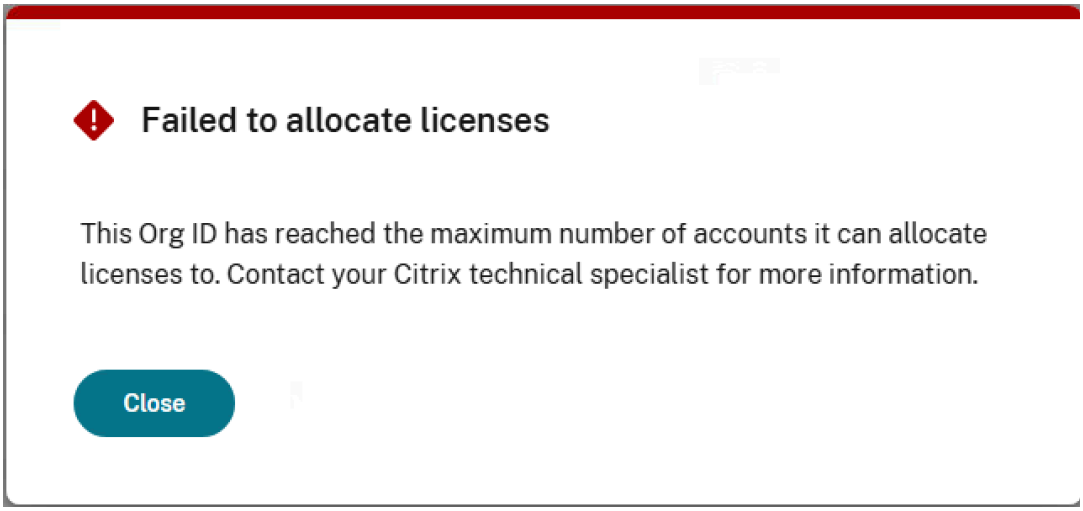
> **Note:**
>
> If you don't see My Organization option, then you don't have the right privilege to access it. Request your MyCitrix Account admin to add you as the correct admin for managing the licenses. For more information, refer to the Support link.
>
> If you are an existing Citrix customer and don't have a Citrix Cloud account, onboard the cloud tenant by visiting My Organization and follow the steps in Citrix Cloud account management.
>
> If you're new to Citrix®, sign up by contacting the account representatives to have your OrgID created.

2. From My Organization home page, click **Create account**.



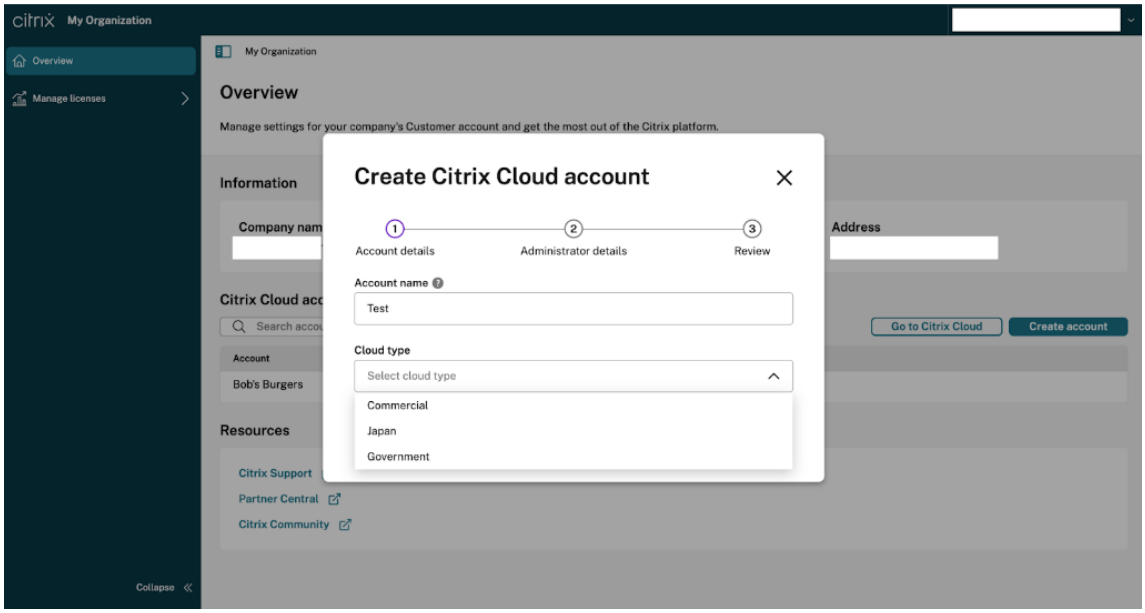
> **Note:**
>
> Citrix Customers can independently create new cloud tenants and manage licenses within My Organization. If you see the below message while allocating the licenses to onboarded cloud tenants, then you have reached the maximum number of accounts you can allocate licenses to, based on your total license quantities. For more information, get in touch with your Citrix Contact.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Citrix Partner is allowed to onboard only their first partner Citrix Cloud Account from My Organization . For onboarding any new customers, refer to My customers Dashboard.

3. Enter the **Account name** and Select the **Cloud type** from the drop-down list options and click **Next**.

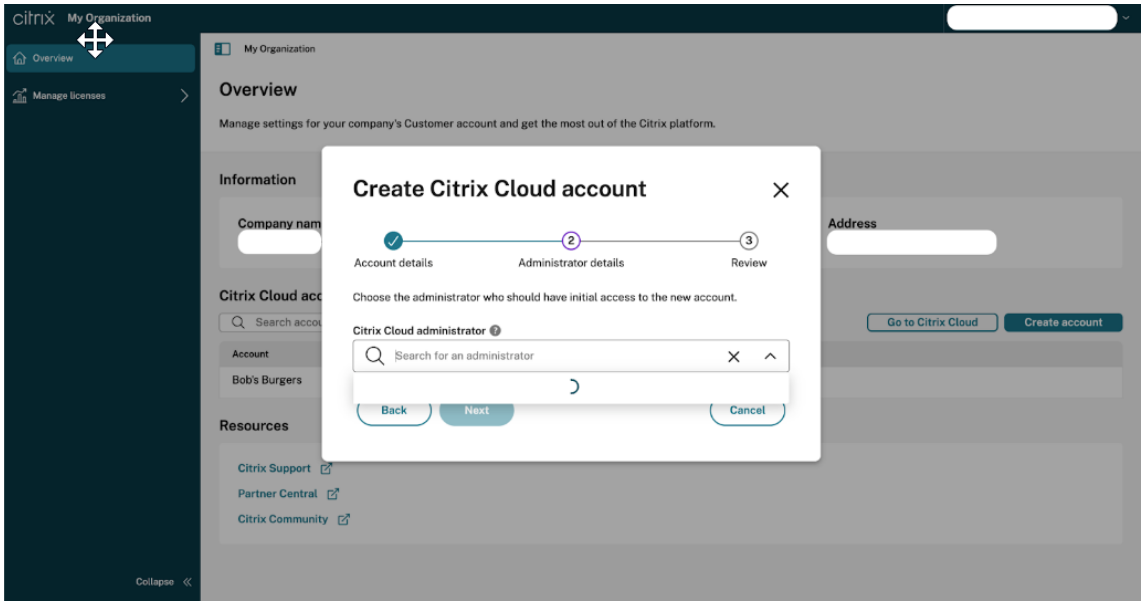


Note:

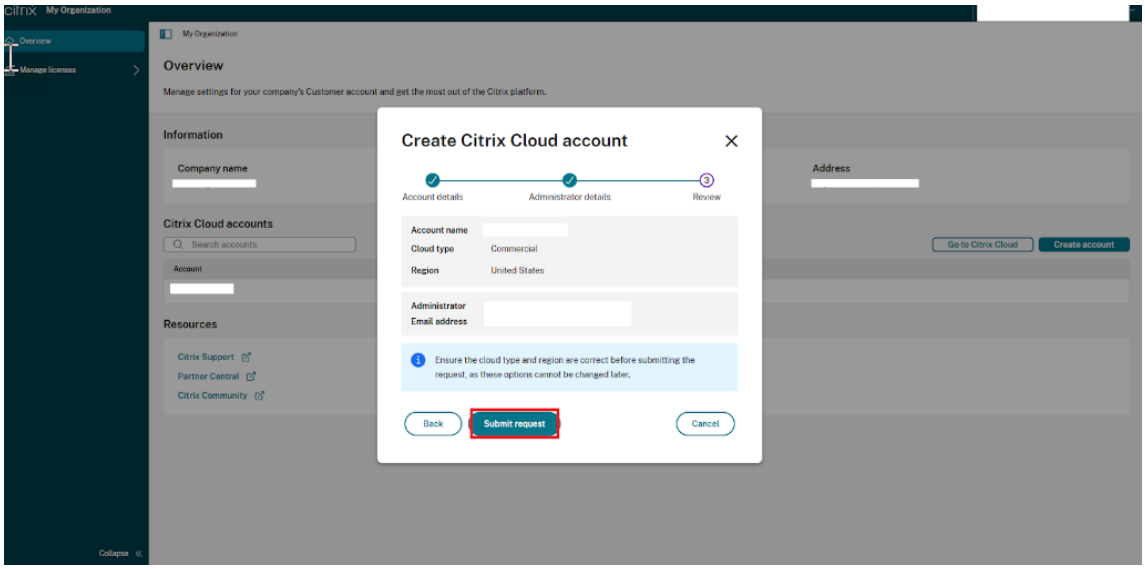
The Cloud type available options are Government, Japan, and Commercial.

4. Select the **Citrix Cloud administrator** who should have initial access to the account. This administrator receives the initial login information. Then click **Next**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

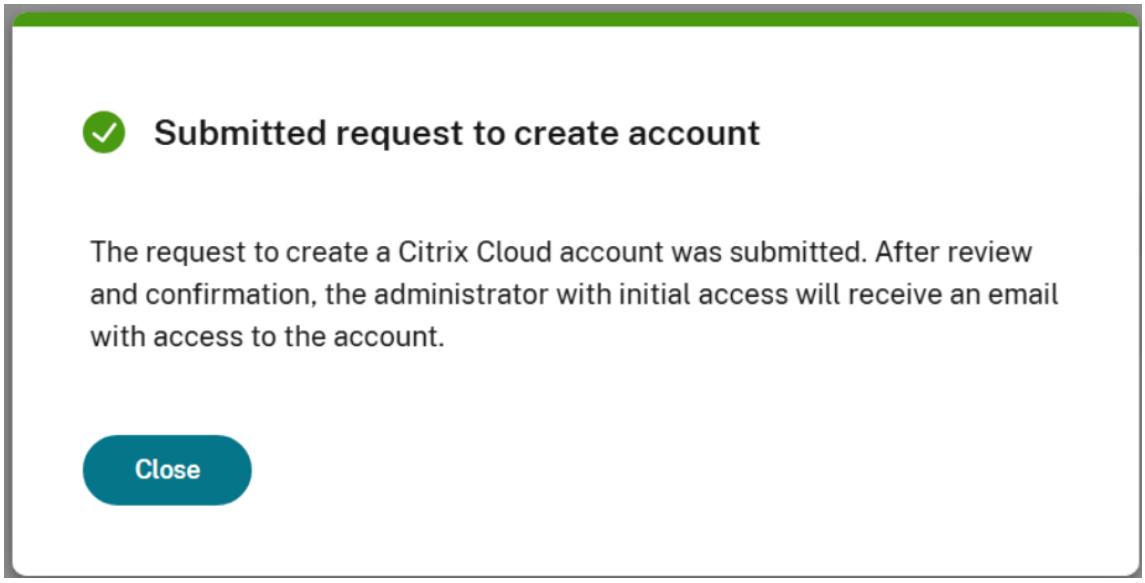


5. Confirm the **Account name**, **Cloud type**, and **Administrator** details, and then click **Submit request**.



6. You notice a pop-up message stating that the Account is successfully created.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> If the submission to create a Citrix Cloud account fails, contact the Customer support team for assistance.

License Management

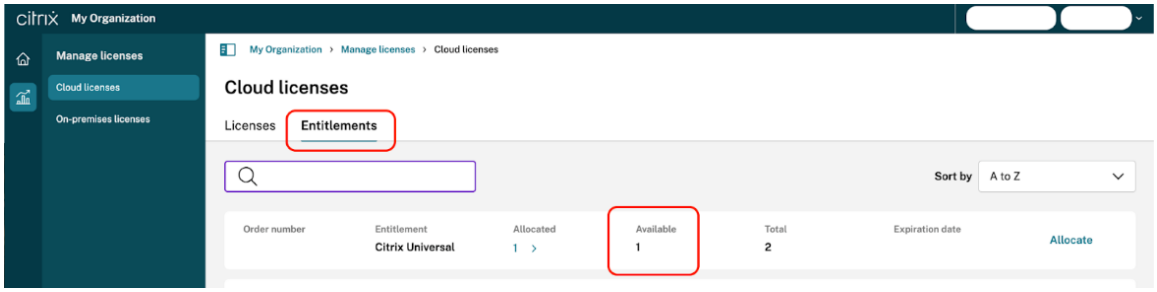
A. Cloud License Management

License Allocation

The user now has access to allocate the licenses to their Citrix Cloud customer accounts.

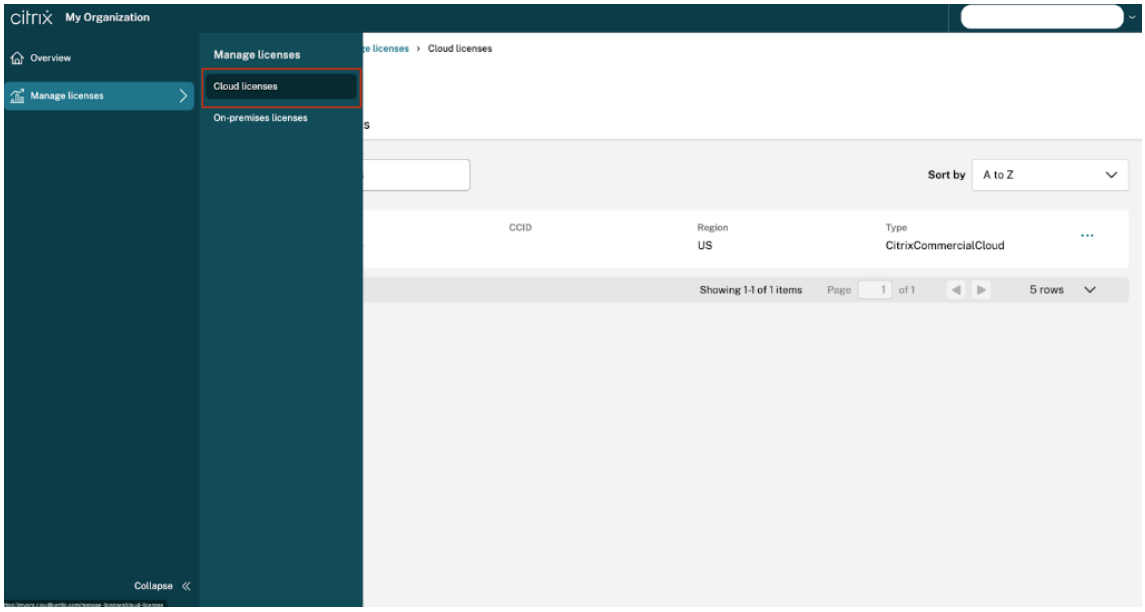
> **Note:**
>
> License allocation across different control planes (such as Government, Japan, and Commercial) from legacy license models (excluding UHMC and CPL) is not supported.
>
> Make sure you have the required licenses available to be allocated to the Citrix Cloud account. Please check the same from **My Organization > Manage Licenses > Cloud Licenses > Entitlements**. Otherwise, make licenses available by performing Deallocation from suitable Entitlements. Refer to the License Deallocation section to learn more on Deallocation steps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

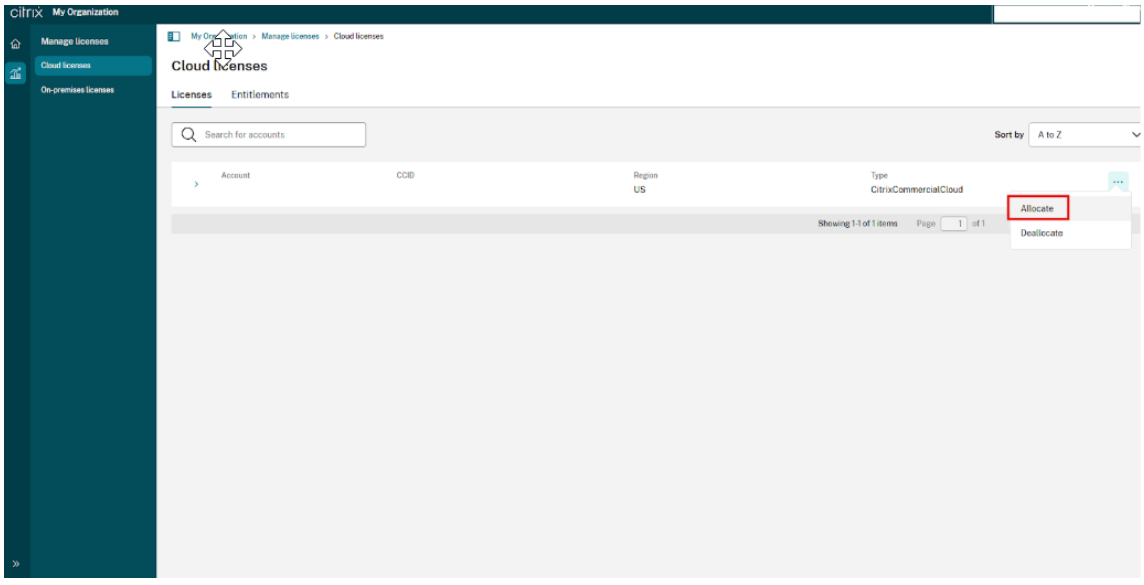


To allocate licenses to an account, use the following steps:

1. Navigate to the **Manage Licenses** section and click **Cloud Licenses**.

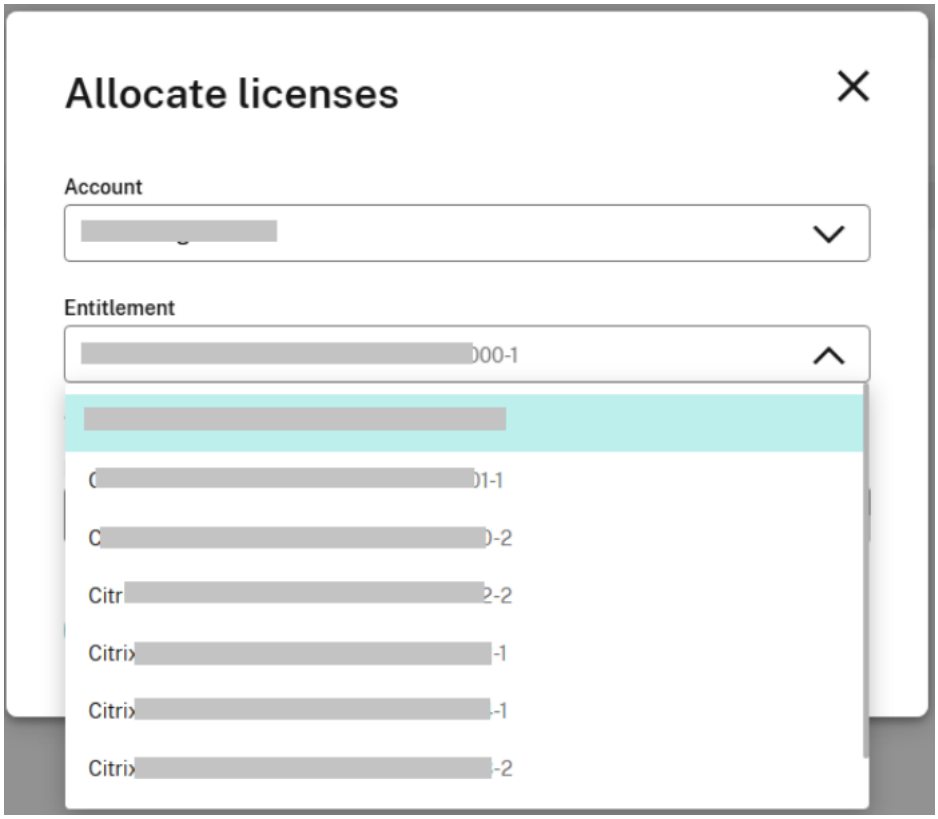


2. Click the ellipses for the new account and select **Allocate**.

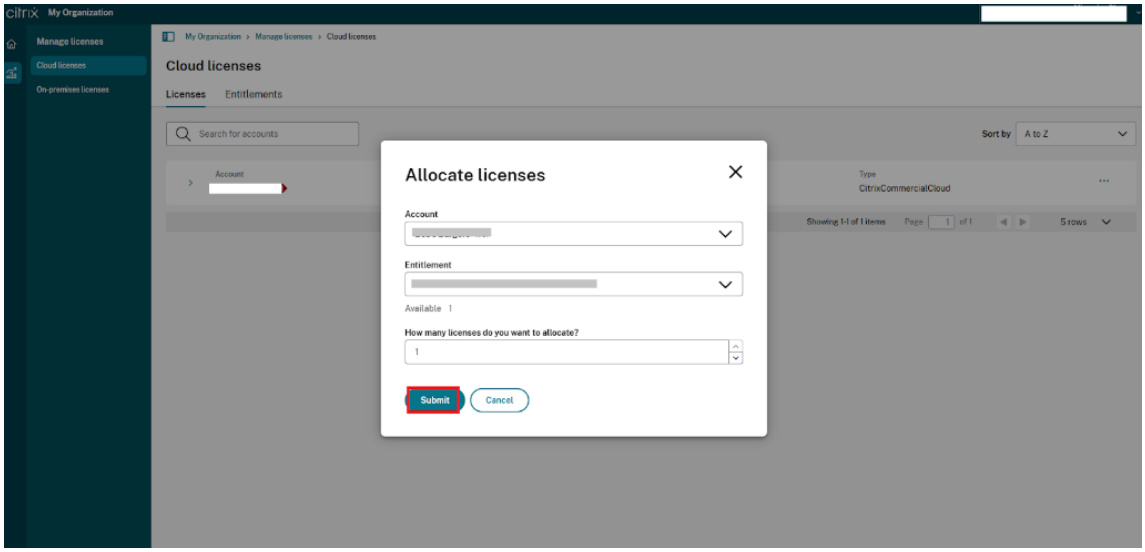


© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Select the **Entitlement** from the available list in the drop-down list options.

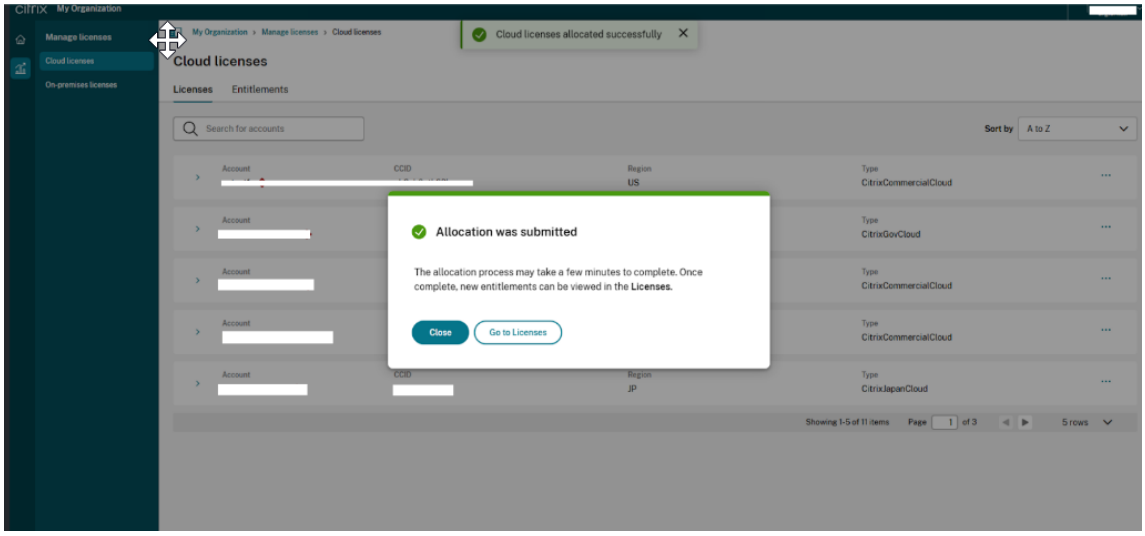


4. Specify the quantity of each product to allocate at the account level and click **Submit**.

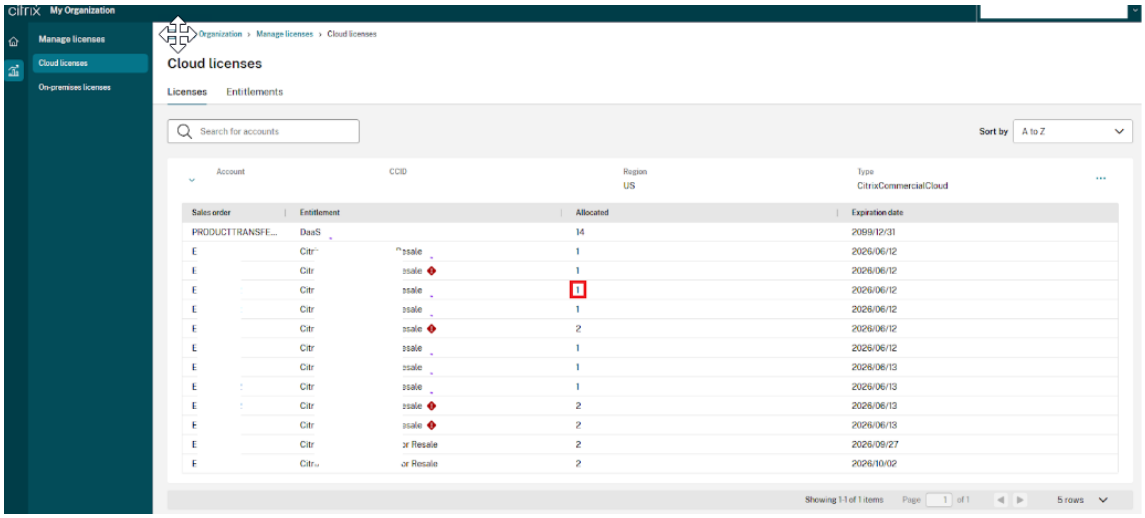


5. After successfully submitting the Allocation request, click **Close**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



6. To verify the allocation, from **Manage Licenses** > **Cloud Licenses**, extend the account to see the quantity after allocation.



> **Note:**
>
> After completing the procedure, allocations will be in progress for a few hours to enable all services and assign licenses to the account. During this time, customers notice an icon indicating the processing status. Once the allocation is completed, the icon disappears, allowing them to proceed to the Cloud Admin console and start using the services. If an allocation fails, contact Citrix Customer Support for assistance.

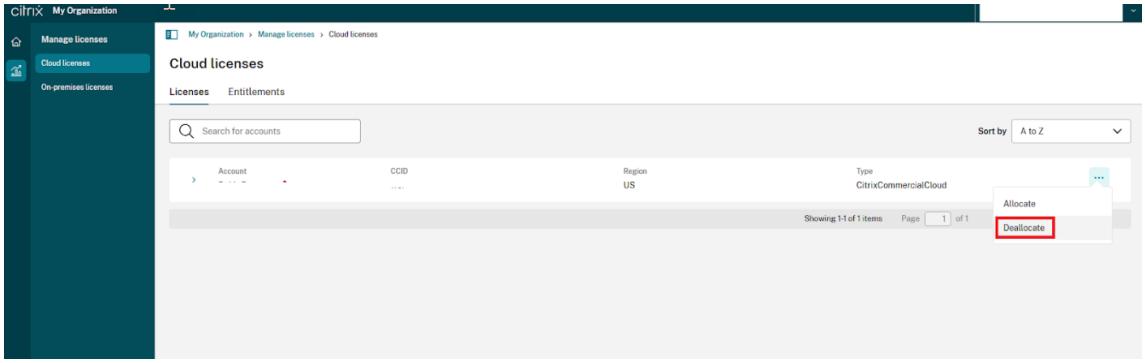
License Deallocation

To deallocate licenses from an account, use the following steps:

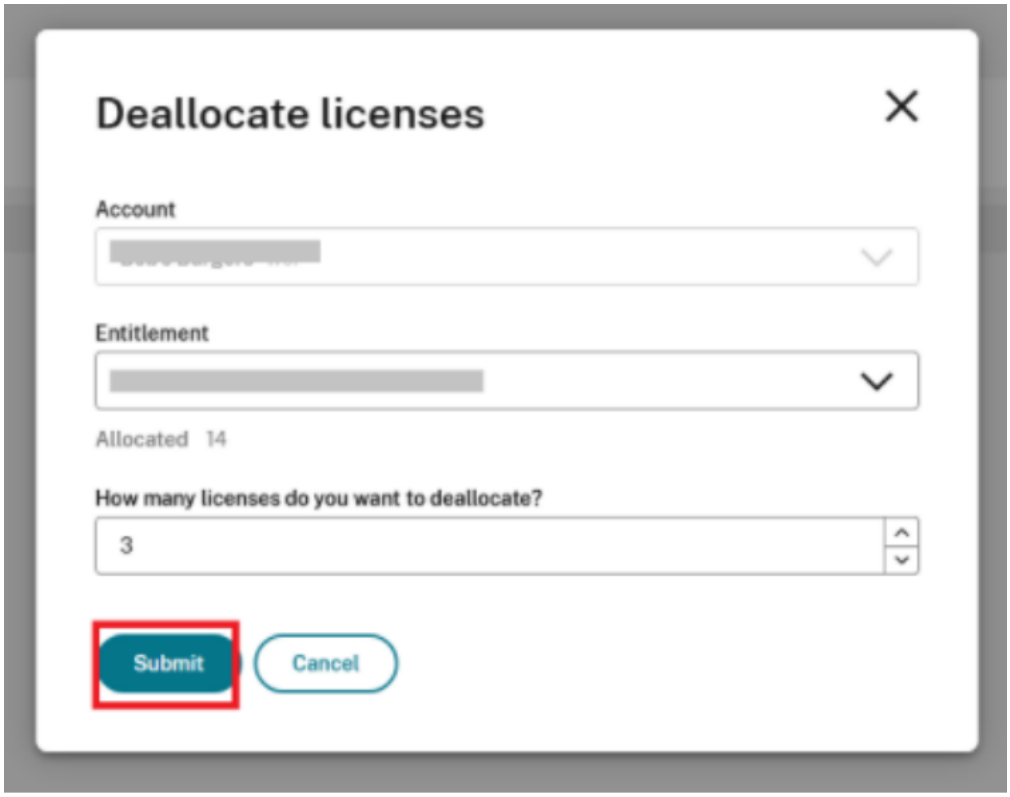
1. Navigate to the **Manage Licenses** page and click **Cloud Licenses**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Click the ellipses for the new account and select **Deallocate**.

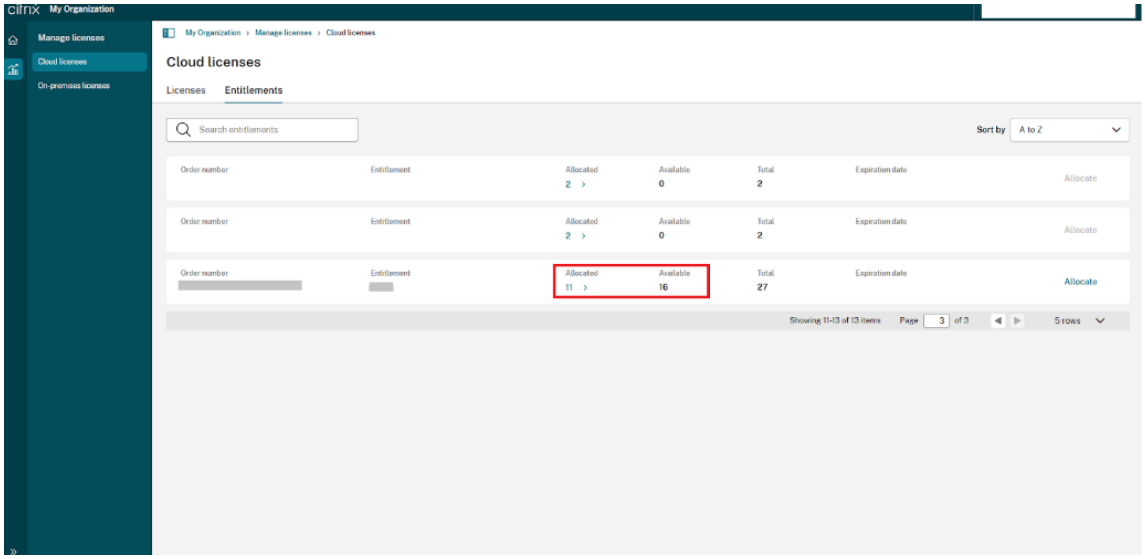


3. Select the **Account** from the drop-down list. Ensure that you select the correct account.
4. Select the **Entitlement** from the drop-down list, enter the number of licenses to deallocate in the **Quantity** tab and click **Submit**.



5. Verify the deallocation. From **Manage Licenses** > **Cloud Licenses>Entitlements**, extend the account to see the quantity after deallocation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Known issue

Duplication of Products (Manage Licenses > Cloud Licenses)

Customers might encounter duplicate product records with the same license quantities associated with a single sales order. These duplicates can show up under Entitlements **(Manage Licenses > Cloud Licenses> Entitlements)** or be directly allocated to their Citrix Cloud account. As a result, customers might be incorrectly entitled to create an additional Citrix Cloud account with the "Create account"button, or to allocate additional licenses from the duplicated products to a new Citrix Cloud account.

Recommendation

This is a known issue, and Citrix is actively working to resolve it by removing ineligible duplicate orders. If a customer creates cloud tenants and performs license allocation or deallocation to and from these tenants, the upcoming fix from Citrix might affect their services. Therefore, if customers find themselves in this situation, they should contact the Citrix Customer Service team to verify their eligibility for creating new Citrix Cloud tenants and to ensure they have the correct privileges for cloud tenant creation and/or for any license allocation or deallocation.

Rebranded Order

Customers might notice multiple allocations for a rebranded product in the **Manage License**. The original product allocation appears alongside two or three additional products, all sharing license quantity, expiry dates, and sales order.

Customers can identify the rebranded orders if they see more than one allocation for the same asset that has identical license quantities and expiry dates. All duplicate allocations display "DaaS"as the product name. Customers can check if they have a rebranded order by:

- Reviewing their purchased assets in **Manage Licenses > Cloud Licenses > Entitlements** and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

comparing them with the packages listed for allocation.
- By examining the network trace in a browser, you can see multiple IDs in the allocations list following the pattern <Random_GUID>-<OrderId>, where the OrderId repeats but the Random_GUID does not.

Recommendation
This is a known issue, and Citrix is actively working to resolve it by removing any invalid orders. Before creating an account, customers are expected to follow the steps outlined in Create a Citrix Cloud account to ensure that they are creating an account they are eligible for and to avoid creating an account, which they are not eligible for. If customers notice any invalid or duplicate orders on their account, they can contact the Customer Service team.Additionally, any Citrix Cloud customer instances created due to eligibility from invalid orders are removed, potentially affecting customer operations.

Custom landing page

September 6, 2025

Many administrators access the Cloud Console to perform specific tasks like managing applications in the Web Studio console or viewing data in DaaS - Monitor.
However, these tasks require multiple clicks and navigating through multiple pages every time the admins log in, which can be time-consuming. This new feature allows admins to set or modify a custom landing page, saving time and providing an enhanced console experience.

Currently, the following pages are available to be configured as a custom landing page, with more expected to be added in the future:

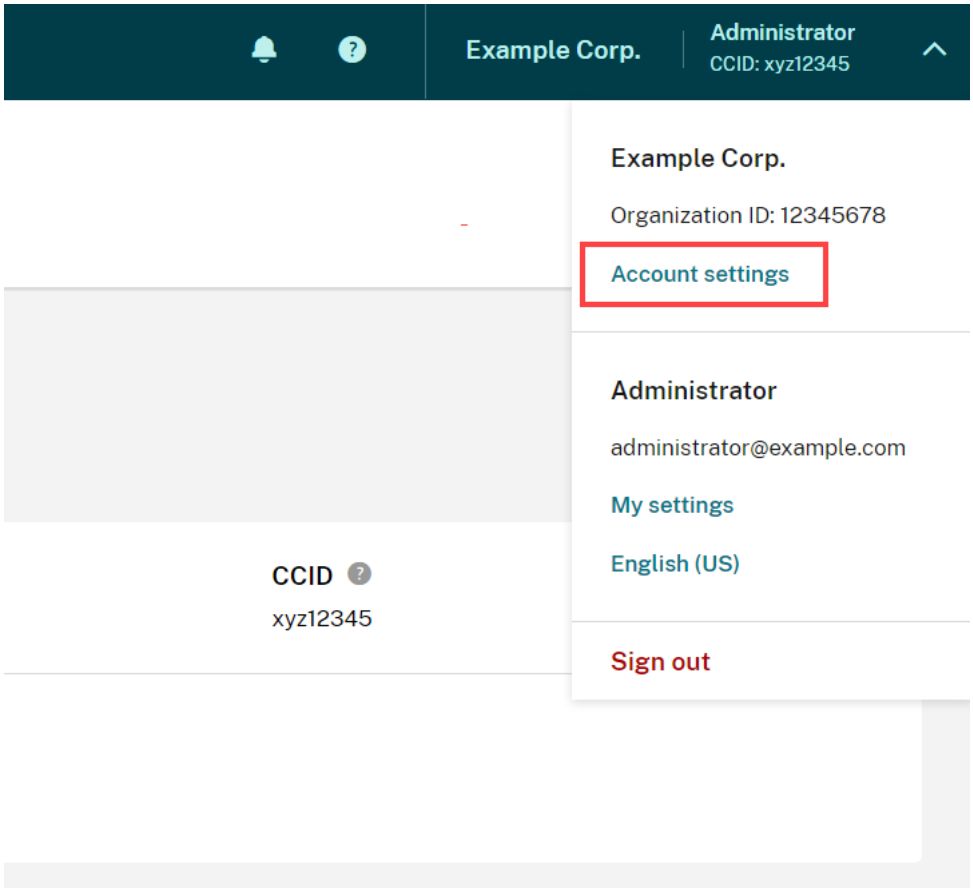
- DaaS
- DaaS-Monitor
- NetScaler® Console
- CAS
- CAS Security
- CAS Performance
- WEM
- General

> **Note:**
>
> The custom landing page setting is optional, and is set on a per account basis. So each administrator can customize their own experience within Citrix Cloud. All admins (whether custom or full) have access to this feature.

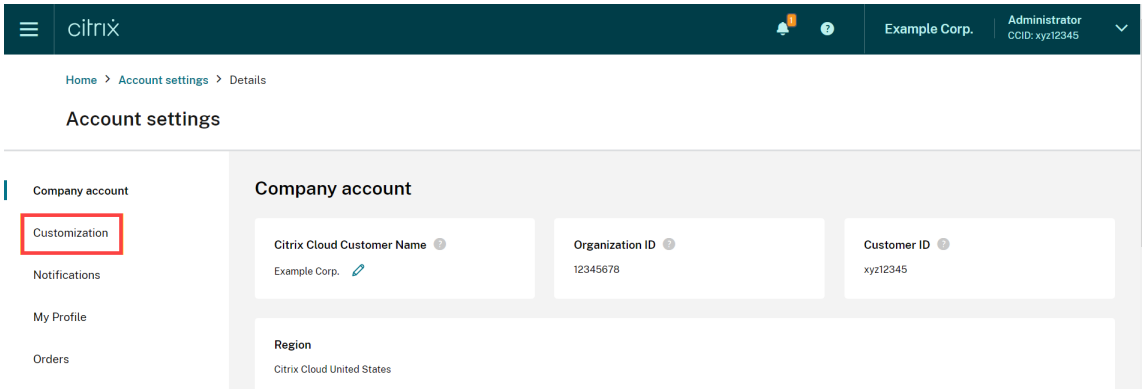
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure a custom landing page

1. Click the profile name and select **Account Settings**.

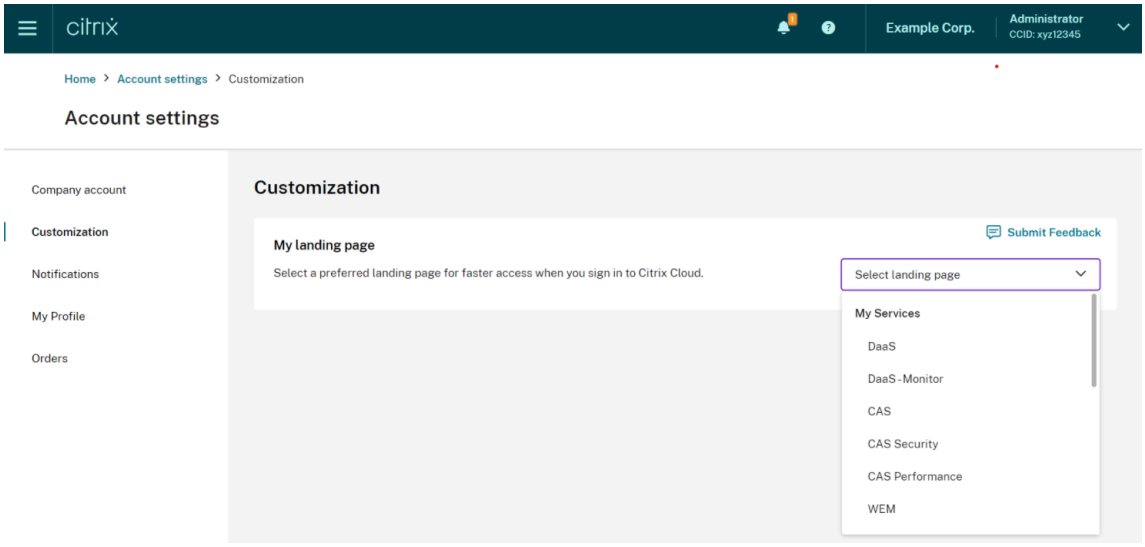


2. Click **Customization**.



3. Select the service you would like to configure as your custom landing page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Click **Apply**.

   Your custom landing page is now set.

> **Note:**
>
> - You can reset your custom landing page to the default Cloud home page anytime by clicking **Reset to default**.
> - If you sign in again on the same page where you just signed out, it will take you to your last viewed page instead of your new landing page.

How to delete Citrix Cloud™ account and re-onboard

March 24, 2026

Citrix Cloud offers the capability for customers to securely delete their Citrix Cloud account and seamlessly re-onboard when required.

Prerequisites

- If your account has active DaaS entitlements and your DaaS environment is provisioned, contact Citrix Technical Support to execute Fast Decommission before proceeding. See Studio Console Shows "Enable DaaS"for First Time Use article for details on how to check if your DaaS environment is provisioned.
- Remove all Cloud Connectors and Connector Appliances associated with this account.

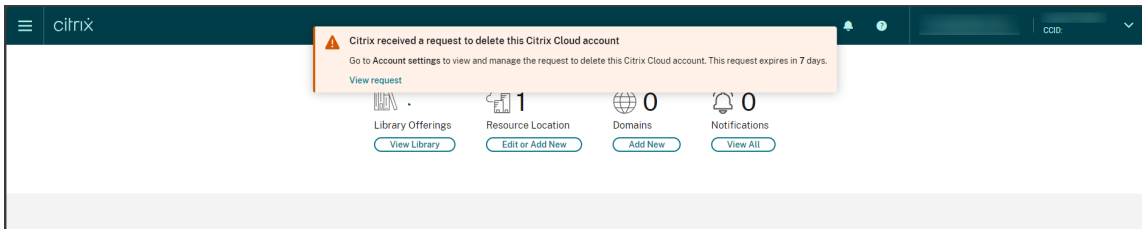
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Customers must have administrator access to their Citrix Cloud account to execute the delete request.
  - For customers without administrator access to their Citrix Cloud account, access must be obtained through SSAO before proceeding with delete requests.
  - If only one administrator has access, that administrator must remove other admins.
- Remove registration of your License Server. If you want to register your License Server with a different or new Citrix Cloud account, see Remove Registration for the required steps.

> **Important**
>
> Consider the following points before deleting a Citrix Cloud account:
>
> - All customer-related data is removed from Citrix® databases.
> - All resources related to Citrix Cloud services, including Citrix-managed VMs, that Citrix provisioned in your cloud environment will be deleted. See Citrix Cloud services for the description of the Citrix-managed components that are included in specific Citrix Cloud services.
> - Administrator and user access to Citrix Cloud and services are disabled.
> - Administrators or users actively using the service will experience service disruption.
> - This action is not reversible. Once the data is deleted, it cannot be recovered.

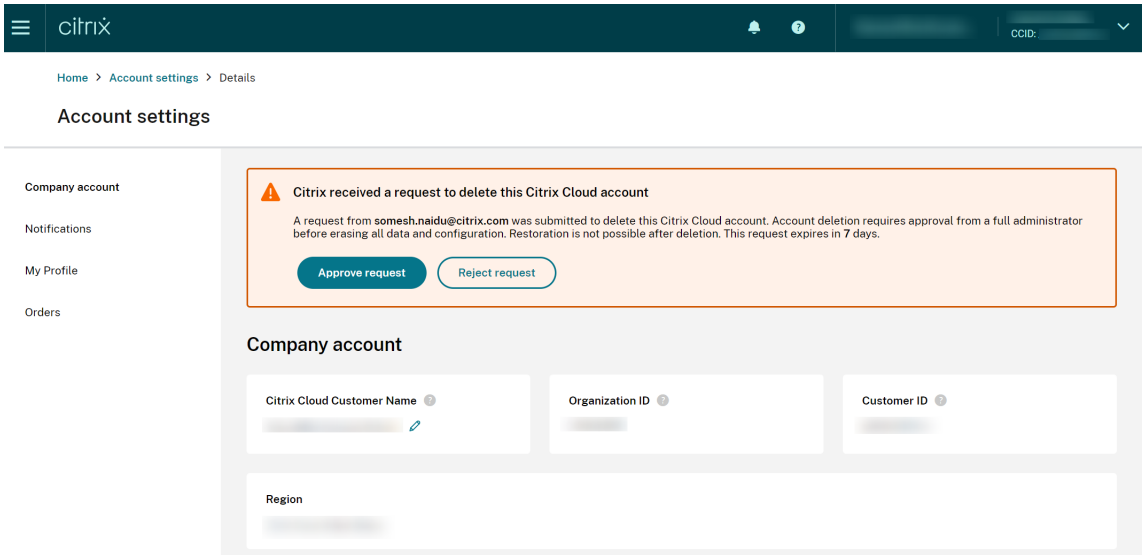
Steps

1. Contact Citrix Customer Service to submit a delete request. A *Full Administrator* on the Citrix Cloud account is required to submit this request.
2. After your request is initiated, login to your Citrix Cloud account. There you'll see the Citrix Cloud account delete workflow.

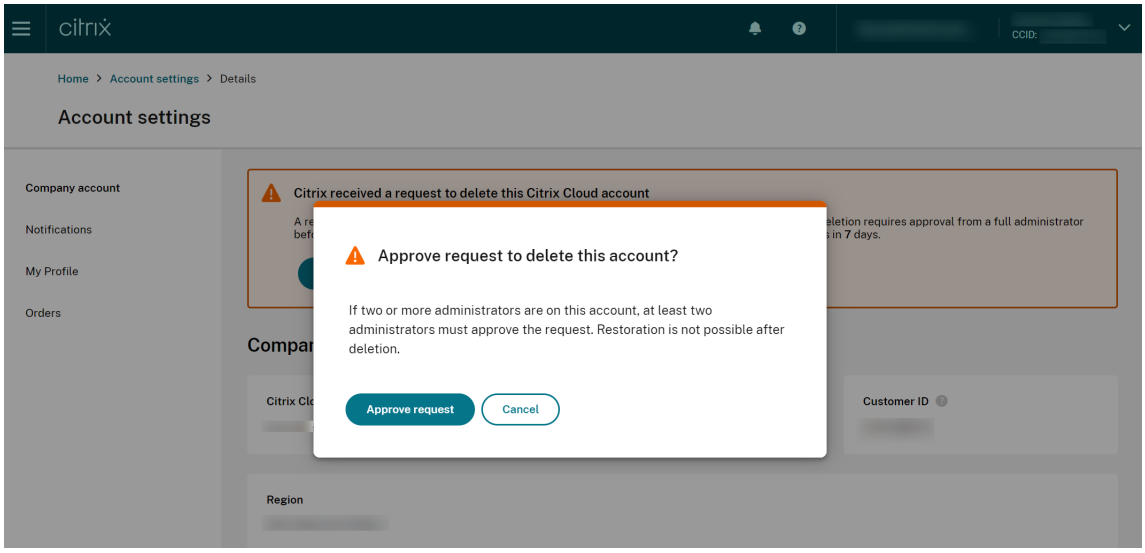


3. Follow the on-screen guidance to either approve or reject this request.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. To approve this request for deletion, sign in to the account, navigate to **Account Settings** and click **Approve request** on the approval workflow banner.



To cancel the request for deletion, sign in to the account, navigate to **Account Settings** and click **Reject and remove request** on the delete approval workflow banner.

> **Note:**
>
> - If this account has two or more administrators associated with it, at least two administrators must approve the request.
> - This request expires if required approvals are not received within 7 days.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Network locations

October 12, 2026

Within Citrix Cloud™, you can configure network locations according to their public IP addresses. These network locations can be used for the following:

- Citrix® StoreFront Cloud uses the network location to determine whether to instruct clients to connect directly to VDAs or via a Citrix Gateway. For more information, see Connectivity to DaaS resources.
- When users connect from a network location, the StoreFront Cloud can add smart access tags that you can use as an input to access policies within Studio. For more information, see Adaptive access based on the user's network location. This functionality is only available when Adaptive Access is enabled.
- You can choose how users authenticate based on the user's network location. For more information, see Conditional Authentication.
- You can configure different timeouts depending on the network location connectivity type. For more information, see Configure sessions per network connectivity type.

Typically you create a Network Location for each of your office locations.

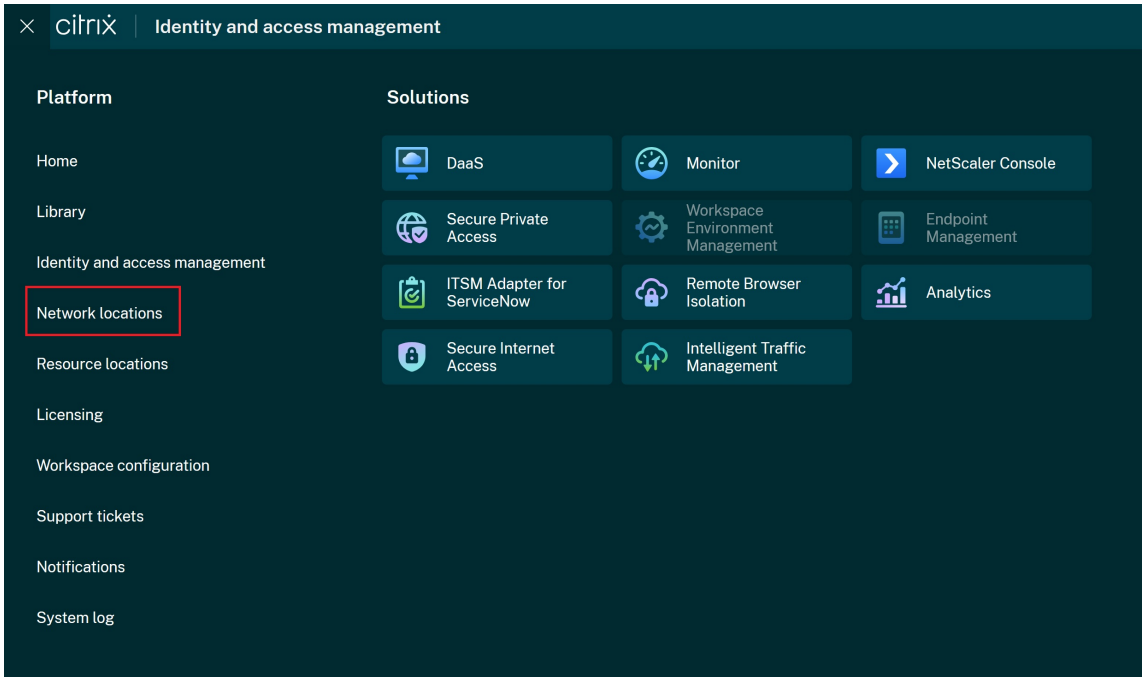
> **Note:**
>
> It is not possible to distinguish between different networks with the same public IP address. For example if your corporate network and guest Wi-Fi network share a public IP address they are considered the same network location.

View network locations

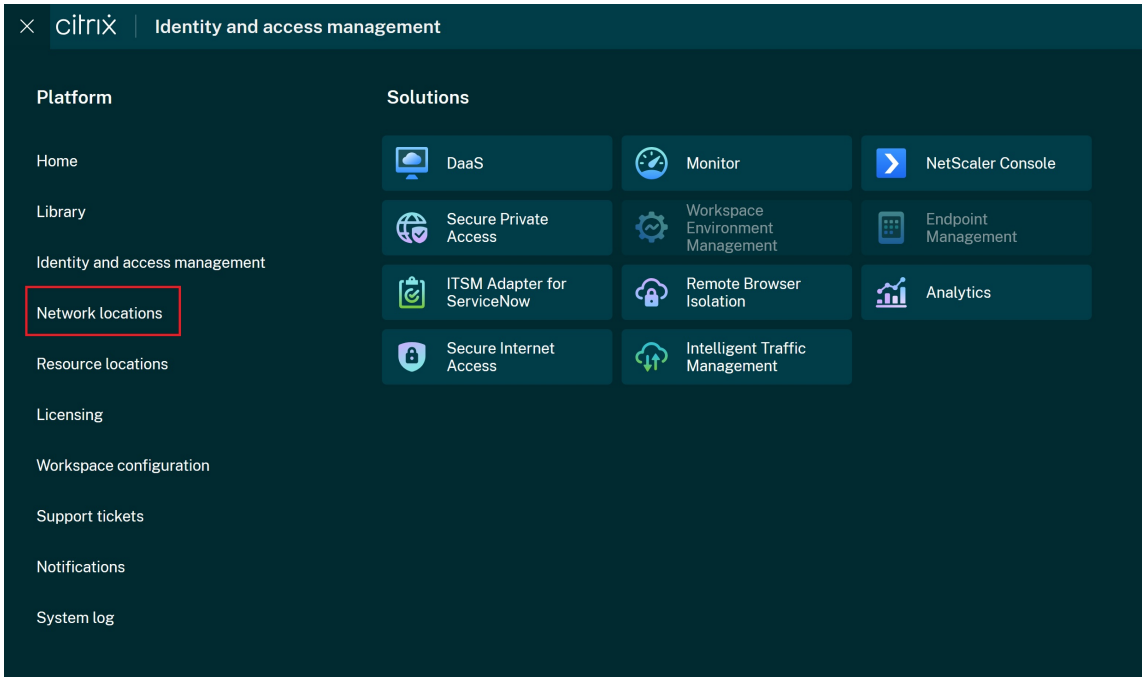
To view the configured network locations:

1. Log in to Citrix Cloud.
2. Open the main menu.
3. From the main menu choose **Network locations**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



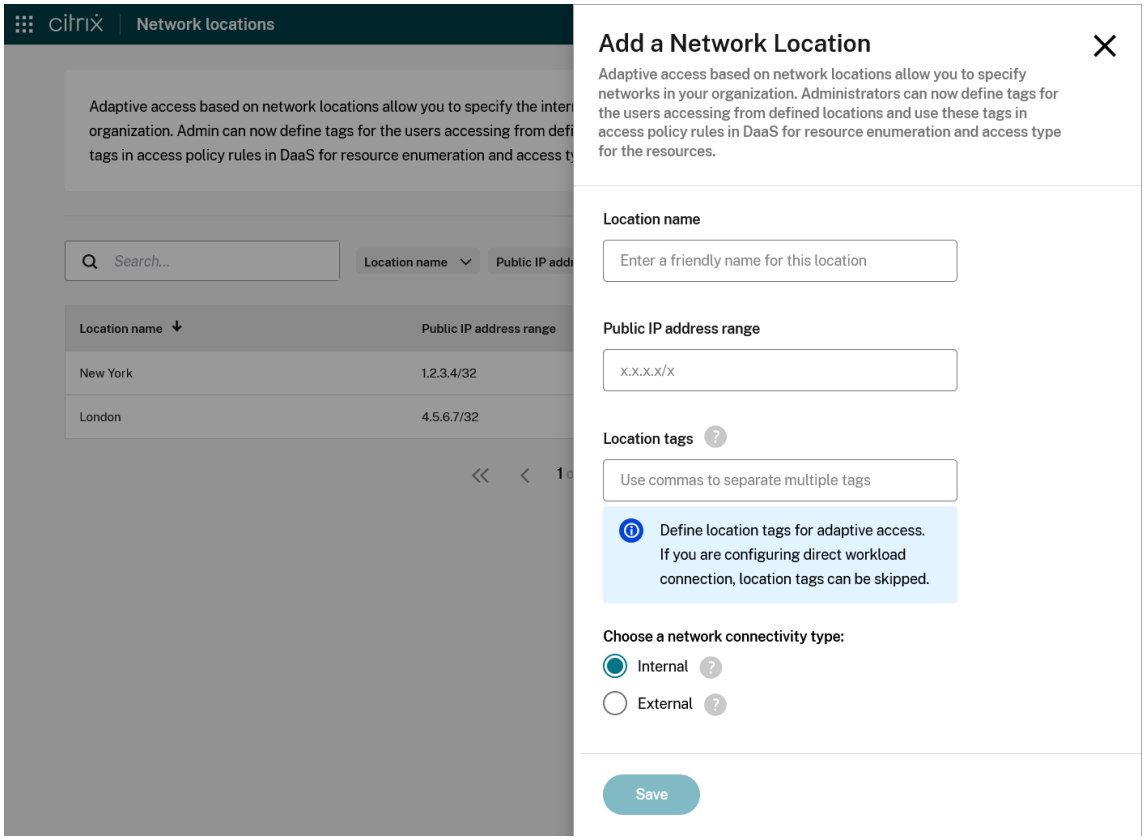
4. The Network location screen loads.



Add network location

1. On the Network locations screen, press **Add network location**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



The **Location tags** and **connectivity type** options are only available if Adaptive Access is enabled.

2. Enter a **Location name**.
3. Enter the **Public IP address range** in CIDR format.
4. If Adaptive Access is enabled, you can optionally enter the name of one or more **Location tags**. Use commas to separate multiple tags. The smart access tag is generated by adding the suffix `LOCATION_TAG_`. For instance if you enter a location tag `BranchOffice` then a smart access tag is generated called `LOCATION_TAG_BranchOffice` that you can use in Studio.
5. If Adaptive Access is enabled, you can choose whether the location is **Internal** or **External**. For all internal locations, a smart access tag is generated called `LOCATION_internal`. For all external locations, a smart access tag is generated called `LOCATION_external`. If the client's IP address does not match a network location then the network location is considered to be **Undefined**.

   If Adaptive Access is disabled then this option is hidden. All configured network locations are considered internal and it does not create any smart access tags.
6. Press **Save**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Edit network location

1. Navigate to the open the Network locations screen
2. On the row you wish to edit, press **...** to open the menu, then select **Edit**.
3. Make the required changes.
4. Press **Save**.

Delete network location

1. Navigate to the open the Network locations screen
2. On the row you wish to edit, press **...** to open the menu, then select **Delete**.
3. On the confirmation screen, press **Yes, delete**.

Manage network locations with PowerShell

Instead of using the Citrix Cloud management console interface, you can use a PowerShell script to configure Direct Workload Connection. Direct Workload Connection configuration with PowerShell involves the following:

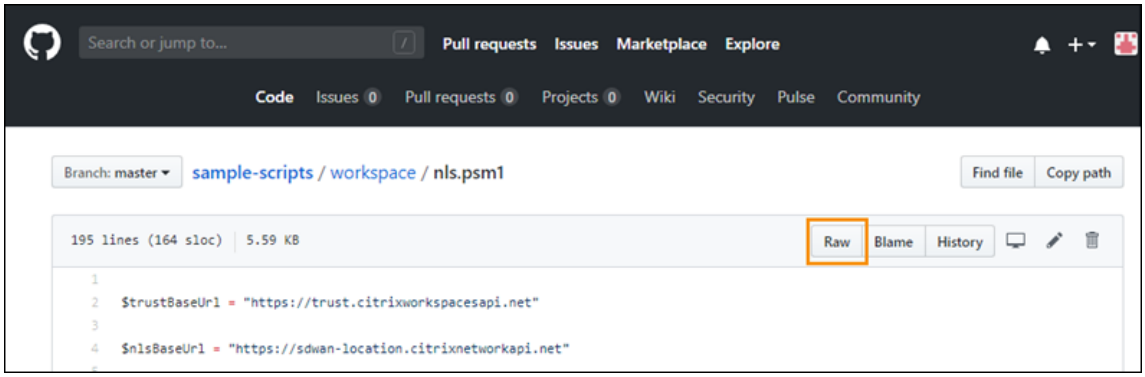
1. Download the PowerShell module.
2. Create a service principal in Citrix Cloud and make a note of the Client ID and secret.
3. Import the PowerShell module and connect to the Network Location Service (NLS) with your API client details.
4. Use the PowerShell cmdlets to create network locations for each of your locations.

Download the PowerShell module

Before you set up your network locations, download the Citrix-provided PowerShell module (nls.psm1) from the Citrix GitHub repository. Using this module, you can set up as many network locations as needed for your VDAs.

1. In a web browser, go to https://github.com/citrix/sample-scripts/blob/master/workspace/NLS2.psm1.
2. Press **Raw**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



3. Press Ctrl+S and select a location to save the file.

Create a service principal

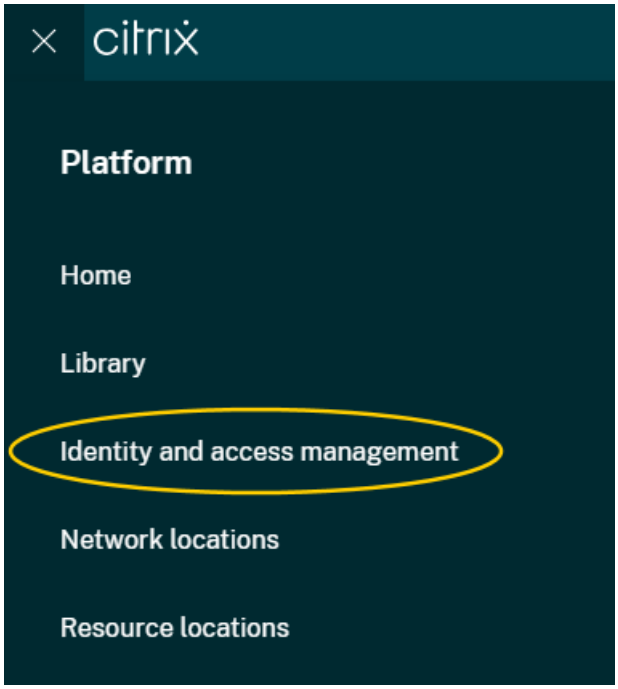
1. In the Citrix Cloud console, click the menu in the upper left corner.

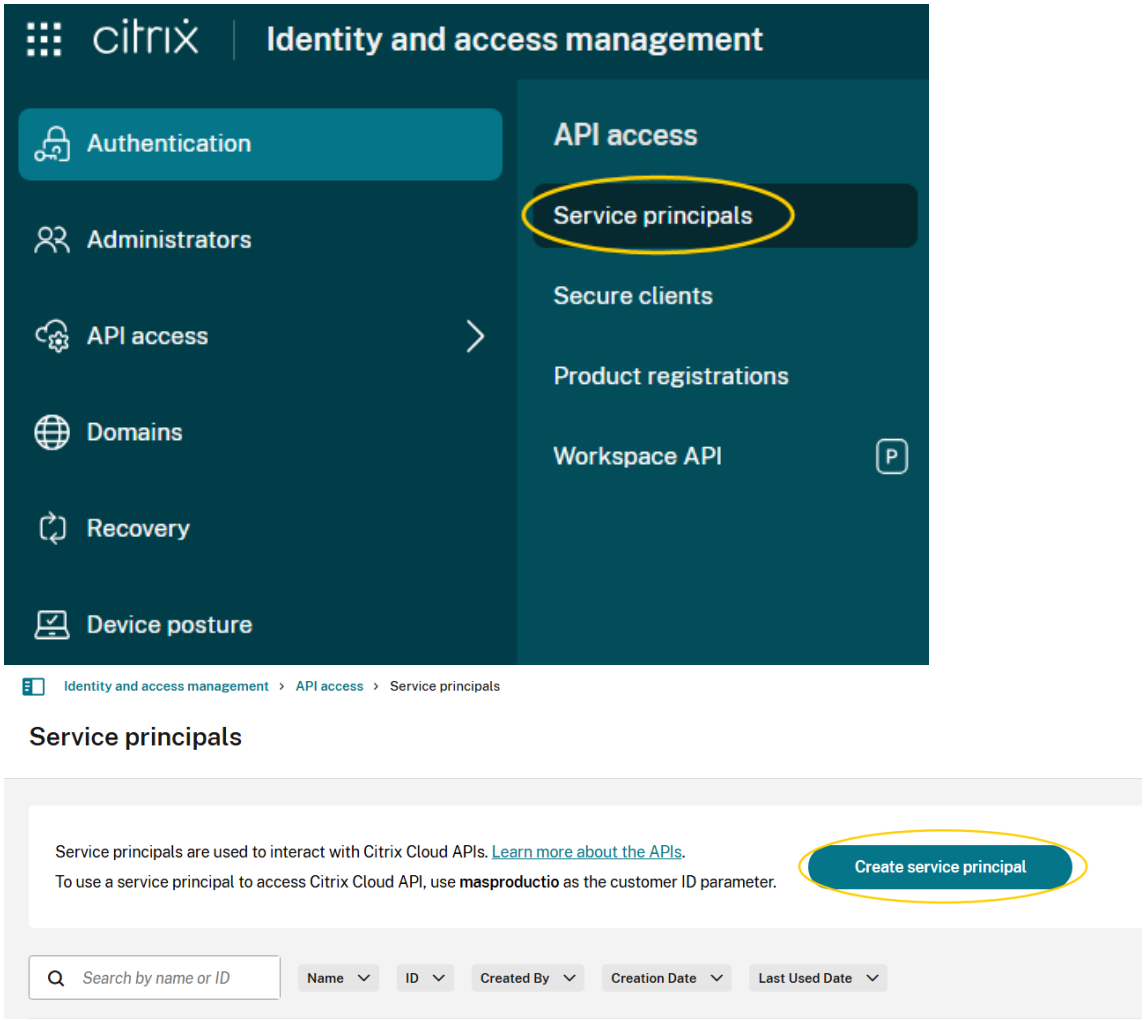
2. Select **Identity and access management** > **API access** > **Service principals** > **Create service principal** and follow the steps to completion.

   If these options do not appear, you might not have sufficient permissions to manage service principals. Contact your administrator to get the required full access permission.

3. On the **Service principal** tab, note your customer ID.

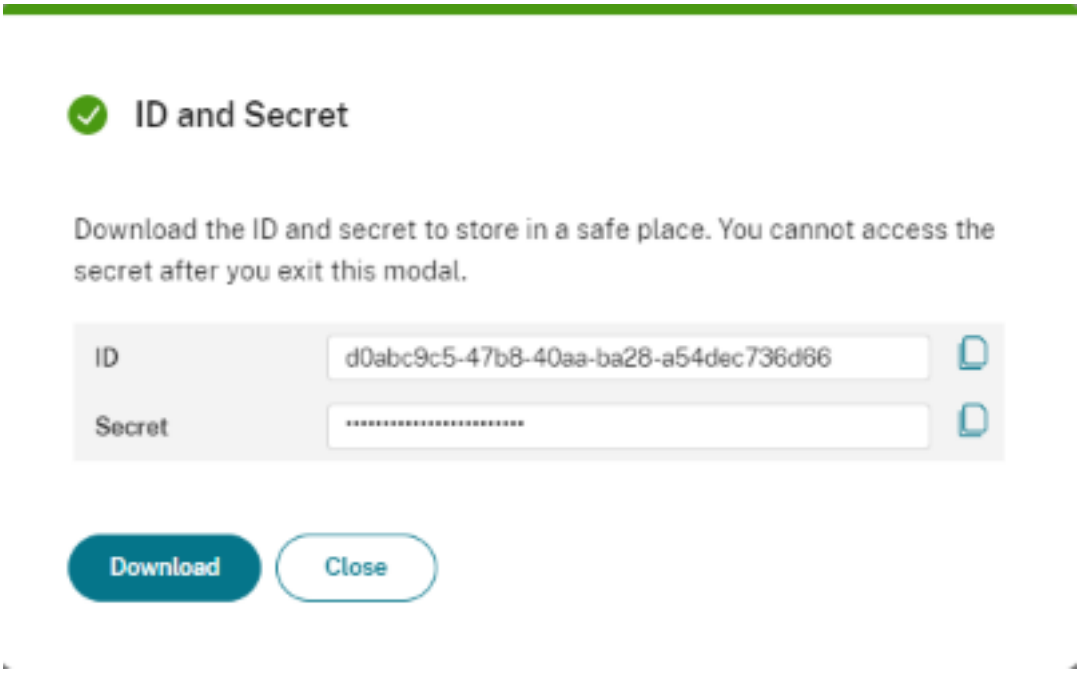
   

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. Add the credentials to your secret management tool as the secret will only appear once.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Configure network locations

1. Open a PowerShell command window and navigate to the same directory where you saved the PowerShell module.
2. Import the module: `Import-Module .\nls.psm1 -Force`
3. Set the required variables with your service principal information from Create a service principal:
   - `$clientId = "YourServicePrincipalClientId"`
   - `$customer = "YourCustomerID"`
   - `$clientSecret = "YourServicePrincipalSecret"`
4. Connect to the Network Location Service with your service principal credentials:

```
Connect-NLS -clientId $clientId -clientSecret $clientSecret -
    customer $customer
```

5. Create a network location, replacing the parameter values with the values that correspond to the internal network where your internal users are directly connecting from:

```
New-NLSSite -name "YourSiteName" -tags @("YourTags") -ipv4Ranges @
    ("PublicIpsOfYourNetworkSites") -longitude 12.3456 -latitude
    12.3456 -internal $True
```

   To specify a single IP address instead of a range, add **/32** to the end of the IP address. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
New-NLSSite -name "YourSiteName" -tags @("YourTags") -ipv4Ranges @
    ("PublicIpOfYourNetworkSite/32") -longitude 12.3456 -latitude
    12.3456 -internal $True
```

> **Important:**
>
> When using the `New-NLSSite` command, include at least one value for each parameter. If you run this command without any command-line arguments, PowerShell prompts you to enter the appropriate values for each parameter, one at a time. The `internal` property is a mandatory Boolean property with possible values: `$True` or `$False` that maps to the UI via PowerShell. For example, `(UI)Network Internal -> (PowerShell)-internal=$True`.

When the network location is created successfully, the command window displays the details of the network location.

6. Repeat Step 5 for all your network locations where users are connecting from.
7. Run the command `Get-NLSSite` to return a list of all the sites you've configured with NLS and verify that their details are correct.

Modify network locations

To change an existing network location:

1. From a PowerShell command window, list all existing network locations: `Get-NLSSite`
2. To modify the IP range for a specific network location, type

```
(Get-NLSSite)[N] | Set-NLSSite -ipv4Ranges @("1.2.3.4/32","
    4.3.2.1/32")
```

where `[N]` is the number corresponding to the location in the list (starting with zero) and `"1.2.3.4/32","4.3.2.1/32"` are the comma-separated IP ranges you want to use. For example, to modify the first listed location, you type the following command:

```
(Get-NLSSite)[0] | Set-NLSSite -ipv4Ranges @("98.0.0.1/32","
    141.43.0.0/24")
```

Remove network locations

To remove network locations that you no longer want to use:

1. From a PowerShell command window, list all existing network locations: `Get-NLSSite`
2. To remove all network locations, type `Get-NLSSite | Remove-NLSSite`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. To remove specific network locations, type `(Get-NLSSite)[N] | Remove-NLSSite`, where `[N]` is the number corresponding to the location in the list. For example, to remove the first listed location, you type `(Get-NLSSite)[0] | Remove-NLSSite`.

Example script

The example script includes all commands that you might need to add, modify, and remove the public IP address ranges for your branch locations. However, you don't need to run all commands to perform any single function. For the script to run, always include the first 10 lines, from **Import-Module** through **Connect-NLS**. Afterward, you can include only the commands for the functions you want to perform.

```
Import-Module .\nls.psm1 -Force

$clientId = "XXXX" #Replace with your clientId
$clientSecret = "YYY"    #Replace with your clientSecret
$customer = "CCCCCC"  #Replace with your customerid

# Connect to Network Location Service
Connect-NLS -clientId $clientId -clientSecret $clientSecret -customer $customer

# Create a new Network Location Service Site (Replace with details corresponding to your branch locations)
New-NLSSite -name "New York" -tags @("EastCoast") -ipv4Ranges @("1.2.3.0/24") -longitude 40.7128 -latitude -74.0060 -internal $True

# Get the existing Network Location Service Sites (optional)
Get-NLSSite

# Update the IP Address ranges of your first Network Location Service Site (optional)
$s = (Get-NLSSite)[0]
$s.ipv4Ranges = @("1.2.3.4/32","4.3.2.1/32")
$s | Set-NLSSite

# Remove all Network Location Service Sites (optional)
Get-NLSSite | Remove-NLSSite

# Remove your third site (optional)
(Get-NLSSite)[2] | Remove-NLSSite
```

Notifications

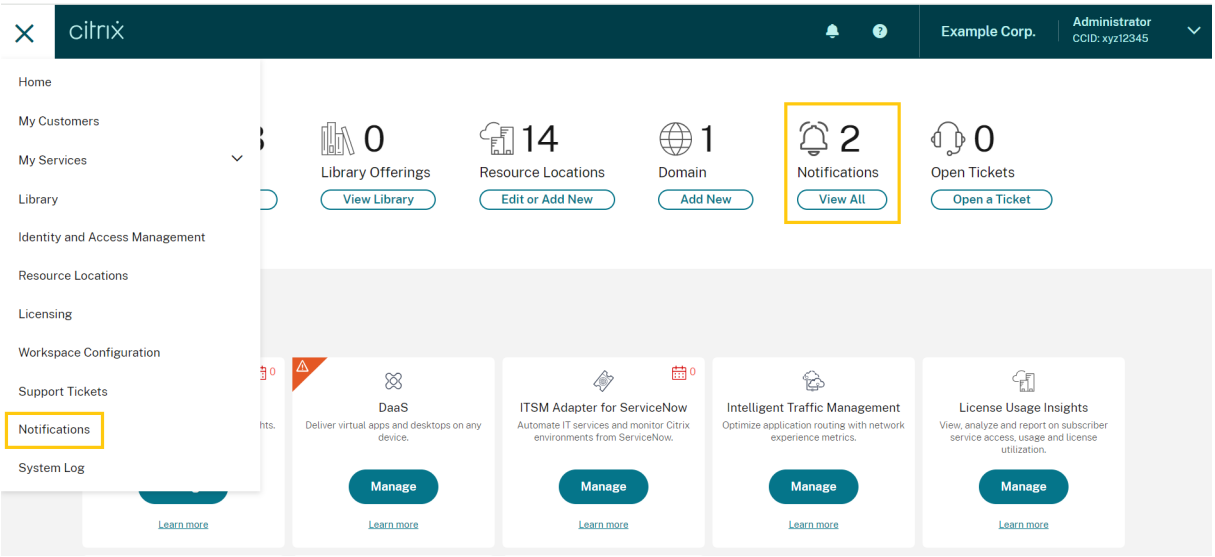
December 17, 2025

© 1997–2026 Citrix Systems, Inc. All rights reserved.

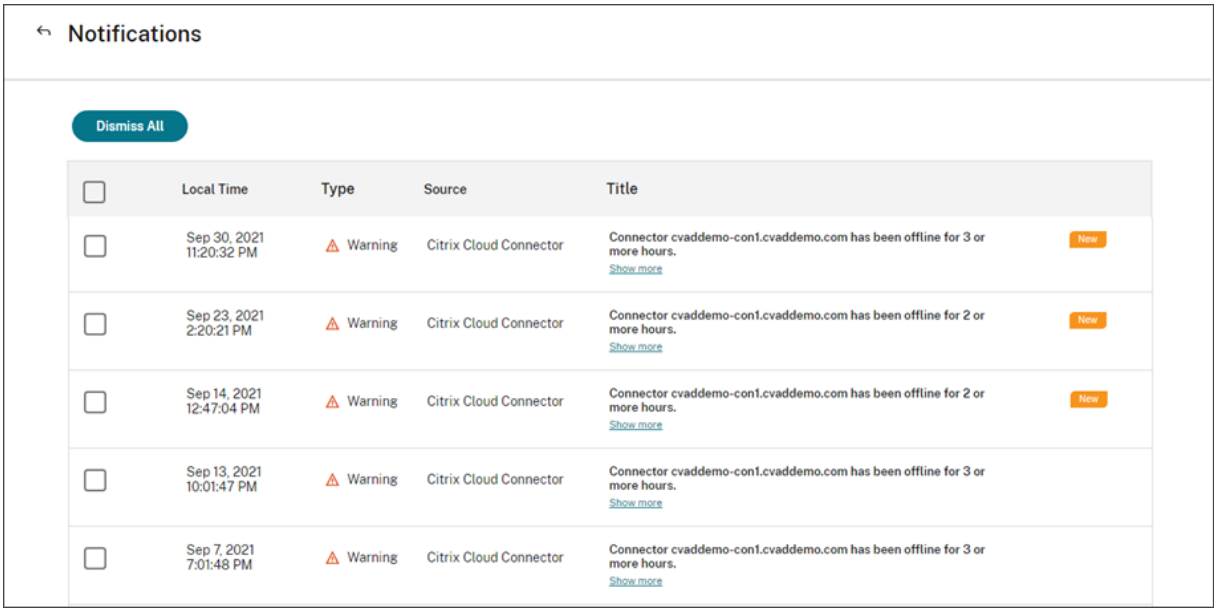
Notifications provide information about issues or events that might be of interest to administrators, such as new Citrix Cloud™ features or problems with a machine in a resource location. Notifications can come from any service within Citrix Cloud.

View notifications

The number of notifications appears near the top of the Citrix Cloud console page. For more details, click **View All** under **Notifications** in the console or select **Notifications** from the console menu.



The Notifications page displays the notifications that you receive. The newest notifications at the top of the list.



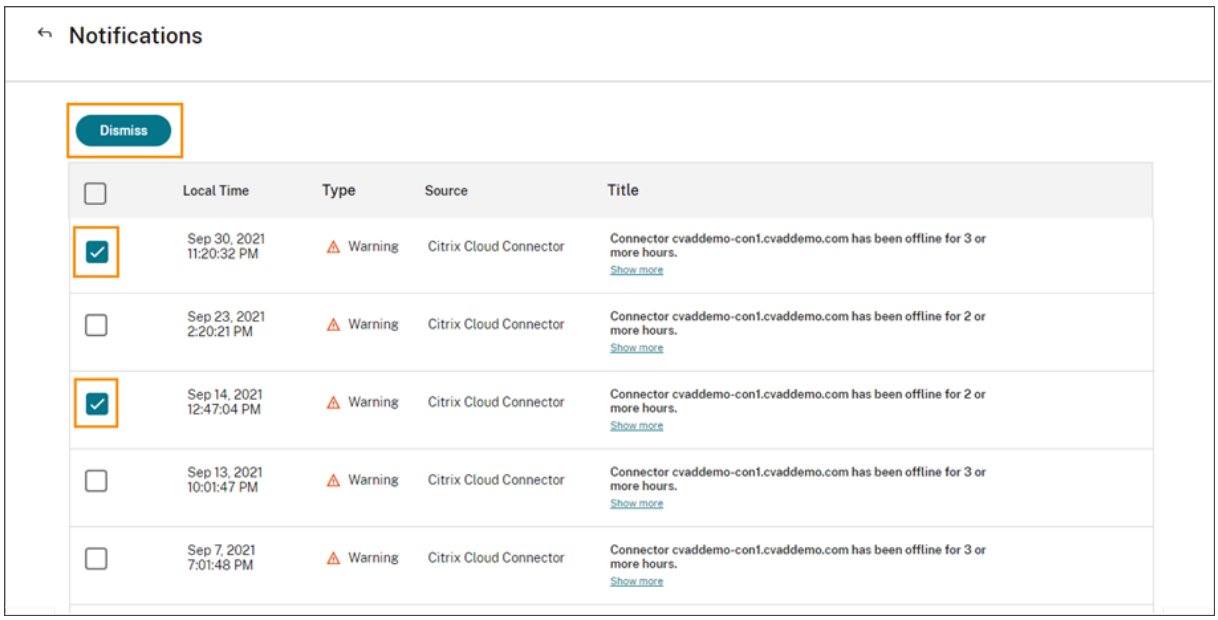
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Dismiss notifications

Notifications are managed on a per-administrator basis. When you dismiss notifications, the dismissal occurs under your own administrator identity in Citrix Cloud. Other administrators can still view and dismiss their own notifications, even if you dismiss all of your notifications.

To dismiss all notifications that you've received, select **Dismiss All** near the top of the page.

To dismiss individual notifications, select each notification and then select **Dismiss**.



Receive email notifications

You can choose to receive notifications by email instead of signing in to view them. By default, email notifications are turned off.

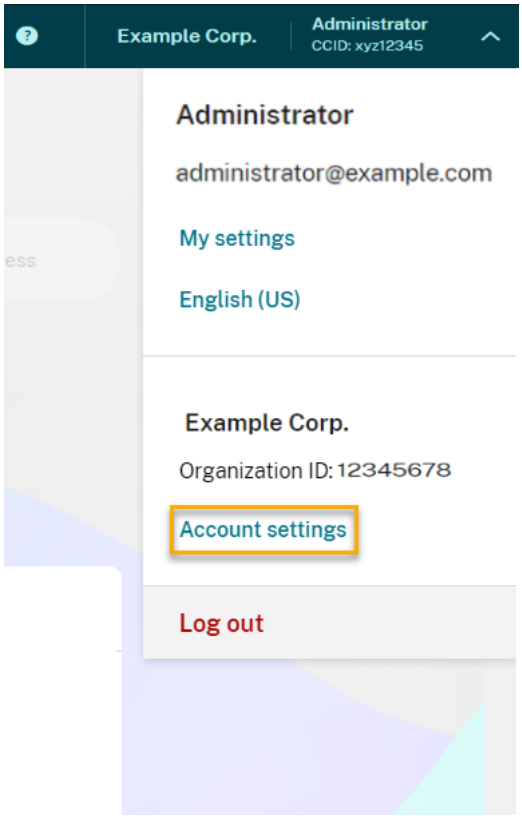
You can also enable email notifications for other stakeholders who don't have administrator access to your Citrix Cloud account, such as members of your organization's security and auditing teams.

When you enable email notifications, Citrix Cloud sends an email for each notification. Notifications are sent as soon as possible. They are not grouped into a single email or batched for sending at a later time.

To enable email notifications for yourself

1. From the Citrix Cloud management console, select **Account Settings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



2. Select **Notifications**.
3. Turn on the **My email notifications** setting.
4. Under **Manage my notification settings**, select the types of notifications you want to receive. By default, only the critical type is selected.
5. Click **Apply** to save your settings.

To enable email notifications for non-administrators

Use the steps in this section to add non-administrators as contacts for email notifications. If you attempt to add an existing administrator as a contact, Citrix Cloud displays an error.

1. From the Citrix Cloud management console, click **Account Settings**.
2. Select **Notifications**.
3. Under **Contact management**, select **Add contact**.
4. Enter the contact's name, email address, and their preferred language.
5. Under **Manage notification settings**, select the notification types to send.
6. Select **Add contact** to save the contact's information.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Modify notification settings

As an administrator, you can change the types of notifications that you receive by selecting or clearing the checkboxes under **Manage my notification settings**. Changing your notifications doesn't affect the notifications that other administrators receive.

You can also modify the notifications that non-administrators receive.

To modify notifications for non-administrators

1. From the Citrix Cloud management console, click **Account Settings**.
2. Select **Notifications**.
3. Under **Contact management**, locate the contact that you want to manage.
4. Point to the contact and then select the pencil icon.
5. Under **Manage notification settings**, select or clear the checkboxes for each notification type.

To modify a contact's email address, you must first delete the contact and then add them as a new contact with their new email address.

Disable email notifications

As an administrator, you can disable your own email notifications at any time by turning off the **My email notifications** setting.

Non-administrators can stop receiving notifications by clicking the unsubscribe link that appears in every notification email. Contacts who have unsubscribed have the **Unsubscribed** notification status in the table in the **Contact management** section.

To disable notifications for non-administrators, you can perform one of the following actions:

- Clear all of the checkboxes in **Manage notification settings** for the contact.
- Delete the contact from the table under **Contact management**.

Delete non-administrator contacts

1. From the Citrix Cloud management console, click **Account Settings**.
2. Select **Notifications**.
3. Under **Contact management**, locate the contact that you want to manage.
4. Point to the contact and then select the trash can icon.

Citrix Cloud removes the contact from the table.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

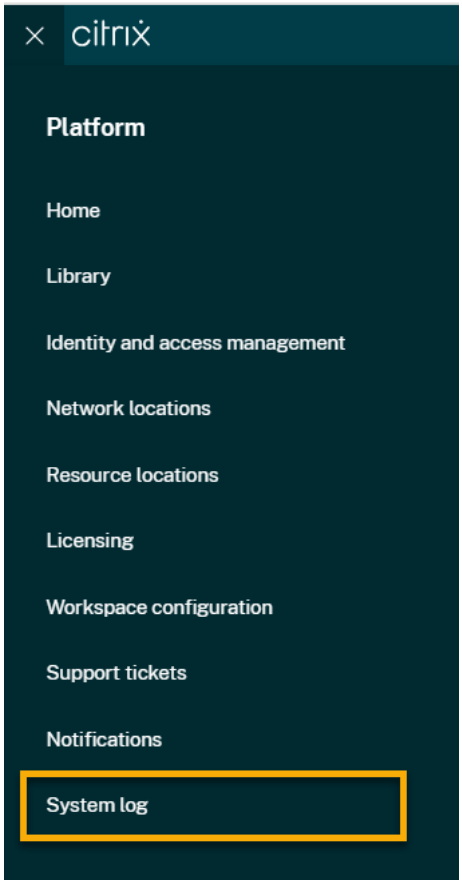
System Log

September 28, 2026

The system log displays a timestamped list of events that occurred in Citrix Cloud. This includes configuration changes along with other events such as connector upgrades. You can export these changes as a CSV file to meet your organization's regulatory compliance requirements or to support security analysis.

> Note:
>
> DaaS Studio writes logs to a separate log. For more information, see Configuration Logging.

To view the system log, select **System Log** from the Citrix Cloud menu.



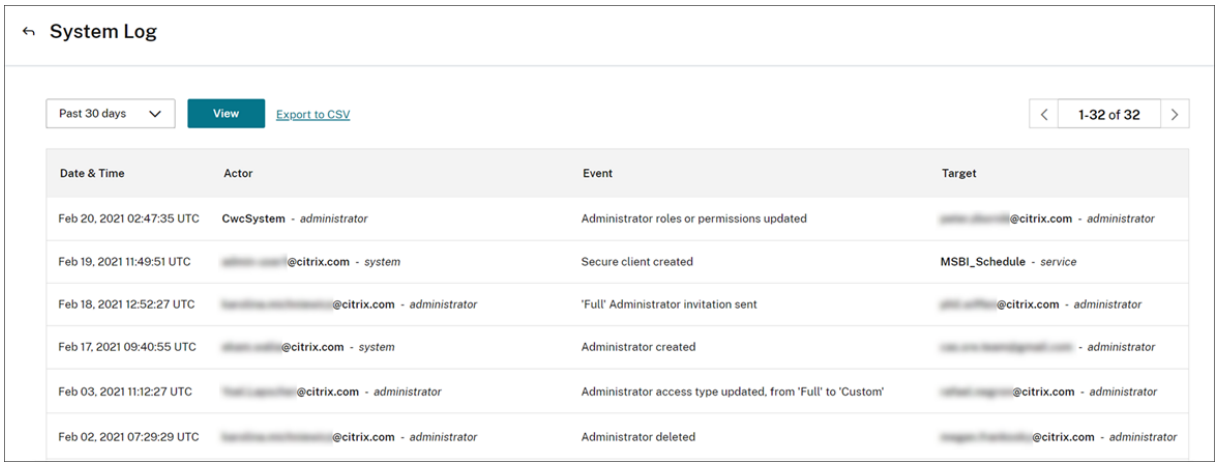
For more information about retention of data in system logs, see Data retention in this article.

Logged events

The system log captures events for certain Citrix Cloud platform and cloud service operations. For a complete list of these events and descriptions of captured data, see System Log Events Reference.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

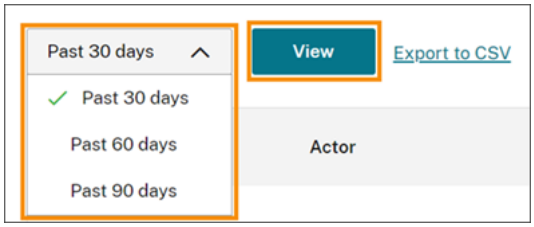
By default, the system log displays events that occurred in the last 30 days. The most recent events are displayed first.



The displayed list includes the following information:

- Date and time (UTC) when the event occurred.
- Actor that initiated the event, such as an administrator or service principal. Entries with the actor **CwcSystem** indicate that Citrix Cloud performed the operation.
- Brief description of the event, such as editing an administrator or creating a new service principal.
- Target of the event. The target is the system object that was impacted or changed as a result of the event. For example, a user who was added as an administrator.

To view events more than 30 days in the past, filter the list by selecting the time period you want to view and select **View**. You can view events that occurred up to 90 days in the past.



To retrieve older events that occurred during a time period that you specify, you can use the System-Log API. For more information, see Retrieve events for a specific time period in this article.

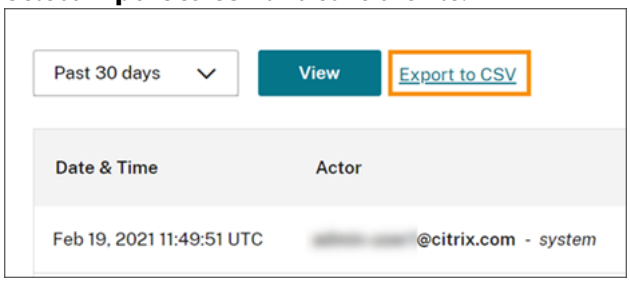
Export events

You can export a CSV file of system log events that occurred up to the last 90 days. The name of the downloaded file follows the format of `SystemLog-CustomerName-OrgID-DateTimeStamp.csv`.

1. From the Citrix Cloud menu, select **System Log**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. If needed, filter the list to display the time period for which you want to export events.
3. Select **Export to CSV** and save the file.



The CSV file includes the following information:

- UTC timestamp of each event
- Details of the actor who initiated the event, including the name and actor ID.
- Event details such as the type of event and the text of the event
- Details of the target of the event such as the target ID, the name of the administrator or service principal.

Retrieve events for a specific time period

If you need to retrieve events for specific periods of time, use the SystemLog API.

SystemLog API

you can use the SystemLog API to read log entires and export them to another system. Before you use the API, you'll need to create a service principal as described in Getting Started on the Citrix Developer Docs web site.

For more information about using the SystemLog API, see Citrix Cloud - SystemLog on the Citrix Developer Docs web site.

For Citrix DaaS logs, see How to get configuration operations in Citrix DaaS.

Data retention

Citrix shares responsibility with you, the customer, for retaining the system log data that Citrix Cloud captures.

Citrix® retains system log records for 90 days after events are recorded.

You are responsible for downloading the system log records that you want to retain to meet your organization's compliance requirements and for storing these records in a long-term storage solution.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

System Log Events Reference

June 9, 2026

To view all System Log events data for your Citrix Cloud™ account, you can:

- Download a CSV file of all events that occurred during the previous 30, 60, or 90 days.
- Use the SystemLog API to retrieve events for a specific time period.

See Event data descriptions in this article for descriptions of the data that are captured when you retrieve System Log events. See Cloud components and services that generate events for event-specific values such as event message text, event types, and whether object field data is recorded before and after events occur.

Cloud components and services that generate events

System Log records events for the following Citrix Cloud entities, components, and services:

- Citrix Cloud platform: Events related to Citrix Cloud platform functions such as managing administrators, device resets for Workspace subscribers, Microsoft Entra ID tenants, and managing domains and network locations.
- Connectors: Events related to registering and updating Citrix Cloud Connectors and Connector Appliances.
- Licensing: Events related to registering on-premises License Servers, managing assigned licenses for cloud services, and exporting licensing data.
- Secure Private Access service: Events related to Secure Private Access service configurations.
- Citrix Workspace: Events related to Workspace Configuration settings.

Event data descriptions

When you download system log events or retrieve them using the SystemLog API, the following data are included:

- **RecordID:** The unique identifier for the event.
- **UtcTimestamp:** The date and UTC time at which the event occurred.
- **CustomerID:** The unique organization identifier of the Citrix Cloud account.
- **EventType:** The identifier for the type of event that was recorded. The event type is recorded using the format `OriginatingService`/`Actor`/`Action`. For example, the event type for creating an administrator is `platform`/`administrator`/`create`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **TargetID:** The ID of the system object that was impacted or changed.
- **TargetDisplayName:** The display name of the system object that was impacted or changed. For example, the name of an administrator that was created.
- **TargetEmail:** The email address of the system object. For example, the email address of an administrator that was created.
- **TargetUserID:** The user ID of the system object that was impacted or changed. For example, when creating an administrator, the target user ID is the user ID of the administrator that was created.
- **TargetType:** The target category for the event.
- **BeforeChanges** and **AfterChanges:** The contents of object fields before and after the event occurred, respectively. For some events, these object fields include:
  - CustomerID
  - User principal
  - UserID
  - Administrator access type, such as Custom or Full
  - CreatedDate
  - UpdatedDate
  - DisplayName
- **AgentID:** The event category.
- **ActorID:** The ID of the system object that initiated the event. For example, for creating an administrator, this is the object ID of the administrator who invited another user to the Citrix Cloud account.
- **ActorDisplayName:** The display name of the person or entity that initiated the event. For example, the name of the administrator who invited another user to the Citrix Cloud account.
- **ActorType:** The service that generated the event.
- **EventMessage:** The brief description of the event that occurred.

System Log events for the Citrix Cloud™ platform

September 28, 2026

This article describes the event data that System Log captures for the Citrix Cloud platform. For more information about System Log event data, see System Log Events Reference.

To learn more about System Log, see System Log.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Entra ID tenants

Event Message	Event Type	Target Type	Actor Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Microsoft Entra ID tenant connected	platform/identityprovider/azuread/connect	identityprovider	administrator		Yes	No
Microsoft Entra ID tenant disconnected	platform/identityprovider/azuread/disconnect	identityprovider	administrator		Yes	No
Microsoft Entra ID auth domain name changed	platform/identityprovider/azuread/authdomain/update	identityprovider	CustomerAdmin		No	No
Microsoft Entra ID auth domain name change failed	platform/identityprovider/azuread/authdomain/update	identityprovider	CustomerAdmin		No	No

Citrix Cloud administrators and service principals

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Actor Type	Current object fields recorded before event	Updated object fields recorded after event
Administrator created	platform/administrator/create	administrator	system	No	Yes
Administrator invitation sent	platform/administrator/invite	administrator	administrator	No	Yes
Administrator roles or permissions updated	platform/administrator/update	administrator	administrator	Yes	Yes
Administrator deleted	platform/administrator/delete	administrator	administrator	No	Yes
Administrator Group created	platform/administrator-group/create	administrator-group	administrator	No	Yes
Administrator Group roles or permissions updated	platform/administrator-group/update	administrator-group	administrator	Yes	Yes
Administrator Group deleted	platform/administrator-group/delete	administrator-group	administrator	Yes	No

Citrix Cloud service principals

Event Message	Event Type	Target Type	Actor Type	Current object fields recorded before event	Updated object fields recorded after event
Service principal created	platform/service-principal/create	service-principal	administrator	n/a	Yes
Failed to create service principal	platform/service-principal/create-failed	service-principal	administrator	n/a	n/a

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Actor Type	Current object fields recorded before event	Updated object fields recorded after event
Service principal roles or permissions updated	platform/serviceprincipal/update	servicePrincipal	administrator	Yes	Yes
Failed to update service principal	platform/serviceprincipal/updatefailed	servicePrincipal	administrator	n/a	n/a
Service principal deleted	platform/serviceprincipal/delete	servicePrincipal	administrator	Yes	n/a
Failed to delete service principal	platform/serviceprincipal/deletefailed	servicePrincipal	administrator	n/a	n/a
Service principal secret rotated	platform/serviceprincipal/secretrotate	servicePrincipal	administrator	Yes	Yes
Failed to rotate service principal secret	platform/serviceprincipal/secretrotatefailed	servicePrincipal	administrator	n/a	n/a
Service principal secondary secret deleted	platform/serviceprincipal/secondarysecretdelete	servicePrincipal	administrator	Yes	Yes
Failed to delete service principal secondary secret	platform/serviceprincipal/secondarysecretdeletefailed	servicePrincipal	administrator	n/a	n/a

Device reset for Active Directory plus token

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Actor Type	Current object fields recorded before event	Updated object fields recorded after event
Subscriber device token reset completed	platform/authentication/device/delete	subscriber	administrator	No	Yes

Domain management

Event Message	Event Type	Target Type	Actor Type	Current object fields recorded before event	Updated object fields recorded after event
Domain removed	platform/domain/service/remove	service	administrator	No	No

Network locations

Event Message	Event Type	Target ID	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Network location created	sdwan/networklocation/create	The ID of the network location that was created	The name of the administrator who added the network location	No	Yes
Network location updated	sdwan/networklocation/edit	The ID of the network location that was modified	The name of the administrator who modified the network location	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target ID	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Network location deleted	sdwan/networklocation/delete	The ID of the network location that was deleted	The name of the administrator who deleted the network location	Yes	No

Resource locations

Event Message	Event Type	Target ID	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Resource Location created	platform/resourcelocation/create	The name of the resource location that was created	The name of the administrator who created the resource location	Yes	Yes
Resource Location updated	platform/resourcelocation/update	The name of the resource location that was modified	The name of the administrator who modified the resource location	Yes	Yes
Resource Location deleted	platform/resourcelocation/delete	The name of the resource location that was deleted	The name of the administrator who deleted the resource location	Yes	Yes

Account name and logo change

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target ID	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Administrator account name updated	platform/account/customer/update	customer	administrator	Yes	Yes
Administrator account logo updated	platform/account/customer/update	customer	administrator	No	No

System Log events for connectors

May 12, 2023

This article describes the event data that System Log captures for the Citrix Cloud Connector and Connector Appliance for Cloud Services. For more information about System Log event data, see System Log Events Reference.

To learn more about System Log, see System Log.

Connector registration

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Connector Registered	platform/edgeservice/cloudconnector/create	**Cloud Connector** or **Connector Appliance**	The administrator who registered the connector	Yes	Yes
Connector Deleted	platform/edgeservice/cloudconnector/delete	**Cloud Connector** or **Connector Appliance**	The administrator who deleted the connector	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Connector updates

Event Message	Event Type	Target ID	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Resource Location Maintenance Window updated	platform/resource-location/maintenance-window	The name of the resource location that was modified	The administrator who changed the configuration	Yes	Yes
Connector upgrade triggered by administrator	platform/edgeservice/manualupgrade	**Cloud Connector** or **Connector Appliance**	The administrator who initiated the update	No	No
Connector upgrade started	platform/edgeservice/upgradestarted	**Cloud Connector** or **Connector Appliance**	**Automatic** or the administrator who initiated the update	Yes	No
Connector upgrade completed	platform/edgeservice/upgradecompleted	**Cloud Connector** or **Connector Appliance**	**Automatic** or the administrator who initiated the update	No	Yes

Connector public keys

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target ID	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Public Key added to trust	platform/authentication/createedge	The	serverkey administrator who performed the operation	No	No
Public Key removed from trust	platform/authentication/deleteedge	The	serverkey administrator who performed the operation	No	No

System Log events for licensing in Citrix Cloud™

September 6, 2025

This article describes the event data that System Log captures for on-premises Citrix Licensing registration with Citrix Cloud. For more information about System Log event data, see System Log Events Reference.

To learn more about System Log, see System Log.

On-premises license servers

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
On-premise license servers deleted	lui/onpremlicenseservers/delete	Licensing	The administrator who deleted the license server	No	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Failed to delete on-premise license servers	lui/onpremlicenseserver/delete/failed	Licensing	The administrator who tried to delete the license server	No	No

Cloud service licensing

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Citrix Cloud service licenses released	lui/cloudlicense/release	Cloud license	The administrator who released licenses for the cloud service	No	No
Failed to release Citrix Cloud service licenses	lui/cloudlicense/release/failed	Cloud license	The administrator who tried to release licenses for the cloud service	No	No

License Usage Insights for Citrix Service Providers

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Partner on-premise user list data exported	lui/csp/userlistdataexport	Licensing	The administrator who exported the Partner user list data	No	No
Failed to export partner on-premise user list data	lui/csp/userlistdataexportfailed	Licensing	The administrator who tried to export the Partner user list data	No	No

License usage for cloud services and on-premises products

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
License usage data exported	lui/cloudlicense/usagedataexport	CloudLicensing or Licensing	The administrator who exported license usage data	No	No
Failed to export license usage data	lui/cloudlicense/usagedataexportfailed	CloudLicensing or Licensing	The administrator who tried to export license usage data	No	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

System Log Events for Secure Private Access

June 22, 2026

This article describes the event data that System Log captures for the Secure Private Access service. For more information about System Log event data, see System Log Events Reference.

To learn more about System Log, see System Log.

Web and SaaS applications

Event Message	Event Type	Target Type	Current object fields recorded before event	Updated object fields recorded after event
Web/SaaS application created	swa/websaasppplicationcreate	web/saasapplication	No	Yes
Web/SaaS application updated	swa/websaasppplicationupdate	web/saasapplication	Yes	Yes
Web/SaaS application deleted	swa/websaasppplicationdelete	web/saasapplication	Yes	No
Web/SaaS application creation failed	swa/websaasppplicationcreatefailed	web/saasapplication	No	No
Web/SaaS application update failed	swa/websaasppplicationupdatefailed	web/saasapplication	Yes	Yes
Web/SaaS application deletion failed	swa/websaasppplicationdeletefailed	web/saasapplication	Yes	Yes

User and group subscriptions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Current object fields recorded before event	Updated object fields recorded after event
User/Group subscription added	swa/websaaspplicationsubscription/subscribe	websaasapplicationsubscription	Subscribers	Yes
User/Group subscription removed	swa/websaaspplicationsubscription/unsubscribe	websaasapplicationsubscription	Subscribers	Yes
User/Group subscription failed	swa/websaaspplicationsubscription/subscribefailed	websaasapplicationsubscription	Subscribers	No
User/Group unsubscription failed	swa/websaaspplicationsubscription/unsubscribefailed	websaasapplicationsubscription	Subscribers	No

Contextual policies

Event Message	Event Type	Target Type	Current object fields recorded before event	Updated object fields recorded after event
Contextual policy created	swa/contextualpolicy/create	contextualpolicy	No	Yes
Contextual policy updated	swa/contextualpolicy/update	contextualpolicy	Yes	Yes
Contextual policy deleted	swa/contextualpolicy/delete	contextualpolicy	Yes	No
Contextual policy creation failed	swa/contextualpolicy/createfailed	contextualpolicy	No	No
Contextual policy update failed	swa/contextualpolicy/updatefailed	contextualpolicy	No	No
Contextual policy deletion failed	swa/contextualpolicy/deletefailed	contextualpolicy	Yes	No

Application domains

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Current object fields recorded before event	Updated object fields recorded after event
Application domain created	swa/applicationdomain/create	applicationdomain	No	Yes
Application domain updated	swa/applicationdomain/update	applicationdomain	Yes	Yes
Application domain deleted	swa/applicationdomain/delete	applicationdomain	Yes	No
Application domain creation failed	swa/applicationdomain/createfailed	applicationdomain	No	No
Application domain update failed	swa/applicationdomain/updatefailed	applicationdomain	Yes	No
Application domain deletion failed	swa/applicationdomain/deletefailed	applicationdomain	Yes	No

Browser extension settings

Event Message	Event Type	Target Type	Current object fields recorded before event	Updated object fields recorded after event
Browser Extension settings updated	swa/browserextensionsettings/update	browserextensionsettings	Yes	Yes
Browser Extension settings update failed	swa/browserextensionsettings/updatefailed	browserextensionsettings	Yes	No

Website URL lists and filter categories

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Current object fields recorded before event	Updated object fields recorded after event
Enabled website filter lists and categories	swa/website/filterlists/enabled/update	website/filterlists/enabledfilteringcategories	No	Yes
Enabled website filter lists and disabled filter categories	swa/website/filterlists/enabled/update	website/filterlists/enabledfilteringcategories	Yes	Yes
Disabled website filter lists and enabled filter categories	swa/website/filterlists/disabled/update	website/filterlists/disabledfilteringcategories	No	Yes
Disabled website filter lists and categories	swa/website/filterlists/disabled/update	website/filterlists/disabledfilteringcategories	Yes	Yes
Failed to enable website filter lists and categories	swa/website/filterlists/enabled/updatefailed	website/filterlists/enabledfilteringcategories	No	Failed
Failed to enable website filter lists and disable filter categories	swa/website/filterlists/enabled/updatefailed	website/filterlists/enabledfilteringcategories	Yes	Failed
Failed to disable website filter lists and enable filter categories	swa/website/filterlists/disabled/updatefailed	website/filterlists/disabledfilteringcategories	No	Failed
Failed to disable website filter lists and categories	swa/website/filterlists/disabled/updatefailed	website/filterlists/disabledfilteringcategories	Yes	Failed
Website URL list created	swa/websiteurlfiltering/list/create	website/urlfilteringlist	No	Yes
Website URL list updated	swa/websiteurlfiltering/list/update	website/urlfilteringlist	Yes	Yes
Website URL list deleted	swa/websiteurlfiltering/list/delete	website/urlfilteringlist	Yes	No
Website URL list creation failed	swa/websiteurlfiltering/list/createfailed	website/urlfilteringlist	No	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Current object fields recorded before event	Updated object fields recorded after event
Website URL list update failed	swa/websiteurlfilterwebsiteurllist/updatefailed	websiteurllist	Yes	No
Website URL list deletion failed	swa/websiteurlfilterwebsiteurllist/deletefailed	websiteurllist	Yes	No
Website URL filter category created	swa/websiteurlfiltercategory/created	category	No	Yes
Website URL filter category updated	swa/websiteurlfiltercategory/updated	category	Yes	Yes
Website URL filter category deleted	swa/websiteurlfiltercategory/deleted	category	No	No
Website URL filter category creation failed	swa/websiteurlfiltercategory/createfailed	category	No	No
Website URL filter category update failed	swa/websiteurlfiltercategory/updatefailed	category	Yes	No
Website URL filter category deletion failed	swa/websiteurlfiltercategory/deletefailed	category	Yes	No

Website filter category presets

Event Message	Event Type	Target Type	Current object fields recorded before event	Updated object fields recorded after event
Updated website filter category preset	swa/websiteurlfiltercategorypreset/updated	categorypreset	Yes	Yes
Failed to update website filter category preset	swa/websiteurlfiltercategorypreset/updatefailed	categorypreset	Yes	Yes

Blocked Website URL lists and filter categories

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Current object fields recorded before event	Updated object fields recorded after event
Blocked Website URL list created	swa/websiteurlfilter/blockedlist/create	website/blocked/list	No	Yes
Blocked Website URL list updated	swa/websiteurlfilter/blockedlist/update	website/blocked/list	No	Yes
Blocked Website URL list deleted	swa/websiteurlfilter/blockedlist/delete	website/blocked/list	No	Yes
Blocked Website URL list creation failed	swa/websiteurlfilter/blockedlist/createfailed	website/blocked/list	No	Yes
Blocked Website URL list update failed	swa/websiteurlfilter/blockedlist/updatefailed	website/blocked/list	No	Yes
Blocked Website URL list deletion failed	swa/websiteurlfilter/blockedlist/deletefailed	website/blocked/list	No	Yes
Blocked Website URL filter category created	swa/websiteurlfilter/category/blockedlist/create	category/blocked/list	No	Yes
Blocked Website URL filter category updated	swa/websiteurlfilter/category/blockedlist/update	category/blocked/list	No	Yes
Blocked Website URL filter category deleted	swa/websiteurlfilter/category/blockedlist/delete	category/blocked/list	No	Yes
Blocked Website URL filter category creation failed	swa/websiteurlfilter/category/blockedlist/createfailed	category/blocked/list	No	Yes
Blocked Website URL filter category update failed	swa/websiteurlfilter/category/blockedlist/updatefailed	category/blocked/list	No	Yes
Blocked Website URL filter category deletion failed	swa/websiteurlfilter/category/blockedlist/deletefailed	category/blocked/list	No	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Allowed Website URL lists and filter categories

Event Message	Event Type	Target Type	Current object fields recorded before event	Updated object fields recorded after event
Allowed Website URL list created	swa/websiteurlfilterwebsiteallowedlist/create	websiteallowedlist	No	Yes
Allowed Website URL list updated	swa/websiteurlfilterwebsiteallowedlist/update	websiteallowedlist	No	Yes
Allowed Website URL list deleted	swa/websiteurlfilterwebsiteallowedlist/delete	websiteallowedlist	No	Yes
Allowed Website URL list creation failed	swa/websiteurlfilterwebsiteallowedlist/createfailed	websiteallowedlist	No	Yes
Allowed Website URL list update failed	swa/websiteurlfilterwebsiteallowedlist/updatefailed	websiteallowedlist	No	Yes
Allowed Website URL list deletion failed	swa/websiteurlfilterwebsiteallowedlist/deletefailed	websiteallowedlist	No	Yes
Allowed Website URL filter category created	swa/websiteurlfiltercategoryallowedlist/create	categoryallowedlist	No	Yes
Allowed Website URL filter category updated	swa/websiteurlfiltercategoryallowedlist/update	categoryallowedlist	No	Yes
Allowed Website URL filter category deleted	swa/websiteurlfiltercategoryallowedlist/delete	categoryallowedlist	No	Yes
Allowed Website URL filter category creation failed	swa/websiteurlfiltercategoryallowedlist/createfailed	categoryallowedlist	No	Yes
Allowed Website URL filter category update failed	swa/websiteurlfiltercategoryallowedlist/updatefailed	categoryallowedlist	No	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Current object fields recorded before event	Updated object fields recorded after event
Allowed Website URL filter category deletion failed	swa/websiteurlfiltercategory/allowedlistdelete	category/allowedlist	Name	Yes

Redirected to Remote Browser Isolation (formerly Secure Browser) website URL lists and filter categories

Event Message	Event Type	Target Type	Current object fields recorded before event	Updated object fields recorded after event
Redirected to Secure Browser Website URL list created	swa/websiteurlfilterwebsiteredirectedlistcreate	websiteredirectedlist	None	Yes
Redirected to Secure Browser Website URL list updated	swa/websiteurlfilterwebsiteredirectedlistupdate	websiteredirectedlist	None	Yes
Redirected to Secure Browser Website URL list deleted	swa/websiteurlfilterwebsiteredirectedlistdelete	websiteredirectedlist	None	Yes
Redirected to Secure Browser Website URL list creation failed	swa/websiteurlfilterwebsiteredirectedlistcreatefailed	websiteredirectedlist	None	Yes
Redirected to Secure Browser Website URL list update failed	swa/websiteurlfilterwebsiteredirectedlistupdatedfailed	websiteredirectedlist	None	Yes
Redirected to Secure Browser Website URL list deletion failed	swa/websiteurlfilterwebsiteredirectedlistdeletefailed	websiteredirectedlist	None	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Current object fields recorded before event	Updated object fields recorded after event
Redirected to Secure Browser Website URL filter category created	swa/websiteurlfiltercategory/redirectedlist/create	category/redirectedlist		Yes
Redirected to Secure Browser Website URL filter category updated	swa/websiteurlfiltercategory/redirectedlist/update	category/redirectedlist		Yes
Redirected to Secure Browser Website URL filter category deleted	swa/websiteurlfiltercategory/redirectedlist/delete	category/redirectedlist		Yes
Redirected to Secure Browser Website URL filter category creation failed	swa/websiteurlfiltercategory/redirectedlist/createfailed	category/redirectedlist		Yes
Redirected to Secure Browser Website URL filter category update failed	swa/websiteurlfiltercategory/redirectedlist/updatefailed	category/redirectedlist		Yes
Redirected to Secure Browser Website URL filter category deletion failed	swa/websiteurlfiltercategory/redirectedlist/deletefailed	category/redirectedlist		Yes

System Log events for Citrix® StoreFront Cloud

July 17, 2026

This article describes the event data that System Log captures for StoreFront Cloud. For more information about System Log event data, see System Log Events Reference.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To learn more about System Log, see System Log.

Store URL

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Workspace URL updated	wxp/url/update	subscriber	The administrator who updated the URL	Yes	Yes
Failed to update Workspace URL	wxp/url/updatefailed	subscriber	The administrator who attempted to update the URL	Yes	Yes
Workspace URL enabled	wxp/url/enable	subscriber	The administrator who enabled customization of the workspace URL	No	Yes
Failed to enable Workspace URL	wxp/url/enablefailed	subscriber	The administrator who attempted to enable customization of the workspace URL	No	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Workspace URL disabled	wxp/url/disable	subscriber	The administrator who disabled customization of the workspace URL	No	Yes
Failed to disable Workspace URL	wxp/url/disablefailed	subscriber	The administrator who attempted to disable customization of the workspace URL	No	Yes

Store authentication

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Workspace identity provider updated	wxp/identityprovider/update	subscriber	The administrator who updated the workspace authentication method	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Failed to update Workspace identity provider	wxp/identityprovider/updatefailed	subscriber	The administrator who attempted to update the workspace authentication method	Yes	Yes

Citrix Federated Authentication Service

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Workspace Federated Authentication Service (FAS) enabled	wxp/fas/enable	subscriber	The administrator who enabled FAS	No	Yes
Failed to enable Workspace Federated Authentication Service (FAS)	wxp/fas/enablefailed	subscriber	The administrator who tried to enable FAS	No	Yes
Workspace Federated Authentication Service (FAS) disabled	wxp/fas/disable	subscriber	The administrator who disabled FAS	No	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Failed to disable Workspace Federated Authentication Service (FAS)	wxp/fas/disablefailed	subscriber	The administrator who tried to disable FAS	No	Yes

Favorites

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Workspace favorites enabled	wxp/favorites/enable	subscriber	The administrator who enabled favorites	No	Yes
Failed to enable Workspace favorites	wxp/favorites/enablefailed	subscriber	The administrator who tried to enable favorites	No	Yes
Workspace favorites disabled	wxp/favorites/disable	subscriber	The administrator who disabled favorites	No	Yes
Failed to disable Workspace favorites	wxp/favorites/disablefailed	subscriber	The administrator who tried to disable favorites	No	Yes

Change password

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Workspace change password options policy updated	wxp/changepasswordoptions/update	subscription	The policy administrator who updated the policy for changing passwords within Citrix Workspace	Yes	Yes
Failed to update Workspace change password options policy	wxp/changepasswordoptions/update	subscription	The policyfailed administrator who tried to update the policy for changing passwords within Citrix Workspace	Yes	Yes
Workspace change password options enabled	wxp/changepasswordoptions/enable	subscription	The administrator who enabled the setting for changing passwords within Citrix Workspace	No	Yes
Failed to enable Workspace change password options	wxp/changepasswordoptions/enable	subscription	The failed administrator who tried to enable the setting for changing passwords within Citrix Workspace	No	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Workspace change password options disabled	wxp/changepasswordoptions/disable	subscription	The administrator who disabled the setting for changing passwords within Citrix Workspace	No	Yes
Failed to disable Workspace change password options	wxp/changepasswordoptions/disable	subscription	The failed administrator who tried to disable the setting for changing passwords within Citrix Workspace	No	Yes

Long-lived tokens

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Workspace long lived token configuration updated	wxp/longlivedtoken/update	subscription	The administrator who updated the token configuration	Yes	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Failed to update Workspace long lived token configuration	wxp/longlivedtoken/update	subscriber	failed	The administrator who tried to update the token configuration	Yes	Yes

Inactivity timeout for Web

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Workspace sessions Configuration updated	wxp/sessions/update	subscriber	The administrator who updated the idle time for the Inactivity Timeout for Web setting	Yes	Yes
Failed to update Workspace sessions configuration	wxp/sessions/update	subscriber	failed	The administrator who tried to update the idle time for the Inactivity Timeout for Web setting	Yes	Yes

Feature rollout

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Assigned users and groups updated for intelligent Workspace experience	wxp/iws/features/subscribers	subscribersgroups	The administrator who updated the assigned users and groups for accessing Activity Feed notifications in Citrix Workspace	No	No
Failed to Assign users and groups updated for intelligent Workspace experience	wxp/iws/features/subscribers	subscribersgroups	The failed administrator who tried to update the assigned users and groups for accessing Activity Feed notifications in Citrix Workspace	No	No
Intelligent Workspace experience enabled	wxp/iws/features/enable	subscriber	The administrator who enabled Activity Feed notifications in Citrix Workspace	No	No

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Event Message	Event Type	Target Type	Actor ID	Current object fields recorded before event	Updated object fields recorded after event
Failed to enable intelligent Workspace experience	wxp/iws/features/enable/failed	user	The administrator who tried to enable Activity Feed notications in Citrix Workspace	No	No
Intelligent Workspace experience disabled	wxp/iws/features/disable	user	The administrator who disabled Activity Feed notifications in Citrix Workspace	No	No
Failed to disable intelligent Workspace experience	wxp/iws/features/disable/failed	user	The administrator who tried to disable Activity Feed notifications in Citrix Workspace	No	No

SDKs and APIs

September 28, 2026

Citrix Cloud™ provides several APIs that you can use to retrieve information and automate complex and repetitive tasks, including:

- Silently install Citrix Cloud Connector™
- Create and consume reports for managing cloud licenses

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Determine a customer's entitlement status
- Send notifications to Citrix Cloud administrators
- Retrieve System Log events
- Retrieve details about your resource locations to use with other APIs

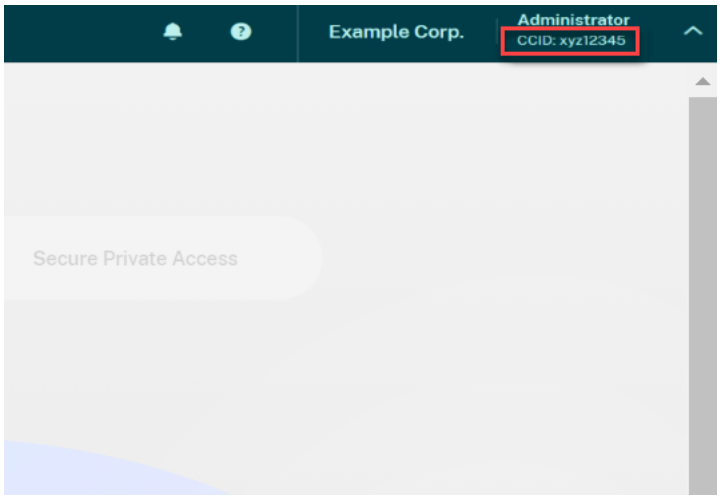
Several Citrix Cloud services also provide SDKs and APIs that allow you to retrieve information, query data, and perform administrative tasks.

You can access APIs through both secure clients or service principals.

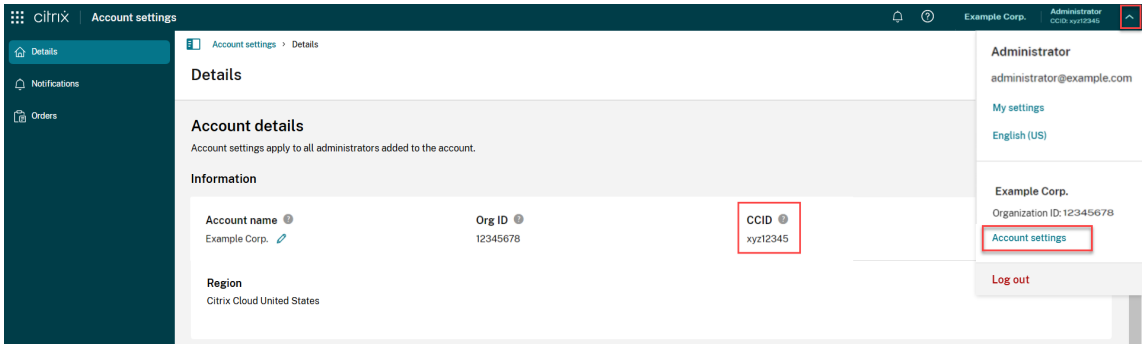
Service principal

To use Citrix Cloud APIs, you need to create a service principal that accesses Citrix Cloud on your behalf. To create a service principal, you'll need to supply the customer ID of your Citrix Cloud account. Your customer ID is located in the following places in the management console:

- The top-right corner of the console, underneath your user name.

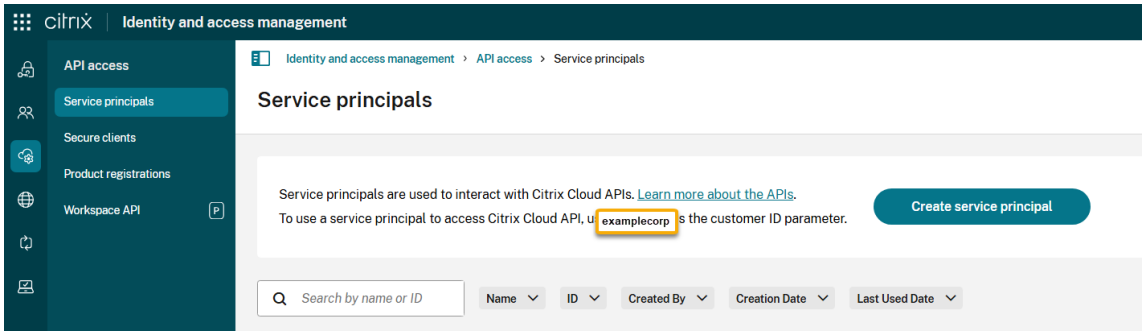


- Your **Account Settings** page.



- The **API Access** page.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Cloud licensing APIs

Enterprise customers can use cloud licensing APIs to perform management tasks like exporting usage data and releasing assigned licenses. Citrix partners can use these APIs to retrieve summary and historical data for on-premises Citrix Virtual Apps and Desktops™ and Citrix DaaS.

For more information, see APIs to manage Citrix cloud licensing in the Citrix Developer documentation.

SystemLog API

The SystemLog API allows you to retrieve events that occurred in your Citrix Cloud account for periods of time that you specify. For more information about using this API, see Citrix Cloud - SystemLog in the Citrix Developer documentation.

Resource Locations API

The Resource Locations API allows you to retrieve information about your resource locations for use with other applications and scripts. For example, let's say that you want to silently install the Citrix Cloud Connector in one of several resource locations in your Citrix Cloud account. You can use this API to retrieve the resource location ID and pass it to your install script.

For more information about using this API, see Citrix Cloud - Resource Location in the Citrix Developer documentation.

Service Entitlement API

The Service Entitlement API retrieves the services a customer is entitled to use, the days remaining on each entitlement, and the quantity of entitlements that the customer purchased. For more information about using this API, see Citrix Cloud - Service Entitlement in the Citrix Developer documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Notifications API

The Notifications API allows you to send messages to other Citrix Cloud administrators. Recipients receive your messages through the Notifications page in the management console. For more information about using this API, see Creating & Viewing notifications.

SDKs and APIs for other services

For more information about the SDKs and APIs that are available for other Citrix Cloud services, see the following articles:

- Citrix® StoreFront Cloud: Includes SDKs and APIs for StoreFront Cloud.
- App delivery and security: Includes SDKs and APIs for networking and app delivery services like Console and SD-WAN Orchestrator.

More information

To learn more about how Citrix Cloud APIs can help you perform complex operations like migrating to the cloud and configuring authentication with push tokens, see the following Tech Zone articles:

- Deployment Guide: Migrating Citrix Virtual Apps and Desktops from VMware vSphere to Citrix Virtual Apps and Desktops service on Microsoft Azure
- PoC Guide: Automated Configuration Tool

Citrix Cloud™ for Partners

July 21, 2026

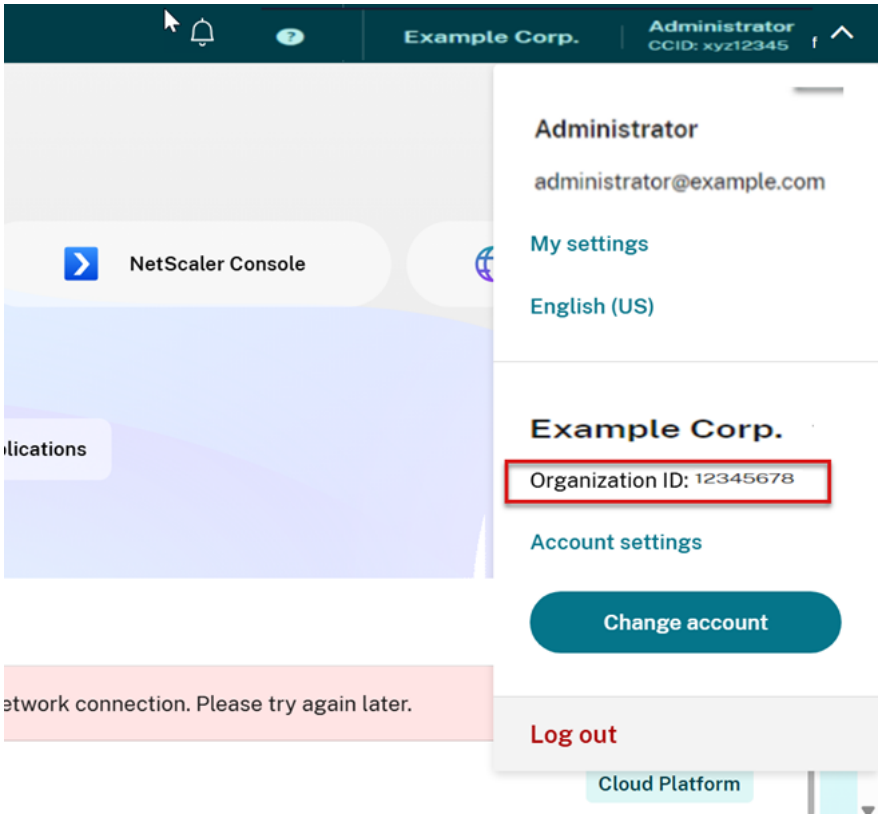
Citrix Cloud includes services, features, and experiences designed for both customers and partners. This section outlines features available to Citrix Partners that help them collaborate with customers on Citrix Cloud services and solutions.

Partner identification

Partners are identified in Citrix Cloud based on their Citrix Organization ID (ORGID). Partners can view the ORGID that's associated with their Citrix Cloud account in the following locations in the Citrix Cloud management console:

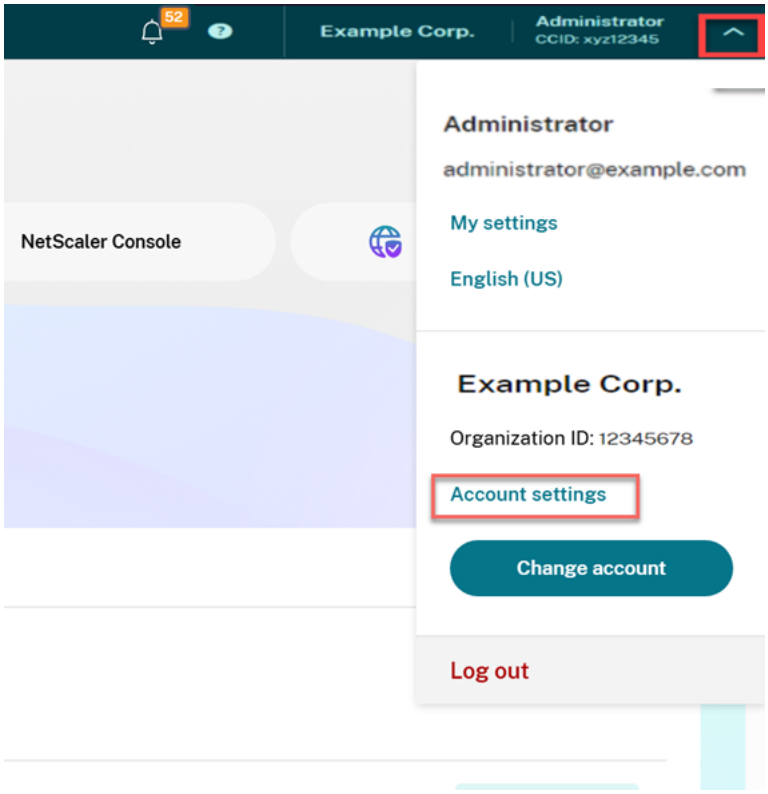
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- From the customer menu. Click your customer name from the top-right corner of the console. Your ORGID appears beneath your company name in the menu.



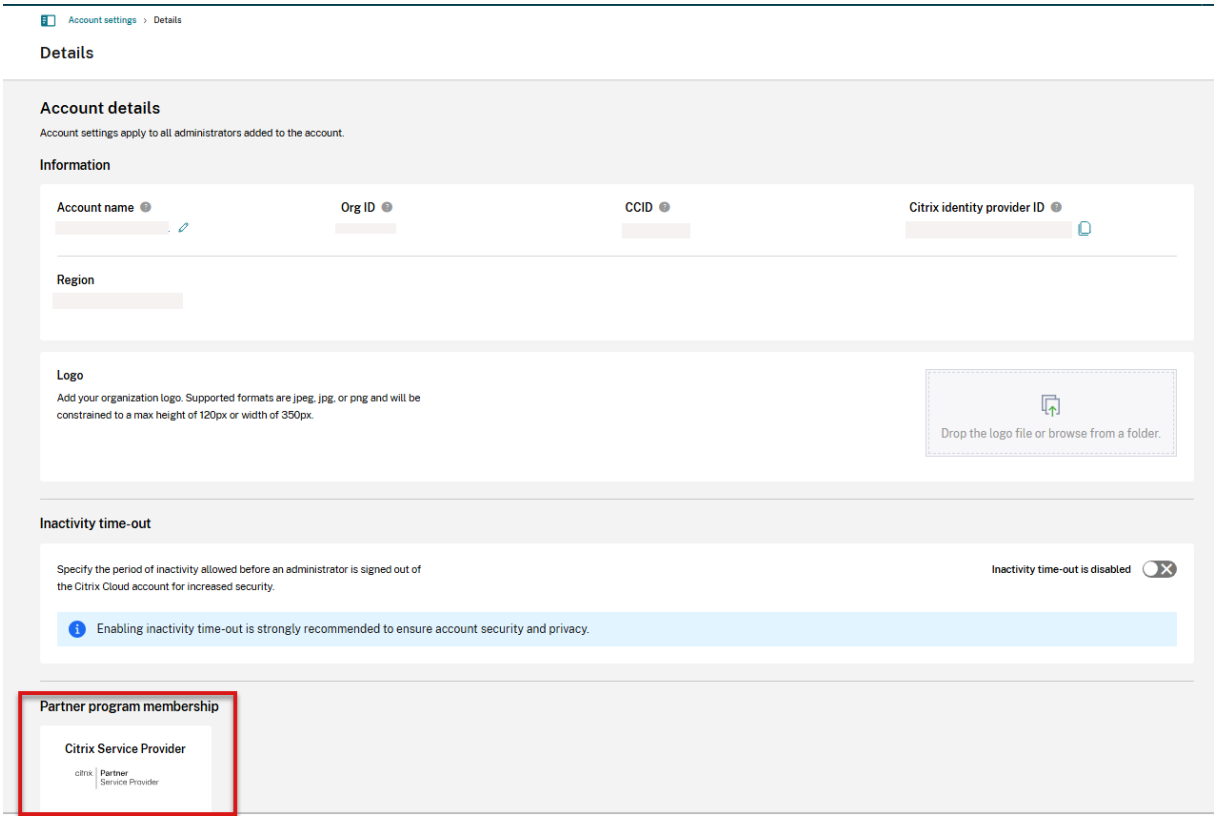
- From the customer menu in the top-right corner, select **Account Settings**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



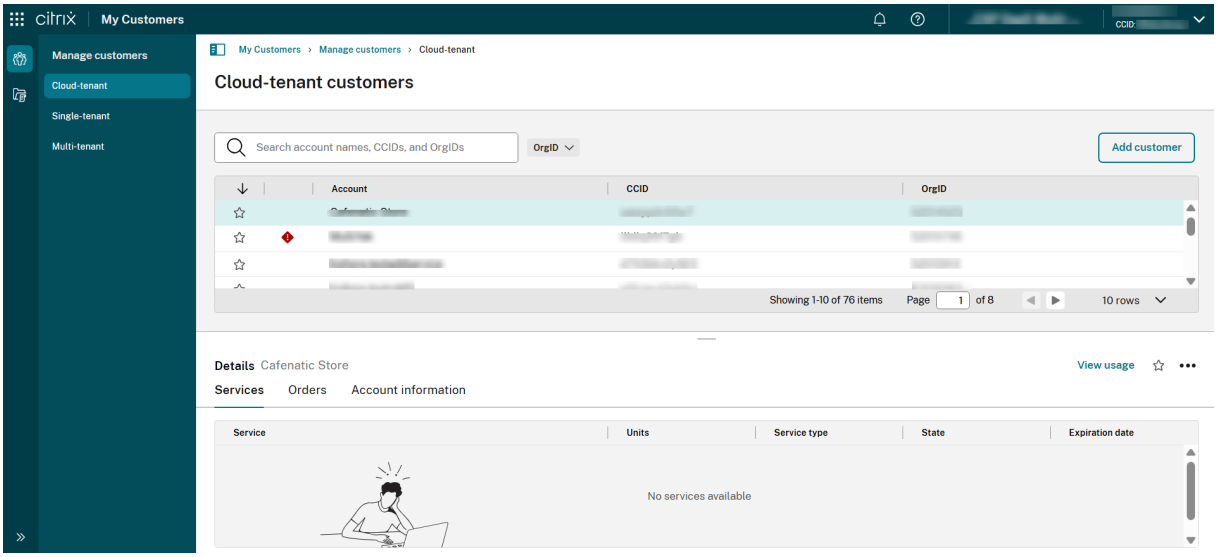
If the ORGID on the account is an active member of a Citrix partner program (such as Citrix Solution Advisor or Citrix Service Provider™) the program badge indicates that a Citrix partner owns this account. Partner identification is then used to govern access to additional cloud services or features.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Customer dashboard

The my customer dashboard is designed for partners to view the status of multiple Citrix Cloud customers in a consolidated view. For a customer to appear on the dashboard, a connection must be established between the partner and customer. The my customer dashboard is available on partner badged Citrix Cloud accounts.

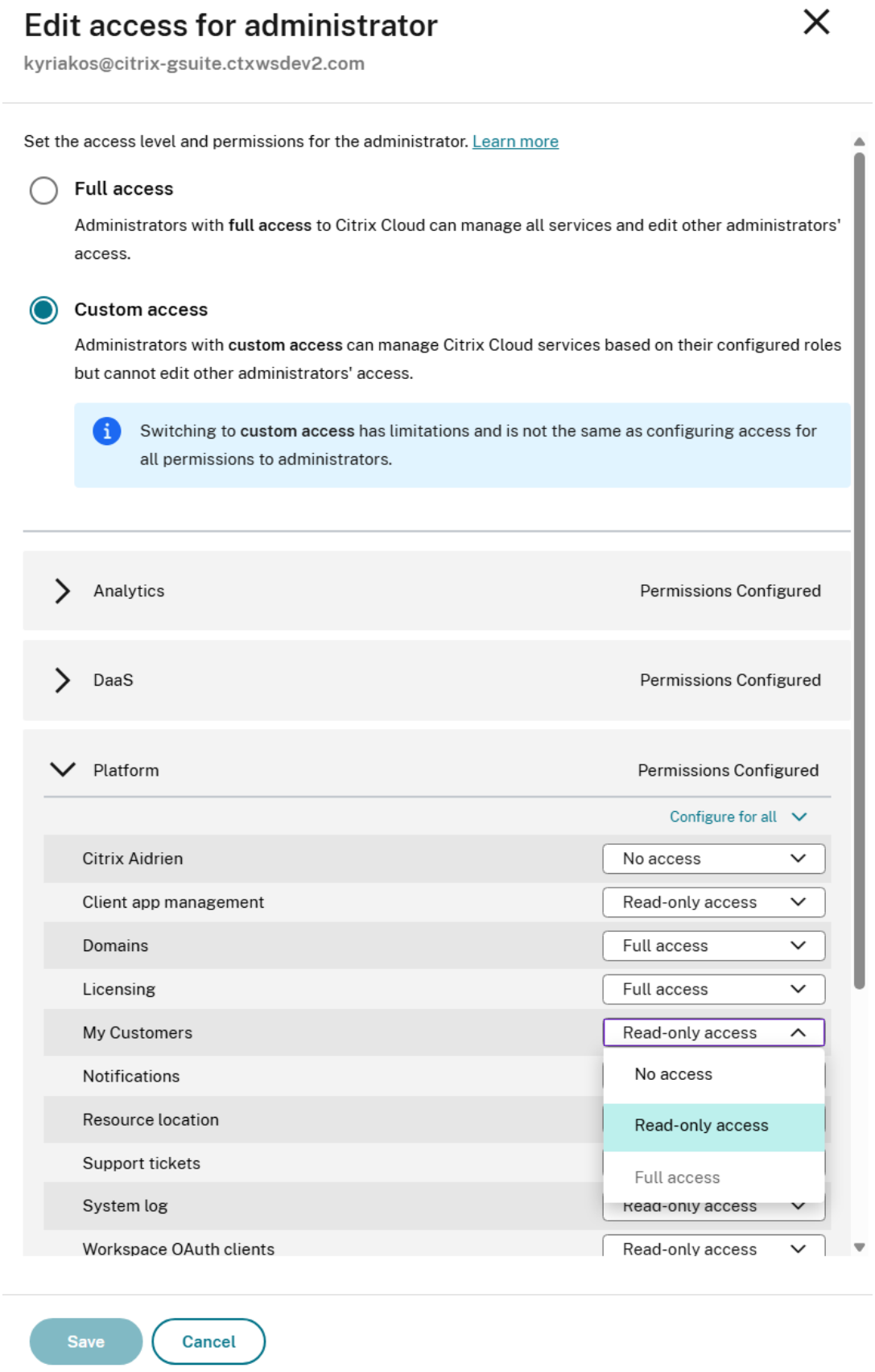


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Who can see customer dashboard ?

By default, full access administrators can view the customer dashboard. Custom access administrators can view the dashboard if the **Customer Dashboard** permission is selected. For more information about administrator permissions in Citrix Cloud, see Modify administrator permissions.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Partner connections with customers

Partners collaborating with customers on Citrix Cloud solutions can establish a trusted link between their accounts. This account level relationship allows a customer to share specific information easily with a partner. By connecting with a partner, a customer grants the partner visibility into information about their Citrix Cloud account and their relationship with Citrix.

Establishing a partner connection enables the following:

- Customer appears on the partner's dashboard
- Partner appears as an active connection in the customer's account settings
- Partner has visibility into Citrix Cloud service entitlements
- Partner has visibility into license usage and active use for Citrix Cloud entitlements

After a partner and customer connect, partner administrators can view the customer's basic account information, orders placed by the customer, and entitlement information, such as services, license counts, and expiration dates.

Partner connections with customers don't expire.

Connections with multiple partners or customers

Partners can establish connections with multiple customers. Alternatively, the partner might consider removing customer accounts that they no longer need to manage.

Customers can establish connections with multiple partners. There is no limit to the number of customer-to-partner connections.

Connection notifications

Citrix Cloud sends notifications to partners when:

- The partner creates a connection to a customer
- A customer terminates their connection to the partner

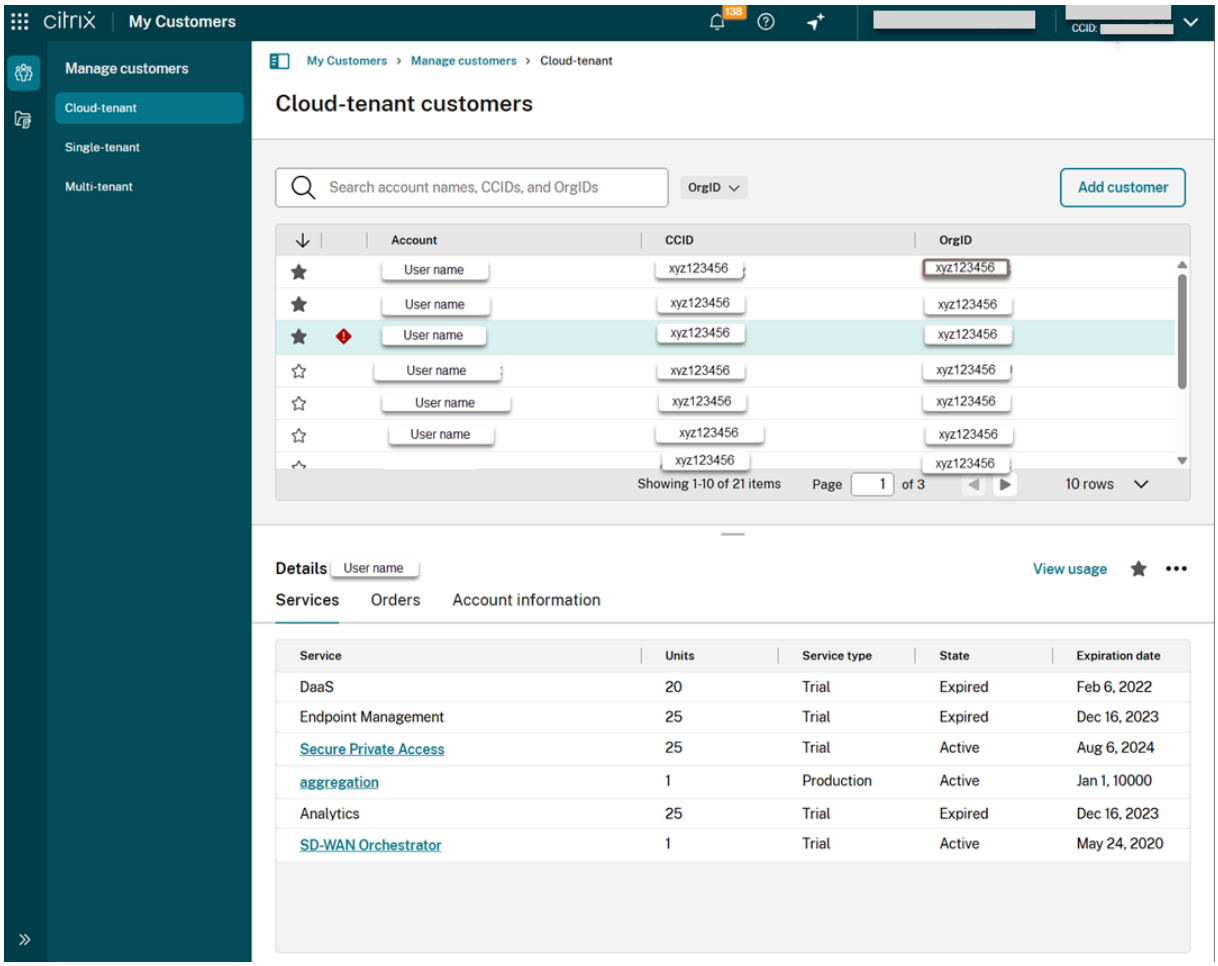
Citrix Cloud sends notifications to customers when the partner terminates their connection with the customer.

Partner visibility into service entitlements

When connected to a customer, the partner can view the service entitlement status for that customer. This information includes the status of both trial and non-trial entitlements. Partners can also view the following information:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Active service entitlements (services purchased or otherwise entitled or enabled for the customer)
- License count and expiration date for the entitlement
- Active service trials
- Expired service trials



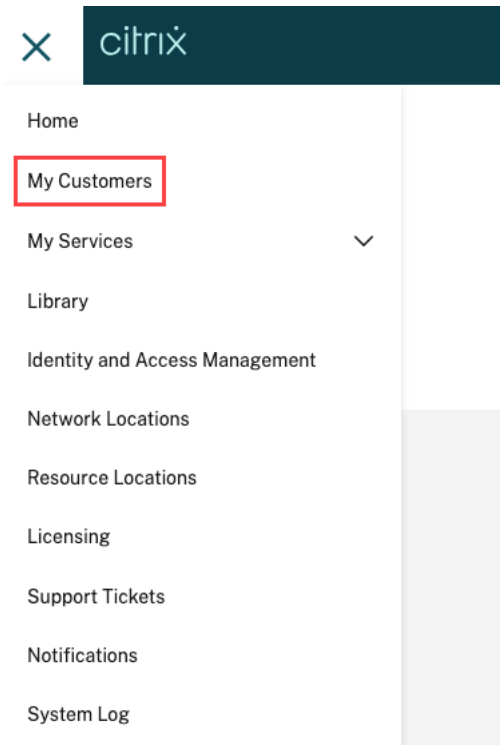
Licensing visibility is limited to viewing summaries of license assignments and historical usage trends.

Add a new customer

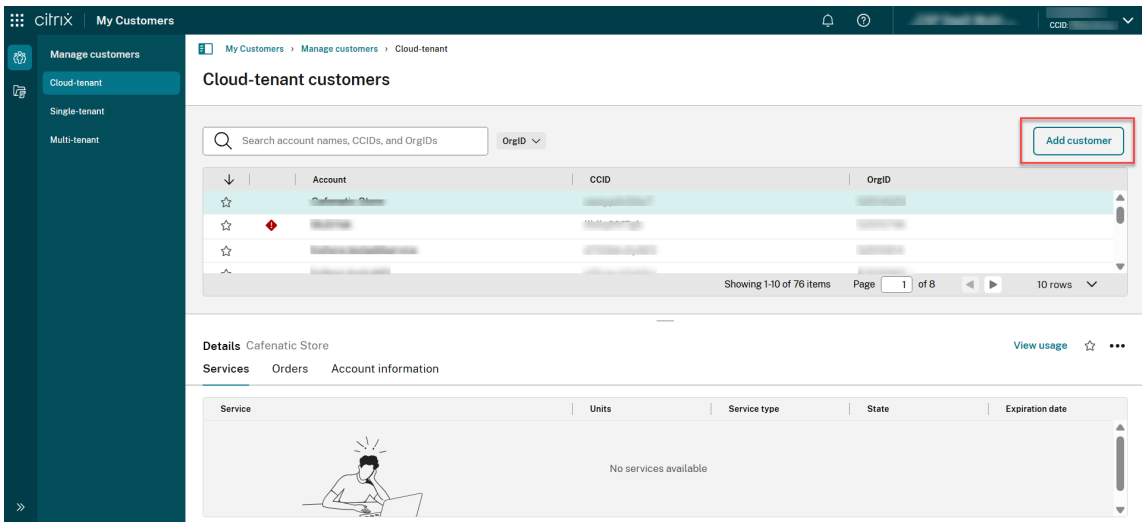
Follow these steps to add a new customer:

1. From the Citrix Cloud menu, click **My Customers**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

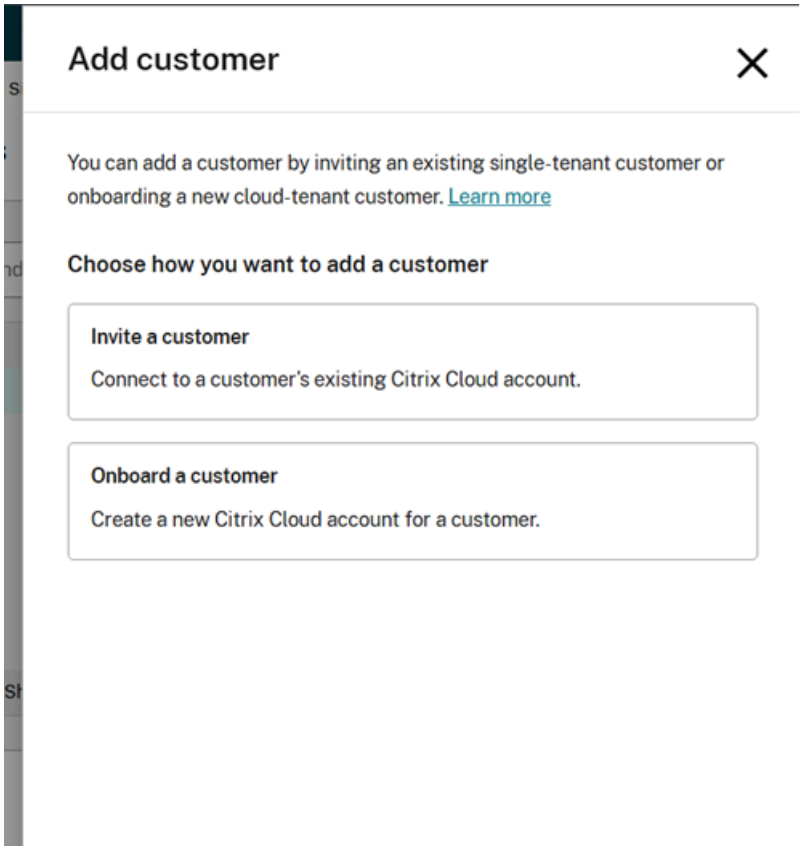


2. Go to **Manage Customers > Cloud Tenant** , click **Add customer**.



3. You'll be prompted to choose between the following options, as shown in the screenshot below.

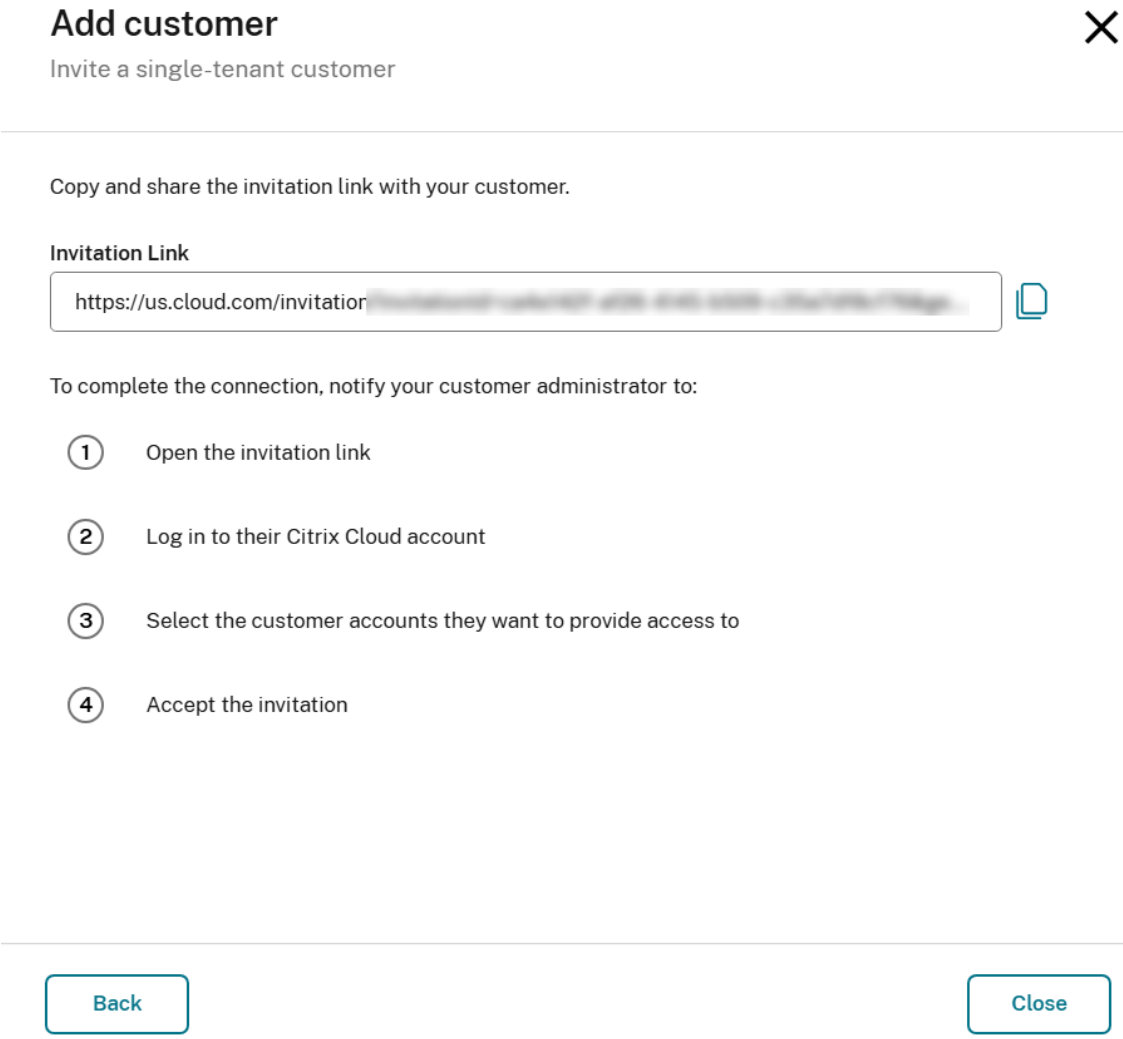
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Note:

- **Invite a Customer**: Use this option to invite an existing single-tenant customer. This invited customer retains their own unique OrgID.

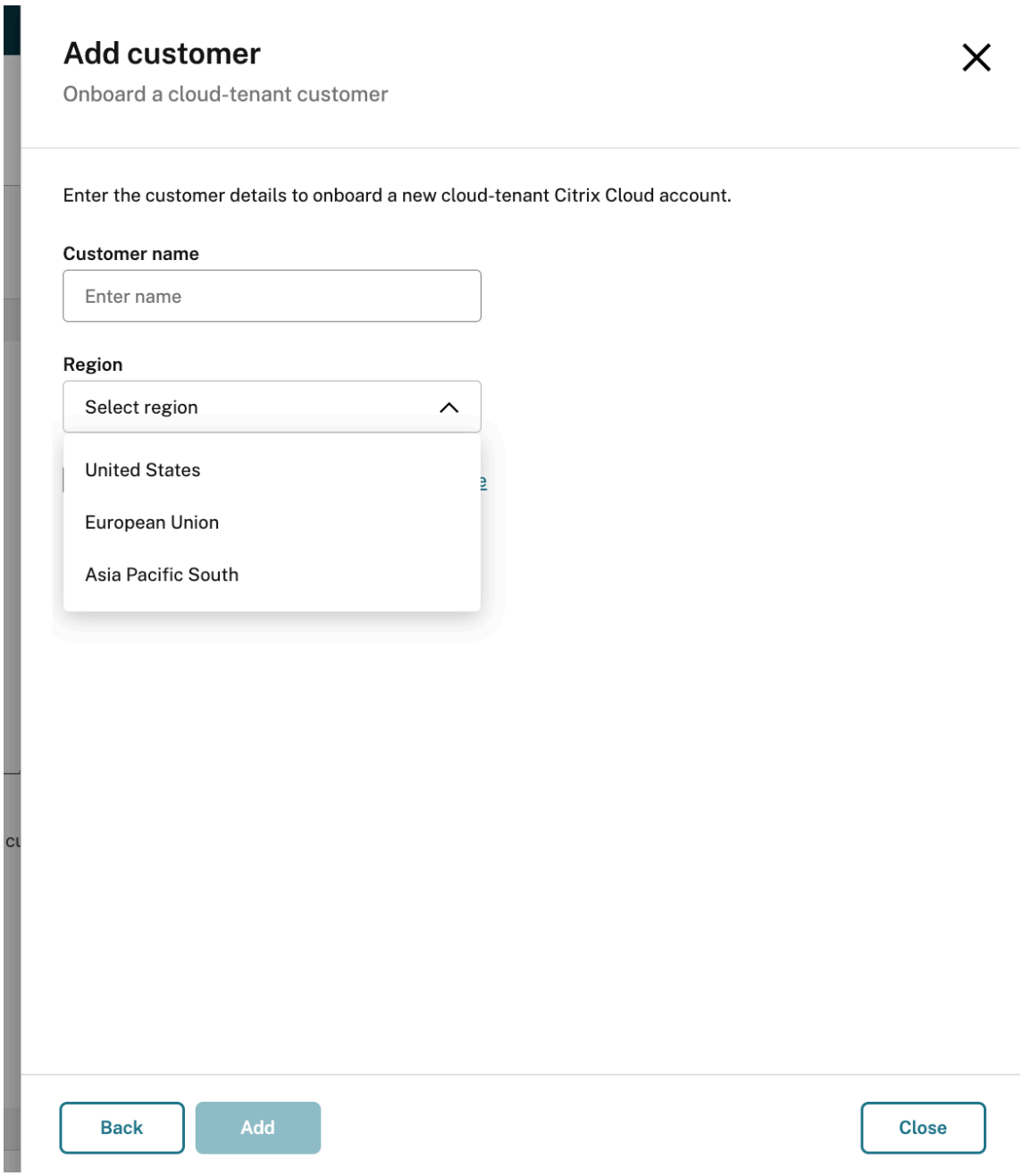
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Note:

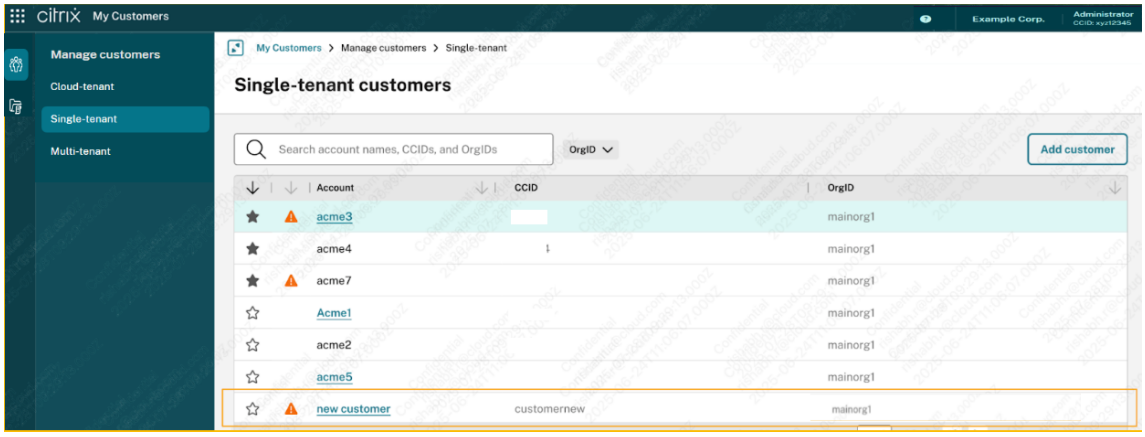
- **Onboard a Customer** option is applicable to onboard a single-tenant and multi-tenant customer. This onboarded customer shares the same OrgID as Partner.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

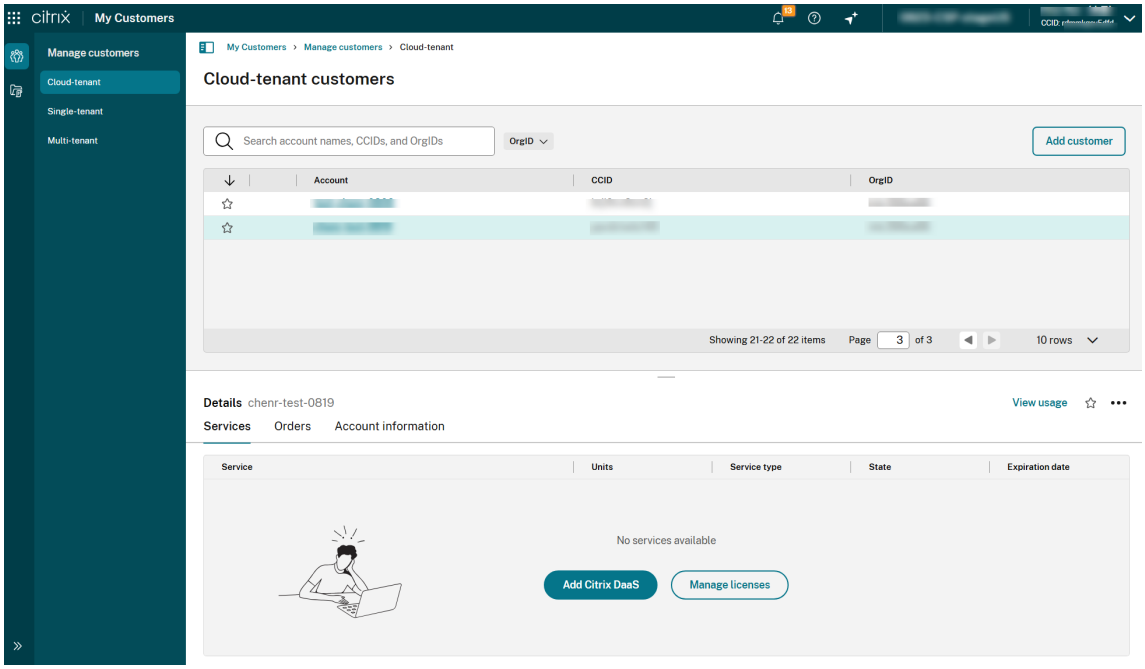


4. Customers added through the **Invite a Customer** flow appear under the Single-tenant customers list. This invited customer has their own unique OrgID.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Customers added through **Onboard a customer** flow appear under the Cloud-tenant customers list. This onboarded customer has the same OrgID as Partner.

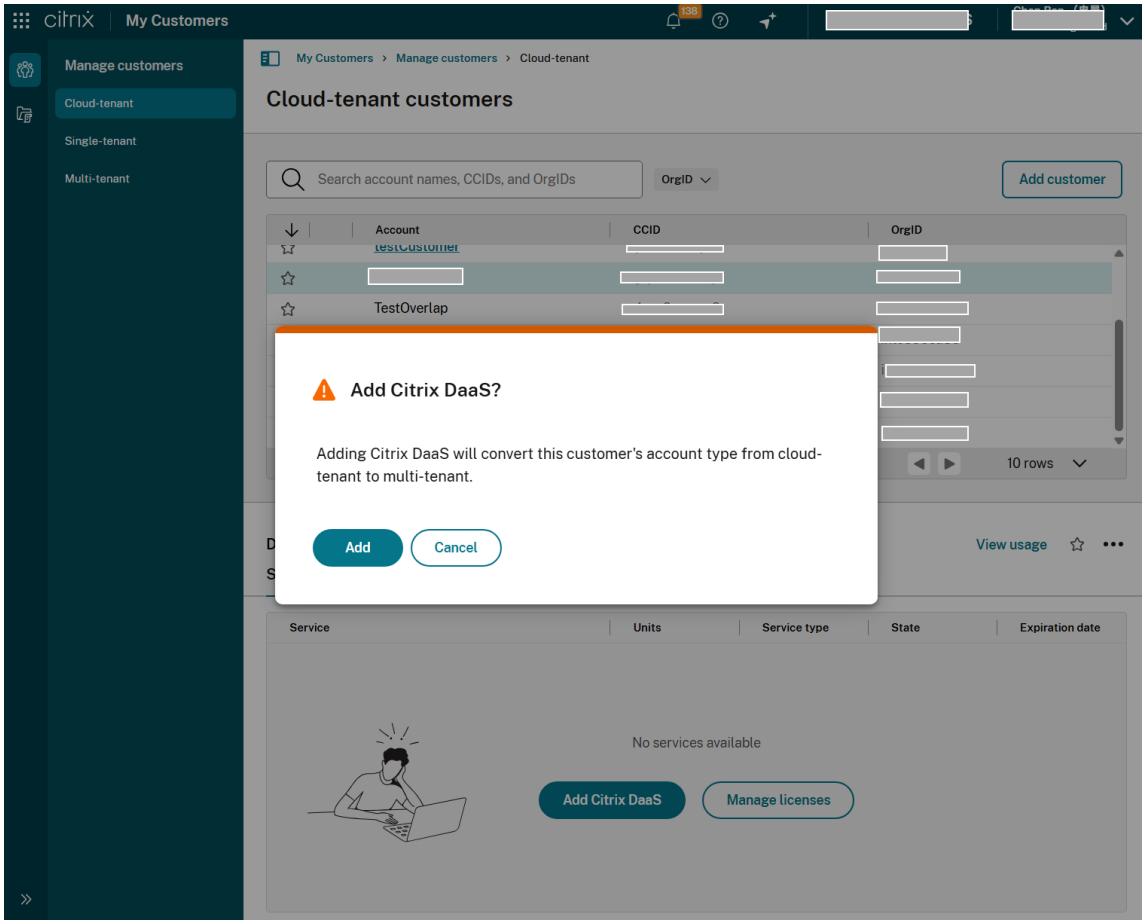


Activating the added customers

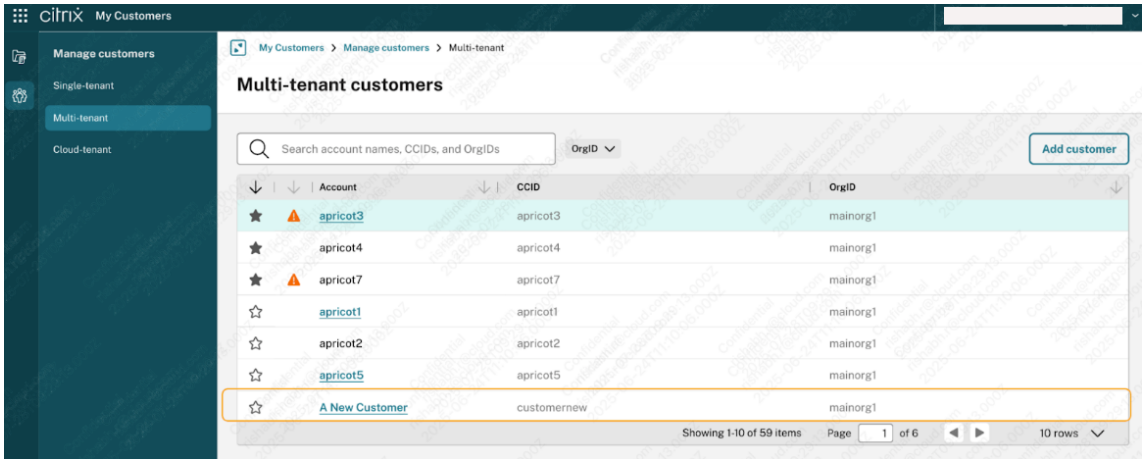
To make a cloud tenant as Multi-tenant DaaS customer

1. Go to **Manage customers > Cloud-tenant**, click on **Add Citrix DaaS™** to assign **DaaS service**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



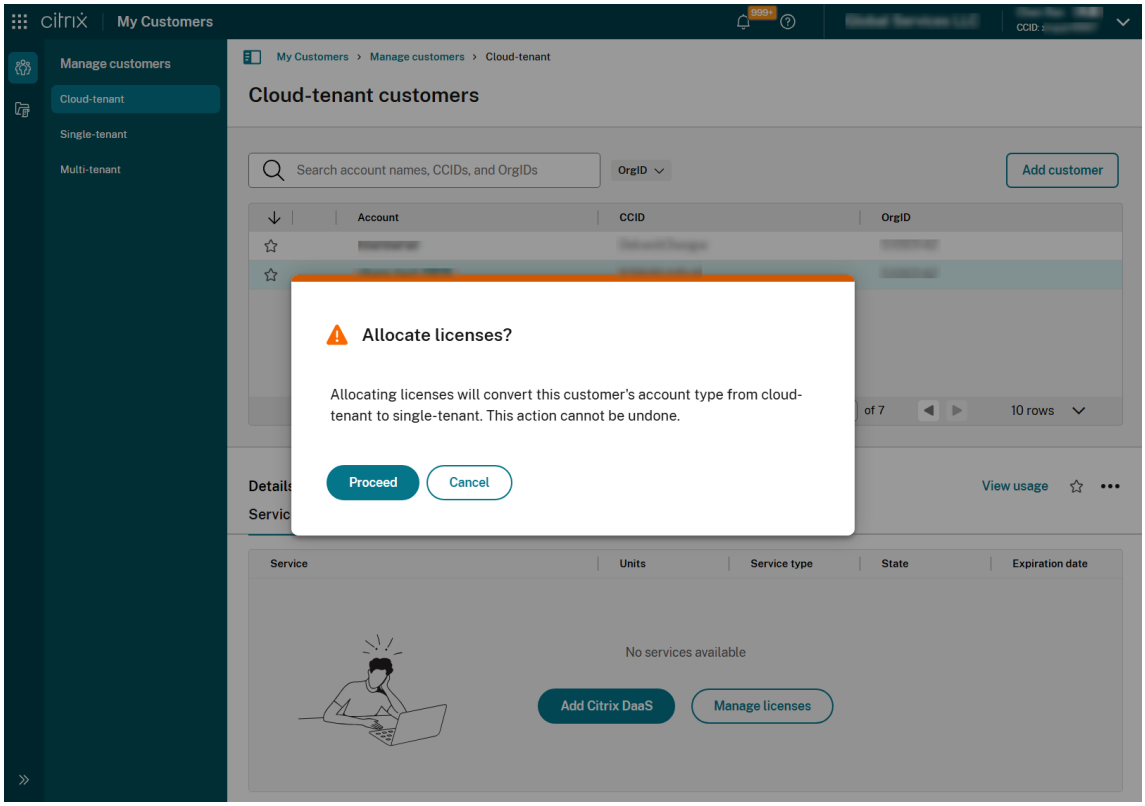
2. Customers will go into the Multi-tenant customers list.



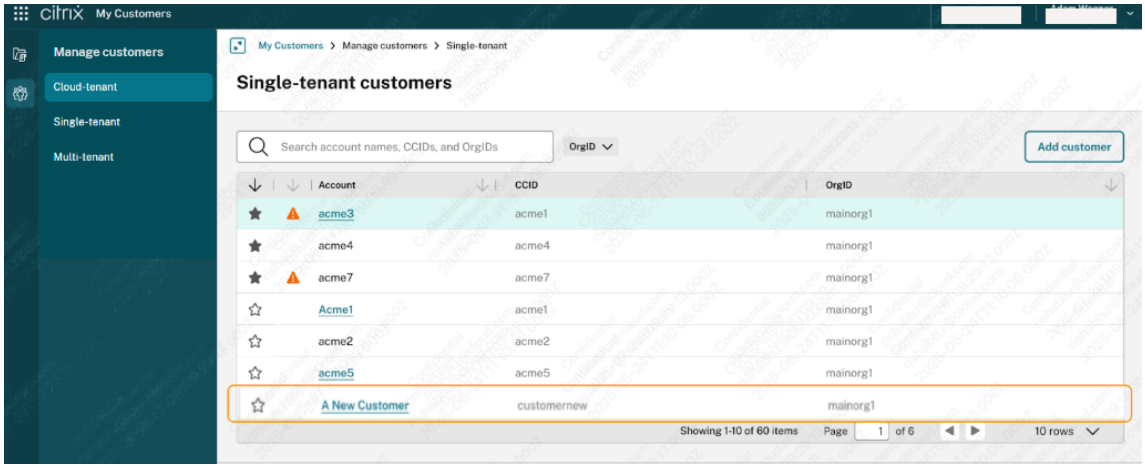
To make a cloud tenant as Single-tenant customer

1. Go to **Manage customers > Cloud-tenant**, click on **Manage licenses** to select **Allocate licenses**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

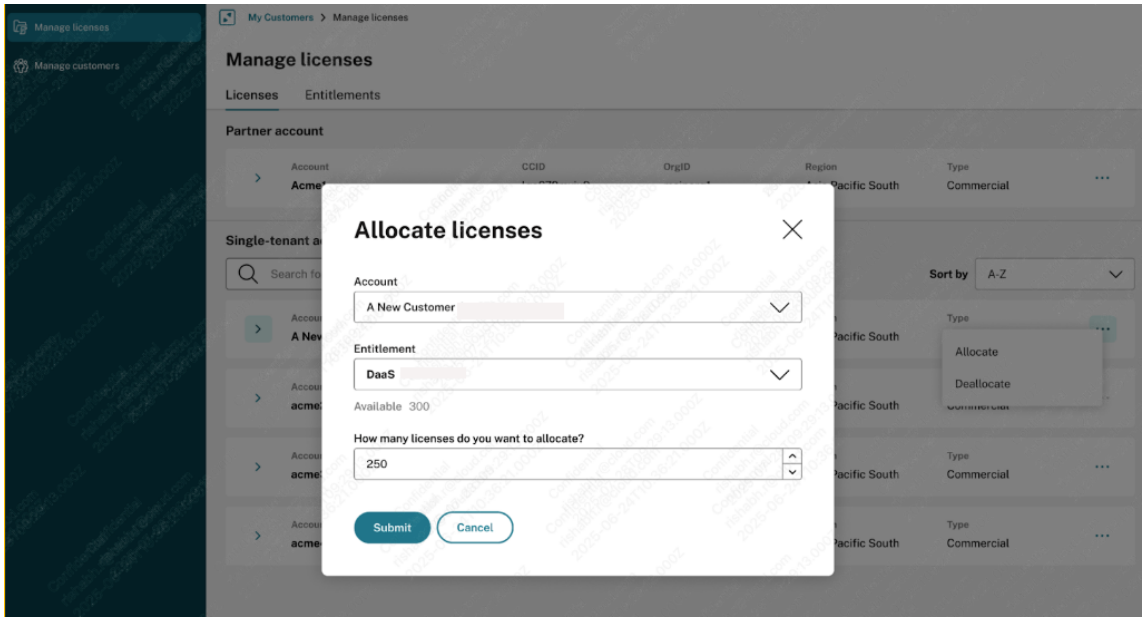


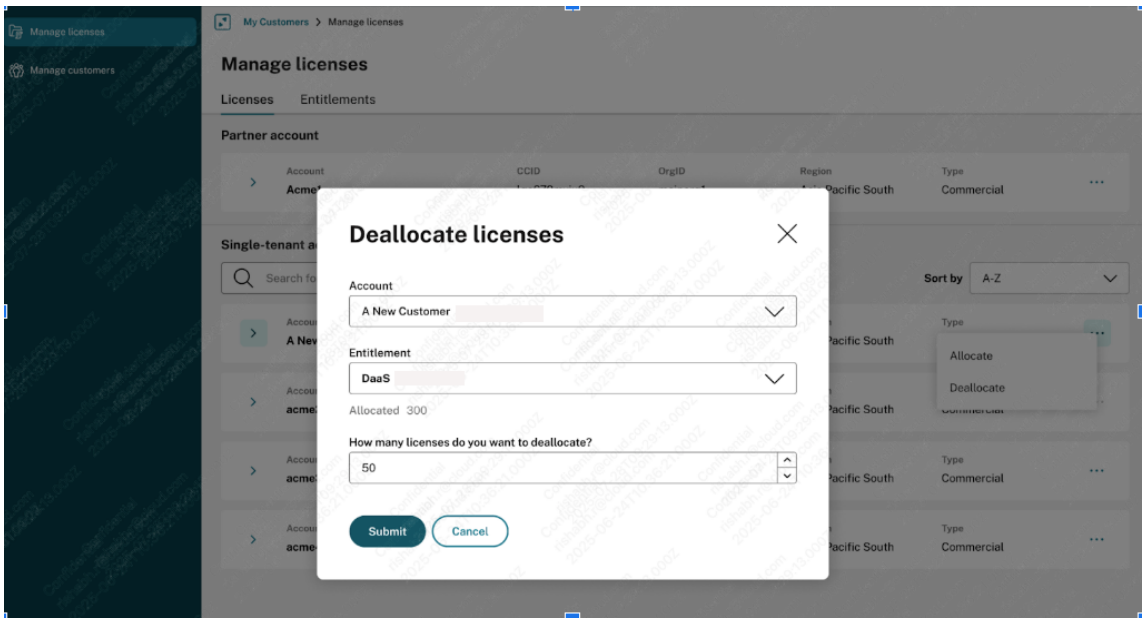
2. Customers will go into the Single-tenant customers list.



3. You can update licenses from the **Manage licenses > Licenses** tab by selecting either the **Allocate** or **Deallocate** options.

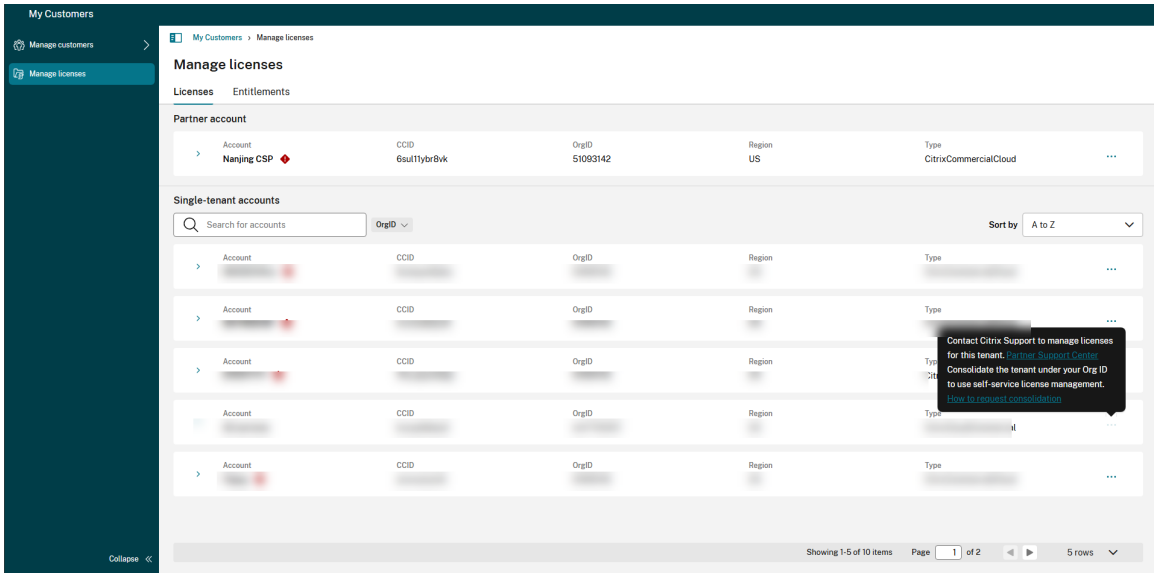
© 1997–2026 Citrix Systems, Inc. All rights reserved.





> **Note:**
>
> Single-tenant customers added through the **Invite a Customer** option have their own unique OrgID. To allocate or deallocate licenses for these customers, the partner must contact Citrix customer service. If a CSP wants to manage licenses (allocate or deallocate) for their Single-Tenant Customers in a self-service way, then CSP must raise a case to Citrix to consolidate their Single-Tenant Customers under the CSP-owned OrgID by following CTX695209. Messages in the UI will direct the partner about this process.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Create connections with customers

Partners create connections with customers using a unique invitation link. This link is fixed and can't be changed or customized.

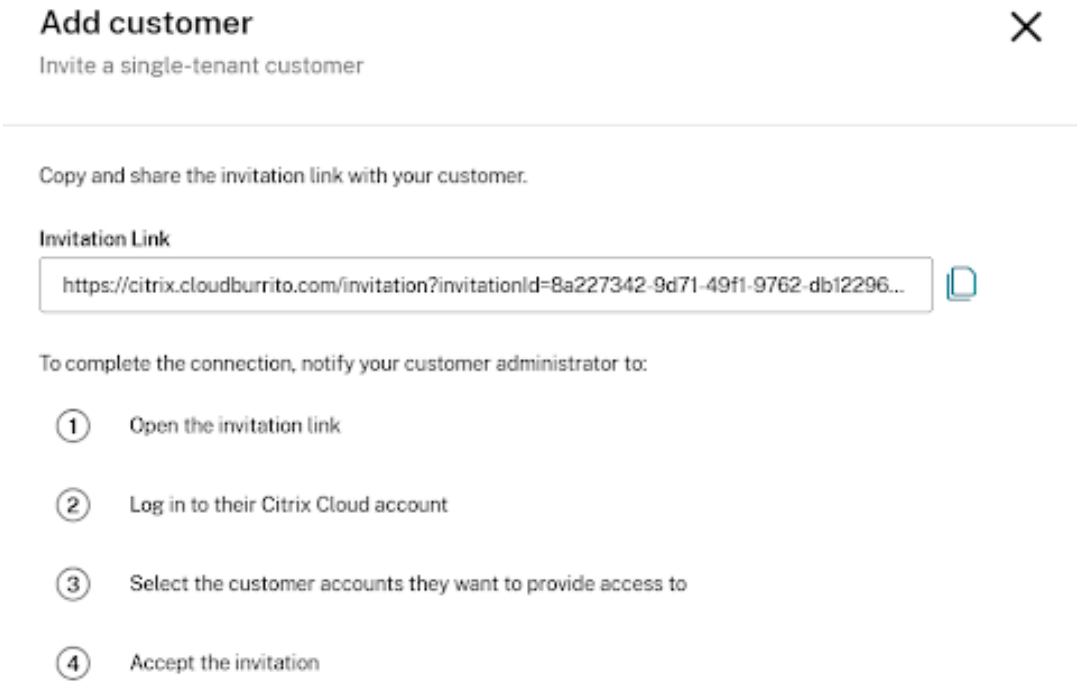
Partners can use their invitation link an unlimited number of times to create or recreate connections. Invitation links don't expire.

> **Note:**
>
> Manual linking of customers described in this section is only for the purpose of onboarding a single tenant customer who already has an existing Org ID and its associated cloud account. Within Citrix Cloud Commercial, partners can create connection with their customers from US, EU an APS regions.

To create a connection:

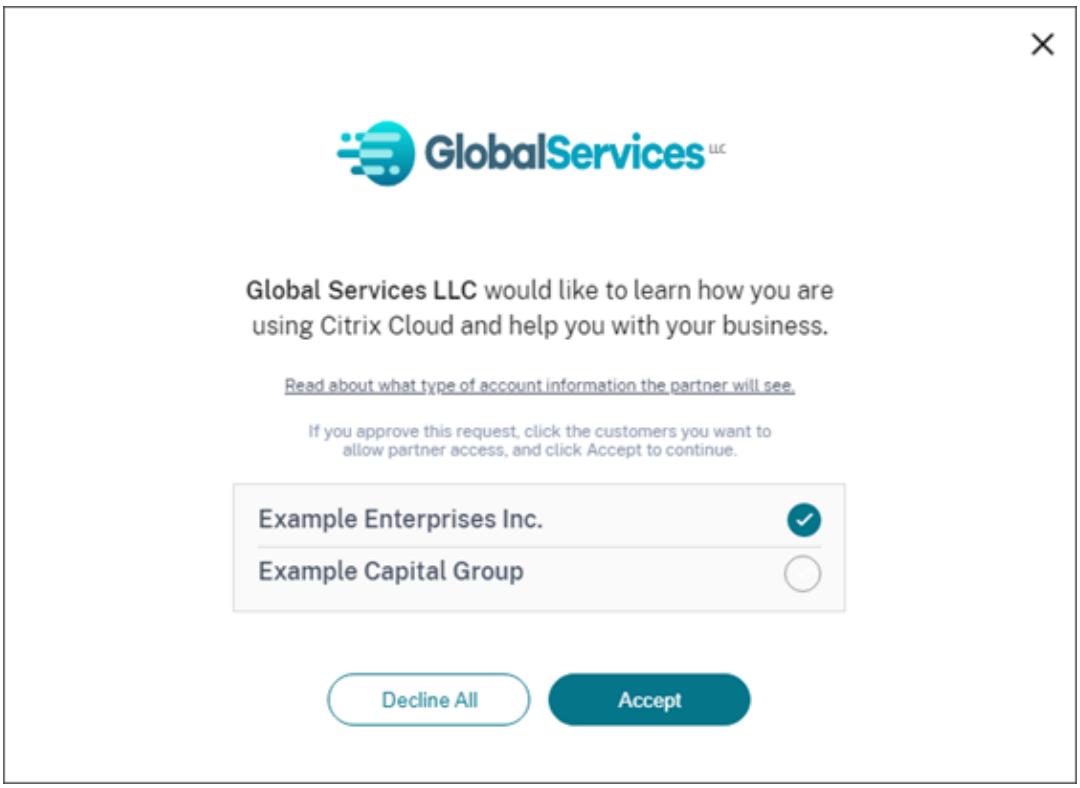
1. From the Citrix Cloud menu, select **My Customers**.
2. From the Customer Dashboard sidebar, select **Manage customers**.
3. To connect with an existing Citrix Cloud customer:
    a) Select **Add customer** and then select **Invite a single-tenant customer**.
    b) Copy the invitation link and send it to the customer.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



To complete the connection, the customer clicks the invitation link, signs in to Citrix Cloud, and accepts the invitation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. To connect with a new customer who doesn't yet have a Citrix Cloud account:

   a) Select **Add a customer** and then select **Onboard a customer**.
   b) Enter the customer's business contact details and then select **Add**. Citrix Cloud creates a new account for the customer.

   Afterward, the customer receives a notification confirming that the partner has been added as an administrator to the new account. The customer can set a password for the account by using the Forgot password? link on the Citrix Cloud sign-in page. After setting their password, the customer can sign in to their account using their business email address and complete the onboarding process as described in Sign up for Citrix Cloud.

Remove partner or customer connections

Either the partner or the customer can terminate a connection at any time.

Remove a connection with a customer

To terminate a connection with a customer, the partner performs the following steps:

1. From the Citrix Cloud menu in the top right corner of the console, select **My Customers**.
2. From the Customer Dashboard, locate the customer you want to manage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Click the ellipsis menu for the customer and then select **Remove Customer**.
4. When prompted to confirm the removal, select **Remove**.

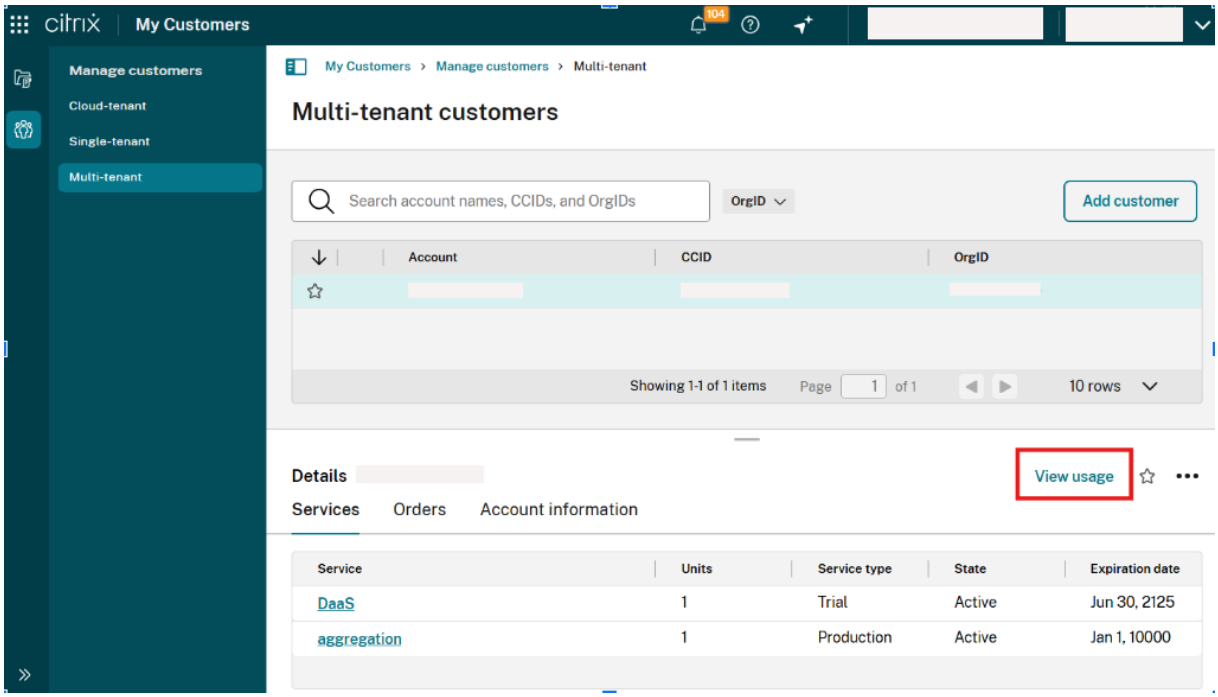
Remove a connection with a partner

To terminate a connection with a partner, the customer performs the following steps:

1. From the user menu in the top left corner, select **Account Settings**.
2. From the **Company Account** page, locate the **Partner Connections** section.
3. Locate the partner you want to manage and then select **Remove**.
4. When prompted to confirm the removal, select **Confirm**.

Licensing trends

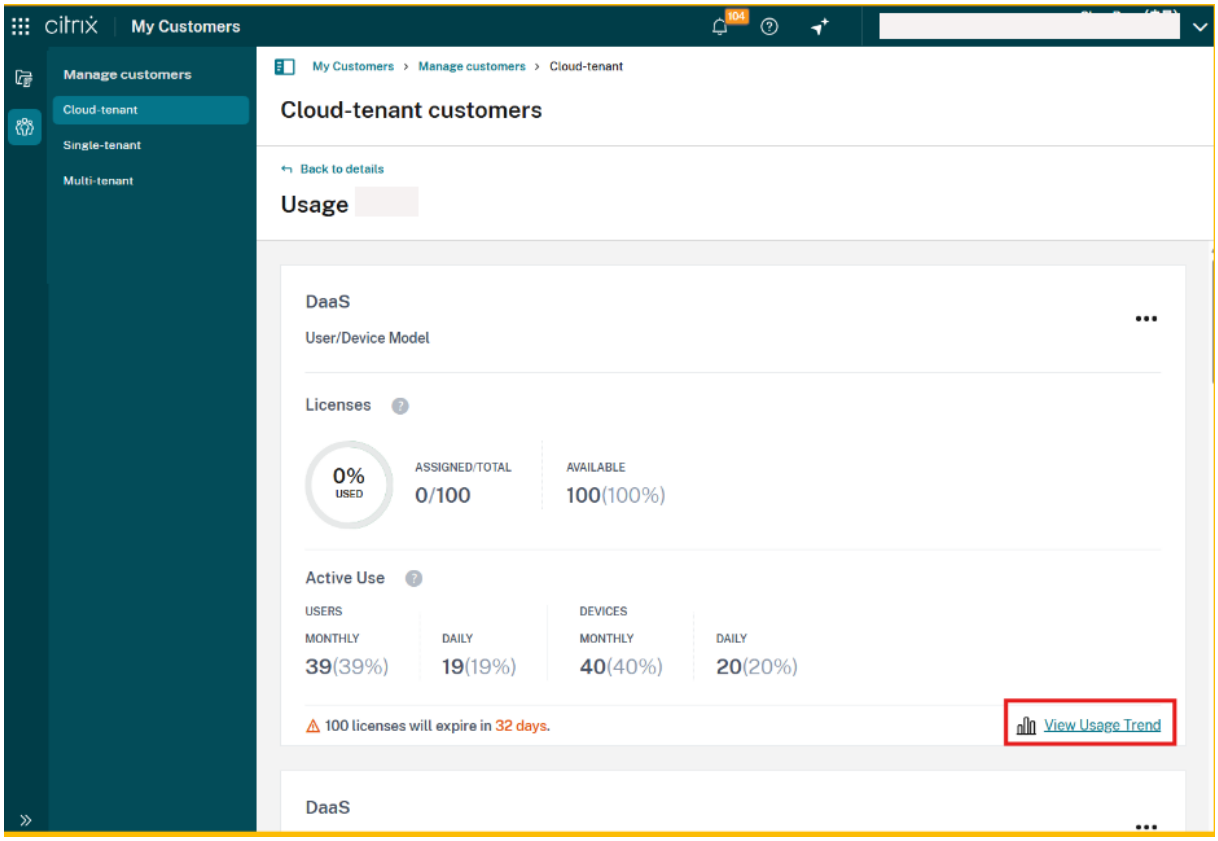
Partners can view licensing information for a customer by clicking **View Usage** in the details panel in the customer dashboard.



> **Note:**
>
> Citrix Partners can view only the Licensing summary view and historical active usage trends. They can't view individual users who consume licenses for a given service.

To view the customer's licensing summary for each service, click the **View Usage** tab. For more usage information, select **View Usage Trend** for the service entitlement you want to view.

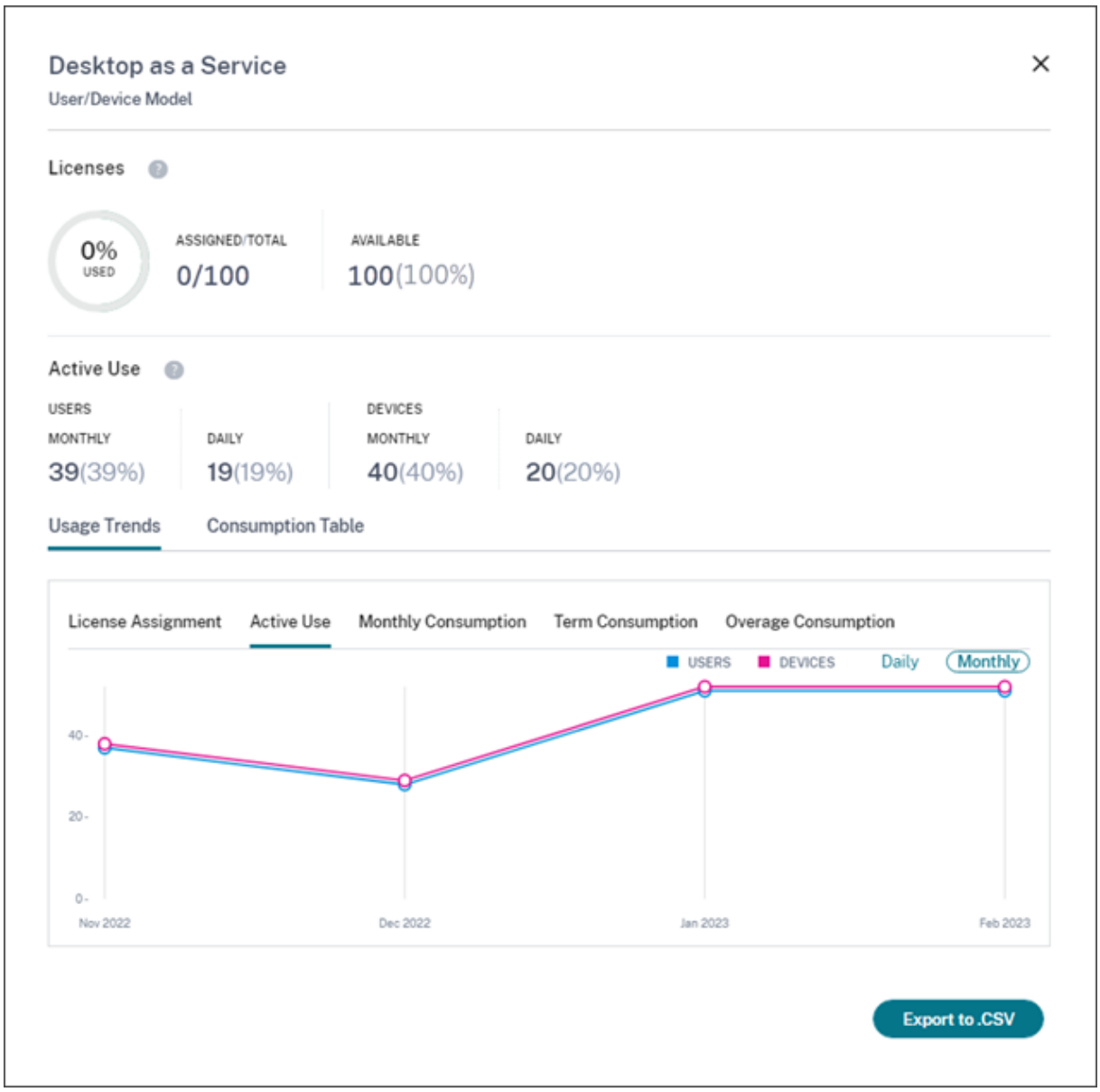
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Depending on the service, usage trends include the following information:

- The ratio of assigned licenses to the total purchased
- Monthly and daily active users
- A visual breakdown of license assignments, active use, consumption per entitlement, and overage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



If needed, partners can export this information as a .csv file.

Bandwidth usage

For Citrix Gateway service, the licensing summary consists of the following information:

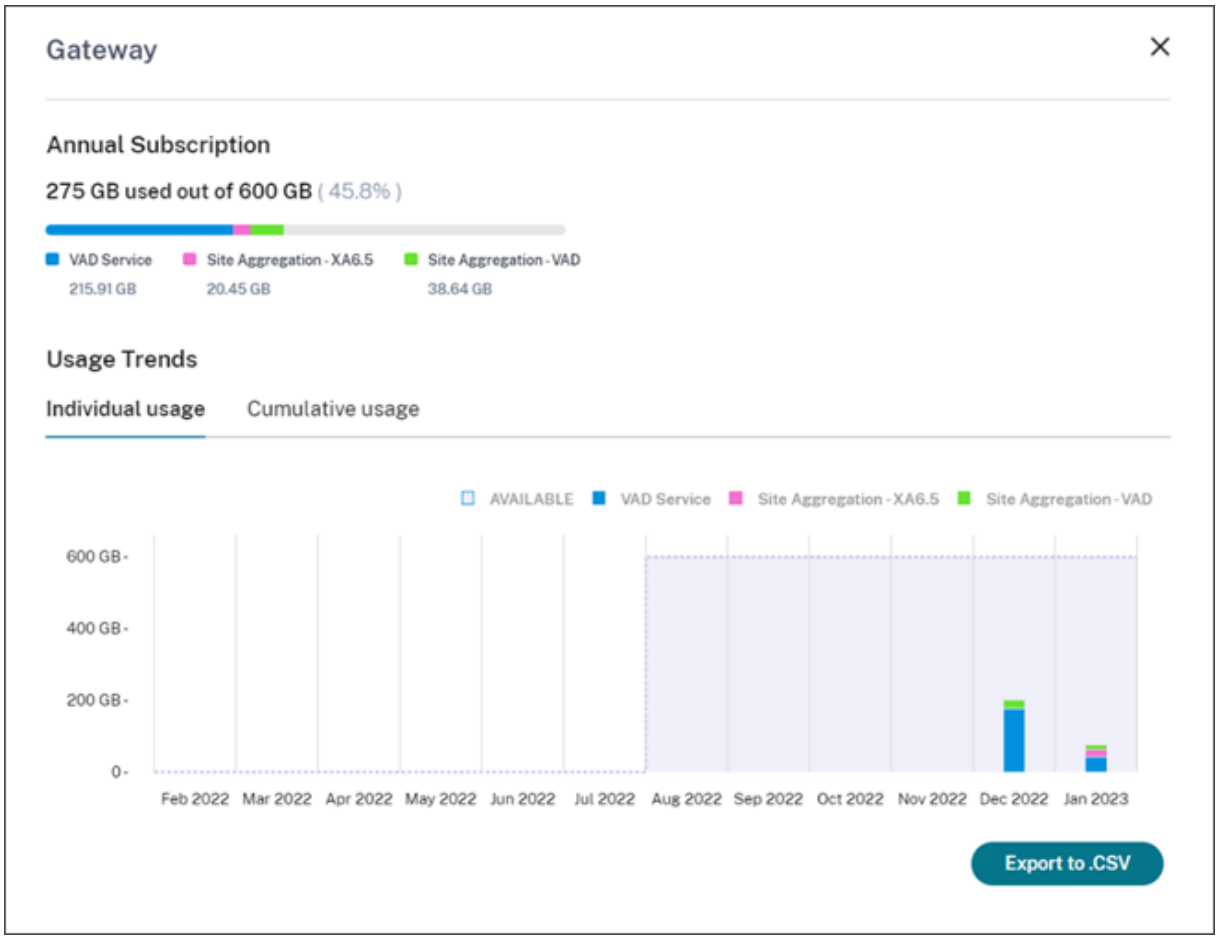
- Total bandwidth usage across all of the customer's entitlements.
- Total bandwidth usage broken down by the customer's monthly, annual, and termed entitlements.
- Total overage for the current month. For more information about how overage is calculated, see Overage.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Select **View Usage Trend** at the far-right side of the page for an entitlement to view the usage summary. Select **View Overage Chart** to view overage over the past 12 months.

Depending on the entitlement, usage trends include the following information:

- The amount of consumed bandwidth among Citrix DaaS (**VAD Service**) and on-premises Virtual Apps and Desktops deployments with site aggregation.
- A visual breakdown of bandwidth usage for each individual month in which it was used. (Monthly entitlements)
- A visual breakdown of **Individual Usage** of bandwidth that occurred during each single month of the billing period. (Annual and Termed entitlements)
- A visual breakdown of **Cumulative Usage** of bandwidth that accumulated at each month in the billing period. (Annual and Termed entitlements)



If needed, partners can export this information as a .csv file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Customer licensing and usage for Citrix Service Providers

The Licensing feature in Citrix Cloud enables customers of Citrix Service Providers (CSP) to monitor their licenses and usage for supported Citrix DaaS (formerly Citrix Virtual Apps and Desktops™) products. CSPs can sign in under their customer's Citrix Cloud account to view and export this information as well. For more information, see the following articles:

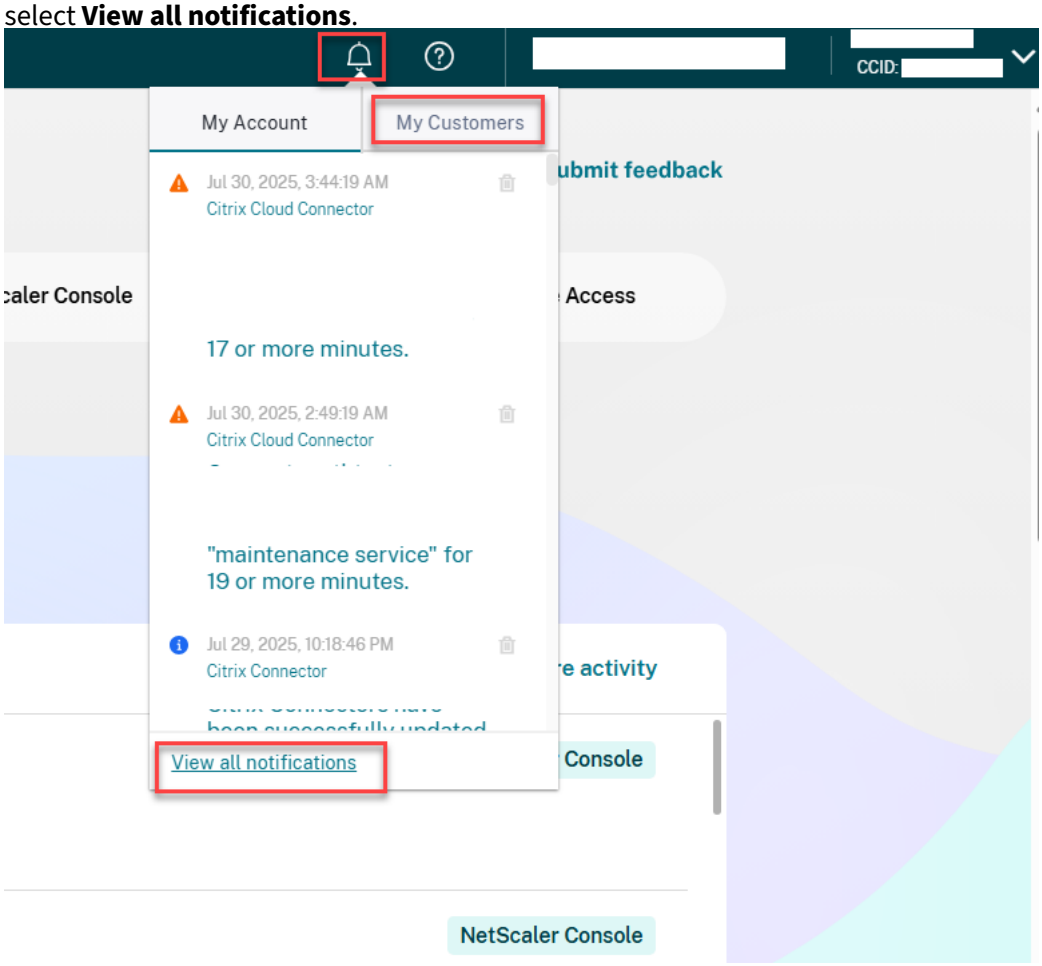
- Customer license and usage monitoring for Citrix DaaS

Partner visibility into customers' notifications

Partners can view notifications for their connected customers. Partners can also filter customer-specific notifications and take action, like dismissing the notification. Dismissed notifications don't show up for the partner. However, customers can still see the notification in their account after they sign in to Citrix Cloud.

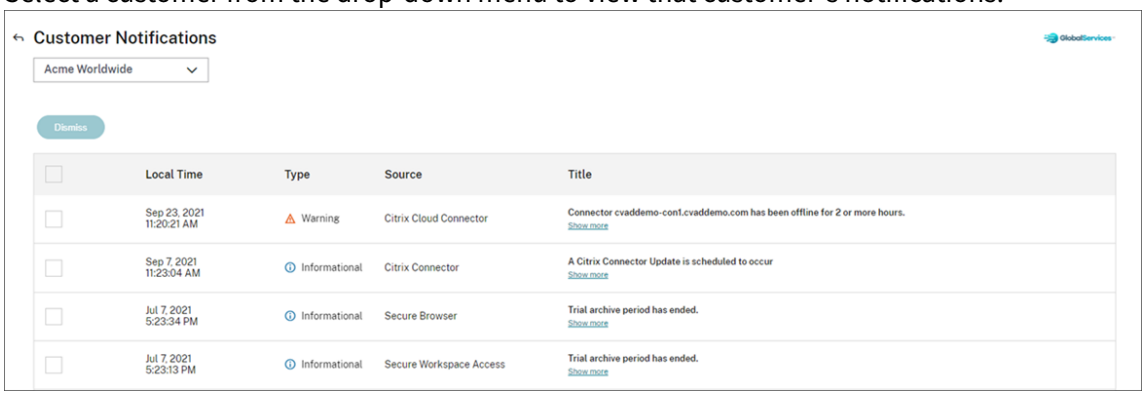
To view customer notifications:

1. Click the bell icon near the top of the management console, select **My Customers**, and then select **View all notifications**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

2. Select a customer from the drop-down menu to view that customer's notifications.



Federated domains for Citrix Service Providers

Federated domains enable customer users to use credentials from a domain attached to your CSP resource location to sign in to the store. This allows you to provide dedicated stores to your customer users with a custom store URL, such as *customer.cloud.com*. The resource location is still on your partner Citrix Cloud account. You can provide dedicated stores alongside the shared store that customers can access using your CSP store URL (for example, csppartner.cloud.com). To enable customers to access their dedicated store, you add them to the appropriate domains that you manage. After configuring the store, customer users can sign in to their store and access the apps and desktops that you've made available through Citrix DaaS.

When you remove a customer from a federated domain, the customer's users can no longer access their stores using credentials from the partner's domain.

For more information about using federated domains to deliver apps and desktops, see Citrix DaaS for Citrix Service Providers.

Store appearance options for Citrix Service Providers

You can configure your store colors and logos with custom themes. To learn how to create custom themes, see Customize the appearance of stores.

> **Note**
>
> Custom theming is a single-tenant feature. Citrix Service Providers where service provider tenants share a resource location, cloud connectors, and active directory domain (multi-tenant) are not currently supported. Citrix Service Provider tenants that have their own dedicated resource location, cloud connectors and dedicated active directory domain (single-tenant) are fully supported.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Cloud Services

September 6, 2025

This article lists the cloud services that are offered through Citrix Cloud and links to the product documentation for each service. For descriptions of these services and the offerings in which they are included, see Service Descriptions for Citrix Services.

Citrix® services

Analytics

- Analytics for Security
- Analytics for Performance
- Analytics - Usage

Citrix DaaS

Citrix DaaS Standard for Azure

Endpoint Management

Gateway

Global App Configuration service

ITSM Adapter for ServiceNow

Remote Browser Isolation

Secure Private Access

Session Recording service

Virtual Apps Essentials

Virtual Desktops Essentials

Workspace Environment Management

NetScaler® services

Console

App Delivery and Security

SD-WAN Orchestrator

Secure Internet Access

Web App Firewall

© 1997–2026 Citrix Systems, Inc. All rights reserved.

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.