Citrix Cloud™ Japan

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

Contents

Citrix Cloud Japan 3

Feature availability for supported services 7

Secure Deployment Guide for Citrix Cloud Japan 9

How to Get Help and Support 15

Sign up for Citrix Cloud Japan 18

Service trials for Citrix Cloud Japan 25

System requirements 28

Service connectivity requirements 30

Citrix Cloud™ Connector requirements 35

Plan and build your deployment 44

Create a resource location 45

Install Cloud Connectors from the command line 48

Citrix Cloud Connector™ proxy and firewall configuration 50

Connector Appliance for Cloud Services 52

Active Directory with Connector Appliance 85

Set up workspaces 91

Identity and access management 92

Connect Active Directory to Citrix Cloud Japan 94

Connect Microsoft Entra ID as an identity provider 95

Microsoft Entra ID Permissions for Citrix Cloud™ Japan 100

Connect an on-premises Citrix Gateway as an identity provider 103

Connect Okta as an identity provider 111

Connect SAML as an identity provider to Citrix Cloud Japan 118

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

License Activation Service **128**

Manage Citrix Cloud Japan **128**

Manage Citrix Cloud Japan administrators **131**

System Log **139**

Citrix Cloud Japan for Partners **142**

SDKs **142**

Citrix Gateway service for Citrix Cloud Japan **144**

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

Citrix Cloud Japan

June 30, 2026

Citrix Cloud Japan is a Cloud that is isolated and separate from Citrix Cloud, allowing Japanese customers to use certain Citrix Cloud services in a dedicated Citrix-managed environment.

The Citrix Cloud Japan documentation provides details on setting up your account and supported services. This documentation also describes any differences in the services and functions of Citrix Cloud Japan as compared to other Citrix Cloud regions. In cases where features and capabilities are identical in both Citrix Cloud Japan and Citrix Cloud, this documentation provides links to the existing information in the Citrix Cloud documentation.

Available services

The following services are available in Citrix Cloud Japan:

- Citrix Gateway
- Citrix DaaS™ (formerly Virtual Apps and Desktops)
- License Usage Insights (Citrix partners only)
- Secure Browser
- Citrix Workspace™
- Workspace Environment Management service (requires Citrix Cloud Connector version `6.29.0.58841` or later)
- License Activation Service

For more information, see Feature availability for services.

Non-regional data

Certain Logs, including information related to the Customer's use of the Cloud Services, are non-regional in nature. This data may be replicated and accessed non-regionally as necessary to support the Cloud Services, including for support or troubleshooting, monitoring performance, security, auditing, and to allow for cross-regional authentication.

Logs might be processed non-regionally by Citrix Third Party Suppliers as necessary to perform the Services. See Citrix Cloud Services Data Protection Overview for further information.

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

Third Party Notifications

Citrix Cloud Japan may include third party software licensed under the terms defined in the Third Party Notices documents for the platform and supported services. For more information, refer to Citrix Cloud Third Party Notifications.

What's new

Citrix aims to deliver new features and updates to Citrix Cloud Japan customers when they're available. New releases provide more value, so there's no reason to delay updates.

This process is transparent to you. Initial updates are applied to Citrix internal sites only and are then applied to customer environments gradually. Delivering updates incrementally maximizes product quality and availability.

For details about the Service Level Agreement for cloud scale and service availability, see the Citrix Cloud Service Level Agreement. To monitor service interruptions and scheduled maintenance, see the Service Health Dashboard.

June 2025

The following features are now available in Citrix Workspace for Citrix Cloud Japan:

- Modern UI experience including Activity Manager.
- Custom announcements.
- Custom Domains.
- Stay logged in to Citrix Workspace app.
- Customize appearance.

March 2025

Connector Appliance for Cloud Services: Citrix Cloud Japan now supports Connector Appliance, which is available as a Citrix component hosted in your hypervisor, enabling secure communication between Citrix Cloud and your resource locations. It simplifies cloud management by removing the need for complex networking or infrastructure configuration. For more information, see Connector Appliance.

November 2024

Session Recording service now available in the Japan region of Citrix Cloud: Citrix Cloud Japan now supports the Session Recording service, enhancing security for Citrix DaaS with streamlined de-

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

ployment and advanced administration. It offers automation, faster troubleshooting, and a unified management experience for organizations. For more information, see Session Recording service.

October 2023

App Protection: Citrix Cloud Japan now supports Workspace App Protection service. For more information, see App Protection.

August 2022

Improved administrator management interface: Citrix Cloud Japan now includes an improved interface for adding individual administrators and administrator groups. For more information, see the following articles:

- Invite individual administrators
- Add administrators to Citrix Cloud Japan from AD

July 2022

SAML authentication for administrators preview: Citrix Cloud Japan now supports using SAML authentication for administrator groups in AD. For more information, see Connect SAML as an identity provider to Citrix Cloud Japan.

April 2022

Enable or disable access to the customer dashboard: Citrix Cloud Japan now supports enabling view-only access to the customer dashboard for administrators. For more information, see Citrix Cloud for Partners.

Improved license release for Citrix DaaS: Citrix Cloud Japan now includes an improved workflow for releasing assigned licenses in bulk. For more information, see Monitor licenses and active usage for Citrix DaaS (User/Device).

March 2022

System Log General Availability: System Log is now generally available. System Log displays a time-stamped list of events that occurred in Citrix Cloud Japan. View events up to the last 90 days and export events to meet regulatory compliance requirements or for security analysis. For more information, see System Log.

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

February 2022

Support for SAML as an identity provider: Citrix Cloud Japan now supports using the SAML provider of your choice to authenticate subscribers to Citrix Workspace. For more information, see Connect SAML as an identity provider to Citrix Cloud Japan.

December 2021

Citrix Gateway service is generally available: Citrix Gateway provides secure remote access for external users of Citrix Workspace. For more information, see Citrix Gateway service for Citrix Cloud Japan.

November 2021

Add administrators in Microsoft Entra ID groups: Citrix Cloud Japan now supports adding administrators to your Citrix Cloud Japan account using Microsoft Entra ID groups. For more information, see Manage administrator groups.

October 2021

Support for Workspace Environment Management service: Citrix Cloud Japan now supports Workspace Environment Management service. The service uses intelligent resource management and Profile Management technologies to deliver the best possible performance, desktop logon, and application response times for Citrix DaaS deployments. The support requires Citrix Cloud Connector version `6.29.0.58841` or later.

September 2021

Support for Citrix Workspace and Citrix Gateway service: Citrix Cloud Japan now supports the following services:

- Citrix Workspace enables you to deliver secure access to the information, apps, and other content that are relevant to a person's role in your organization. Users subscribe to the services you make available and can access them from anywhere, on any device.
- Citrix Gateway service provides secure remote access for external users of Citrix Workspace.

For more information, see Feature availability for services.

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

June 2021

System Log preview: Citrix Cloud Japan now includes the System Log preview feature which displays a timestamped list of events that occurred in Citrix Cloud Japan. View events up to the last 90 days and export events to meet regulatory compliance requirements or for security analysis. For more information, see System Log.

Feature availability for supported services

September 6, 2025

In general, service availability implies that all corresponding service features are available to you. However, in some cases, certain service features might not be available immediately when a service is included in Citrix Cloud Japan.

The sections in this article describe the services that are supported in Citrix Cloud Japan. These sections also list the service features that are not currently available. Features that are not included in this article are available in Citrix Cloud Japan and function in the same manner as in Citrix Cloud. To help you learn more about available features, this article include links to the documentation for each service.

Citrix DaaS™

Citrix DaaS (formerly Virtual Apps and Desktops service) enables you to deliver secure virtual apps and desktops, leaving most of the installation, setup, and upgrades to Citrix. You maintain complete control over applications, policies, and users while delivering the best user experience on any device.

Citrix DaaS is generally available to Citrix Cloud Japan customers. All service features are available and function in the same manner as in Citrix Cloud.

For more information, see the Citrix DaaS documentation.

App Protection

App Protection feature is an add-on feature that provides enhanced security when using Citrix Virtual Apps and Desktops™ and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). The feature restricts the ability of clients to compromise with keylogging and screen capturing malware. App Protection prevents exfiltration of confidential information such as user credentials and sensitive information on the screen. The feature prevents users and attackers from taking screenshots and from using keyloggers to glean and exploit sensitive information.

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

App Protection is generally available to Citrix Cloud Japan customers. All service features are available and function in the same manner as in Citrix Cloud.

For more information, see the App Protection documentation.
For more information about supported features of App Protection, see the App Protection Compatibility Matrix documentation.

License Usage Insights

The License Usage Insights service is a free cloud service that helps Citrix Service Providers understand and report on product licenses and usage. This service is generally available to Citrix Cloud Japan customers. All service features are available and function in the same manner as in Citrix Cloud.

For more information, see Licensing for Citrix Service Providers in the Citrix Cloud documentation.

Secure Browser

The Citrix Secure Browser Service isolates web browsing to protect the corporate network from browser-based attacks. It delivers consistent, secure remote access to internet hosted web applications, with no need for user device configuration.

Secure Browser service is generally available to Citrix Cloud Japan customers. All service features are available and function in the same manner as in Citrix Cloud.

For more information, see Secure Browser service in the Citrix Cloud documentation.

Citrix Workspace™

Citrix Workspace is the access tier for Citrix DaaS managed by Citrix, as an alternative to deploying Citrix StoreFront. Citrix Workspace generally available to Citrix Cloud Japan customers. All service features are available and function in the same manner as in Citrix Cloud.

Citrix Gateway service

Citrix Gateway service provides secure remote access for external users of Citrix Workspace.

Citrix Gateway service is generally available to Citrix Cloud Japan customers. The following service features are not available:

- Support for SaaS and enterprise web apps via secure private access.

For more information, see Citrix Gateway service for Citrix Cloud Japan.

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

Workspace Environment Management™

Workspace Environment Management uses intelligent resource management and Profile Management technologies to deliver the best possible performance, desktop logon, and application response times for Citrix DaaS deployments.

Workspace Environment Management service is generally available to Citrix Cloud Japan customers. All service features are available and function in the same manner as in Citrix Cloud.

For more information, see the Workspace Environment Management service documentation.

Other services

The following other services are not available in Citrix Cloud Japan:

- Device Posture Service
- Adaptive Authentication service
- Secure private access
- Global app configuration service

Secure Deployment Guide for Citrix Cloud Japan

June 30, 2026

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

Technical security overviews for other services

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

- Citrix Gateway service Technical Security Overview
- Citrix DaaS Technical Security Overview (formerly Virtual Apps and Desktops service)
- Workspace Environment Management service Customer Data Management

Guidance for administrators

- Use strong passwords and regularly change your passwords.

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

- All administrators within a customer account can add and remove other administrators. Ensure that only trusted administrators have access to Citrix Cloud Japan.
- 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 administrators is achieved using Citrix Cloud Japan's integration with Microsoft Entra ID.

Password compliance

Citrix Cloud Japan 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 Japan control plane does not store sensitive customer information. Instead, Citrix Cloud Japan retrieves information such as administrator passwords on-demand (by asking the administrator explicitly). There is no data-at-rest that is sensitive or encrypted; therefore, you do not need to manage any keys.

For data-in-flight, Citrix uses industry standard TLS 1.2 or higher with the strongest cipher suites. Customers cannot control the TLS certificate in use, as Citrix Cloud Japan is hosted on the Citrix-owned

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

cloud.jp domain. To access Citrix Cloud Japan, customers must use a browser capable of TLS 1.2 or higher, 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

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

Data sovereignty

The Citrix Cloud Japan control plane is hosted in Japan. Customers do not have control over this.

The customer owns and manages the resource locations that they use with Citrix Cloud Japan. 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 the customer's control.

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 to updates about the platform or individual services.

Citrix Cloud Connector™

Installation

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 reside within the customer's private network and not in the DMZ. For network and system requirements and instructions for installing the Cloud Connector, see Create a resource location.

Configuration

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

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

Customers can use antivirus alongside the Cloud Connector. Citrix tests with McAfee VirusScan Enterprise + AntiSpyware Enterprise 8.8. Citrix will support customers who use other industry standard AV products.

In the customer's Active Directory (AD) the Cloud Connector's machine account should be restricted to read-only access. This is the default configuration in Active Directory. Additionally, 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™

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 additional 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 additional possible security attack vectors and might reduce the security of the overall Citrix Cloud Japan solution.

Inbound and outbound ports configuration

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

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

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

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

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

Client Port(s)	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
49152 -65535/TCP	3269/TCP	LDAP GC SSL
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

Each of the services used within Citrix Cloud Japan will extend the list of open ports required. For more information, consult Connectivity requirements for Citrix Cloud Japan.

Monitoring outbound communication

The Cloud Connector communicates outbound to the Internet on port 443, both to Citrix Cloud Japan 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 Japan user interface.

Each service within Citrix Cloud Japan extends the list of servers and internal resources that the Cloud Connector might contact in the course of 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)
- Connectivity Requirements for supported cloud services

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

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.

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

Connector updates

When Citrix software updates are available, the Cloud Connector self-manages by default. For more information about configuring an update schedule, see Connector updates.

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 and updates for Citrix software.

Guidance for handling compromised accounts

- Audit the list of administrators in Citrix Cloud Japan and remove any who are not trusted.

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

- 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 will continue to function normally. The old authorization secrets will 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.

How to Get Help and Support

June 30, 2026

Signing in to your account

If you're having trouble signing in to your Citrix Cloud Japan account:

- Verify you're signing in at https://citrix.citrixcloud.jp/ and the sign-in page displays the Citrix Cloud Japan logo. The sign-in URL for Citrix Cloud Japan uses the `.jp` top-level domain, not the `.com` top-level domain.
- Make sure you sign in with the **email address** and password you provided when you signed up for your account. For more information about the email addresses accepted for account sign-up, see Sign up for Citrix Cloud Japan.
- If your organization uses Microsoft Entra ID as an identity provider for Citrix Cloud Japan administrators, click **Sign in with my organization credentials** and enter your organization's sign-in URL. You can then enter your organization credentials to access your organization's Citrix Cloud Japan account. If you don't know your organization's sign-in URL, contact your organization's administrator for assistance.

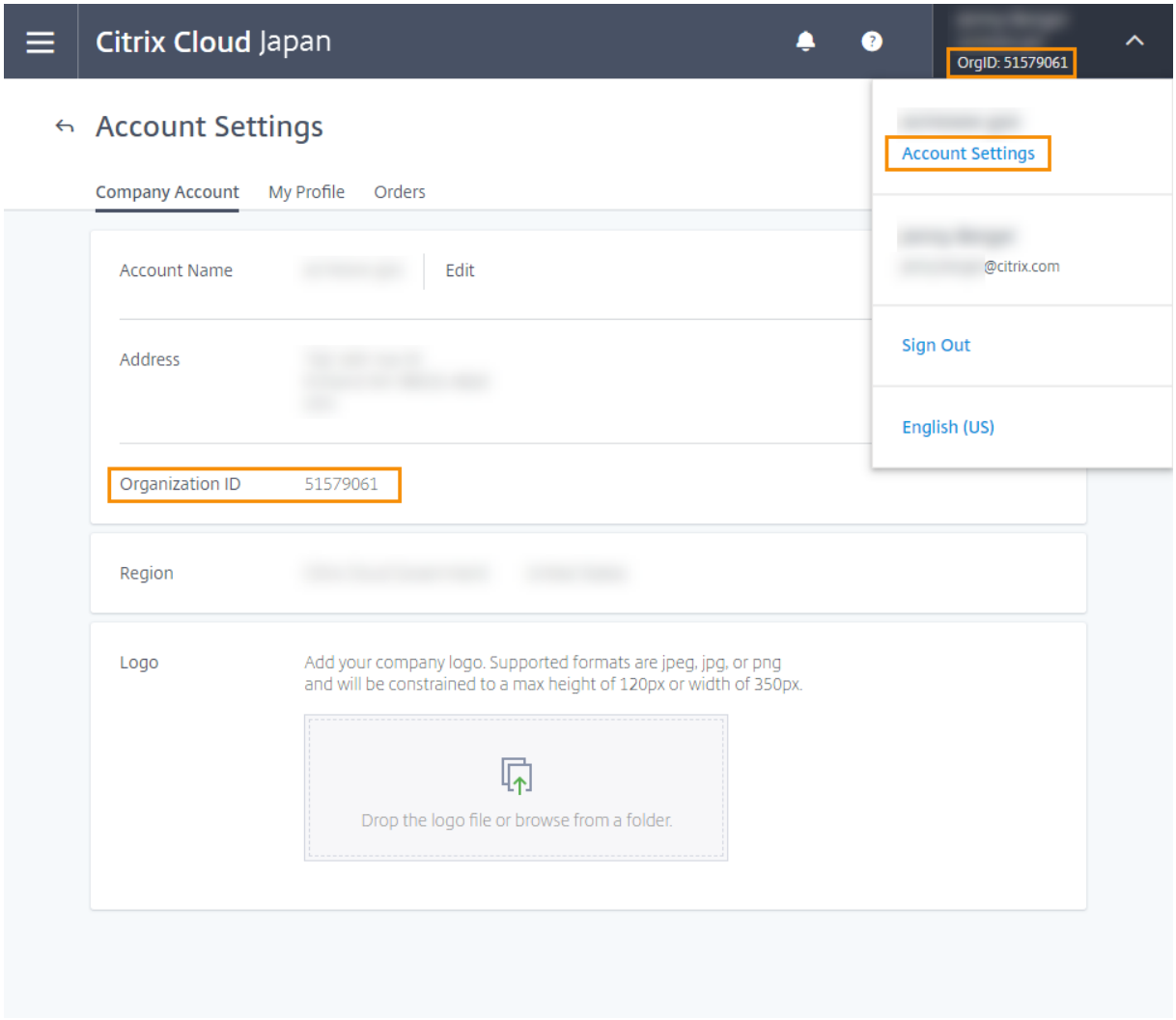
> **Note:**
>
> You can sign in with your organization credentials if Microsoft Entra ID is enabled as the identity provider for your account. For more information about using Microsoft Entra ID as your identity provider, see Connect Microsoft Entra ID as an identity provider.

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

Purchasing services

Visit https://www.citrix.com/buy/ to convert a service trial to a production service or to renew or extend an existing subscription.

To complete the purchase, you'll need your Organization ID, available in the Citrix Cloud Japan management console.



If you don't purchase before the end of your 60-day trial, the service is terminated and Citrix® archives all data and settings for 90 days.

If you don't purchase before the end of your subscription period:

- The service is blocked to administrators and users 30 days after the service expires.
- The service is terminated 90 days after the service expires and Citrix deletes any remaining data.

If you purchase within the 90-day period, your expired service is reactivated as a production service.

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

If you need additional assistance renewing or extending your subscription, contact Citrix Customer Service.

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
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.
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.
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.

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

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.

Support forums

Citrix Discussions is a community of Citrix technical experts where you can request help and contribute your knowledge about Citrix products and services. Visit the Citrix Cloud community at https://community.citrix.com/forums/forum/1479-citrix-cloud/.

Support articles and documentation

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

Citrix Knowledge Center

Search the Citrix Knowledge Center for help with specific technical issues. You can select the product you're working with or simply enter a description of your issue. The Knowledge Center displays the articles, security bulletins, and updates that are relevant to your search query.

Citrix Tech Zone

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

Sign up for Citrix Cloud Japan

June 30, 2026

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

This article walks you through the process of signing up for Citrix Cloud Japan and performing the required tasks for onboarding your account successfully.

What is an OrgID?

An OrgID is the unique identifier assigned to your Citrix Cloud Japan account. Your OrgID is associated with a physical site address, typically your company's business address. So, organizations 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 an organization to have multiple OrgIDs.

What is a Citrix Cloud Japan account?

A Citrix Cloud Japan account enables you to use one or more Citrix Cloud services to securely deliver your apps and data. A Citrix Cloud Japan account is also uniquely identified by an OrgID. It's important to use the right Citrix Cloud Japan account, based on how your organization has set up OrgIDs, so that your purchases and administrator access can continue on the same OrgIDs.

Multifactor authentication requirements

To keep your account safe and secure, Citrix Cloud Japan requires all customers to enroll in multifactor authentication. To enroll, you need only a device, such as a computer or mobile device, with an authenticator app installed, such as Citrix SSO.

If you're an existing Citrix customer, Citrix Cloud Japan prompts you to enroll when you visit the sign-up page and enter the credentials associated with your Citrix.com account. If you're new to Citrix, please sign up by contacting the account representatives to have your OrgID created.

Onboard your Citrix Cloud account

- If you are an existing Citrix customer and don't have a Citrix Cloud account, please onboard the cloud tenant by visiting My Organization and follow the steps in Citrix Cloud account management.
- If you're new to Citrix®, please sign up by contacting the account representatives to have your OrgID created.

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

Enroll in multifactor authentication

To keep your administrator account safe and secure, Citrix Cloud Japan requires you to use multifactor authentication when you sign in. Enrolling in multifactor authentication prevents unauthorized access to your administrator account and only requires a device, such as a computer or mobile device, with an authenticator app installed that follows the Time-Based One-Time Password standard, such as Citrix SSO.

If you're not enrolled in multifactor authentication, Citrix Cloud Japan prompts you to enroll when you sign in.

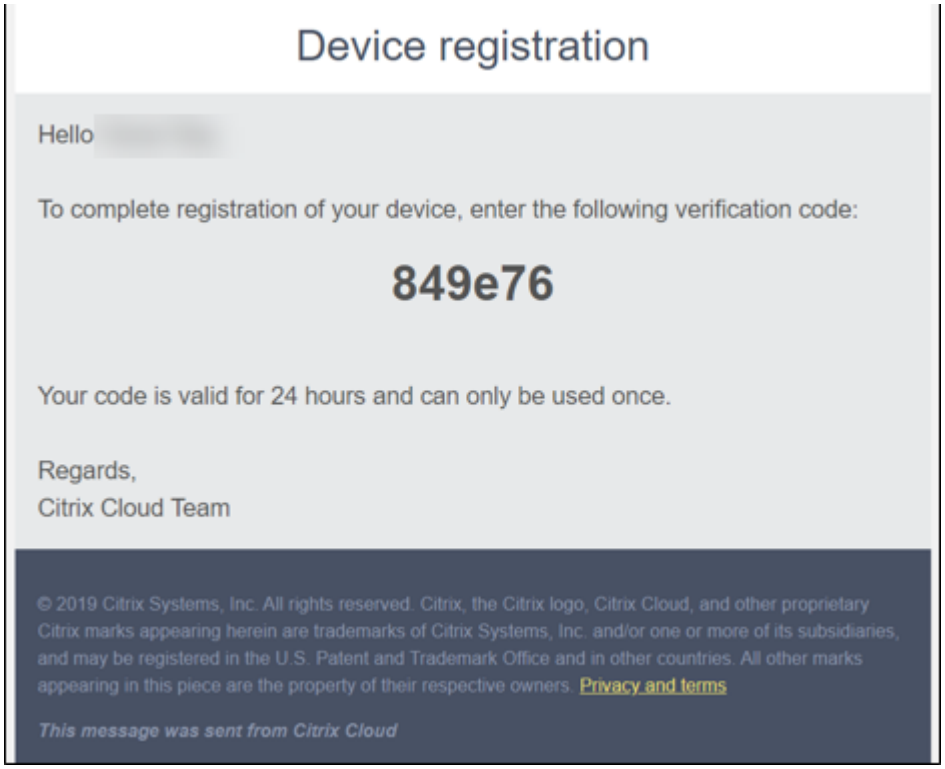
During enrollment, Citrix Cloud Japan presents a QR code and a key. Depending on your authenticator app, you can either scan the QR code or enter the key to register your device. For a smooth enrollment process, Citrix recommends downloading and installing this app on your device beforehand. Citrix Cloud Japan also generates one-time use backup codes that you can use to access your account in the event you lose your device or can't use your authenticator app.

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

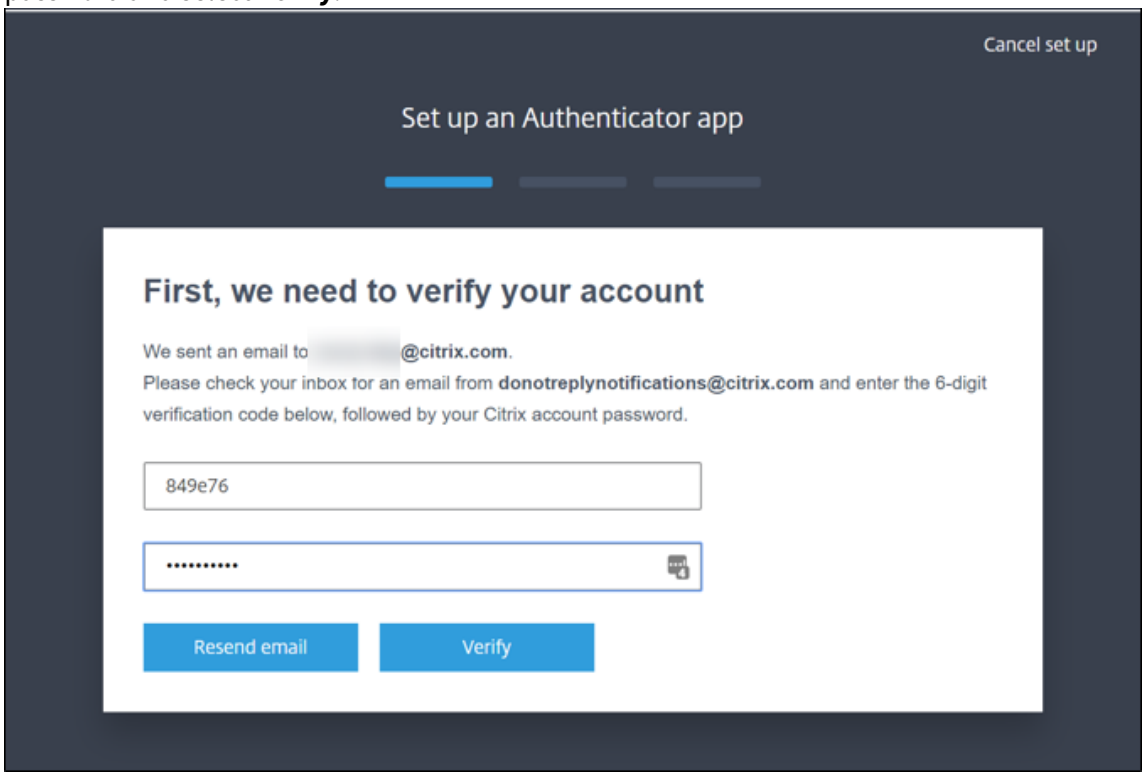
To enroll your device in multifactor authentication

1. Visit https://citrix.citrixcloud.jp and enter your Citrix Cloud Japan credentials.
2. When prompted to enroll in multifactor authentication, select **Enroll now**. Citrix Cloud Japan sends you an email with a verification code.

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

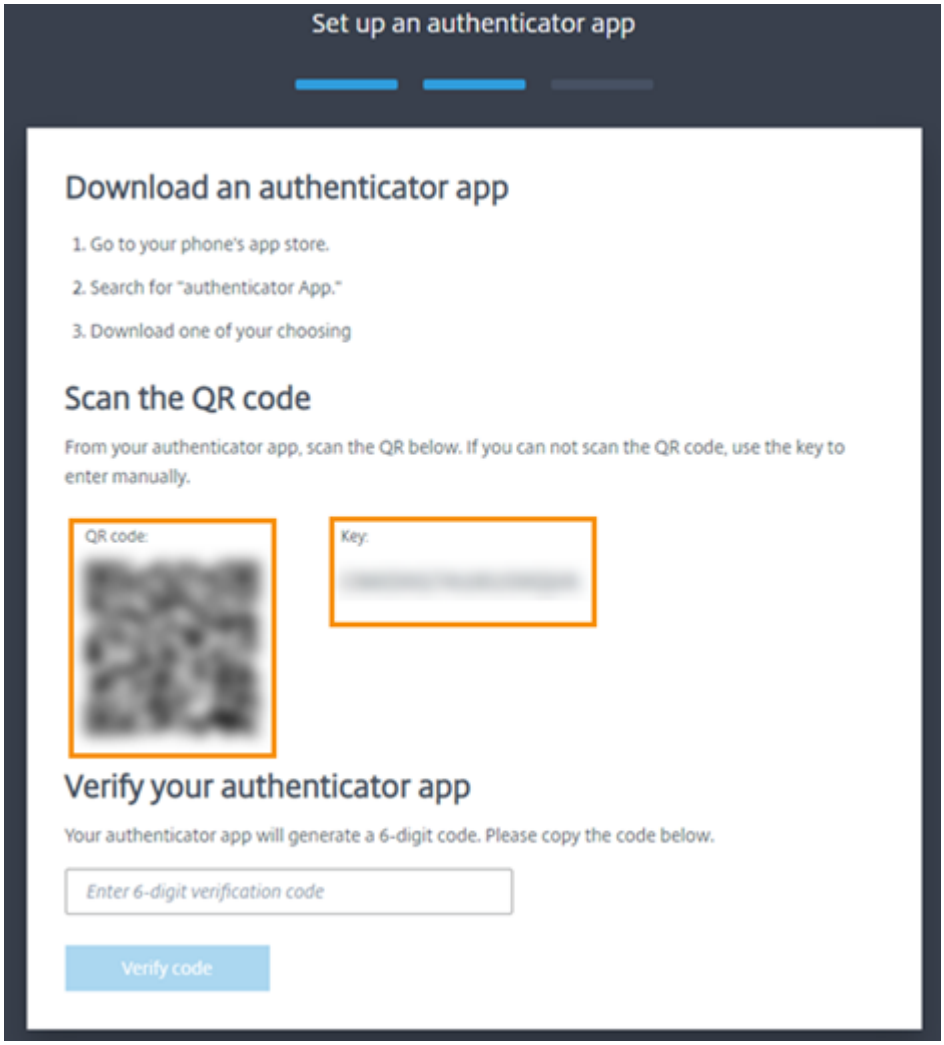


3. After you receive the email, enter the 6-digit verification code and your Citrix Cloud Japan password and select **Verify**.



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

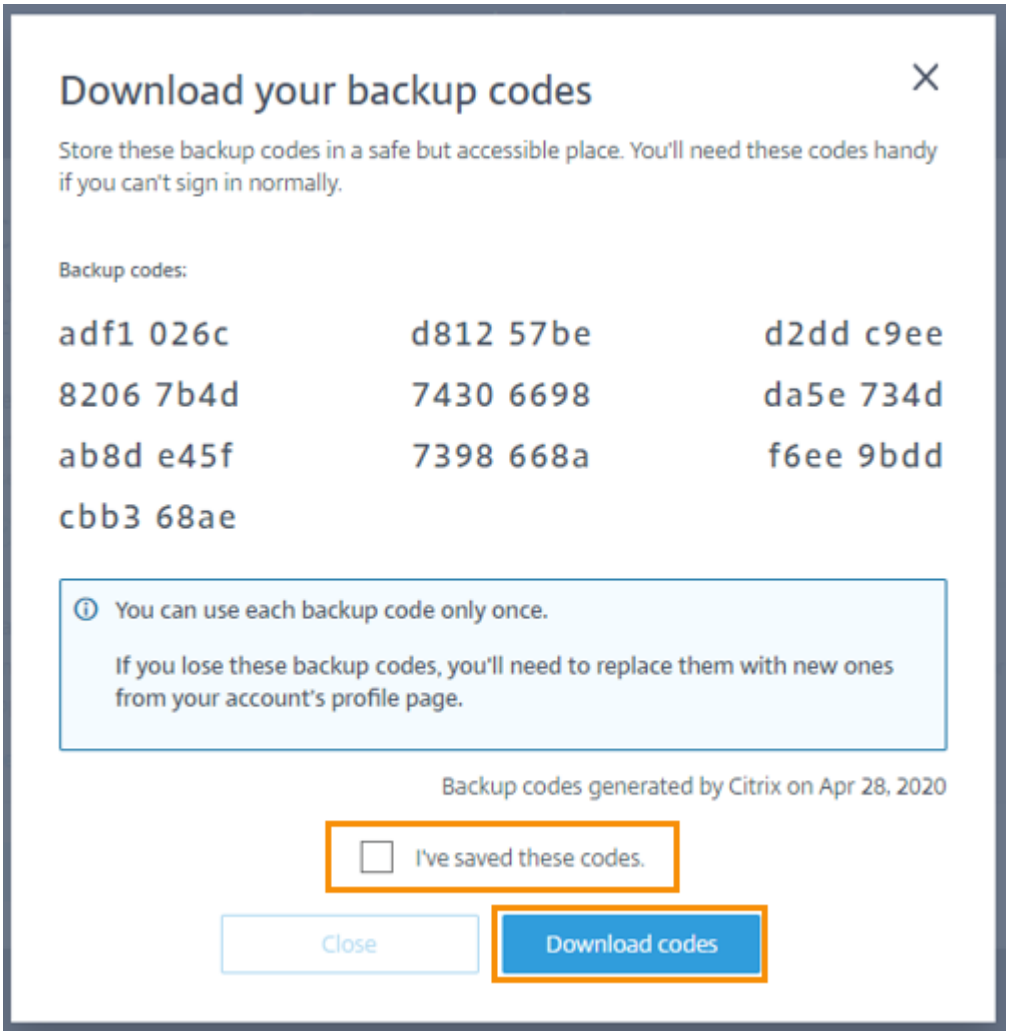
© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. Under **Verify your authenticator app**, enter the code from your authenticator app and select **Verify code**.
6. Configure the following account recovery methods in the event you lose your device or can't use your authenticator app:

    - Recovery phone (required): Select **Add a recovery phone** and enter a phone number that a Citrix Support representative can use to call you and verify your identity. Citrix Support uses this phone number only when you request help to sign in. Citrix recommmends using a landline phone number.
    - Backup codes (required): Select **Generate backup codes** to create a set of one-time use backup codes to help you sign in if you can't use your authenticator app. When prompted, select **Download codes** to download your backup codes as a text file. Then, select **I've saved these codes** and select **Close**.

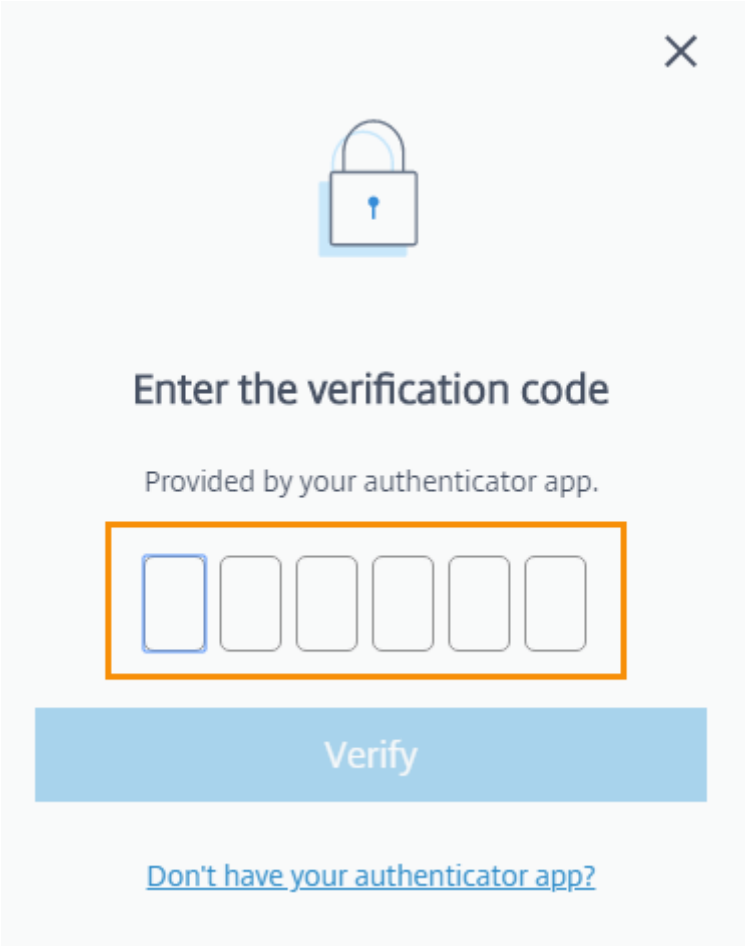
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

The next time you sign in with your Citrix Cloud Japan administrator credentials, Citrix Cloud Japan prompts you for the verification code from your authenticator app.

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



Manage your device enrollment

If you need to register a different device, generate more backup codes, or update your recovery phone number later, you can perform these tasks from your My Profile page. For instructions, see the following articles:

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

Purchase Citrix Cloud Japan

To purchase Citrix Cloud Japan for your organization, contact a Citrix sales representative. After you complete the order, you receive a confirmation email with a link to set up your account. In setting up your account, you will create the first account administrator using the email address from your order and a password you specify.

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

Review your order

Click the link in your order confirmation email. A Citrix Cloud Japan setup page displays in a browser window, showing your order details. Click **Continue**.

Create a password

Enter and confirm the strong password you want to use with your Citrix Cloud Japan account and then click **Continue**. As the first administrator of the account, you will use this password with the email address on your order to sign in to Citrix Cloud Japan.

Sign in with your Citrix Cloud Japan credentials

1. Sign in to Citrix Cloud Japan at https://citrix.citrixcloud.jp using the email address you used on your order and the password you chose earlier. Citrix Cloud Japan displays your home region. Currently, Citrix Cloud Japan includes only one geographical region, so only this region appears.
2. Agree to the Terms of Service and then click **Continue**. The Citrix Cloud Japan management console appears.

Service trials for Citrix Cloud Japan

September 6, 2025

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

To customize your experience and deliver the services that matter most to your users, trial access is managed on a per-service basis.

When you're ready to buy services, you'll convert your trial to a production account, so there's no need to reconfigure anything or create a separate production account.

Fast facts about service trials

	Citrix Cloud Japan Trial
Number of subscribers allowed	25

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

		Citrix Cloud Japan Trial
	Maximum Length	60 calendar days. You can request a trial for the service only once.
	Availability	Restricted availability
	Resource location	Customer provided and configured
	User session length	Unlimited
	Local Microsoft Active Directory integration	Yes
	Choice of resource locations	Yes
	Deploy to on-premises	Yes
	Citrix DaaS™	Full feature set
	Customizable	Yes

Request a service trial

To request a service trial, you'll need to speak to a Citrix® sales representative and provide your Organization ID (OrgID). The sales representative will ensure you have all the information you need to start using the service.

To request a trial and locate your OrgID, use the following steps:

1. Sign in to your Citrix Cloud Japan account.
2. Under **Available Services**, locate the service you want to try out and click **Request Trial**.
3. Note the OrgID displayed on the notification that appears.
4. Click **Speak to a sales representative** to register your trial request.

When your trial is approved and ready to use, you'll receive an email notification. You have 60 days to complete the trial.

> **Note:**
>
> To ensure the best customer experience, Citrix reserves the right to limit trials to a certain number of participants at any given time.

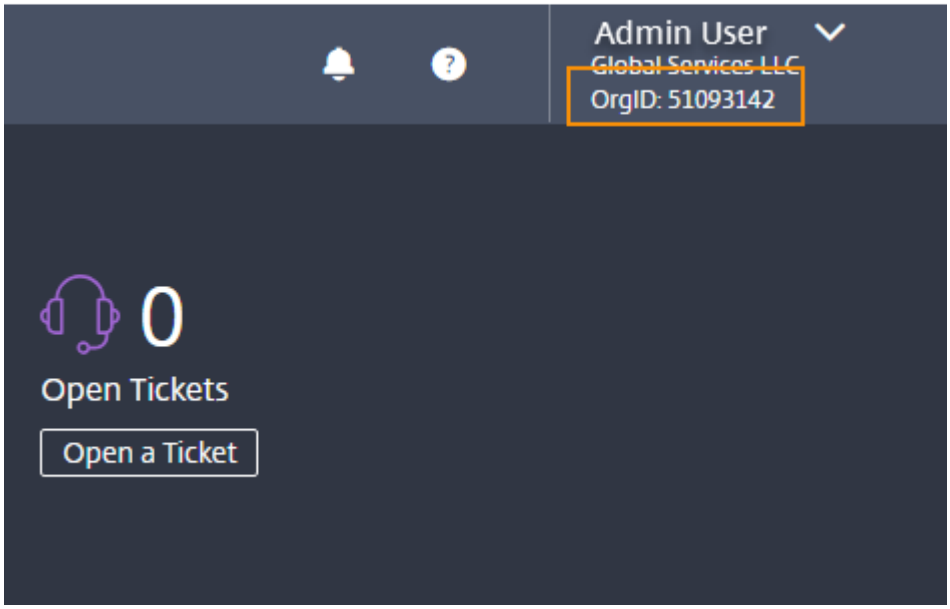
Purchase services

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

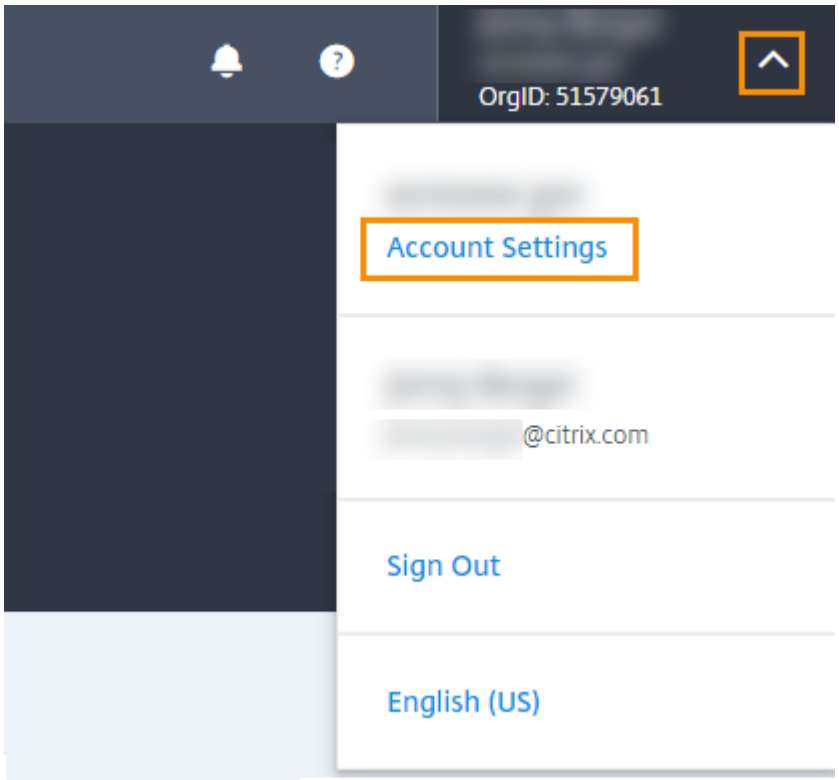
© 1997–2026 Citrix Systems, Inc. All rights reserved.

To complete the purchase, you'll need your OrgID, available in the Citrix Cloud Japan management console. Your OrgID appears in the following places:

- In the top-right corner of the management console, your OrgID is displayed beneath your account name.

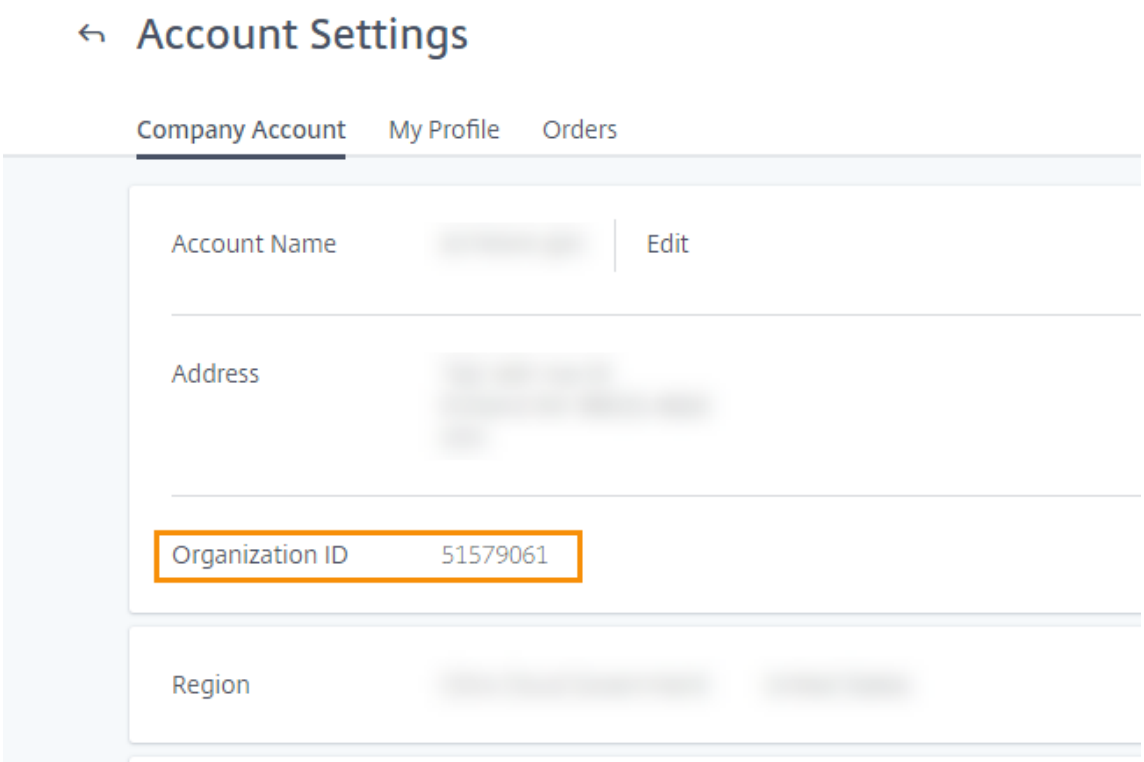


- From the top-right menu, click **Account Settings**.



Your OrgID is shown in the Organization ID field.

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



> **Important:**
>
> If you do not purchase before the end of your 60-day trial, the service is terminated and Citrix archives all data and settings for 90 days. If you purchase within the 90-day period, your trial is reactivated and converted to a production service.

System requirements

September 6, 2025

System requirements for components not covered here (such as Workspace app) are covered in their respective documentation.

For product components and features that you can install on Windows servers, Server Core installations are not supported, unless noted.

Specific recommendations for sizing VMs that deliver desktops and applications cannot be provided because of the complex and dynamic nature of hardware offerings. Every deployment has unique needs. Generally, sizing a VM is based on the hardware and not the user workloads (except for RAM; you need more RAM for applications that consume more). For guidance about VM sizing, refer to the following resources on the Citrix Tech Zone web site:

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

- Design Decision: The scalability and economics of delivering Citrix DaaS on Azure
- Sizing VDA Instances on Google Cloud Compute Engine
- Reference Architecture: Citrix DaaS - AWS
- Tech Brief: Local Host Cache / High Availability mode for Citrix Desktops-as-a-Service (DaaS)

Minimum system requirements

Citrix Cloud Japan requires the following components:

- An Active Directory domain
- Two physical or virtual machines, joined to your domain, with the Citrix Cloud Connector software installed. For more information, see Citrix Cloud Connector Technical Details
- Physical or virtual machines, joined to your domain, for hosting workloads and other components required for the services that you want to provide to your users.

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

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

Additional requirements

- Service connectivity: Connectivity requirements
- Citrix Cloud Connector: Citrix Cloud Connector requirements
- Citrix DaaS (formerly Virtual Apps and Desktops service): System requirements
- Workspace app: Requirements vary depending on the platform. For more information, see the Workspace app documentation.

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

Service connectivity requirements

April 10, 2026

Citrix Cloud Japan provides administrative functions (through a web browser) and operational requests (from other installed components) that connect to resources within a customer's deployment. This document defines the requirements and considerations for establishing connectivity between your resources and Citrix Cloud Japan.

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 Citrix Cloud Connector proxy and firewall configuration.

Management console

The Citrix Cloud Japan management console is a web-based console that you can access after signing in to https://citrix.citrixcloud.jp. 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 and firewall 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.

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, see Citrix Cloud Connector proxy and firewall 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/`

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

> **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 DaaS™ (formerly Virtual Apps and Desktops service)
- Citrix Workspace™

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 timeouts

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

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.

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 you use with Citrix Cloud Japan reside. The Cloud Connector connects to Citrix Cloud Japan, allowing it to operate and manage your resources as needed.

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

For requirements for installing the Cloud Connector, see Citrix Cloud Connector 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 cloud service with which it is being used.

Common service connectivity requirements

The following table lists the addresses that are common to most Citrix Cloud Japan services and their function. These addresses are provided only as domain names because Citrix Cloud Japan services are dynamic and their IP addresses are subject to routine changes.

Required address	Function
`https://*.citrixworkspacesapi.jp`	Provides access to Citrix Cloud APIs that the services use.
`https://*.citrixcloud.jp`	Provides access to the Citrix Cloud Japan 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.

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.

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 the following requirements:

- HTTP port 80 is open to *.digicert.com. This port is used during Cloud Connector installation and during periodic Certificate Revocation List checks.
- The following addresses must be contactable:
  - `http://*.digicert.com`
  - `https://*.digicert.com`
  - `https://dl.cacerts.digicert.com/DigiCertAssuredIDRootCA.crt`
  - `https://dl.cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA.crt`

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

For more information about these certificates, see Certificate validation requirements.

SSL Decryption

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

Citrix Gateway

- Common service connectivity requirements
- `https://*.*.nssvc.jp`

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

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

Citrix DaaS

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

Citrix resource location / Cloud Connector:

- Common service connectivity requirements
- `https://*.citrixworkspacesapi.jp`
- `https://*.citrixcloud.jp`
- `https://*.blob.core.windows.net`
- `https://*.citrixworkspacesapi.net`
- `https://*.servicebus.windows.net`
- For in-product messages including new features, critical communications, and customer surveys:
  - `https://citrix-cloud-content.customer.pendo.io/`
  - `https://citrix-cloud-data.customer.pendo.io/`

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

Administration console:

- `https://*.citrixworkspacesapi.jp`

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

- https://*.citrixcloud.jp
- https://*.blob.core.windows.net
- https://*.apps.citrixworkspacesapi.net

Citrix DaaS Remote PowerShell SDK

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

- https://*.citrixcloud.jp
- https://*.citrixworkspacesapi.net/[customerid]
- https://[customerid].xendesktop.net:443

Citrix Workspace

- https://*.citrixcloud.jp
- https://*.citrixdata.com
- For in-product messages including new features, critical communications, and customer surveys:
  - https://citrix-cloud-content.customer.pendo.io/
  - https://citrix-cloud-data.customer.pendo.io/

Workspace Environment Management™ service

- https://*.wem.citrixcloud.jp

Authentication

- accounts.citrixcloud.jp
- accounts-dsauthweb.citrixcloud.jp

Ensure that your identity provider URLs are also accessible from your end user devices.

Authentication graphical interface assets

- accounts-webassets.citrixcloud.jp

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

Citrix Cloud™ Connector requirements

September 6, 2025

The Citrix Cloud Connector comprises Windows services installed on Windows Server 2016, 2019, or 2022.

System requirements

The machines hosting the Cloud Connector must meet the following requirements. Citrix® strongly recommends installing at least two Cloud Connectors in each resource location to ensure high availability.

For best practices on configuring Cloud Connector machines for Citrix DaaS, 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

Microsoft .NET Framework 4.7.2 or later is required.

Server requirements

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

- Use dedicated machines for hosting the Cloud Connector. Do not install any other components on these machines.
- The machines are **not** configured as Active Directory domain controllers. Installing the Cloud Connector on a domain controller is not supported.
- The server clock is set to the correct UTC time.

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

- Internet Explorer Enhanced Security Configuration (IE ESC) is turned off. If Internet Explorer Enhanced Security Configuration is turned on, the Cloud Connector might not be able to establish connectivity with Citrix Cloud Japan.

Windows Update guidance

Citrix strongly recommends enabling Windows Update on all machines hosting the Citrix Cloud Connector. The Citrix 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 Citrix Cloud Connector isn't left in a pending update state for an extended period, thereby maintaining system stability.

The Citrix Cloud platform manages restarts to maintain availability, permitting only one Citrix 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 Citrix 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 Citrix Cloud Connector to reboot during business hours, we suggest that the customer schedule Windows Updates accordingly outside of business hours.
> - Each Citrix 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 Citrix 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 Citrix Cloud Connectors in the tenant.

Certificate validation requirements

Cloud Connector binaries and endpoints that the Cloud Connector contacts are protected by X.509 certificates issued by widely respected enterprise certificate authorities (CAs). Certificate verification in Public Key Infrastructure (PKI) includes the Certificate Revocation List (CRL). When a client receives a certificate, it verifies the CA's trustworthiness and checks if the certificate is listed on a Certificate Revocation List (CRL).

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

If the certificate is on a CRL, the certificate is revoked and should not be trusted, even though it appears valid.

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 X.509 certificates are verified during the Cloud Connector installation. Therefore, all Cloud Connector machines must trust these certificates to ensure successful installation of the Cloud Connector software.

Endpoints in Citrix Cloud Japan are secured by certificates issued by DigiCert or by one of the Root Certificate Authorities employed by Azure. For more information on the Root CAs used by Azure, see https://docs.microsoft.com/en-us/azure/security/fundamentals/tls-certificate-changes.

To validate the certificates, each Cloud Connector machine must meet the following requirements:

- HTTP port 80 is open to the following addresses. This port is used during Cloud Connector installation and during the periodic CRL checks. 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 on the DigiCert web site.
  - 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
- Communication with the following addresses is enabled:
  - https://*.digicert.com
- The following root certificates are installed:
  - 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

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

  - 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

- The following intermediate certificates are installed:
  - https://cacerts.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA384.crt

If any certificate is missing, the Cloud Connector installer downloads it from http://cacerts.digicert.com.

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

Active Directory requirements

- Joined to an Active Directory domain that contains the resources and users that you use to create offerings for your users.
- Each Active Directory forest that you plan to use with Citrix Cloud Japan should be reachable by two Cloud Connectors always.
- The Cloud Connector must be able to reach the parent domain controllers as well as the child domain controllers. This is essential for completing the Active Directory workflows in which the Cloud Connector is installed.

For more information, refer to the following Microsoft support articles:
- How to configure domains and trusts
- Systems services ports

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 Internet Connectivity Requirements.

Supported Active Directory functional levels

The Citrix Cloud Connector supports the following forest and domain functional levels in the Active Directory.

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

Forest Functional Level	Domain Functional Level	Supported Domain Controllers
Windows Server 2008 R2	Windows Server 2008 R2	Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2012	Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2008 R2	Windows Server 2016	Windows Server 2016
Windows Server 2012	Windows Server 2012	Windows Server 2012, Windows Server 2012 R2, Windows Server 2016
Windows Server 2012	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2012	Windows Server 2016	Windows Server 2016
Windows Server 2012 R2	Windows Server 2012 R2	Windows Server 2012 R2, Windows Server 2016
Windows Server 2012 R2	Windows Server 2016	Windows Server 2016
Windows Server 2016	Windows Server 2016	Windows Server 2016, Windows Server 2019, Windows Server 2022

Federal Information Processing Standard (FIPS) support

The Cloud Connector currently supports the FIPS-validated cryptographic algorithms that are used on FIPS-enabled machines. Only the latest version of the Cloud Connector software available in Citrix Cloud Japan includes this support. If you have existing Cloud Connector machines in your environment (installed before November 2018) and you want to enable FIPS mode on these machines, perform the following actions:

1. Uninstall the Cloud Connector software on each machine in your resource location.
2. Enable FIPS mode on each machine.
3. Install the latest version of the Cloud Connector on each FIPS-enabled machine.

> **Important:**

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

> - Do not attempt to upgrade existing Cloud Connector installations to the latest version. Always uninstall the old Cloud Connector first and then install the newer one.
> - Do not enable FIPS mode on a machine hosting an older Cloud Connector version. Cloud Connectors older than Version 5.102 do not support FIPS mode. Enabling FIPS mode on a machine with an older Cloud Connector installed prevents Citrix Cloud Japan from performing regular maintenance updates for the Cloud Connector.

For instructions to download the latest version of the Cloud Connector, see Task 3: Install Cloud Connectors.

Allowed FQDNs for Cloud Connector

For a complete list of the fully qualified domain names (FQDNs) that the Cloud Connector accesses, refer to the JSON file at https://fqdnallowlistsa.blob.core.windows.net/fqdnallowlist-japan/allowlist.json. The list is organized by product, and for each group of FQDNs, there is an accompanying change log.

Some of these FQDNs are specific to a customer and include templated sections in angular brackets. These templated sections must be replaced with the actual values before use. For example, for <CUSTOMER_ID>.xendesktop.net, you replace <CUSTOMER_ID> with the actual customer ID for your Citrix Cloud account. You can find the customer ID at the top of the **API Access** tab in **Identity and Access Management**.

Installation requirements

- Download the Cloud Connector software only from Citrix Cloud Japan and install it on prepared machines. By default, the Cloud Connector installer attempts to connect with the control plane from which it is downloaded. So, if you attempt to install the software downloaded from a Citrix Cloud (citrix.cloud.com) account, the installer does not connect with Citrix Cloud Japan.
- Because the Cloud Connector software is downloaded, your browser must allow downloading executable files.

Considerations for cloned machines

Each machine hosting the Cloud Connector must have a unique SID and connector ID so that Citrix Cloud Japan can communicate with the machines in your resource location. Installing the Cloud Connector on a machine template (before cloning) is not supported. Cloning a machine with the Cloud Connector installed will result in the Cloud Connector services not running, rendering the machine unable to connect to Citrix Cloud Japan.

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

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.

Important usage considerations

- Keep all Cloud Connectors powered on always to ensure an always-on connection to Citrix Cloud Japan.
- Do not upgrade a previously installed Cloud Connector with a newer version. Instead, uninstall the old Cloud Connector and then install the new one.
- Citrix strongly recommends enabling Windows Update on all machines hosting the Cloud Connector.
- Citrix strongly recommends installing at least two Cloud Connectors in each resource location. In general, the number of Cloud Connectors you should install is N+1, where N is the capacity needed to support the infrastructure within your resource location and ensure that the connection between Citrix Cloud Japan and your resource location remains intact in the event any single Cloud Connector becomes unavailable.
- Each Active Directory forest that you plan to use with Citrix Cloud Japan should be reachable by two Cloud Connectors always.
- After installation, do not move the machine hosting the Cloud Connector into a different domain. If the machine requires joining a different domain, uninstall the Cloud Connector, then reinstall it after domain joining.

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.

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

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

Connector needs to perform an action requiring Local System permissions, it does so through a pre-defined 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, reboot, 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 Japan to facilitate management of resources associated with the Active Directory domain accounts in which it is installed.	Network Service
Citrix Cloud Services Agent Discovery	Enables Citrix Cloud Japan 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

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

Service Name	Description	Runs As
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® Cloud Gateway	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
Citrix Remote HCL Server	Proxies communications between the Delivery Controller™ and one or more Hypervisors.	Network Service
Citrix Session Manager Proxy	Manages anonymous pre-launched sessions, and uploads session count information to the cloud-based Session Manager service.	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 Secure Ticketing Authority Service	Provides secure ticketing authority for Citrix Cloud services	Network Service

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

Event messages and logs

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

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

Download Cloud Connector event messages. (ZIP file)

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 is "not in contact," the event logs provide some initial information.

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.

Plan and build your deployment

September 6, 2025

After you sign up for Citrix Cloud Japan, use the following sequence to set up your connection to Citrix Cloud Japan. Review the entire process beforehand so you know what to expect.

Set up a resource location

Resource locations contain infrastructure servers, such as Active Directory domains and Cloud Connectors, and the machines that deliver resources, like applications and desktops, to users. Setting up a resource location is required for using Citrix DaaS™ (formerly Virtual Apps and Desktops service).

For instructions, see Create a resource location.

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

The following video provides a demonstration of creating a resource location and adding Cloud Connectors:

This is an embedded video. Click the link to watch the video

Connect an identity provider

Identity providers are used to authenticate Citrix Cloud Japan administrators and workspace subscribers, and to provide access to user lists for assigning Library offerings to subscribers.

For more information about supported identity providers, see Identity and access management.

Set up Citrix DaaS

To get started with Citrix DaaS, complete the following tasks:

1. Request a service trial if you don't have a subscription. Service trials last for 60 days and have all the same functionality as the production service.
2. Review the system requirements for the customer-managed components in your Citrix DaaS deployment and prepare your machines accordingly.
3. Review the sequence of tasks in Plan and build a deployment in the Citrix DaaS documentation and follow the steps in each task.

Set up Citrix Workspace

Setting up a workspace for your end-users involves the following tasks:

1. Enable the Virtual Apps and Desktops service integration in Workspace Configuration.
2. Select the identity provider you connected earlier as the workspace authentication method.
3. Configure the workspace features that you want to provide to your end-users.

For more information about the features available in Citrix Workspace for Citrix Cloud Japan, see Set up workspaces.

Create a resource location

October 8, 2026

After you sign up for Citrix Cloud Japan, continue setting up your account by creating a resource location.

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

What is a resource location?

A resource location contains the compute and network resources required to deliver services to your users. The resources that your resource location contains depends on the services you want to deliver. For example, if you plan to deliver applications and desktops through Citrix DaaS™ (formerly Virtual Apps and Desktops service), your resource location might include the following components:

- An Active Directory domain to authenticate and authorize users who want to access applications and desktops.
- One or more Virtual Delivery Agents (VDAs) are required. They manage the connection between the machines hosting the applications and desktops that you want to deliver. They also handle the devices used to access those resources.
- A supported hypervisor or cloud service, like Citrix XenServer® 8, XenServer® 9 or Microsoft Azure, to provision the virtual machines that deliver applications and desktops.

Default resource locations

If you have no resource locations in your Citrix Cloud Japan account, and you install Cloud Connectors in your domain:

- Citrix Cloud Japan creates a resource location.
- This created resource location 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 Japan. 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.

Task 1: Prepare machines

1. Review Citrix Cloud Connector requirements for:
    - Requirements
    - Important considerations
    - Supported Active Directory functional levels
    - troubleshooting information.
2. Prepare machines that meet the configuration requirements.
3. Join the prepared machines to your domain.

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

Task 2: Verify connectivity

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.

1. Review Connectivity requirements for a list of contactable addresses for available services.
2. Ensure port 443 (HTTPS) is open for outbound connections.
3. Ensure that the necessary addresses are reachable to enable the operation and consumption of cloud services.
4. Review Citrix Cloud Connector proxy and firewall configuration for information about using the Cloud Connector with a web proxy.

Task 3: Install Cloud Connectors

> **Note:**
>
> Connector Appliance is not available for Citrix Cloud Japan.

During installation, the Cloud Connector requires access to the Cloud to

- Verify the user's identity to authorize the installation process
- Validate the installer's permissions
- Download and configure the services that the Cloud Connector provides.

The installation occurs with the privileges of the user who initiates the install.

1. From the Citrix Cloud Japan menu, select **Resource Locations**.
2. Click **Download** to download the Cloud Connector installer.
3. Double-click the installer. Citrix Cloud Japan performs an initial connectivity check and prompts you for your Citrix Cloud Japan administrator user name and password.
4. Follow the wizard to install and configure the Cloud Connector. When the installation finishes, Citrix Cloud Japan performs a final connectivity check to verify that the Cloud Connector can communicate with Citrix Cloud Japan.

After installation, Citrix Cloud Japan registers your domain in **Identity and Access Management**.

> **Notes:**
>
> - If you're an administrator for multiple organization accounts, Citrix Cloud Japan prompts you to select the account you want to associate with the Cloud Connector.
> - If your organization account has multiple resource locations already, Citrix Cloud Japan prompts you to select the resource location you want to associate with the Cloud Connector.

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

> - It's not recommended to use the same Cloud Connector installer for multiple installations over an extended period. Download a new Cloud Connector from the Resource Locations page in the Citrix Cloud console.

Create additional resource locations

1. From the Citrix Cloud Japan management console, click the menu button and select **Resource Locations**.
2. Click **Resource Location** and enter a friendly name.
3. Click **Save**. Citrix Cloud Japan 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.

Cloud Connector installation logs

Cloud Connector installation logs are present at **%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup**.

All logs are added to **%ProgramData%\Citrix\WorkspaceCloud\InstallLogs** after installation.

Install Cloud Connectors from the command line

September 28, 2026

You can install the Citrix Cloud Connector™ software interactively or use silent or automated installation.

During installation, the Cloud Connector needs cloud access to authenticate the user, validate permissions, download, and configure services. The installation occurs with the privileges of the user who initiates it.

> **Important:**
>
> Avoid using the same installer for repeated installations over time. Instead, obtain a new Cloud Connector from the Resource Locations page in the Citrix Cloud Japan console.

Requirements

To use the command-line installation with Citrix Cloud Japan, you need to supply the following information:

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

- The customer ID of the Citrix Cloud Japan 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 client ID and secret of the secure API client you want to use to install the Cloud Connector. To acquire these values, you must first create a service principal. The client ID and secret ensures that your access to the Citrix Cloud API is secured appropriately. When creating a service principal, it operates with the same administrator permissions you possess. To install a Cloud Connector, use a service principal created by a Full Access administrator, which ensures full access permissions.
- 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 Japan uses the ID of the default resource location.

Create a service principal

When creating a service principal, Citrix Cloud Japan generates a unique client ID and secret. You must supply these values when you invoke the API through the command line.

1. From the Citrix Cloud Japan menu, select **Identity and access management** and then select **API Access**.
2. From the **service principals** tab, enter a name for your client and select **Create Client**. Citrix Cloud Japan generates and displays a client ID and secret for the service principal.
3. Select **Download** to download the client ID and secret as a CSV file and store it in a secure location. Alternatively, select **Copy** to manually acquire each value. When finished, select **Close** to return to the console.

Supported parameters

For service principal security details, the installer requires a JSON configuration file. Delete this file after installation completion. Supported configuration file values include:

- **customerName** Required. The customer ID shown on the API Access page in the Citrix Cloud Japan console.
- **clientId** Required. The service principal ID, created by an administrator, is found on the API Access page.
- **clientSecret** Required. The service principal secret that can be downloaded after the service principal is created and it is found 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

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

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**.

A sample configuration file:

```
{

"customerName": "CustomerID",
"clientId": "ClientID",
"clientSecret": "ClientSecret",
"resourceLocationId": "ResourceLocationId"
"acceptTermsOfService": "true",
 }
```

A sample command line that installs using the parameter file:

```
CWCConnector.exe /q /ParametersFilePath:c:\cwcconnector_install_params.
   json
```

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.

Troubleshooting

Installation Logs

Installation logs are available at **%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup**.

Also, logs are added to **%ProgramData%\Citrix\WorkspaceCloud\InstallLogs** after installation.

Exit codes

- 1603 - An unexpected error occurred.
- 2 - A prerequisite check failed.
- 0 - Installation completed successfully.

Citrix Cloud Connector™ proxy and firewall configuration

September 6, 2025

Port 443 using HTTP traffic, egress only. For full connectivity details, see the following articles:

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

- Connectivity requirements
- Citrix Cloud Connector requirements

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

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

Excluding traffic using wildcards and FQDNs

When configuring a proxy server to exclude Cloud Connector traffic, use the allowed Cloud Connector FQDNs that are included in the allowlist.json file for Citrix Cloud Japan. Don't use wildcards to exclude this type of traffic.

The following command is an example of excluding traffic using an allowed FQDN for Citrix Cloud Connector:

```
netsh winhttp set proxy bypass-list agenthub-jp.citrixworkspacesapi.jp
```

For more information, see Allowed FQDNs for Cloud Connector

Using wildcard addresses to exclude Cloud Connector traffic isn't supported. If you configure the bypass list using wildcards, these addresses are ignored and you might still see Cloud Connector traffic.

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.

See Changing proxy server settings in Windows for details about configuring the proxy settings.

Services at Runtime

The runtime service operates in the context of a local service. It does not use the setting defined for the user as described above. You need to import the setting from the browser.

To configure the proxy settings for this, open a Command Prompt window and use **netsh** as follows:

```
netsh winhttp import proxy source =ie
```

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

After executing the command, restart the machine hosting the Cloud Connector so that the services start up with these proxy settings.

For complete details, see Netsh Commands for Windows Hypertext Transfer Protocol (WINHTTP).

> **Note:**
>
> Auto-detect or PAC scripts are not supported.

Connector Appliance for Cloud Services

October 8, 2026

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

The Connector Appliance provides the following 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. For more information, see Active Directory with Connector Appliance.

However, there might be other services in preview that also depend on the Connector Appliance like:

- Image Portability Service
- Citrix Secure Private Access™

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)

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

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 both the **Resource Locations** and the **Connectors** page.

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 during a specific maintenance window.

As part of the update, the Connector Appliance becomes temporarily unavailable. Updates are applied to only one Connector Appliance in a resource location 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

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

Service	Port	Supported Domain Protocol	Configuration details
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:**
>
> You must include `https://` at the start of the IP address.

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 during Connector Appliance registration, 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://*.citrixcloud.jp`
- `https://*.citrixworkspacesapi.jp`
- `https://*.citrixnetworkapi.jp`
- `https://*.nssvc.jp`
    - Customers who can't enable all subdomains can use the following addresses instead:

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

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

- Citrix Hypervisor 8.2 CU1 LTSR
- VMware ESXi version 7 update 2
- Hyper-V on Windows Server 2016, Windows Server 2019, or Windows Server 2022.
- Nutanix AHV
- Microsoft Azure
- AWS
- Google Cloud Platform

Your hypervisor must provide the following minimum capabilities:

- 20 GB root disk
- 2 vCPUs
- 4 GB memory
- An IPv4 network

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

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.

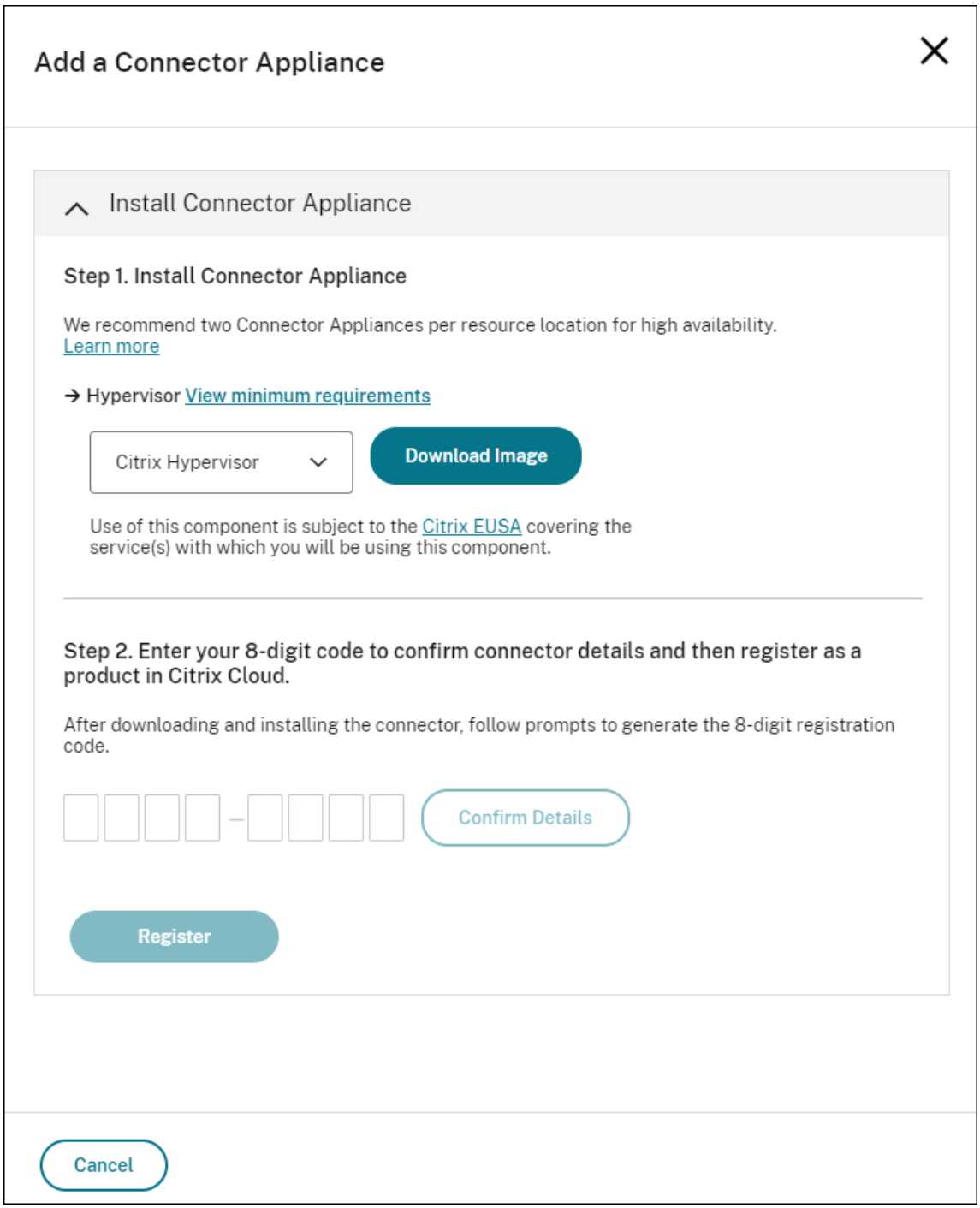
Obtain the Connector Appliance

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**.
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.

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



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 Appliance within Citrix Cloud:

     a) Click **Download Image**.

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

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

- Citrix Hypervisor™
- VMware ESXi
- Hyper-V
- Nutanix AHV
- Microsoft Azure
- Google Cloud Platform
- AWS

Citrix Hypervisor

This section describes how to import the Connector Appliance to a Citrix Hypervisor server by using XenCenter.

1. Connect to your Citrix Hypervisor server 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**.
4. Select the Citrix Hypervisor server where you want to host the Connector Appliance. Alternatively, you can select the pool to host the Connector Appliance in and Citrix Hypervisor chooses a suitable available server. Click **Next**.
5. Specify the storage repository to use for your Connector Appliance. Click **Import**.

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

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**.

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

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

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**.
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**.

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

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**.
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.

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

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.
    - 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.

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

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.

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.

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

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:

- 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.

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

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**:

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:

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

- 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.
- 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.

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

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**

   Click **Launch instance**.
7. After the instance is created, in the **Success** section, click the instance ID link to view your Connector Appliance instance.

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

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.)

   a) In the top navigation bar, select **Services** > **S3** > **Create bucket**.

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

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**.

Click **Create**.

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

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.
- You have S3 permissions and API access.

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

- 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.

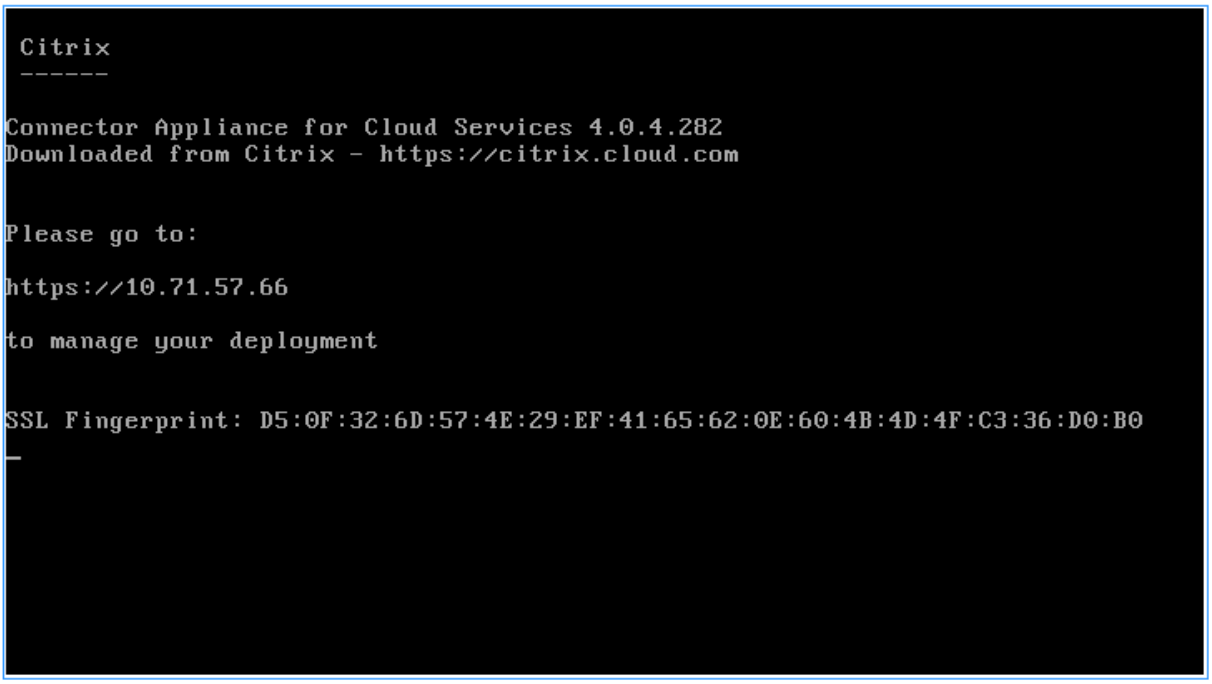
Next step: Register your Connector Appliance with Citrix Cloud.

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.

This section describes registering the Connector Appliance using the eight-digit code from the Key Registration Service (KRS).

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. Enter the Connector Appliance IP Address in this format: `https://xx.xx.xx.xx/?deployment=productionjp`
   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:

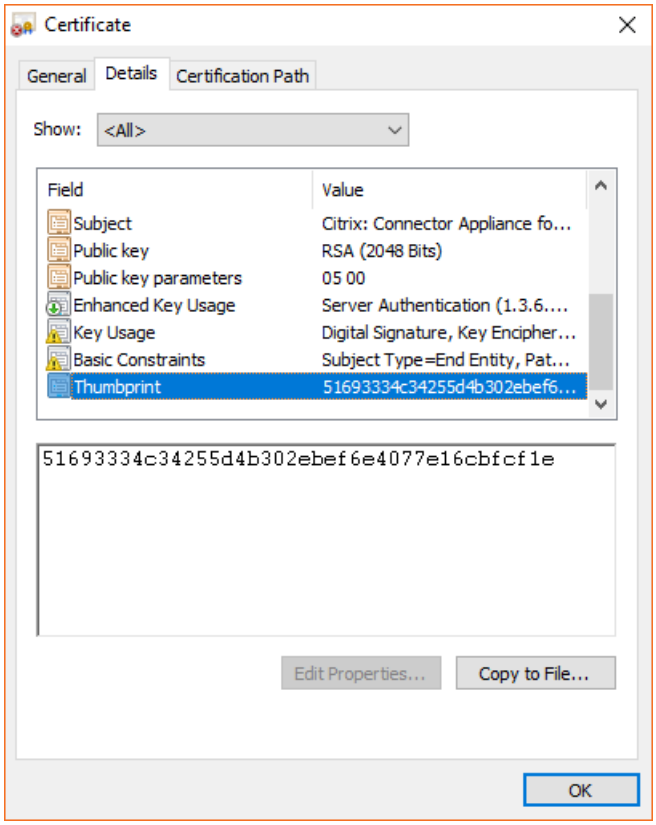
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



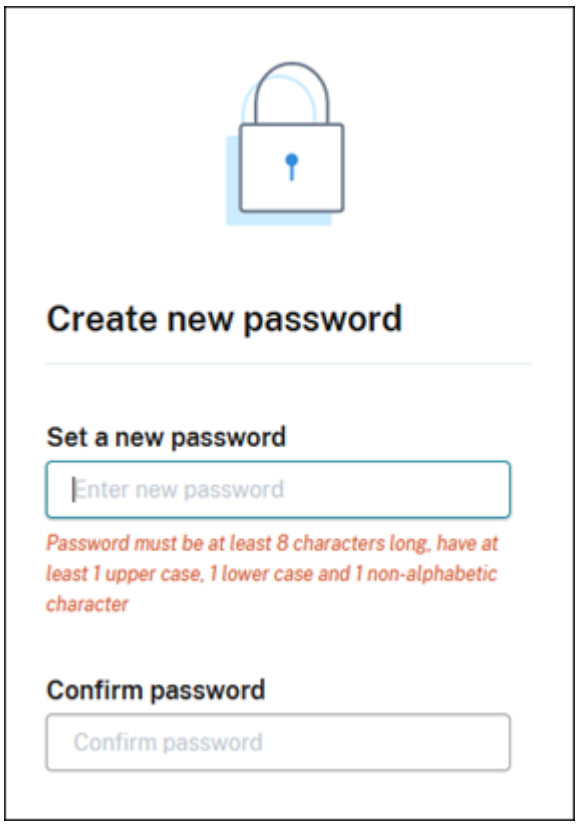
You can replace this self-signed certificate with one of your own that is signed by your organization or generated by using your organization's chain of trust. For more information, see Managing certificates.

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.



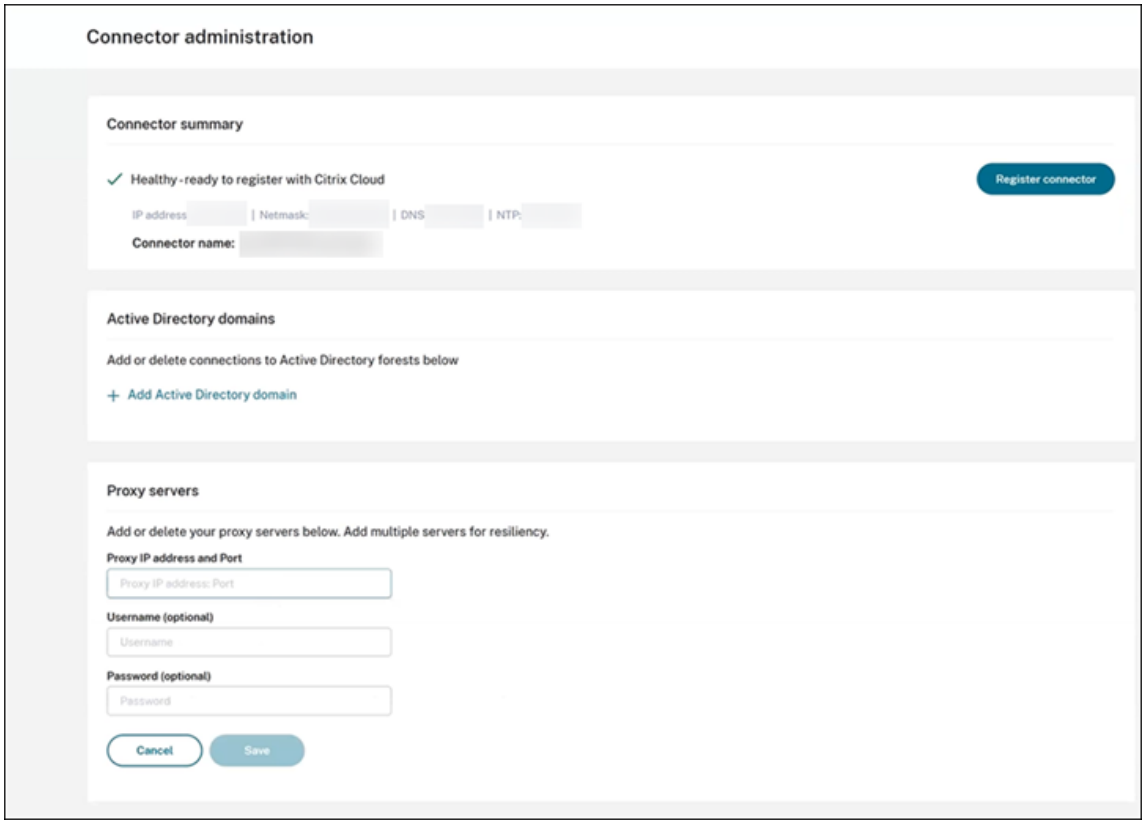
The password you set must meet the following requirements:

- 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.

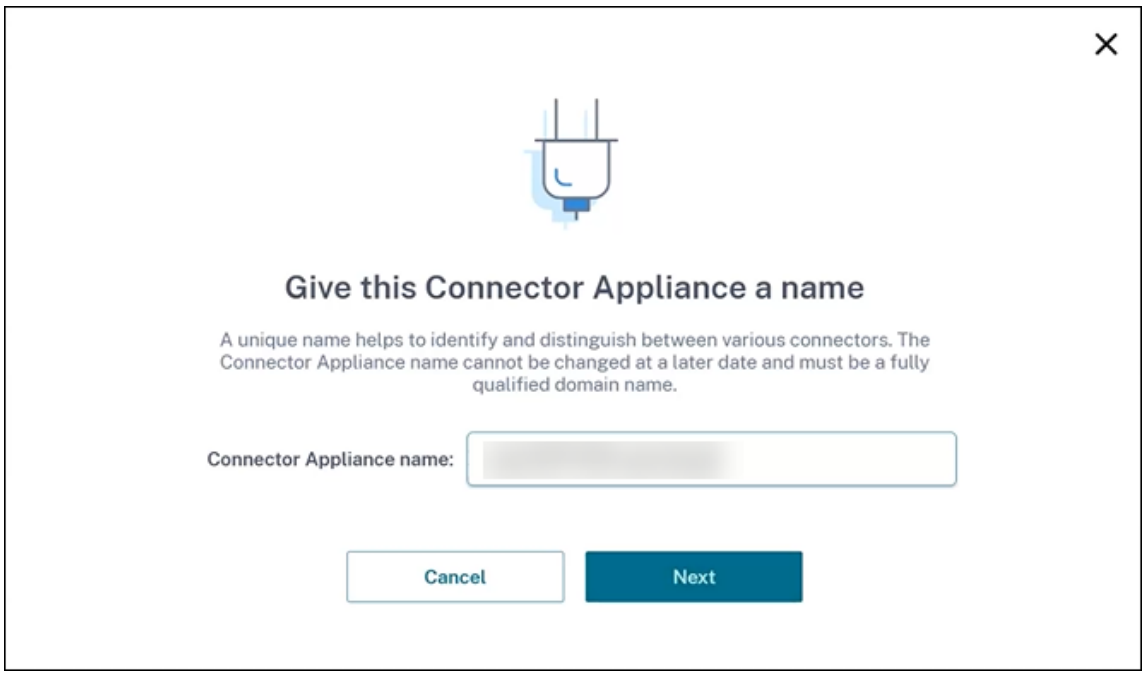
d) Select **Add Certificate**.

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**.



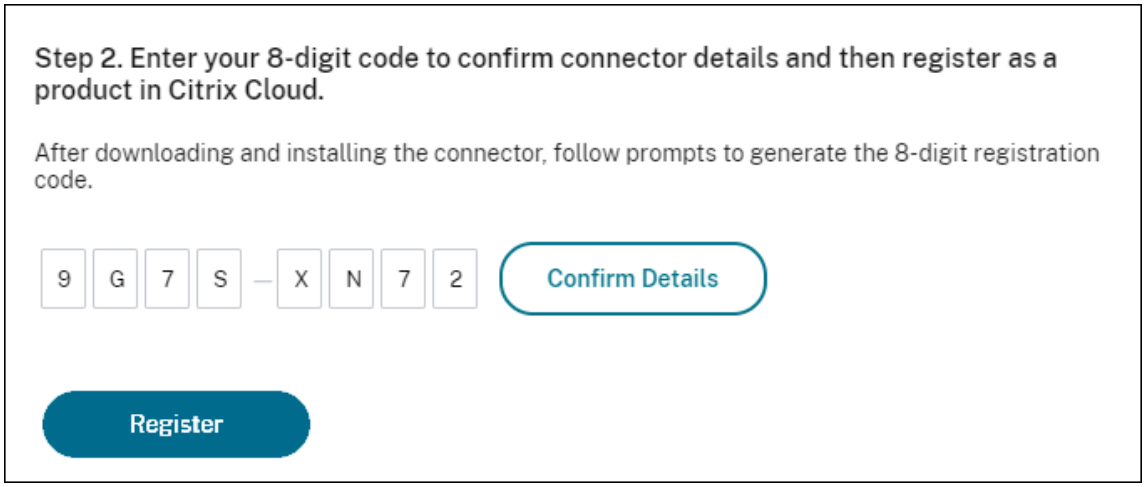
   The webpage provides a code to use to register with Citrix Cloud. This code expires in 15 minutes.

© 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.

You can also register the Connector Appliance using a secure client. For more information, see Registering your Connector Appliance unattended. For `deployment` enter `productionjp`.

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.

Do not clone, suspend, or take a snapshot of your Connector Appliance VMs. These actions are not supported.

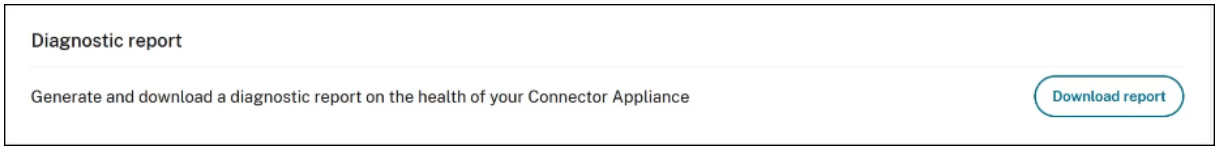
You are only presented with the **Create new password** page the first time that you connect to the Connector Appliance UI. Ensure that you store this password in a safe place for future use. This password cannot be reset. If you forget the password, you must reinstall the Connector Appliance. On subsequent connections to the UI, you are asked to input the password you set when registering the Connector Appliance.



© 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 94 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.

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 Virtual Apps and Desktops customers with some forests only are used for user authentication.

For more information, see Active Directory with Connector Appliance.

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**.
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**.

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

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:



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:

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

```
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.

Active Directory with Connector Appliance

September 28, 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 Virtual Apps and Desktops, customers with some forests only are 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.

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

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
- 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
End Point Mapper (DCE/RPC Locator Service)	135	TCP
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

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

Service	Port	Supported Domain Protocol
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.

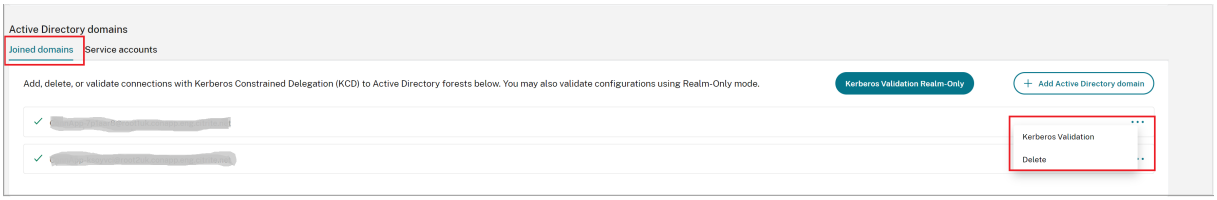
Forest Functional Level	Domain Functional Level	Supported Domain Controllers
Windows Server 2016	Windows Server 2016	Windows Server 2019

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.



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

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.

   The Connector Appliance checks the domain. If the check is successful, the **Join Active Directory** dialog opens. This new window allows you to input the user name and password to join the domain.

5. Click **Add**.
6. Provide the user name and password of an Active Directory user with join permission for the domain.
7. The Connector Appliance suggests a machine name. You can choose to override the suggested name and provide your own machine name that is up to 15 characters in length.

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

8. Click **Join**.

   The domain is now listed in the **Active Directory domains** section of the Connector Appliance UI.

9. To add more **Active Directory domains**, select **+ Add Active Directory domain** and repeat the preceding steps.
10. Go to the domains page in **Citrix Cloud Console** and select **Connector Appliance** to service your domains.
11. If you have not already registered your Connector Appliance, continue with the steps as described in Register your Connector Appliance with Citrix Cloud.

> **Note**
>
> If you encounter an error while attempting to join the domain, ensure that your environment meets the necessary Active Directory requirements and the network requirements.

© 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.

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.

Use the Connector Appliance to connect your resource location to the Active Directory forest in the following situations:

- You have one or more forests that are only used for user authentication
- 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 Workspace 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 Citrix Workspace™: Supported for all users
- User logons to an on-premises StoreFront™: 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.

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

- 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 Workspace: Supported for all users
- User logons to an on-premises StoreFront: Supported for all users

Set up workspaces

September 6, 2025

Citrix Workspace is a complete digital workspace solution that allows your end-users to get work done anywhere, at any time, on any device. Users sign in to Citrix Workspace, either through their web browser or through a Workspace app that's installed on their device. After signing in, users can access the applications and desktops that they're authorized to use.

Workspace features

- Enable single sign-on through the Citrix Federated Authentication Service.
- Create a sign-in policy for your end-users that describes the appropriate use of your organization's resources.
- Use network locations to ensure that your internal users can connect quickly to their workspace resources and that your internal users are routed to their workspace through Citrix Gateway.
- Allow your end-users to change their domain password when needed, without leaving Citrix Workspace.
- Use site aggregation to provide access to resources in your on-premises Virtual Apps and Desktops deployment through Citrix Workspace instead of StoreFront.
- Enable service continuity to ensure that your end-users can still access their workspace resources in the event of a cloud service outage.

More information

- Differences in Workspace for Citrix Cloud Japan: Feature availability for services
- Single sign-on: Enable single sign-on for workspaces with Citrix Federated Authentication Service
- Network locations: Optimize connectivity to workspaces with Direct Workload Connection
- Site aggregation: Aggregate on-premises virtual apps and desktops in workspaces
- Service continuity

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

- Changing domain passwords: Allow subscribers to change their account password
- Sign-in policies: Configure a sign-in policy

Configure workspaces

After setting up your Citrix DaaS deployment, configure your workspace by performing the following tasks:

1. Enable the service integration with Citrix Workspace. The service integration for Citrix DaaS might still retain the former name, Virtual Apps and Desktops. See Integrate services into workspaces in the Citrix Workspace documentation.
2. In **Workspace Configuration > Authentication** select the identity provider you configured earlier as your preferred workspace authentication method for your end-users.
3. Configure secure access to your workspace for remote end-users through an on-premises Citrix Gateway or the Citrix Gateway service.
4. Configure workspace features such as single sign-on and service continuity.

Customize your workspace

1. Customize the default theme of your workspace.
2. Customize the Workspace URL that your end-users will access.
3. Customize how favorite apps and desktops appear to end-users in their workspace.
4. Configure inactivity timeouts for end-users accessing their workspace from a web browser or through Workspace app.
5. Customize how your end-users launch the apps and desktops that you deliver through your Citrix DaaS deployment.

Identity and access management

June 30, 2026

Identity providers are used for the following purposes:

- Authenticate administrators when they sign in to Citrix Cloud Japan
- Provide access to user lists for assigning Library offerings to workspace subscribers
- Authenticate workspace subscribers when they sign in through Citrix Workspace™ app.

Citrix Cloud Japan supports the following identity providers. These identity providers can be used to authenticate Citrix Cloud administrators, workspace subscribers, or both.

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

Identity provider	Administrator authentication	Subscriber authentication
Citrix® identity provider (default)	Yes	No
On-premises Active Directory (AD)	No	Yes
Microsoft Entra ID	Yes	Yes
On-premises Citrix Gateway	No	Yes
Okta	No	Yes
SAML 2.0	Yes (AD groups only - preview)	Yes

Administrator authentication

By default, Citrix Cloud Japan uses the built-in Citrix identity provider to authenticate administrators when they sign in. Alternatively, you can connect your Microsoft Entra ID as an identity provider to authenticate Citrix Cloud Japan administrators. You can also use SAML 2.0 to authenticate administrator groups in your AD.

If you use your Microsoft Entra ID or SAML 2.0 for administrator authentication, administrators can sign in to Citrix Cloud Japan using a unique URL. To sign in, administrators enter the identifier for the Citrix Cloud Japan account.

> **Note:**
>
> If using Microsoft Entra ID for administrator authentication, Citrix recommends maintaining at least one full access account under the Citrix identity provider to ensure that:
>
> - You won't be locked out of your Citrix Cloud Japan account if Microsoft Entra ID is disconnected before setting up an alternative identity provider.
> - You can access your Citrix Cloud Japan account to perform certain operations that can't be completed when signed in as an administrator through Microsoft Entra ID. For instance, if Citrix updates the Microsoft Entra ID application connecting to your Microsoft Entra ID, ensure it's also updated in your Citrix Cloud Japan account. Only a full access administrator under the Citrix identity provider can perform this update.

Workspace authentication

Except for the Citrix identity provider, you can use all supported identity providers for authenticating workspace subscribers when they sign in through Citrix Workspace app.

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

Prerequisites for identity providers

Before linking with Citrix Cloud Japan, the installation of the Citrix Cloud Connector™ in your on-premises environment is necessary for the following supported identity providers:

- Active Directory
- On-premises Citrix Gateway
- Okta
- SAML 2.0

To learn more about the prerequisites for each supported identity provider, refer to the articles in More information in this article.

Application and desktop delivery to users

When using Citrix DaaS™, assign users and groups from your AD or Microsoft Entra ID to resources using one of the following methods.

- In Studio, create a delivery group comprising the desired applications and desktops, specifying the authorized users from your AD for access.
- In Studio, form a delivery group encompassing the desired applications and desktops for delivery, and present it as an offering in the Library. Then, use the Library to select the users from your AD or Microsoft Entra ID who are authorized to access the resources in the delivery group. This method requires connecting your AD or Microsoft Entra ID to Citrix Cloud Japan as an identity provider.

More information

For instructions for connecting identity providers to Citrix Cloud Japan, refer to the following articles:

- Connect Active Directory as an identity provider
- Connect Microsoft Entra ID as an identity provider
- Connect an on-premises Citrix Gateway as an identity provider
- Connect Okta as an identity provider
- Connect SAML as an identity provider

Connect Active Directory to Citrix Cloud Japan

September 28, 2026

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

By default, Citrix Cloud Japan uses the Citrix Identity provider to manage the identity information for all users in your Citrix Cloud Japan account. You can change this to use Active Directory (AD) instead.

Connecting your on-premises Active Directory to Citrix Cloud Japan involves installing Cloud Connectors in your domain. Citrix recommends installing two Cloud Connectors for high availability. For requirements and instructions, see Citrix Cloud Connector requirements.

To connect your Active Directory to Citrix Cloud Japan

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.
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.

Enable AD authentication for workspaces

After you connect your AD to Citrix Cloud Japan, you can allow your subscribers to authenticate to their workspaces through AD.

1. In Citrix Cloud Japan, click the menu button in the top-left corner and select **Workspace Configuration**.
2. From the **Authentication** tab, select **Active Directory**.
3. Click **Confirm** to accept the workspace experience changes that will occur when Microsoft Entra ID authentication is enabled.

Connect Microsoft Entra ID as an identity provider

September 28, 2026

By default, Citrix Cloud Japan uses the Citrix identity provider to manage the identity information for all users in your Citrix Cloud Japan account. You can change this to use Microsoft Entra ID to authenticate Citrix Cloud Japan administrators as well as workspace subscribers.

By using Microsoft Entra ID with Citrix Cloud Japan, you can:

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

- Use your own Active Directory so you can control auditing, password policies, and easily disable accounts when needed.
- Configure multi-factor 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 applications and permissions

Citrix Cloud Japan includes an Microsoft Entra ID app that allows Citrix Cloud Japan to connect with your Microsoft Entra ID without the need for you to be logged in to an active Microsoft Entra ID session. For more information about the Microsoft Entra ID applications and permissions that Citrix Cloud Japan uses to connect with your Microsoft Entra ID, see Microsoft Entra ID permissions for Citrix Cloud Japan.

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 Japan 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 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 Japan requires that administrators added from Microsoft Entra ID have different email addresses than administrators who sign in using a Citrix-hosted identity.

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

2. Install and configure Microsoft Entra ID Connect. For complete instructions, see Integrate your on-premises directories with Microsoft Entra ID on the Microsoft Azure web site.

Connect Citrix Cloud Japan to Microsoft Entra ID

When connecting your Citrix Cloud Japan account to your Microsoft Entra ID, Citrix Cloud Japan will need permission to access your user profile (or the profile of the signed-in user) as well as 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.

1. Sign in to Citrix Cloud Japan at https://citrix.citrixcloud.jp.
2. Click the menu button in the top-left corner of the page and select **Identity and access management**.
3. Locate **Microsoft Entra ID**, click the ellipsis button, and then select **Connect**.
4. 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 Japan.
5. When prompted, sign in to the Azure account with which you want to connect. Azure shows you the permissions that Citrix Cloud Japan needs to access the account and acquire the information required for connection.
6. Click **Accept** to accept the permissions request.

Add administrators to Citrix Cloud Japan from Microsoft Entra ID

1. From the Citrix Cloud Japan management console, from the **Identity and access management** page, click the **Administrators** tab.
2. Select **Add administrator/group**.
3. In **Administrator details**, select **Microsoft Entra ID**.
4. Type the name of the user you want to add and then click **Next**. Inviting Microsoft Entra ID guest users is not supported.
5. In **Set access**, configure the appropriate permissions for the administrator.
6. Review the administrator details. Select **Back** to make any changes.
7. Select **Send invitation**. Citrix Cloud Japan sends an invitation to the user you specified and adds the administrator to the list.

After clicking the email link, the user signs in to the company's Microsoft Entra ID. This verifies the user's email address and completes the connection between the Microsoft Entra ID user account and Citrix Cloud Japan.

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

Add Microsoft Entra ID administrator groups to Citrix Cloud Japan

You can add administrators to your Citrix Cloud Japan account using Microsoft Entra ID groups. You can then manage service access permissions for all administrators in the group.

This feature is supported for use only with **Citrix DaaS™** (formerly Virtual Apps and Desktops service). Administrators in the group don't have access to manage any other services in the Citrix Cloud Japan account.

For more information, see Manage administrator groups.

Sign in to Citrix Cloud Japan using Microsoft Entra ID

After the Microsoft Entra ID user accounts are connected, administrators can sign in to Citrix Cloud Japan 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.citrixcloud.jp/go/myorganization`
- From the Citrix Cloud Japan sign-in page, click **Sign in with my company credentials**, type the identifier you created when you initially connected Microsoft Entra ID, and click **Continue**.

Enable Microsoft Entra ID authentication for workspaces

After you connect Microsoft Entra ID to Citrix Cloud Japan, you can allow your subscribers to authenticate to their workspaces through Microsoft Entra ID.

> **Important:**
>
> Before enabling Microsoft Entra ID workspace authentication, review the Microsoft Entra ID section for considerations for using Microsoft Entra ID with Citrix Workspace.

1. From the Citrix Cloud Japan menu in the upper-left corner, select **Workspace Configuration**.
2. Select the **Authentication** tab and then select **Microsoft Entra ID**.
3. Click **Confirm** to accept the workspace experience changes that will occur when Microsoft Entra ID authentication is enabled.

Enable advanced Microsoft Entra ID capabilities

Microsoft Entra ID provides advanced multi-factor authentication, world-class security features, federation to 20 different identity providers, and self-service password change and reset, among many other features. Turning these features on for your Microsoft Entra ID users enables Citrix Cloud Japan to use those capabilities automatically.

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

Reconnect to Microsoft Entra ID for the updated app

In April 2022, the Microsoft Entra ID app used in Citrix Cloud Japan 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 Japan before April 2022 and you want to use the latest updated app, you need to disconnect your Microsoft Entra ID from Citrix Cloud Japan 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 a Global Admin in Microsoft Entra ID. When reconnecting your Microsoft Entra ID, you grant application-level permissions to Citrix Cloud Japan through the Global Admin role in Microsoft Entra ID. This allows Citrix Cloud Japan to reconnect to Microsoft Entra ID on your behalf. For more information, see Microsoft Entra ID Permissions for Citrix Cloud Japan.
- You must be an administrator with full access permissions under the default Citrix identity provider. If you are signed in to Citrix Cloud Japan 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 workspace subscribers, select a different identity provider temporarily. Citrix Cloud Japan doesn't allow you to disconnect your Microsoft Entra ID if it's also used as an authentication method for Citrix Workspace. For more information, see Choose or change authentication methods in the Citrix Workspace documentation.

To reconnect Microsoft Entra ID

1. Sign in to Citrix Cloud Japan as an administrator with full access permissions under the Citrix identity provider.
2. From the Citrix Cloud Japan 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**.
5. When prompted, sign in to your Azure account using your Global Admin credentials. Azure shows you the permissions that Citrix Cloud Japan needs to access the account and acquire the information required for the connection.

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

6. Select **Accept** to accept the permissions request.

Microsoft Entra ID Permissions for Citrix Cloud™ Japan

June 30, 2026

This article describes the permissions that Citrix Cloud Japan requests when connecting and using Microsoft Entra ID (AD). Depending on how Microsoft Entra ID is used with the Citrix Cloud Japan account, one or more enterprise applications might be created in the target Microsoft Entra ID tenant. You can connect multiple Citrix Cloud Japan 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 Japan 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 Japan. This action ensures your account is using the latest Microsoft Entra ID app in Citrix Cloud Japan. For more information, see Reconnect to Microsoft Entra ID for the updated app.
>
> 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 Japan uses when connecting and using Microsoft Entra ID and the purpose for which each application is used.

Name	Application ID	Usage
Citrix Cloud ProductionJP	f751768a-a91d-4306-af65-448ab59e2c85	Workspace subscriber login
CC-Directory-ProductionJP	6550e1c7-8970-46bc-82b6-ebd920ff255d	Default connection between Microsoft Entra ID and Citrix Cloud Japan
Athena ProductionJP	6464247d-8d40-42b9-a75e-4660db847454	Administrator invitations and logins

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

Permissions

The permissions in Citrix Cloud Japan's enterprise applications allow Citrix Cloud Japan to access certain data in your Microsoft Entra ID tenant. Citrix Cloud Japan uses these data to perform specific functions such as connecting to your Microsoft Entra ID tenant and enabling administrators to sign in to Citrix Cloud Japan using a dedicated sign-in URL. Citrix Cloud Japan can only access these data with your consent. These permissions represent the least amount of privilege that Citrix Cloud Japan 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:

- **API Name:** The resource applications from which Citrix Cloud Japan requests permissions. These applications are Microsoft Graph and Windows Microsoft Entra ID. Citrix Cloud Japan requests the same permissions from both of these resource applications.
- **Type:** The levels of access that Citrix Cloud Japan 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 Japan administrators to add users from the connected Microsoft Entra ID as administrators on the Citrix Cloud Japan account.
  - **User.ReadBasic.All:** Gathers basic info from the user's profile. This is a subset of `User.Read.All` but the permission itself remains for backwards compatibility.
  - **User.Read.All:** Citrix Cloud Japan 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 workspace. Citrix Cloud Japan can't use `User.ReadBasic.All` as Citrix Cloud Japan needs to access properties outside of the basic profile such as `onPremisesSecurityIdentifier`.
  - **GroupMember.Read.All:** Citrix Cloud Japan 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.

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

Workspace subscriber login

The Citrix Cloud ProductionJP application (ID: f751768a-a91d-4306-af65-448ab59e2c85) uses the same permissions for both the Microsoft Graph and the Windows Microsoft Entra ID resource applications.

API Name	Claim Value	Permission Name	Type
Microsoft Graph	User.Read	Sign in and read user profile	Delegated
Windows Microsoft Entra ID	User.Read	Sign in and read user profile	Delegated

Default connection between Microsoft Entra ID and Citrix Cloud Japan

The CC-Directory-ProductionJP application (ID: 6550e1c7-8970-46bc-82b6-ebd920ff255d) 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

The Athena ProductionJP application (ID: 6464247d-8d40-42b9-a75e-4660db847454) uses the following permissions:

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

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

Connect an on-premises Citrix Gateway as an identity provider

September 28, 2026

Citrix Cloud™ Japan supports using an on-premises Citrix Gateway as an identity provider to authenticate subscribers signing in to their workspaces.

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 Workspace.
- Use the Citrix Gateway authentication, authorization, and auditing (AAA) functions with Citrix Workspace.
- 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 Citrix Workspace.

> **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 Japan and enabling authentication for Citrix Workspace.

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

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

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:

- Meets the system requirements described in Cloud Connector 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 Service connectivity requirements.
- Citrix recommends two servers for Cloud Connector high availability. After installation, the Cloud Connectors allow Citrix Cloud Japan to locate and communicate with your Site.

For more information about installing the Cloud Connector, refer to the following articles:

- Install Cloud Connectors
- Install Cloud Connectors from the command line

Active Directory

Before enabling Citrix Gateway authentication, perform the following tasks:

- Verify that your workspace subscribers have user accounts in Active Directory (AD). Subscribers without AD accounts can't sign in to their workspaces successfully.
- Ensure that the user properties in your subscribers'AD accounts are populated. Citrix Cloud Japan requires these properties to establish the user context when subscribers sign in. If these properties aren't populated, subscribers can't sign in to their workspace. 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 Japan account. In this task, you install the Cloud Connector software on the servers you prepared, as described in the Cloud Connec-

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

tors section. The Cloud Connectors enable Citrix Cloud Japan to communicate with your on-premises environment. For instructions, see Connect Active Directory to Citrix Cloud Japan.

- If you are performing federation with Citrix Gateway authentication, synchronize your AD users to the federation provider. Citrix Cloud Japan requires the AD user attributes for your workspace subscribers so they can sign in successfully.

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 for Citrix Cloud Japan, 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 Japan. 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 subscribers to Citrix Workspace, the Gateway acts as an OpenID Connect provider. Messages between Citrix Cloud Japan 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 Japan 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, subscribers can't access their workspace 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 Japan assumes that tokens are stale when checking their validity.

Task overview

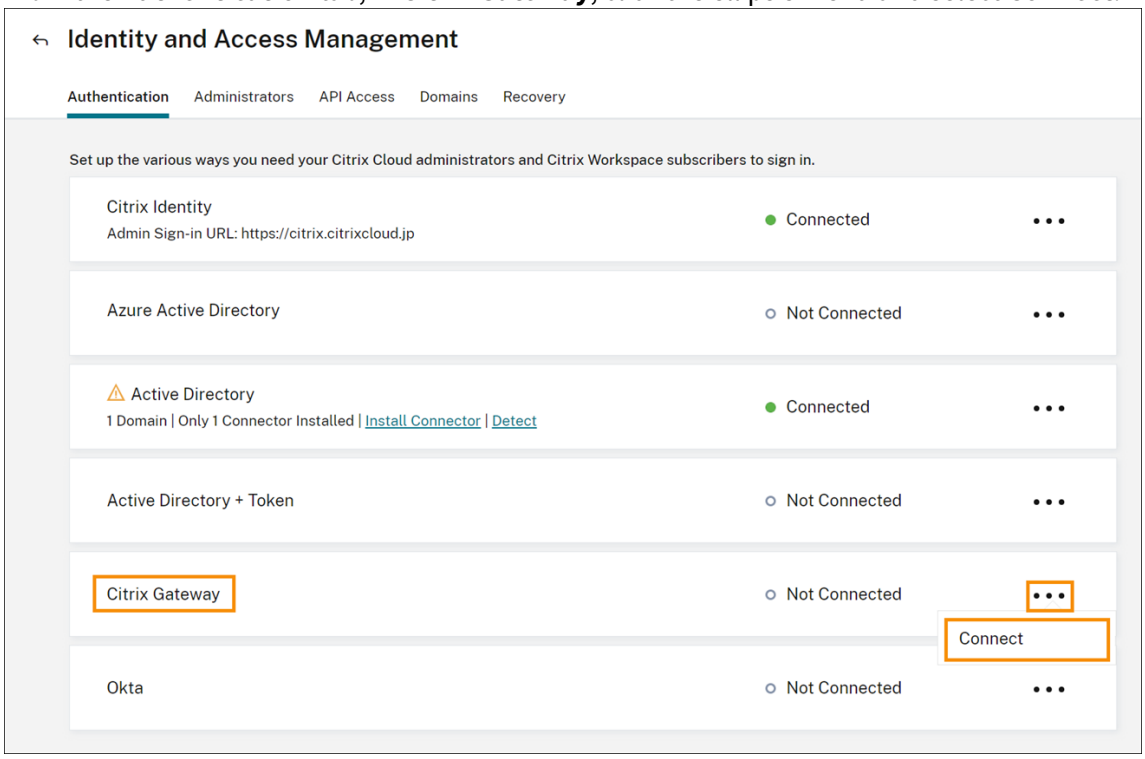
To set up Citrix Gateway authentication, you perform the following tasks:

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

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 Japan. This enables Citrix Cloud Japan 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
   - Citrix Gateway 13.0: Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud
3. In **Workspace Configuration**, enable Citrix Gateway authentication for subscribers.

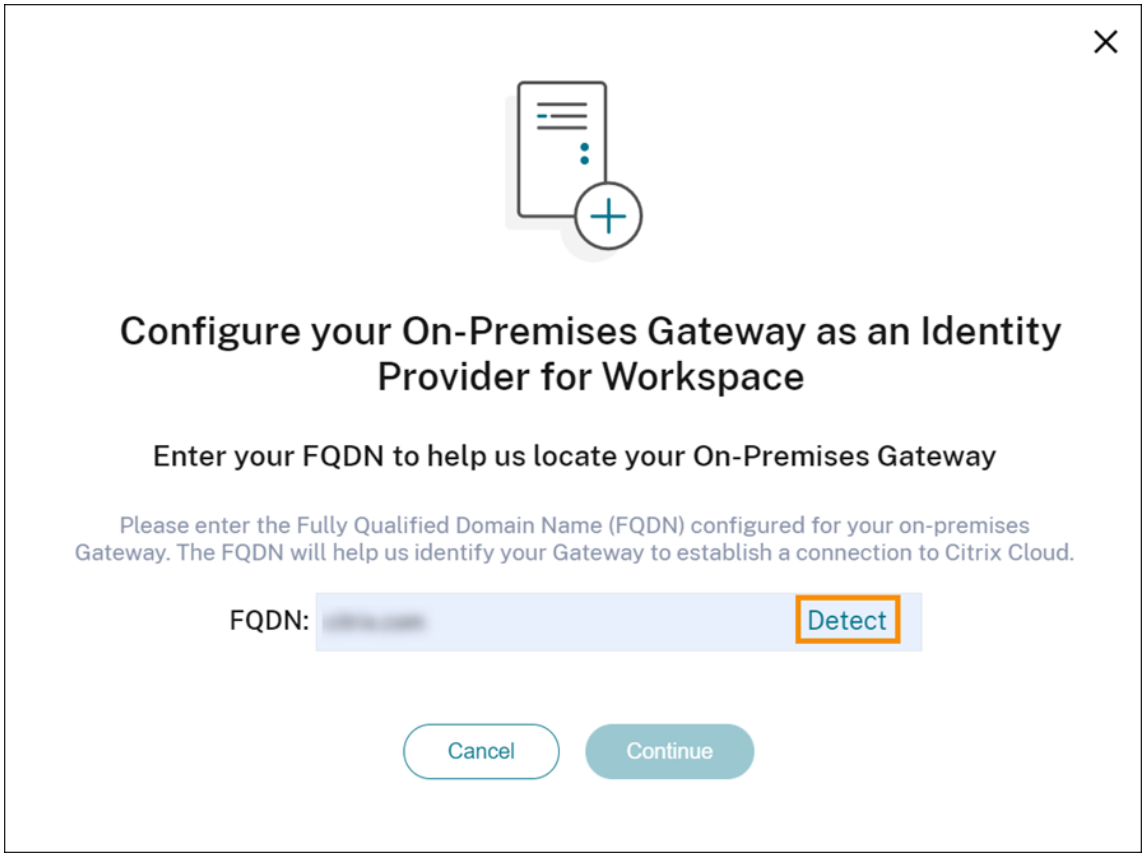
Configure Citrix Gateway authentication

1. From the Citrix Cloud Japan 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.

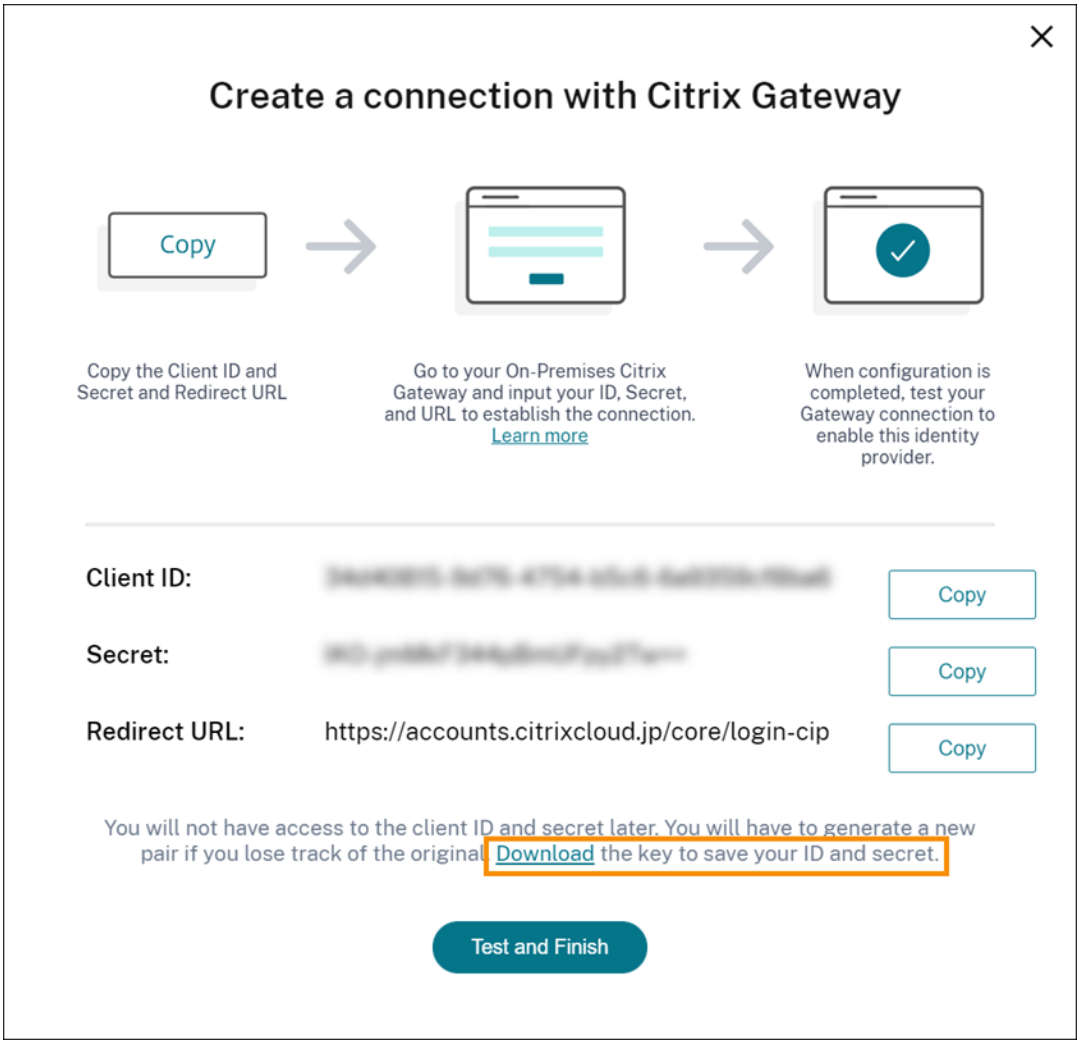


After Citrix Cloud Japan detects it successfully, click **Continue**.

4. Create a connection with your on-premises Gateway:

   a) Copy the Client ID, Secret, and Redirect URL that Citrix Cloud Japan 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 Japan 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 Japan. 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 Japan verifies that your Gateway is reachable and configured correctly.

Enable Citrix Gateway authentication for workspace subscribers

1. From the Citrix Cloud Japan menu, select **Workspace Configuration**.
2. From the **Authentication** tab, select **Citrix Gateway**.

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

3. Select **I understand the impact on subscriber experience** and then click **Save**.

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, workspace authentication with Citrix Gateway does not work.

If you experience an issue establishing a connection between Citrix Cloud Japan 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 Japan.
- You have entered the Gateway URL correctly in the `-issuer` parameter of the OAuth IdP policy (for example, `-issuer https://GatewayFQDN.com`). The `issuer` parameter is case sensitive.
- The client ID, secret, and redirect URL values from Citrix Cloud Japan 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 Japan. Instead, you must configure the individual ADs in the LDAP action. If you have multiple domains or forests, you can configure multiple LDAP policies.

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

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 subscriber sign-in, verify that AD lookup is configured. Gateway requires AD lookups to retrieve subscribers'AD 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**.

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

- 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:

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 for workspace subscribers, Gateway uses the last factor's password as the default password for single sign-on. This password is sent to Citrix Cloud Japan when subscribers sign in to their workspace. 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 Japan. Enable **SSOCredentials** on the login schema corresponding to the LDAP factor.

Connect Okta as an identity provider

September 28, 2026

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

Citrix Cloud™ Japan supports using Okta as an identity provider to authenticate subscribers signing in to their workspaces. By connecting your Okta organization to Citrix Cloud Japan, you can provide a common sign-in experience for your subscribers to access resources in Citrix Workspace.

After enabling Okta authentication in Workspace Configuration, subscribers have a different sign-in experience. Selecting Okta authentication provides federated sign-in, not single sign-on. Subscribers sign in to workspaces 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 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 Japan. For more information, see Enable single sign-on for workspaces with Citrix Federated Authentication Service.

Prerequisites

Cloud Connectors

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 Japan and your resource location. Citrix recommends two servers for Cloud Connector high availability. These servers must meet the following requirements:

- Meets the requirements described in Cloud Connector 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 workspace 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 Citrix Workspace.
- Connected to the Internet. For more information, see Service connectivity requirements.

For more information about installing the Cloud Connector, refer to the following articles:

- Install Cloud Connectors
- Install Cloud Connectors from the command line

Okta domain

When connecting Okta to Citrix Cloud Japan, you must supply the Okta domain for your organization. Citrix supports the following Okta domains:

- okta.com

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

- okta-eu.com
- oktapreview.com

You can also use Okta custom domains with Citrix Cloud Japan. 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 Japan. After you create and configure the application, note the Client ID and Client Secret. You supply these values to Citrix Cloud Japan 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

Workspace URL

When creating the Okta application, you must supply your Workspace URL from Citrix Cloud Japan. To locate the Workspace URL, select **Workspace Configuration** from the Citrix CloudJapan menu. The Workspace URL is shown on the **Access** tab.

> **Important:**
>
> If you modify the workspace URL later on, you must update the Okta application configuration with the new URL. Otherwise, your subscribers might experience issues with signing out of their workspace.

Okta API token

Using Okta as an identity provider with Citrix Cloud Japan 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.

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.

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

> **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 Japan to your Okta organization.

Sync accounts with 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 Workspace, 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
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**.

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

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 the following options:
   - Authorization Code (selected by default)
   - Implicit (Hybrid)
7. In **Sign-in redirect URIs**, enter `https://accounts.citrixcloud.jp/core/login-okta`.
8. In **Sign-out redirect URIs**, enter your Workspace URL from Citrix Cloud Japan.
9. 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.
10. Select **Save**. After you save the app integration, the console displays the application configuration page.
11. In the **Client Credentials** section, copy the **Client ID** and **Client Secret** values. You use these values when you connect Citrix Cloud Japan 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 Japan. Citrix Cloud Japan requires these settings to authenticate your subscribers through Okta when they sign in to their workspaces.

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, under **General Settings**, select **Edit**.
   b) In the **Application** section, under **Client acting on behalf of user**, clear the **Allow Access Token with implicit grant type**.
   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.
   c) Under **Attributes**, select **Add attribute**.
   d) Enter the following information:
      - Display Name: cip_email
      - Variable Name: cip_email
      - Description: AD User Security Identifier
      - Attribute Length: Greater than 1

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

- Attribute Required: Yes

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: Greater than 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: Greater than 1
- 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: Greater than 1
- Attribute Required: Yes

k) Select **Save**.

3. Edit attribute mappings for the application:

a) From the Okta console, select **Directory > Profile Editor**.

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 Profile** column, locate the attributes you created in Step 2 and map as follows:

- 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`.

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

- 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**.

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 Japan.

Connect Citrix Cloud Japan to your Okta organization

1. Sign in to Citrix Cloud Japan at https://citrix.citrixcloud.jp.
2. From the Citrix Cloud Japan menu in the upper-left corner of the management console, 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 Japan verifies your Okta details and tests the connection.

Enable Okta authentication for workspaces

1. From the Citrix Cloud Japan menu, select **Workspace Configuration > Authentication**.

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

2. Select **Okta**. If prompted, select **I understand the impact on the subscriber experience**.
3. Click **Accept** to accept the permissions request.

Connect SAML as an identity provider to Citrix Cloud Japan

September 28, 2026

Citrix Cloud Japan supports using SAML (Security Assertion Markup Language) as an identity provider to authenticate administrators (in preview) and subscribers signing in to their workspaces. You can use the SAML 2.0 provider of your choice with your on-premises Active Directory (AD).

For most SAML providers, use the information in this article to set up SAML authentication. To use SAML authentication with Microsoft Entra ID, you can opt for the Citrix Cloud Japan SAML SSO app in the Microsoft Entra ID app gallery. For more information about using the Citrix Cloud Japan SAML SSO app to set up SAML authentication in Citrix Cloud Japan, see Tutorial: Microsoft Entra ID single sign-on (SSO) integration with Citrix Cloud SAML SSO on the Microsoft Entra ID app documentation website.

Prerequisites

Using SAML authentication with Citrix Cloud Japan 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 that Citrix Cloud Japan 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 Citrix Cloud Connector 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.

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

- Joined to the domain where your resources reside. If users access resources in multiple domains, you must install at least two Cloud Connectors in each domain.
- Connected to a network that can contact the resources that subscribers access through Citrix Workspace.
- Connected to the Internet. For more information, see Connectivity requirements.

For more information about installing the Cloud Connector, see Task 3: Install Cloud Connectors.

Active Directory

Before configuring SAML authentication, perform the following tasks:

- Verify that your workspace subscribers have user accounts in Active Directory (AD). Subscribers without AD accounts are not allowed to sign in to their workspaces successfully when SAML authentication is configured.
- Ensure that the user properties in your subscribers'AD accounts are populated. Citrix Cloud Japan requires these properties to establish the user context when subscribers sign in to Citrix Workspace. If these properties aren't populated, subscribers can't sign in. These properties include:
  - Email address
  - Display name (optional)
  - Common name
  - SAM account name
  - User Principal Name
  - Object GUID
  - SID
- Establish a connection between your on-premises Active Directory (AD) and your Citrix Cloud Japan account by deploying Cloud Connectors.
- Synchronize your AD users to the SAML provider. Citrix Cloud Japan requires the AD user attributes for your workspace subscribers so they can sign in successfully.

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 Japan in the SAML assertion:

- SecurityIDentifier (SID)
- objectGUID (OID)
- userPrincipalName (UPN)

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

- Mail (email)

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.
2. If the custom attributes corresponding to the AD user attributes mentioned earlier are not available, generate the custom attributes and link them to Active Directory (AD). 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.

> **Note:**
>
> If you've already created custom attributes mapping to the listed AD user attributes, no further creation or mapping is required. Instead, use your existing custom attributes when you configure the metadata from your SAML provider in Citrix Cloud Japan.

For more information about integrating your AD with your SAML provider, consult your SAML provider's product documentation.

Administrator authentication with SAML 2.0

> **Note:**
>
> SAML authentication for Citrix Cloud Japan administrators is in technical preview. Citrix recommends using preview features only in non-production environments.

AD groups

You can add administrators to Citrix Cloud Japan using only AD groups. You can't add administrators individually if you're using SAML authentication.

Sign-in URL

When configuring SAML authentication, you configure a sign-in URL that administrators can use to sign in to Citrix Cloud Japan. This URL uses the format `https://citrix.citrixcloud.jp/go/myorganization`, where "myorganization"is the unique identifier you choose for your organization.

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

After you add AD groups, the administrators in the group can sign in to Citrix Cloud Japan immediately using the sign-in URL you specified. Citrix doesn't send any notifications to let administrators know that they have access to Citrix Cloud Japan.

Supported permissions

Only custom access permissions are supported. When you add an AD group, you must select the permissions that you want to grant to the administrators in the group. Full access permissions are not supported.

Task overview

To set up SAML authentication, you perform the following tasks:

1. In **Identity and access management**, connect your on-premises AD to Citrix Cloud Japan as described in Connect Active Directory to Citrix Cloud Japan.
2. Integrate your SAML provider with your on-premises AD as described in SAML integration with Active Directory in this article.
3. In **Identity and access management**, configure SAML authentication in Citrix Cloud Japan configure your SAML provider with Citrix Cloud Japan's metadata, and reciprocally configure Citrix Cloud Japan with your SAML provider's metadata to establish the SAML connection.
4. If you're using SAML to authenticate administrators:
    a) Configure the sign-in URL that administrators can use to sign in to Citrix Cloud Japan.
    b) Add administrators to Citrix Cloud Japan by specifying the AD groups that they belong to.
5. If you're using SAML to authenticate workspace subscribers, enable the SAML authentication method in **Workspace Configuration**. If you're using SAML only for authenticating Citrix Cloud administrators, you don't need to perform this task.

Create and map custom SAML attributes

If you've already configured custom attributes for SID, UPN, OID, and email attributes in your SAML provider, there's no need to complete this task. Proceed to Create a SAML connector application and use your existing custom SAML attributes in Step 8.

> **Note:**
>
> The steps in this section describe actions that you perform in your SAML provider's administration console. The specific commands that you use to perform these actions might vary from

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

> 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 details on the relevant commands specific to 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 the following attributes:
   - cip_sid
   - cip_upn
   - cip_oid
   - cip_email
3. Select the AD that you connected with Citrix Cloud Japan. 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**.
5. Select the option for adding attributes and map the following AD attributes to the custom user attributes you created in Step 2:
   - Select `objectSid` and map to the `cip_sid` attribute.
   - Select `userPrincipalName` and map to the `cip_upn` attribute.
   - Select `ObjectGUID` and map to the `cip_oid` attribute.
   - Select `mail` and map to the `cip_email` attribute.

Configure the administrator sign-in URL

1. Sign in to Citrix Cloud at https://citrix.citrixcloud.jp.
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

This task involves creating a connector application using the SAML metadata sourced from Citrix Cloud Japan. After you configure the SAML application, you use the SAML metadata from your connector application to configure the SAML connection to Citrix Cloud Japan.

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

> **Note:**
>
> Some steps in this section describe actions that you perform in your SAML provider's administration console. The specific commands that 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 details on the relevant commands specific to 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 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. In Citrix Cloud Japan's **Configure SAML** screen, select **Download** under **SAML Metadata**. The metadata XML file appears in another browser tab.

   > **Note:**
   >
   > If needed, you can also download this file from `https://saml.citrixcloud.jp/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.citrixcloud.jp`.
   - In the **Recipient** field, enter `https://saml.citrixcloud.jp/saml/acs`.
   - In the field for ACS URL validator, enter `https://saml.citrixcloud.jp/saml/acs`.
   - In the field for ACS URL, enter `https://saml.citrixcloud.jp/saml/acs`.
5. Add your custom SAML attributes as parameter values in the application:

Create this field	Assign this custom attribute
cip_sid	cip_sid or your existing SID attribute
cip_upn	cip_upn or your existing UPN attribute
cip_oid	cip_oid or your existing OID attribute
cip_email	cip_email or your existing email attribute

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

6. Add your Workspace subscribers as users to allow them to access the application.

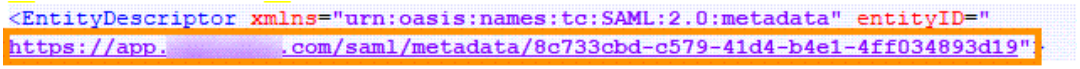
Add SAML provider metadata to Citrix Cloud Japan

1. Acquire the SAML metadata from your SAML provider. The following image is an example of what this file might look like:



2. In the **Configure SAML** screen in Citrix Cloud Japan, enter the following values from your SAML provider's metadata file:

   - In **Entity ID**, enter the **entityID** value from the **EntityDescriptor** element in the metadata.

   - In **Sign Authentication Request**, select **Yes** to allow Citrix Cloud Japan to sign authentication requests, certifying they came from Citrix Cloud Japan 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 **Single-**

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

SignOnService elements with Binding values of either **HTTP-POST** or **HTTP-Redirect**.



- In **Binding Mechanism**, select the mechanism that matches the binding for the SSO Service URL you chose from the metadata file.
- In **SAML Response**, select the signing method your SAML provider uses for the SAML Response and SAML Assertion. By default, Citrix Cloud Japan 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 PEM file.
4. In the **Configure SAML** screen in Citrix Cloud Japan, select **Upload File** and select the PEM 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 Japan 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**.
7. In **Logout URL**, locate the **SingleSignOnService** element with the HTTP-Redirect binding in your SAML provider's metadata file and enter the URL. If you choose to omit the Logout URL, Citrix Cloud Japan does not send a logoff request to the identity provider. Instead, Citrix Cloud Japan redirects to the Workspace URL. Citrix Cloud Japan doesn't support Single Log Out (SLO) or sending signed logout requests.
8. Verify the following default name attribute values in Citrix Cloud Japan match the corresponding attribute values in your SAML provider's administration console. If your SAML provider has different values, you can change these values in Citrix Cloud Japan to ensure they match your SAML provider.
   - **Attribute name for User Display Name**: `displayName`
   - **Attribute name for User Given Name**: `givenName`
   - **Attribute name for User Family Name**: `familyName`
9. In Citrix Cloud Japan, enter the custom SAML attributes from your SAML provider:
   - In **Attribute name for Security Identifier (SID)**, enter your custom SID attribute name. The default value is `cip_sid`.
   - In **Attribute name for User Principal Name (UPN)**, enter your custom UPN attribute name. The default value is `cip_upn`.

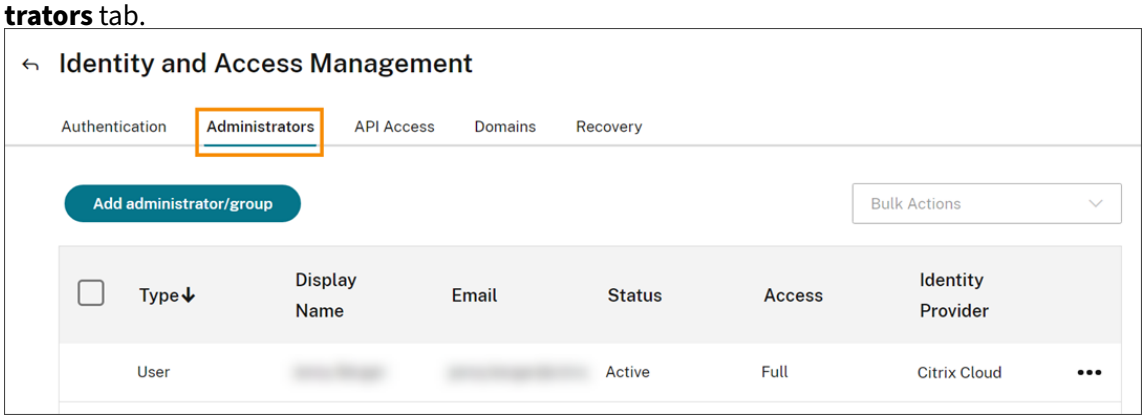
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- In **Attribute name for Email**, enter your custom Email attribute name. The default value is `cip_email`.
- In **Attribute name for AD Object Identifier (OID)**, enter your custom OID attribute name. The default value is `cip_oid`.

10. Select **Test and Finish** to verify you configured the connection successfully.

Add administrators to Citrix Cloud Japan from AD

1. In Citrix Cloud Japan, from the **Identity and Access Management** page, select the **Administrators** tab.



2. In **Administrator details**, select **Active Directory** and then select the domain you want to use.
3. In **Search for a group to add**, start typing the name of the group you want to add in the search box. When it appears, click the plus sign (+) to select the group.
4. Select **Next**.
5. Select the custom access permissions or roles that you want to assign to the group. Select **Next**.
6. Review the administrator details. Select **Back** to make any changes.
7. When you're finished, select **Save**.

Enable SAML authentication for workspaces

1. From the Citrix Cloud Japan menu, select **Workspace Configuration**.
2. Select the **Authentication** tab
3. Select **SAML 2.0**.

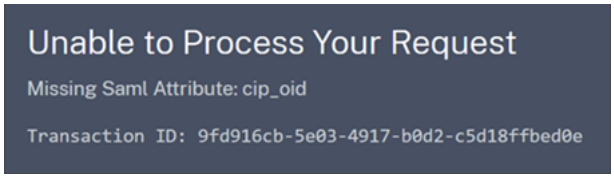
Troubleshooting

Attribute errors

Attribute errors might arise if the required attributes in your SAML configuration are not encoded correctly. When an attribute error occurs, Citrix Cloud Japan displays an error message that includes the

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

faulty attribute.



To resolve this type of error, ensure that these attributes are encoded as described in the following table.

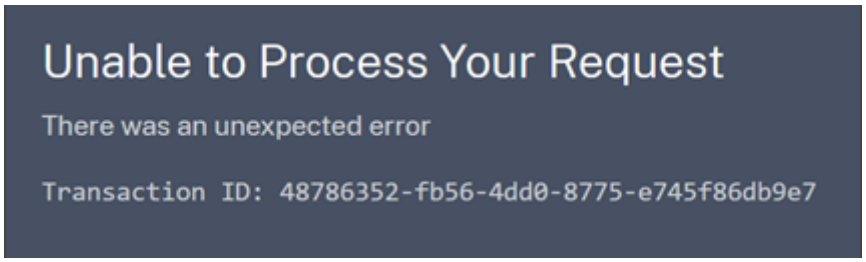
Attribute	Encoding
cip_email	Must be in String format (`user@domain`)
cip_oid	Must be in Base64 or String format
cip_sid	Must be in Base64 or String format
cip_upn	Must be String format (`user@domain`)

Unexpected errors

Citrix Cloud Japan might experience an unexpected error when:

- A user initiates a SAML request using an IDP-initiated flow. For example, rather than accessing the workspace URL directly, the request is initiated by selecting a tile within the identity provider's app portal. (`customer.citrixcloud.jp`).
- The SAML certificate is invalid or has expired.
- The authentication context is invalid.
- SAML assertion and response signature are mismatched.

When this error occurs, Citrix Cloud Japan displays a generic error message.



If this error results from navigating to Citrix Cloud Japan 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 workspace URL (for example, `https://customer.citrixcloud.jp`).

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

2. Assign users to both the SAML app and the bookmark app.
3. Change the visibility settings in the app portal to display the bookmark app while hiding the SAML app.
4. Disable the Prompt=Login parameter to remove additional password prompts.

License Activation Service

February 4, 2026

The License Activation Service (LAS) is a modern, cloud-based licensing solution for on-premises Citrix License Servers. Designed as a streamlined alternative to traditional Citrix legacy licensing, LAS introduces new modules for product activation, ensuring a seamless approach to license management.

Instead of manually managing license file lifecycles, you can connect your License Server to Citrix Cloud™ for Online activation. Once registered, the License Server communicates regularly with the LAS endpoint to ensure activations remain up to date and aligned with your entitlement expiry or contract end date.

For more information, see License Activation Service.

Manage Citrix Cloud Japan

September 6, 2025

Citrix Cloud Japan includes the following administrative features:

- Inviting administrators and delegating access to cloud services
- Assigning users to service offerings in the Library
- Monitoring service notifications
- View the system log of events that occurred in Citrix Cloud Japan

Administrators

Administrators use their identity to access Citrix Cloud Japan, 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 Japan.

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

Add new administrators

During the account onboarding process, an initial administrator is created. The administrator can then invite other administrators to join Citrix Cloud Japan. These new administrators can use their existing Citrix Cloud Japan account credentials or set up a new account if needed. You can also fine-tune the access permissions of the administrators you invite. This allows you to define access that's aligned with the administrator's role in your organization.

To invite other administrators and fine-tune their access to Citrix Cloud Japan, see Add administrators to a Citrix Cloud Japan account.

Change your password

If you want to change your password from within Citrix Cloud Japan, go to **Account Settings** and select **My Profile**. Click **Change Password** to enter your current password and confirm your new password.

Remove administrators

You can remove administrators from your Citrix Cloud Japan account on the Administrators tab. When you remove an administrator, they can no longer sign in to Citrix Cloud Japan. If an administrator is logged in when you remove the account, the administrator will stay active for a maximum of one minute. Afterward, access to Citrix Cloud Japan is denied.

> **Note:**
>
> - If there's only one administrator in the account, you can't remove that administrator. Citrix Cloud Japan requires at least one administrator for each customer account.
> - Cloud Connectors are not linked to administrator accounts. So, Cloud Connectors will continue operating even if you remove the administrator who installed it.

Subscribers

A subscriber's identity defines the services to which they have access in Citrix Cloud Japan. This identity comes from Active Directory domain accounts provided from the domains within the resource location. Assigning a subscriber to a Library offering authorizes the subscriber to access that offering.

> **Important:**
>
> If you are using an on-premises StoreFront with Citrix DaaS™ (formerly Virtual Apps and Desk-

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

> tops service), do not use Library to assign resources when creating delivery groups. Instead, use Studio to assign resources to users. If you use Library in this scenario, resources might not be enumerated to users.
>
> When creating a delivery group in Studio, on the Users page, do not select **Leave user management to Citrix Cloud**. Instead, select a different option (**Allow any authenticated users to use this delivery group** or **Restrict use of this delivery group to the following users**).

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 Cloud Connectors in each forest. Citrix® recommends at least two Cloud Connectors to maintain a high availability environment.

The process for assigning users to Library offerings is the same for Citrix Cloud Japan and Citrix Cloud (citrix.cloud.com). For instructions, see Assign users and groups to service offerings using Library.

> **Note:**
>
> - Disabling domains prevents new identities only from being selected. It does not prevent subscribers from using identities that are already allocated.
> - Each Cloud Connector can enumerate and use all the domains from the single forest in which it is installed.

Manage subscriber usage

You can add subscribers to offerings using individual accounts or Active Directory groups. Using Active Directory groups does not require management through Citrix Cloud Japan after you assign the group to an offering.

When an administrator removes an individual subscriber or group of subscribers from an offering, those subscribers can no longer access the service. For more information about removing subscribers from specific services, refer to the service's documentation on the Citrix Product Documentation web site.

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 Japan. 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 Japan.

The process for selecting a primary resource location is the same for Citrix Cloud Japan and Citrix Cloud (citrix.cloud.com). For more information, see Select a primary resource location.

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

Notifications

Notifications provide information about issues or events that might be of interest to administrators, such as new Citrix Cloud Japan features or problems with a machine in a resource location. Notifications can come from any service within Citrix Cloud Japan.

Managing notifications is the same in Citrix Cloud Japan and Citrix Cloud (citrix.cloud.com). For more information about notifications, see Notifications.

System Log

The system log displays a timestamped list of events that occurred in Citrix Cloud Japan. You can export these changes as a CSV file to meet your organizations's regulatory compliance requirements or to support security analysis.

System log functions are the same in Citrix Cloud Japan and Citrix Cloud (citrix.cloud.com), with some important limitations. For more information, see System Log.

Manage Citrix Cloud Japan administrators

September 28, 2026

Administrators are managed from the Citrix Cloud Japan console. Depending on the identity provider you use to authenticate administrators, you can add administrators individually or using groups.

By default, new administrators have Full Access permissions to all functions in the Citrix Cloud Japan account. See Configure administrator permissions in this article to learn how to delegate account administration.

Add new administrators

Citrix Cloud Japan 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 Microsoft Entra ID groups. Administrators in Microsoft Entra ID groups are limited to accessing Citrix DaaS only. For more information, see Manage administrator groups.
- SAML 2.0: Supports adding administrators through AD groups only. Administrators in AD groups are limited to managing Citrix DaaS only. For more information, see Connect SAML as an identity provider to Citrix Cloud Japan.

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

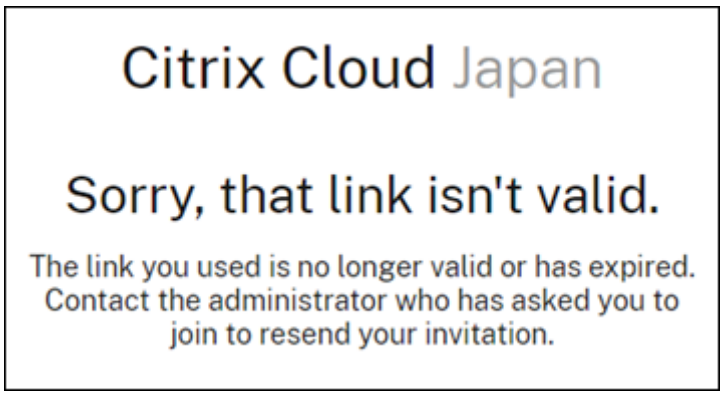
Adding new administrators uses the following workflow:

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 Configure administrator permissions in this article.

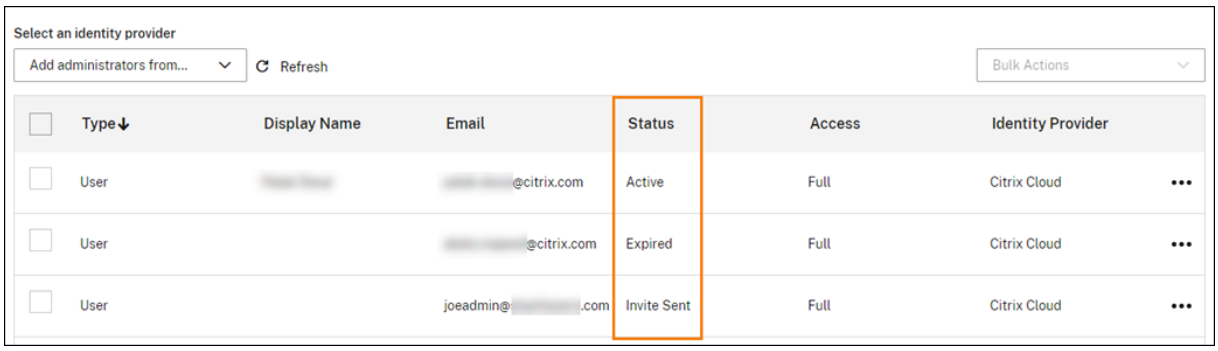
Invite individual administrators

Adding individual administrators involves inviting them to join your Citrix Cloud Japan 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 email is valid for five consecutive days from the day you send it. After five days have elapsed, the invitation link expires. If the invited administrator uses the expired link, Citrix Cloud Japan displays a message indicating the link is not valid.



Citrix Cloud Japan also displays the status of the invitation so you can see whether the administrator accepted it and signed in to Citrix Cloud Japan.



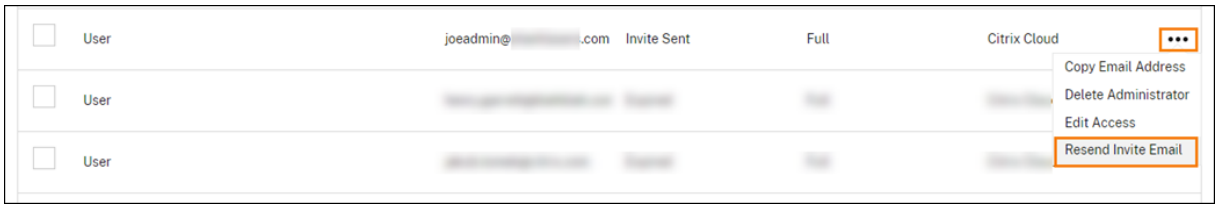
© 1997–2026 Citrix Systems, Inc. All rights reserved.

To invite an administrator

1. After signing in to Citrix Cloud Japan, 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.
3. Select **Add administrator/group**.
4. In **Administrator details**, select the identity provider you want to use. If using Microsoft Entra ID, Citrix Cloud Japan 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 Microsoft Entra 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 Japan 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 Japan 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.



Resend an invitation with a new sign-in link

If the original invitation email expires and you want to send a new one to the administrator, delete the administrator from Citrix Cloud Japan and then invite them again.

Accept an administrator invitation

If you are invited to a Citrix Cloud Japan account, Citrix Cloud Japan sends you an email that includes the organization ID and the customer name of the account.

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

To accept the invitation, click **Sign In**. Afterwards, a browser window opens. If you don't already have a Citrix account, the browser displays a page where you can create your password. If you already have an account, Citrix Cloud Japan prompts you to use your existing password to sign in.

Add administrator groups

You can add administrators using AD groups (for SAML authentication) or Microsoft Entra ID groups (for Microsoft Entra ID authentication). For more information, see the following articles:

- Manage administrator groups
- Connect SAML as an identity provider to Citrix Cloud Japan

Configure administrator permissions

When you add administrators to your Citrix Cloud Japan account, you might need to assign different levels of access to them, such as:

- Help desk access for Citrix DaaS™
- Access to manage one or more specific cloud services
- Access to manage specific Citrix Cloud Japan functions such as Library or resource locations

With delegated administration, you can configure the access permissions all of your administrators need in accordance with their role in your organization.

Console permissions

Use the following permissions to configure custom access to the Citrix Cloud Japan management console:

- **Customer Dashboard (View Only):** For Citrix Service Providers (CSPs) only. Grants view access to the Customer Dashboard.
- **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.
- **Library:** Grants access to the **Library** console page.
- **Licensing:** Grants access to the **Cloud Services** and **Licensed Deployments** tabs of the **Licensing** console page.
- **Notifications:** Grants access to the **Notifications** console page. Administrators can view and dismiss Citrix Cloud notifications.

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

- **Resource Locations:** Grants access to the **Resource Locations** console page. Administrators can add new resource locations and add FAS servers for Citrix Workspace single sign-on. They can also add connectors and manage connector updates.
- **System Log:** Grant access to the **System Log** console page. Administrators can view system log events and export events to a CSV file.
- **Workspace Configuration:** Grants access to the **Workspace Configuration** console page. Administrators can change authentication methods, customize workspace appearance and behavior, enable and disable services, and configure site aggregation. For more information, see the Citrix Workspace product documentation.

To change existing permissions

Only Citrix administrators with Full access can define access permissions for other administrators.

1. Sign in to Citrix Cloud Japan at https://citrix.citrixcloud.jp.
2. Click the menu button in the top-left corner of the page and select **Identity and access management**.
3. Click the **Administrators** tab.
4. Locate the administrator you want to manage, click the ellipsis button, and select **Edit access**.
5. Select **Custom access**.
6. Select or clear each permission as needed.
7. Click **Save**.

Change your device for multifactor authentication

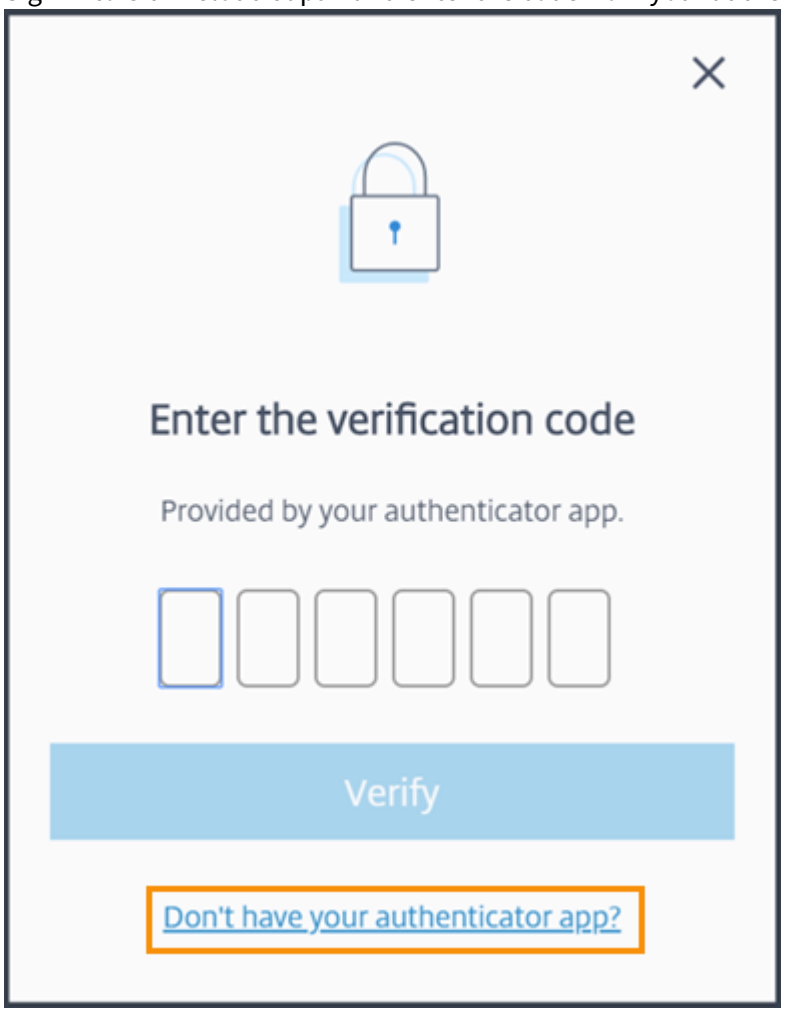
If you lose your enrolled device, want to use a different device with Citrix Cloud Japan, or reset your authenticator app, you can re-enroll in Citrix Cloud Japan multifactor authentication.

> **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 Japan 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 Japan entries with differing codes which can cause confusion when signing in to Citrix Cloud Japan.
> - 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 recom-

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

> mends installing an authenticator app before you re-enroll your device.

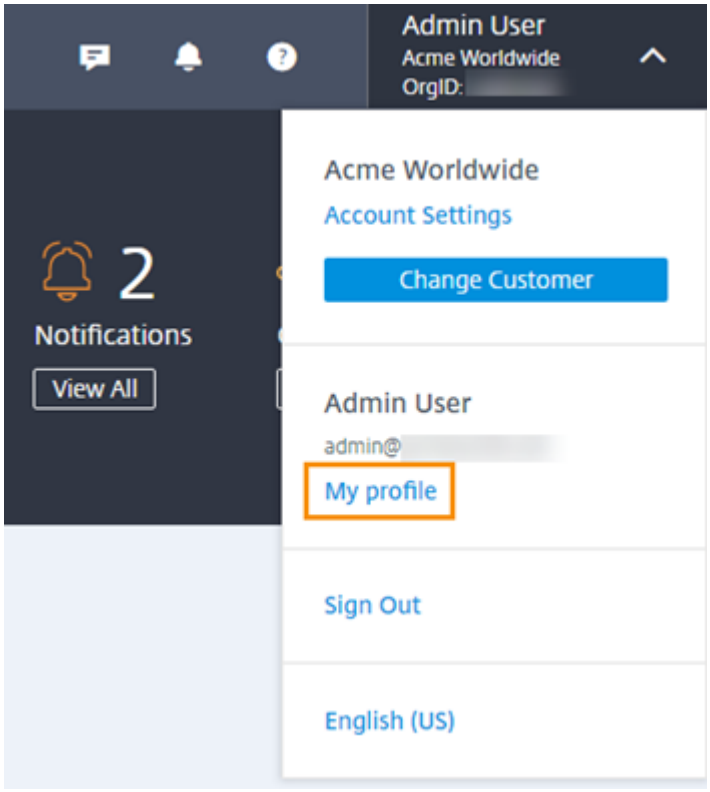
1. Sign in to Citrix Cloud Japan and enter the code from your authenticator app.



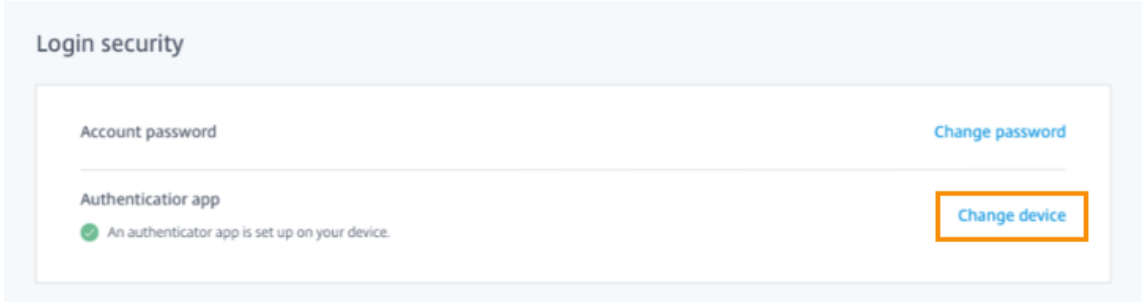
   If you don't have your authenticator app, click **Don't have your authenticator app?** and select a recovery method to help you sign in. Depending on the recovery method selected, enter the recovery code you received or an unused backup code and select **Verify**.

2. If you are an administrator for multiple customer organizations, select any customer organization.
3. From the top-right menu, select **My Profile**.

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



4. In **Authenticator app**, select **Change device**.

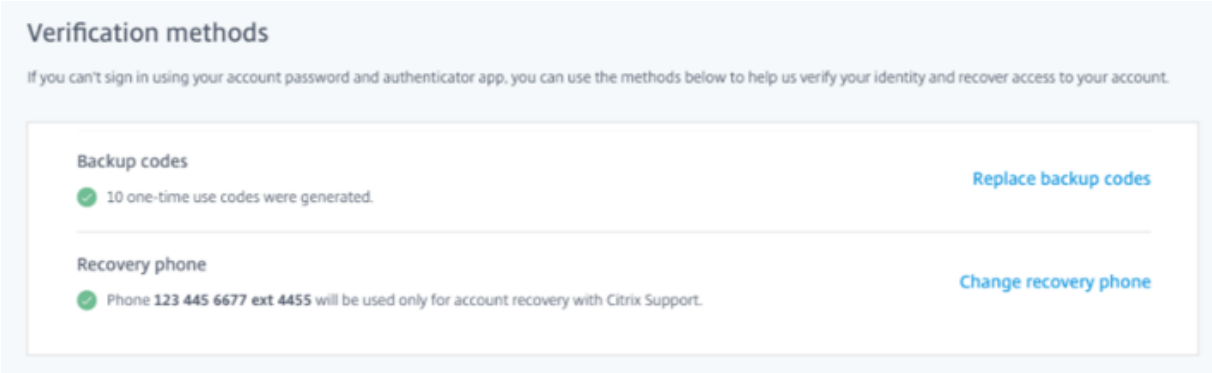


5. When prompted to confirm changing your device, select **Yes, change device**.
6. Verify your identity by entering a verification code from your authenticator app. If you don't have an authenticator app, select **Don't have your authenticator app?** and select a recovery method. Depending on the recovery method you select, enter the verification code or recovery code you receive or an unused backup code. Select **Verify**.
7. If you are using the device you originally enrolled and your original authenticator app, delete the existing Citrix Cloud Japan 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**.

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

Manage your verification methods

> **Important:**
>
> To ensure your Citrix Cloud Japan account remains secure, keep your verification methods up-to-date with accurate information. If you lose access to your authenticator app, these verification methods are the only way you can recover access to your account.



Generate new backup codes

If you lose or need to generate more one-time use backup codes, you can generate a new set of backup codes at any time. After you generate new backup codes, be sure to store them in a safe place.

1. Sign in to Citrix Cloud Japan and enter the code from your authenticator app.
2. If you are an administrator for multiple customer organizations, select any customer organization.
3. From the top-right menu, select **My Profile**.
4. Under **Verification methods**, in **Backup codes**, select **Replace backup codes**.
5. Verify your identity by entering a verification code from your authenticator app.
6. When prompted to replace your backup codes, select **Yes, replace**. Citrix Cloud Japan generates and displays a new set of backup codes.
7. Select **Download codes** to download your new codes as a text file. Then, select **I've saved these codes** and select **Close**.

Change your recovery phone number

1. Sign in to Citrix Cloud Japan and enter the code from your authenticator app.
2. If you are an administrator for multiple customer organizations, select the customer organization from which you originally enrolled in multifactor authentication.
3. From the top-right menu, select **My Profile**.
4. Under **Verification methods**, in **Recovery phone**, select **Change recovery phone**.

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

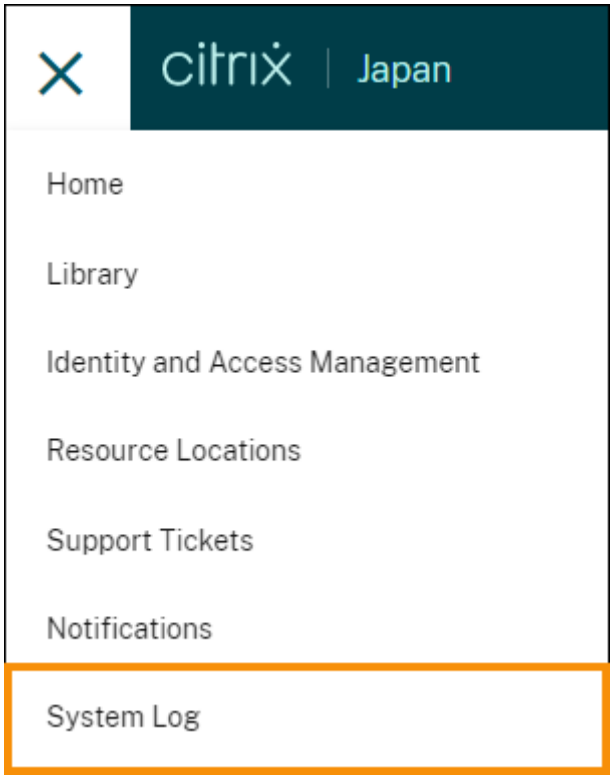
5. Enter the new phone number you want to use and then select **Save**.

System Log

September 28, 2026

The system log displays a timestamped list of events that occurred in Citrix Cloud Japan. You can export these changes as a CSV file to meet your organizations's regulatory compliance requirements or to support security analysis.

To view the system log, select **System Log** from the Citrix Cloud Japan menu.



For more information about retention of system log data, see Data retention in this article.

Limitations

While the system log functions the same in Citrix Cloud Japan and Citrix Cloud (citrix.cloud.com), the following items are not available for use with Citrix Cloud Japan:

- SystemLog API
- Splunk add-on for the system log

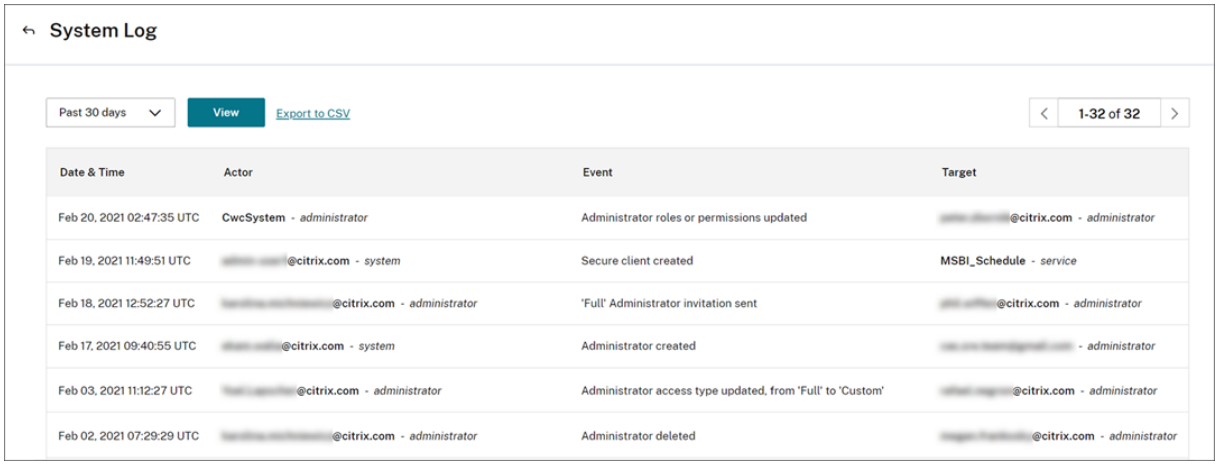
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Logged events

The system log captures events for certain Citrix Cloud Japan platform and cloud service operations. For a complete list of these events and descriptions of captured data, see System Log Events Reference.

> **Note:**
>
> The System Log Events Reference includes platform and service-related events that occur in Citrix Cloud. The events that are generated in Citrix Cloud Japan are a subset of the events that are documented in the reference article. For notifications about new events that are supported in Citrix Cloud Japan, see What's new in Citrix Cloud Japan.

The system log displays events that occurred in the last 30 days by default, up to a maximum of 90 days. The most recent events are displayed first.

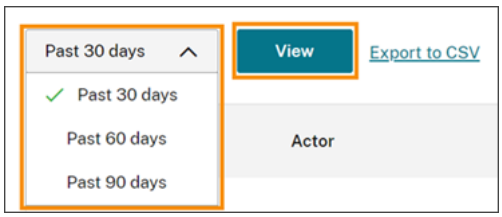


The displayed list includes the following information:

- 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 Japan 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 that occurred up to 90 days in the past, filter the list by selecting the time period you want to view and select **View**.

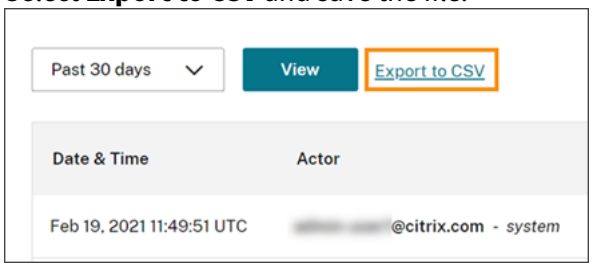
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 Japan menu, select **System Log**.
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 a service principal.

Data retention

Citrix shares responsibility with you, the customer, for retaining the system log data that Citrix Cloud Japan 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.

Citrix Cloud Japan for Partners

September 6, 2025

Citrix Cloud Japan includes services, features, and experiences designed for both customers and partners. The partner experience in Citrix Cloud Japan is the same as it is in Citrix Cloud.

Partners can take advantage of the following functions:

- Invite customers to connect with Citrix Cloud Japan.
- View customers' service entitlements, including trials.
- Enable or disable access to the customer dashboard through the Administrators console.
- View licensing trends from the customer dashboard.
- View customer licensing and usage for Citrix DaaS™ entitlements through the Licensing console.
- View customers' notifications from the Citrix Cloud Japan management console.

For more information about the partner experience, see Citrix Cloud for Partners.

SDKs

September 6, 2025

The **Citrix DaaS™ Remote PowerShell SDK** automates complex and repetitive tasks. It provides the mechanism to set up and manage the Citrix DaaS (formerly Virtual Apps and Desktops) environment without having to use the Studio user interface.

Requirements

Ensure PowerShell 3.0 or later is available on the machine.

Install or remove the Remote PowerShell SDK

To install the Remote PowerShell SDK for use with Citrix Cloud Japan:

1. Download the installer: https://download.apps.cloud.com/CitrixPoshSdk.exe.
2. Run the command `CitrixPoshSdk.exe EnvironmentName=Japan`. This command enables the SDK to run in the context of Citrix Cloud Japan by default.

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

> **Note:**
>
> Alternatively, you can run the SDK installer and follow the dialogs to complete the installation. However, you will need to specify the Citrix Cloud Japan environment when you authenticate using the Get-XdAuthentication cmdlet. See To run the Remote PowerShell SDK in this article.

Installation logs are created in %TEMP%\CitrixLogs\CitrixPoshSdk. Logs can help resolve installation issues.

To uninstall the Remote PowerShell SDK:

1. From the Windows feature for removing or changing programs, select **Citrix DaaS Remote PowerShell SDK**.
2. Right-click and select **Uninstall**.
3. Follow the dialog.

To run the Remote PowerShell SDK

Run the Remote PowerShell SDK on a domain-joined computer within that resource location:

1. Open a PowerShell command prompt. You do not need to run as an administrator.
2. Add the Citrix® snap-ins: `asnp citrix.*`
3. You can explicitly authenticate by running the command `Get-XdAuthentication`. Alternatively, you can execute your first Remote PowerShell SDK command, which will prompt you for the same authentication as Get-XdAuthentication. However, if you did not install the SDK as described in Install or remove the Remote PowerShell SDK earlier in this article, you must use the command `Get-XdAuthentication -EnvironmentName Japan` to authenticate to Citrix Cloud Japan.
4. Continue executing PS SDK cmdlets or PS SDK automation scripts. For an example script, see Example activities in the Citrix DaaS documentation.

> Notes:
>
> - Once authenticated, remote access remains valid in the current PowerShell session for 24 hours. After this time, you must enter your credentials.
> - Citrix recommends that you do not run this SDK's cmdlets on Cloud Connectors. The SDK's operation does not involve the Cloud Connectors.

For a complete list of supported and disabled snap-ins, see Support and limitations in the Citrix DaaS documentation.

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

Citrix Gateway service for Citrix Cloud Japan

September 6, 2025

Citrix Gateway service is generally available for Citrix Cloud Japan. All customers'traffic passes through dedicated Citrix Cloud Japan PoPs only. For more information, see CTX340508: Citrix Gateway Service Points of Presence (PoPs) - Citrix Cloud Japan. If you use Citrix DaaS (formerly Virtual Apps and Desktops service), you can now use the gateway service for HDX Proxy within Citrix Cloud Japan. Citrix Gateway service is available in two regions (PoPs): Tokyo and Osaka.

Supported Citrix Gateway service features

The following are some of the features supported by the Citrix Gateway service in Citrix Cloud Japan.

HDX™ Proxy

The HDX Proxy functionality within the Citrix Gateway service provides secure and reliable access to Citrix Vrtuial Apps and Desktops

High availability

Multi-Layered resiliency approach by the Citrix Gateway service provides resiliency at every level. Within a particular Citrix Gateway service POP, the micro services and tenants that form the service are deployed in a highly available form. The components are deployed in the N+1 model. In this model, all components are load balanced and can do a quick failover with standby, if there is some failure. In rare cases, when all the services of a particular component within a POP are down, the Citrix Gateway service marks itself as down. This enables the DNS server to redirect users to the next nearest POP, providing a POP level high availability.

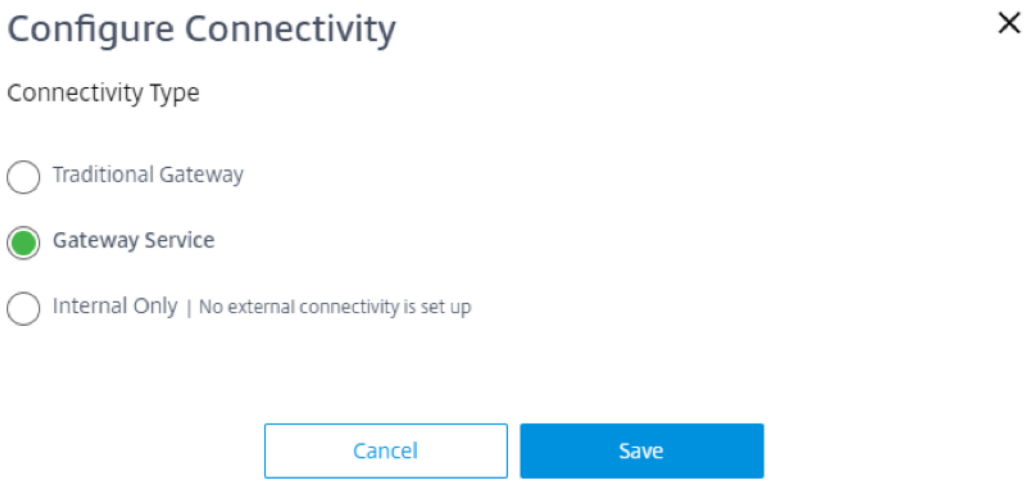
Optimal gateway routing

Citrix Gateway service is deployed in multiple regions across Japan and there is a need for a mechanism to choose the optimum POP for best performance. Optimal Gateway routing or proximity routing a DNS based service is used to return end users with the closest POP location when they try connecting to the Citrix Gateway Service. This DNS service uses the source IP address of the query as one of the metadata to return the closest Citrix Gateway service POP IP address.

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

How to enable Citrix Gateway service

1. From the **Resource Locations** page, locate the resource location you want to configure and click **Gateway**. The Configure Connectivity dialog appears.



2. Click **Citrix Gateway service** to provide secure access to applications and desktops for external users.
3. Click **Save**.

Citrix Cloud Connector™ connectivity requirements

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 you use with Citrix Cloud Japan reside. The Cloud Connector connects to Citrix Cloud Japan, allowing it to operate and manage your resources as needed. For more details on Citrix resource location / Cloud Connector, see Cloud Connector common service connectivity requirements.

The following URLs must be accessible to use the gateway service: `https://*.*.nssvc.jp`.

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

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

Migrate from an on-premises Citrix Gateway to cloud based Citrix Gateway service

You can migrate from an on-premises Citrix Gateway to cloud based Citrix Gateway service. For details, see Migrate Citrix Gateway to Citrix Gateway service for HDX proxy.

© 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.