Citrix Cloud Japan

Contents

Citrix Cloud Japan

November 30, 2020

Citrix Cloud Japan is a cloud that is isolated and separate from Citrix Cloud, allowing Japanese customers to use Citrix Cloud services in a dedicated Citrix-managed environment. Citrix Cloud Japan is a geographical boundary within which Citrix operates, stores, and replicates services and data for delivery of Citrix Cloud services. Citrix may use multiple public or private clouds located in one or more states within the US to provide services.

Available services

Only Citrix Virtual Apps and Desktops service is available.

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.

Secure Deployment Guide for Citrix Cloud Japan

January 13, 2021

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.

The Virtual Apps and Desktops service Technical Security Overview provides similar information for the Virtual Apps and Desktops service.

Control Plane

Guidance for administrators

- Use strong passwords and regularly change your passwords.
- All administrators within a customer account can add and remove other administrators. Ensure that only trusted administrators have access to Citrix Cloud 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 Azure Active Directory.

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 with the strongest cipher suites. Customers cannot control the TLS certificate in use, as Citrix Cloud Japan is hosted on the Citrix-owned cloud.jp domain. To access Citrix Cloud Japan, customers must use a browser capable of TLS 1.2 with strong cipher suites.

Consult the per-service documentation for details about encryption and key management within each service.

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.

Audit and change control

There is currently no customer-visible auditing or change control available in the Citrix Cloud Japan user interface or APIs.

Citrix has extensive internal auditing information. If a customer has a concern, they are advised to contact Citrix within 30 days. Citrix will review the audit logs to determine the administrator who performed an operation, the date on which it was performed, the IP address associated with the action, and so on.

Citrix Cloud Connector

Installation

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

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

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 contains sensitive security information such as administrative passwords. Only the most privileged administrators should be able to log on to the machines hosting the Cloud Connector (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.

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	636/TCP	LDAP SSL
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 listed as **Use for subscriptions** on the **Identity and Access Management** page in the Citrix Cloud Japan user interface.

In selecting the domains to configure as **Use for subscriptions**, the Cloud Connector communicates with domain controllers in all domains in the Active Directory forest where the machines hosting the Cloud Connector reside.

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. Additionally, 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 Connectivity Requirements.

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 base Cloud Connector configuration does not need any special SSL/TLS configuration.

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

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

Connector updates

When Citrix software updates are available, the Cloud Connector will self-manage. 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.
- 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

January 8, 2021

Signing in to your account

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

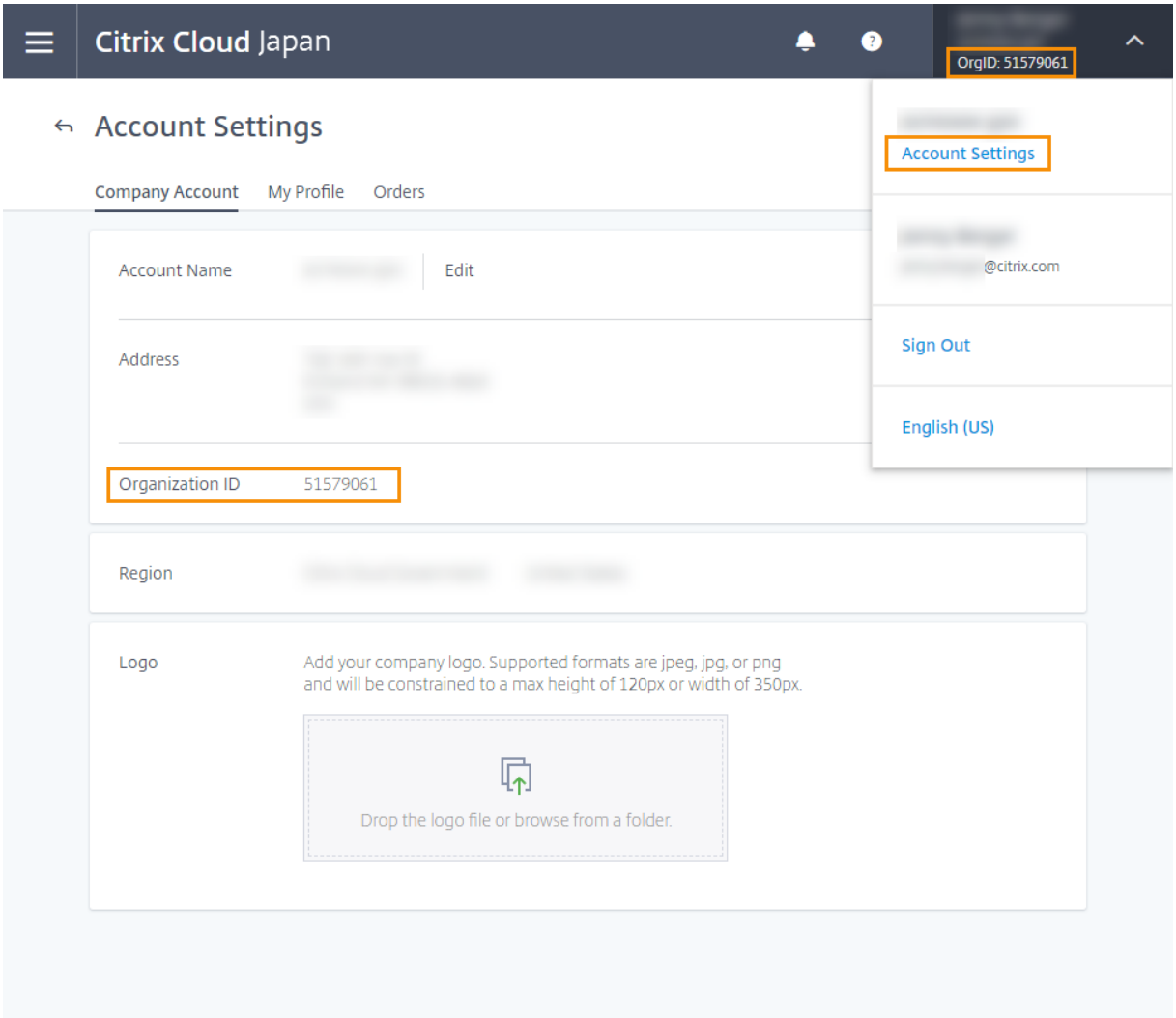
- Verify you're signing in at https://citrixcloud.jp and the sign-in page displays the Citrix Cloud Japan logo. The sign-in URL for Citrix Cloud Japan uses the `.jp` top-level domain, not the `.com` top-level domain.
- Make sure you sign in with the **email address** and password you provided when you 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 Azure AD 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 Azure Active Directory is enabled as the identity provider for your account. For more information about using Azure Active Directory as your identity provider, see Connect Azure Active Directory as an identity provider.

Purchasing services

Visit https://www.citrix.com/products/citrix-cloud/buy.html 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.

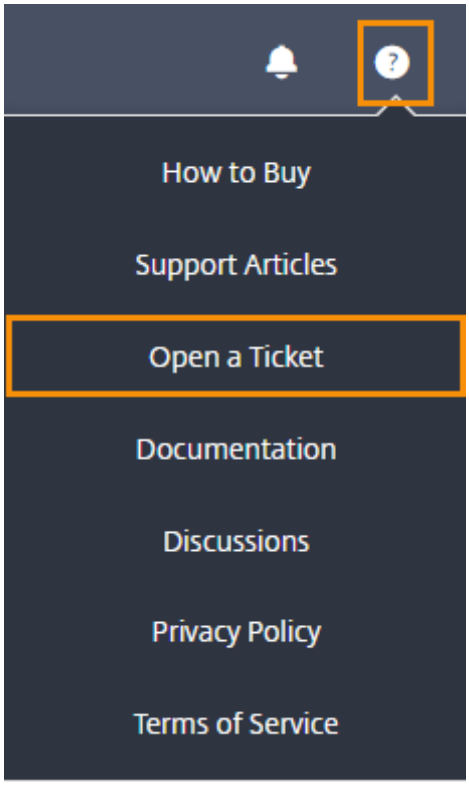
If you need additional assistance renewing or extending your subscription, contact Citrix Customer

Service.

Technical support

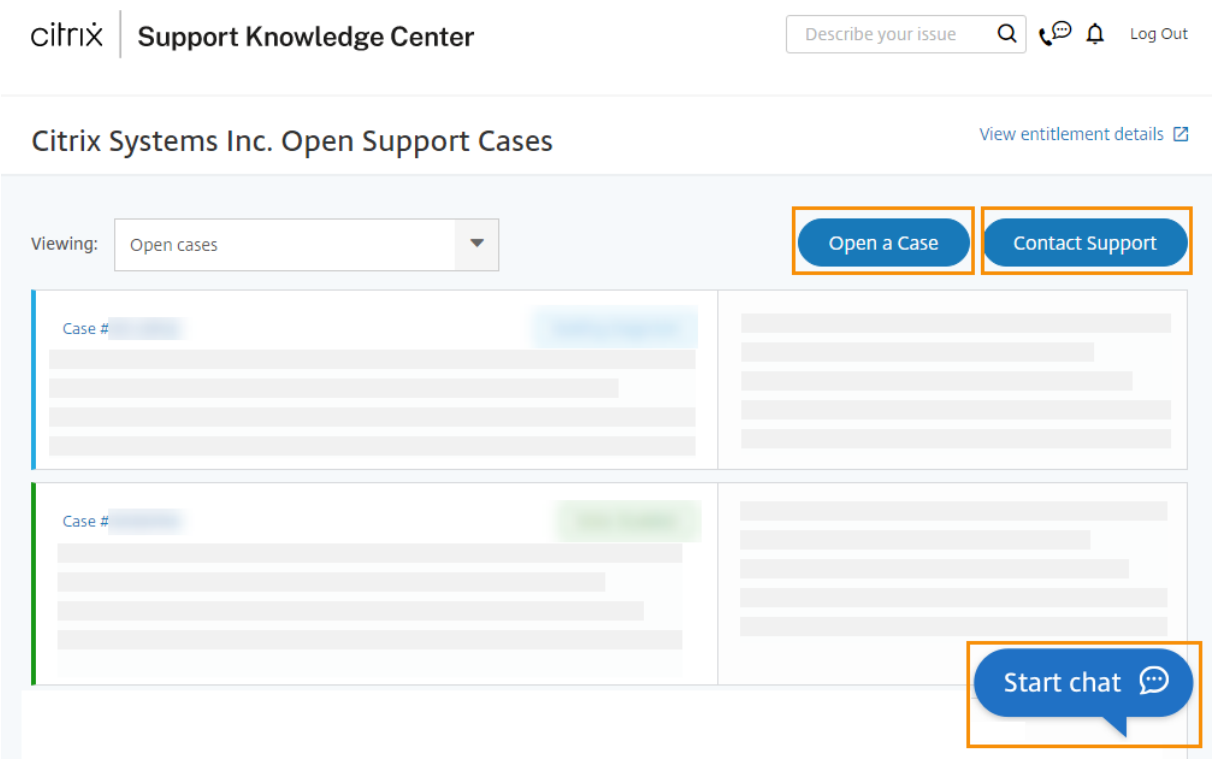
If you're experiencing an issue that requires technical help, you can access the Citrix Support Knowledge Center to open a support case or talk with a Citrix Technical Support representative.

To access the Support Knowledge Center, visit https://support.citrix.com/case/manage. Alternatively, in the Citrix Cloud Japan management console, click the **Help** icon near the top-right of the screen and then select **Open a Ticket > Go to My Support**. You can then sign in with your Citrix account.



After signing in, contact Citrix Technical Support using one of the following methods:

- Start a support case: Select **Open a Case** and then provide the details of the issue you're experiencing.
- By telephone: Select **Contact Support** to view a list of local phone numbers you can use to call Citrix Technical Support.
- Live Chat: Select **Start chat** in the lower-right corner of the page to chat with a Citrix Technical Support representative.



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://discussions.citrix.com/forum/1704-citrix-cloud/ or select **Help > Discussions** from the Citrix Cloud Japan management console.

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

January 8, 2021

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, Citrix Cloud Japan prompts you to enroll after you create a Citrix account during the sign-up process.

Visit the sign-up page

Visit https://onboarding.citrixcloud.jp/ and complete the sign up form.

Citrix Cloud Japan uses your business email address as your user name when signing in. The business email address you specify must meet the following requirements:

- **The email address must be different than others you might have already used with commercial Citrix Cloud.** For example, if you're an administrator on a commercial Citrix Cloud account, Citrix Cloud has a record of that email address. If you sign up for Citrix Cloud Japan with that same email address, Citrix Cloud Japan does not accept it.
- **The email address must be different than others you might have already used with Citrix Cloud Japan.** For example, if you have accepted an invitation to be an administrator on a Citrix Cloud Japan account, Citrix Cloud Japan has a record of that email address. If you sign up with that same email address, Citrix Cloud Japan does not accept it.
- **The email address cannot use the citrix.com domain.** Citrix Cloud Japan does not accept email addresses with the citrix.com domain.

Accept the terms of service

After you submit the sign up form, Citrix Cloud Japan displays your home region. Currently, Citrix Cloud Japan includes only one geographical region, so only this region appears.

Agree to the Terms of Service and then click **Continue**. Citrix Cloud Japan displays a confirmation page and sends you a confirmation email so you can set up your account password.

Confirm your email address

Locate the confirmation email and click the **Sign In** link. If you haven't received the confirmation email after a few minutes, click the **Resend** link on the Citrix Cloud Japan confirmation page in your browser.

Create a password and sign in

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

You can then sign in to Citrix Cloud Japan using the email address and password you chose earlier.

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.

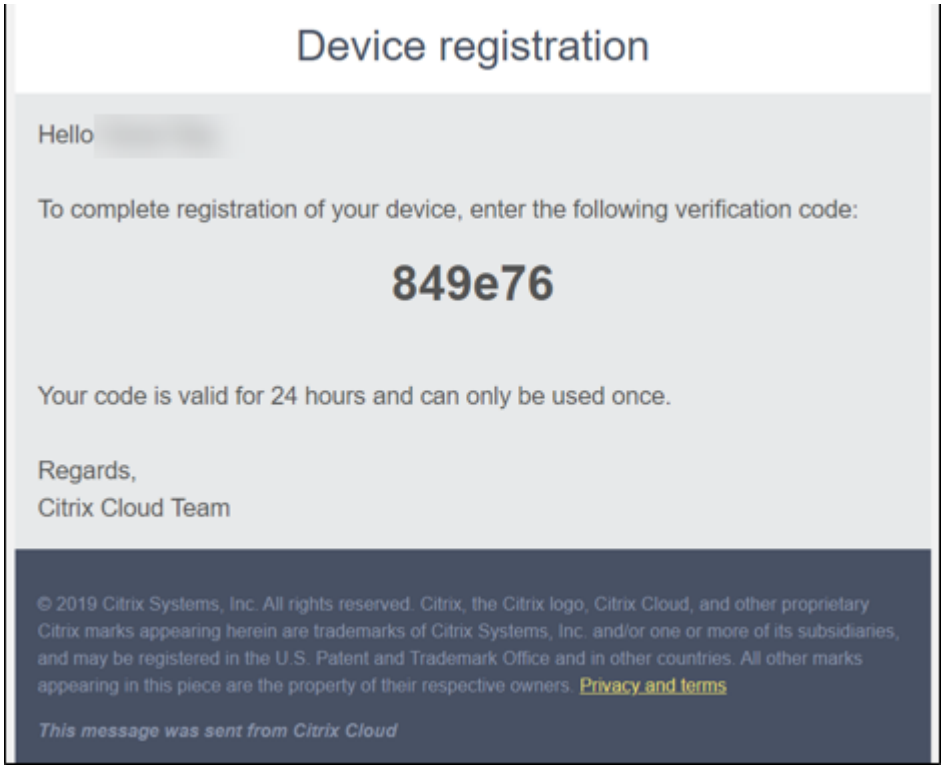
If you're not enrolled in multifactor authentication, Citrix Cloud Japan prompts you to enroll when you sign in.

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.

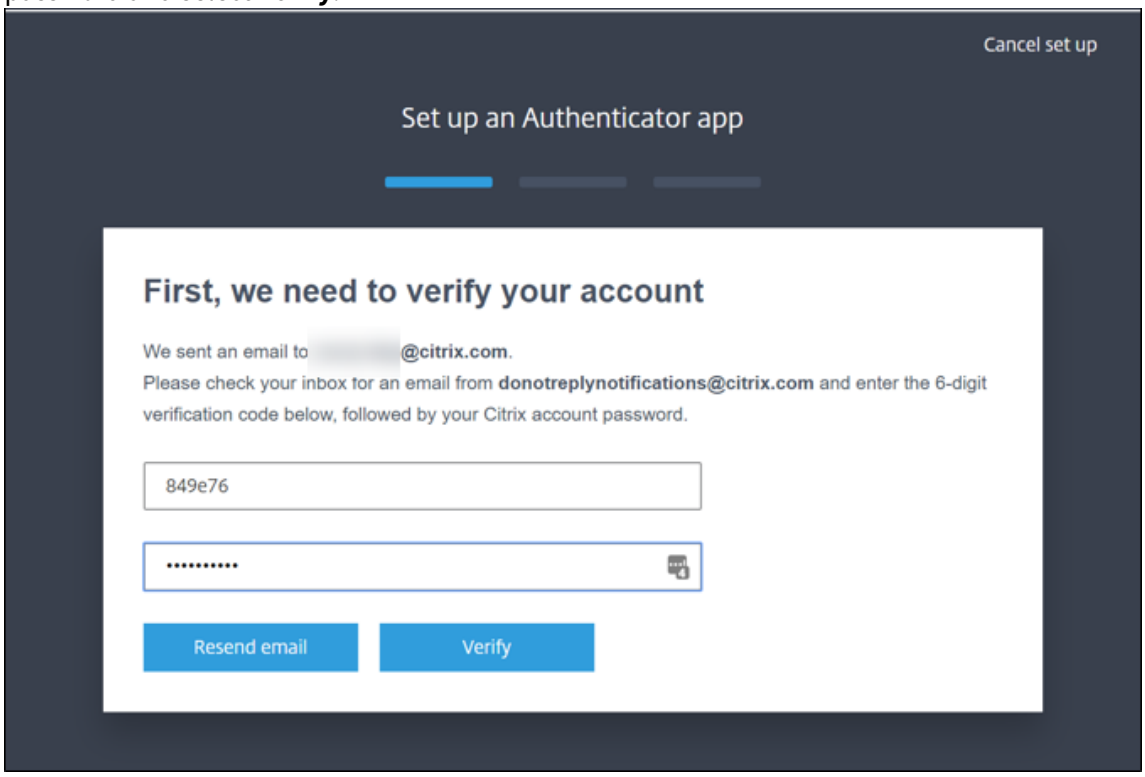
> **Notes:**
>
> - Only administrators under the Citrix identity provider can enroll in multifactor authentication through Citrix Cloud Japan. If you use Azure AD to manage Citrix Cloud Japan administrators, you can configure multifactor authentication using the Azure portal. For more information, see 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 Change your device for multifactor authentication.

To enroll your device in multifactor authentication

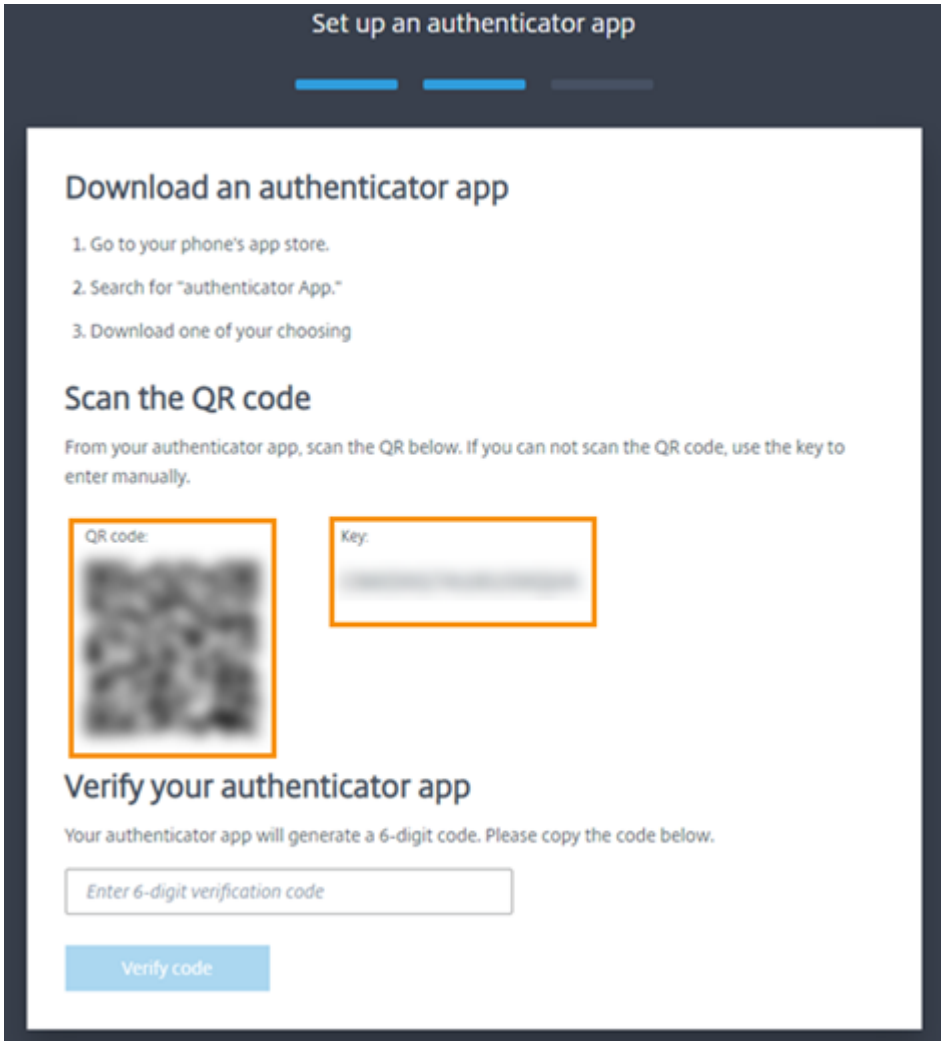
1. Visit https://citrixcloud.jp and enter your Citrix Cloud Japan credentials.
2. When prompted to enroll in multifactor authentication, select **Enroll now**. Citrix Cloud Japan sends you an email with a verification code.



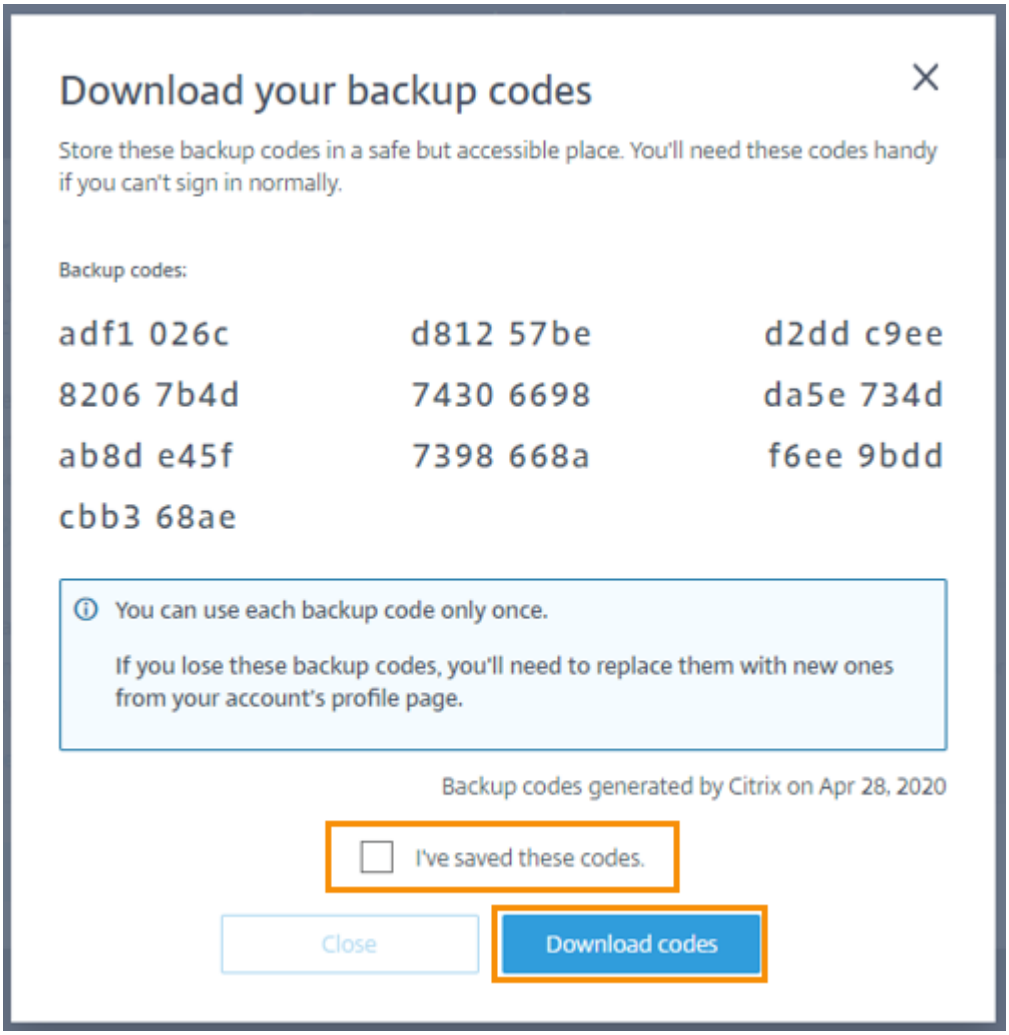
3. After you receive the email, enter the 6-digit verification code and your Citrix Cloud Japan password and select **Verify**.



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.

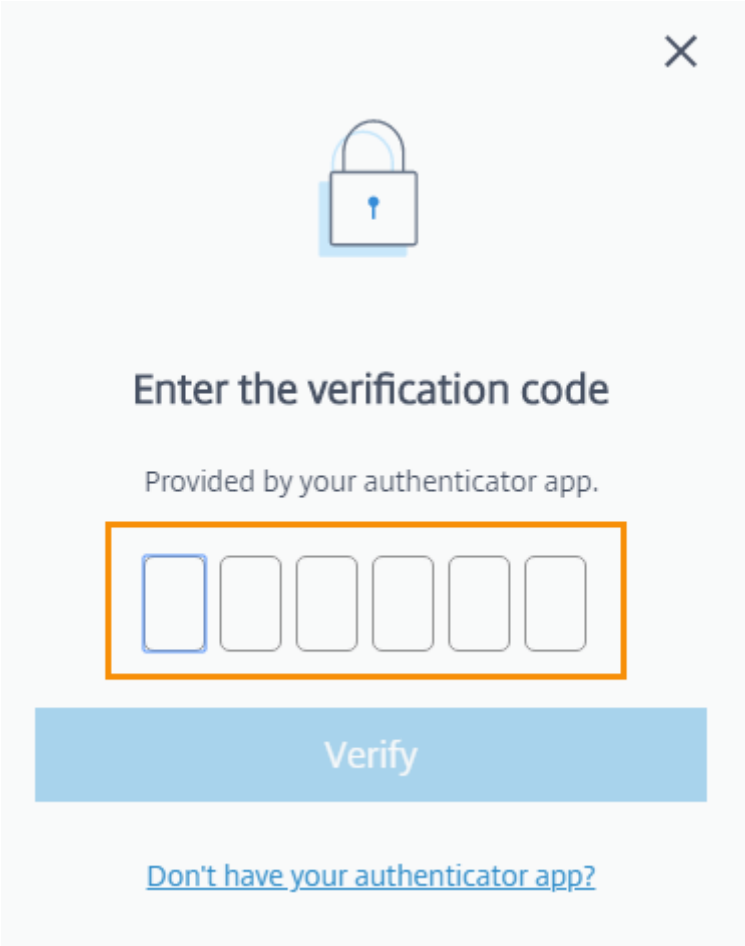


5. Under **Verify your authenticator app**, enter the code from your authenticator app and select **Verify code**.
6. Configure the following account recovery methods in the event you lose your device or can't use your authenticator app:
    - Recovery phone (required): Select **Add a recovery phone** 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**.



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.



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:

- Change your device for multifactor authentication
- Manage your verification 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.

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://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

January 8, 2021

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
Maximum Length	60 calendar days. You can request a trial for the service only once.

	Citrix Cloud Japan Trial
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
Virtual Apps and Desktops service	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.

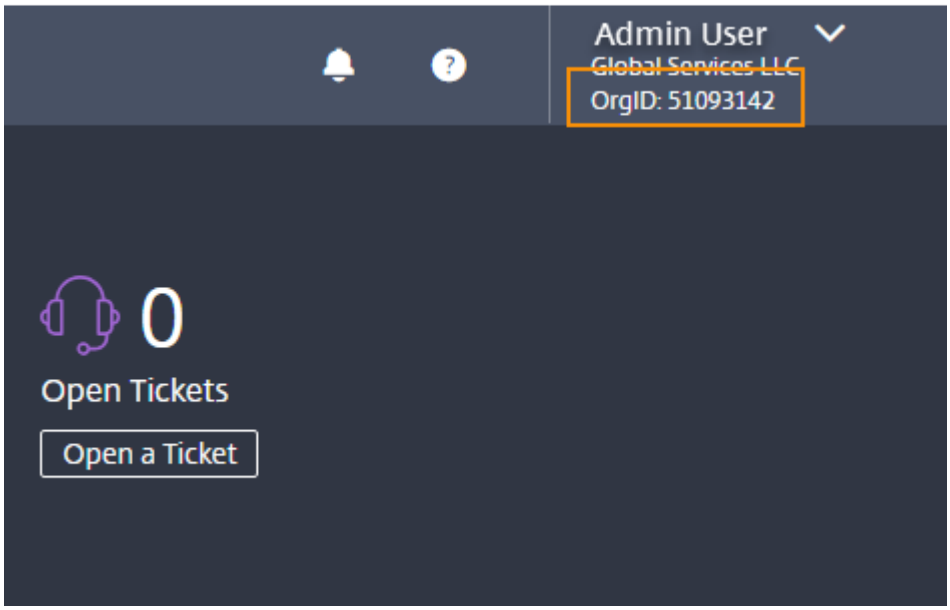
> **Note:**
>
> To ensure the best customer experience, Citrix reserves the right to limit trials to a certain number of participants at any given time.

Purchase services

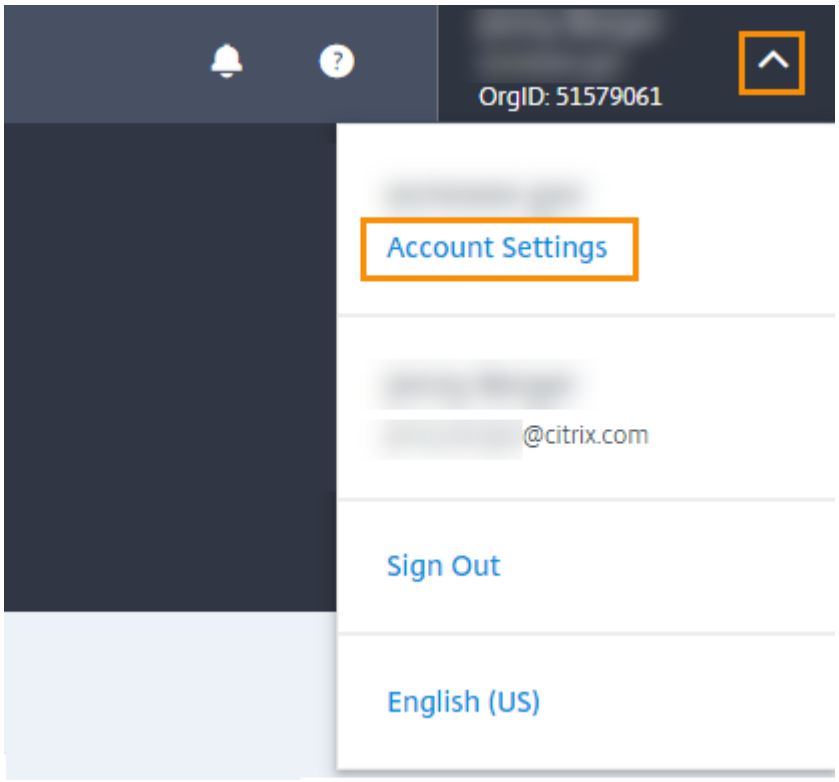
When you're ready to convert your trial to a production service, visit https://www.citrix.com/products/citrix-cloud/buy.html.

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

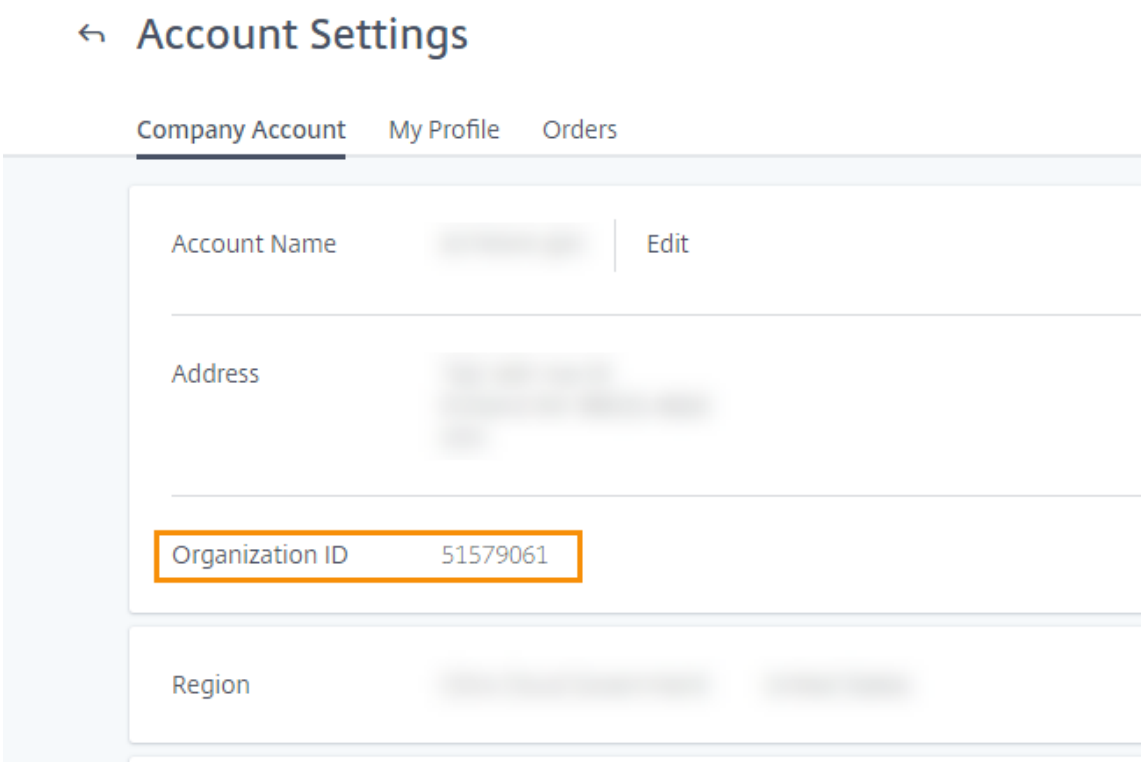
- In the top-right corner of the management console, your OrgID is displayed beneath your account name.



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



Your OrgID is shown in the Organization ID field.



> **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

December 2, 2020

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:

- Citrix VDI Handbook and Best Practices
- Scale and size considerations for Cloud Connectors

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
- Microsoft Internet Explorer 11
- Latest version of Apple Safari

Additional requirements

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

Service connectivity requirements

January 8, 2021

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 re-

strictions, further configuration might be needed. For more information, see Cloud Connector Proxy and Firewall Configuration.

The addresses for each service in this article must be contactable to properly operate and consume the service. The following 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://*.cloud.com`	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 by the Active Directory agent and Machine Creation Services.
`https://*.cloudapp.net`	Provides access to Azure Cloud Services, which hosts compute resources and APIs for Citrix Cloud Japan.

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.

Virtual Apps and Desktops

Citrix resource location / Cloud Connector:

- `https://*.citrixworkspacesapi.jp`
- `https://*.citrixnetworkapi.net`
- `https://*.cloud.com`
- `https://cwsproduction.blob.core.windows.net`
- `https://*.xendesktop.net`
- `https://*.servicebus.windows.net`

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

Administration console:

- https://*.citrixworkspacesapi.jp
- https://*.citrixnetworkapi.net
- https://*.cloud.com
- https://*.xendesktop.net

Management console

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

Session timeouts

After an administrator signs in to Citrix Cloud Japan, the management console session times out after the following intervals have elapsed:

- Idle sessions (no console activity detected): 60 minutes
- Maximum session timeout (regardless of console activity): 24 hours

After the maximum session timeout elapses, any unsaved configuration changes are lost and the administrator must sign in again.

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.

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.

For help with troubleshooting connectivity between the Cloud Connector and Citrix Cloud Japan, use the Cloud Connector Connectivity Check Utility. This utility runs a series of checks on the Cloud Connector machine to verify it can reach Citrix Cloud Japan and related services and helps you add any missing connectivity addresses to the Trusted Sites zone in Internet Explorer. If you use a proxy server in your environment, all connectivity checks are tunneled through your proxy server. To download the utility, see CTX260337 in the Citrix Support Knowledge Center.

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`

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 Cloud Connector requirements

January 7, 2021

The Citrix Cloud Connector is a component with a collection of Windows services installed on Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019.

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 practice recommendations for configuring Cloud Connector machines for Citrix Virtual Apps and Desktops, see Scale and size considerations for Cloud Connectors.

Operating systems

The following operating systems are supported:

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2

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.
- Server clock is set to the correct UTC time.
- Internet Explorer Enhanced Security Configuration (IE ESC) is turned off. If this is turned on, the Cloud Connector might not be able to establish connectivity with Citrix Cloud Japan.
- Citrix strongly recommends enabling Windows Update on all machines hosting the Cloud Connector. When configuring Windows Update, automatically download and install updates, but do not allow automatic restarts. The Citrix Cloud Japan platform handles machine restarts, allowing them for only one Cloud Connector at a time when needed. Alternatively, you can control when the machine is restarted after an update using Group Policy. For more information, see https://docs.microsoft.com/en-us/windows/deployment/update/waas-restart.

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, the client checks whether it trusts the CA that issued the certificates and whether the certificate is on a CRL. 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. So, all Cloud Connector machines must be configured to trust these certificates to ensure the Cloud Connector software can be installed successfully.

Citrix Cloud Japan endpoints are protected by certificates issued by DigiCert or by one of the Root Certificate Authorities used 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://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 certificates are installed:
  - `https://dl.cacerts.digicert.com/DigiCertAssuredIDRootCA.crt`
  - `https://dl.cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA.crt`
  - `https://cacerts.digicert.com/DigiCertGlobalRootG2.crt`
  - `https://cacerts.digicert.com/DigiCertGlobalRootCA.crt`

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

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 will use to create offerings for your users.
- Each Active Directory forest you plan to use with Citrix Cloud Japan should be reachable by two Cloud Connectors at all times.
- The Cloud Connector must be able to reach the parent (root) domain controllers as well as the child domain controllers in the Active Directory infrastructure (to complete 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 will 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 Active Directory.

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

Forest Functional Level	Domain Functional Level	Supported Domain Controllers
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

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:**
>
> - 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 per-

> forming regular maintenance updates for the Cloud Connector.

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

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 commercial Citrix Cloud (citrix.cloud.com) account, the installer will 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 reliably with the machines in your resource location. Installing the Cloud Connector on a machine template (before cloning) is not supported. If you clone a machine with the Cloud Connector installed, the Cloud Connector services will not run and the machine cannot connect to Citrix Cloud Japan.

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 at all times 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 (2) 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. This ensures the con-

nection between Citrix Cloud Japan and your resource location remains intact in the event any single Cloud Connector becomes unavailable.
- Each Active Directory forest you plan to use with Citrix Cloud Japan should be reachable by two Cloud Connectors at all times.
- After installation, do not move the machine hosting the Cloud Connector into a different domain. If the machine needs to be joined to be a different domain, uninstall the Cloud Connector and then re-install it after the machine is joined to the different domain.

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 Connector needs to perform an action requiring Local System permissions, it does so through a predefined set of operations that the Citrix Cloud Agent System can perform.

Service Name	Description	Runs As
Citrix Cloud Agent System	Handles the system calls necessary for the on-premises agents. Includes installation, reboots, and registry access. Can only be called by Citrix Cloud Services Agent WatchDog.	Local System
Citrix Cloud Services Agent WatchDog	Monitors and upgrades the on-premises agents (evergreen).	Network Service
Citrix Cloud Services Agent Logger	Provides a support logging framework for the Citrix Cloud Connector services.	Network Service

Service Name	Description	Runs As
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
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

Service Name	Description	Runs As
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 the Hypervisor(s).	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

Event messages and logs

Event messages are available in the Windows Event viewer on the connector machine. The Windows event logs that the Cloud Connector generates are in the following documents:

- Connector Agent Provider [XML format]
- Connector AgentWatchDog Provider [XML format]

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

Troubleshooting

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

the event logs will provide some initial information.

Connectivity

If the Cloud Connector is “disconnected,” the Cloud Connector Connectivity Check Utility can help you verify the Cloud Connector can reach Citrix Cloud Japan and its related services.

The Cloud Connector Connectivity Check Utility runs on the machine hosting the Cloud Connector. If you use a proxy server in your environment, the utility can help you verify connectivity through your proxy server by tunneling all connectivity checks. If needed, the utility can also add any missing Citrix trusted sites to the Trusted Sites zone in Internet Explorer.

For more information about downloading and using this utility, see CTX260337 in the Citrix Support Knowledge Center.

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.

Install and configure

January 8, 2021

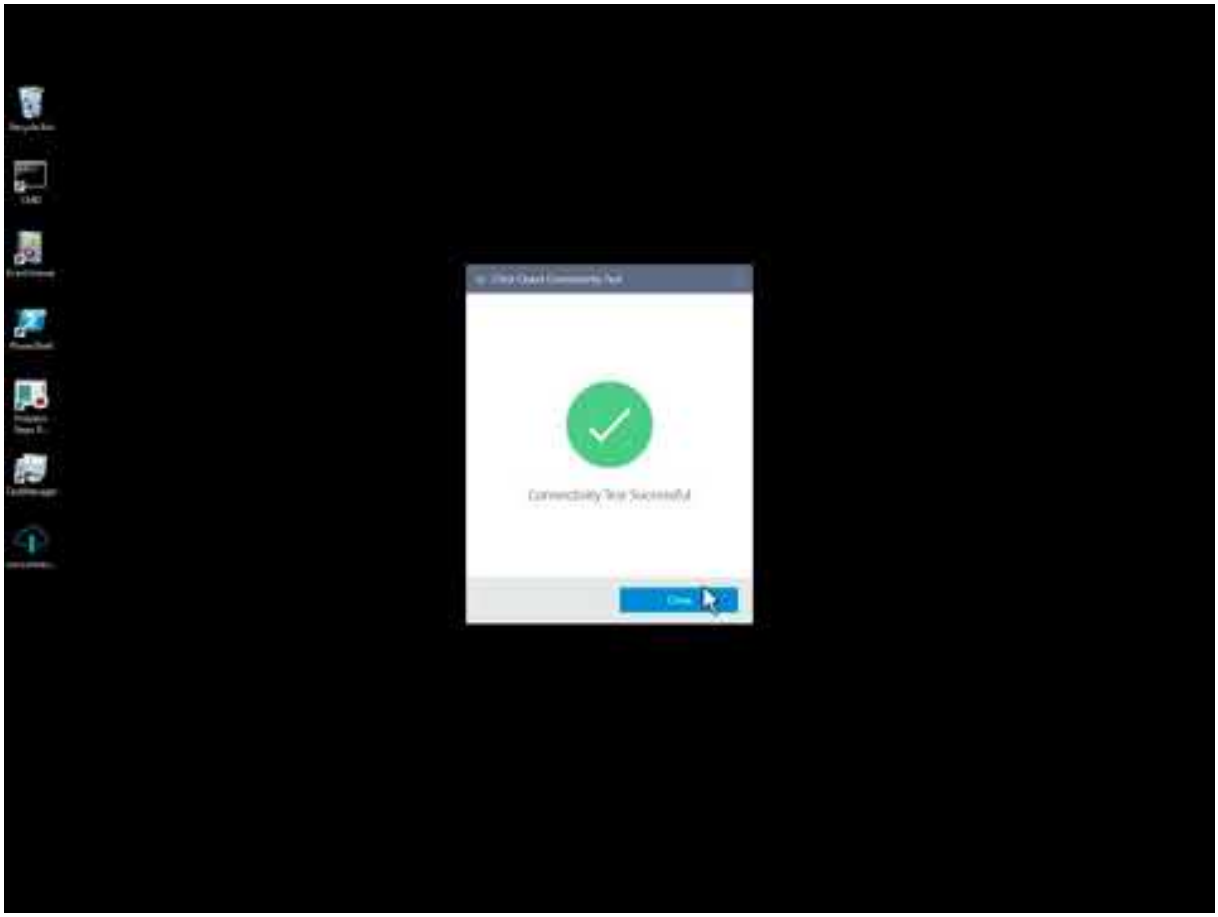
After you sign up for Citrix Cloud Japan, use the following sequence to set up your connection to Citrix Cloud Japan. Review the entire process beforehand so you know what to expect.

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 the Virtual Apps and Desktops service.

For instructions, see Create a resource location.

View a video about installing Cloud Connectors:



Connect an identity provider

Identity providers are used to authenticate administrators when they sign in to Citrix Cloud Japan and to provide access to user lists for assigning Library offerings to users. Citrix Cloud Japan supports the following identity providers:

- Active Directory (AD)
- Azure Active Directory

Administrator authentication

By default, Citrix Cloud Japan uses Citrix Identity, a built-in identity provider, to authenticate administrators when they sign in. Alternatively, you can connect your AD or Azure AD as an identity provider to Citrix Cloud Japan to authenticate Citrix Cloud Japan administrators.

Application and desktop delivery to users

When delivering applications and desktops through the Virtual Apps and Desktops service, you can assign users and groups from your AD or Azure AD to those resources using one of the following methods:

- Create a delivery group in Studio that includes the applications and desktops you want to deliver and specifies the users from your AD who are authorized to access them.
- Create a delivery group in Studio that includes the applications and desktops you want to deliver and make it available as an offering in the Library. Then, use the Library to select the users from your AD or Azure AD who are authorized to access the resources in the delivery group. This method requires connecting your AD or Azure AD 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 Azure Active Directory as an identity provider

Set up Virtual Apps and Desktops

To get started with the Virtual Apps and Desktop service, 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 Virtual Apps and Desktops service deployment and prepare your machines accordingly.
3. Review the sequence of tasks in Install and configure in the Virtual Apps and Desktops service documentation and follow the steps in each task.

Create a resource location

January 7, 2021

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

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 the 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) to manage the connection between the machines hosting the applications and desktops you want to deliver and the devices used to access those resources.
- A supported hypervisor or cloud service, like Citrix XenServer 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, the resource location that Citrix Cloud Japan creates becomes the default resource location. You can have only one default resource location in your account. If needed, you can create additional resource locations in Citrix Cloud Japan and then select the one you want when you install Cloud Connectors in other domains.

Alternatively, you can first create the resource locations you need in the console, before you install Cloud Connectors in your domains. The Cloud Connector installer will prompt 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, and troubleshooting information.
2. Prepare machines that meet the configuration requirements.
3. Join the prepared machines to your domain.

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 the required addresses can be contacted so you can operate and consume 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

During installation, the Cloud Connector requires access to the cloud to authenticate the user performing the installation, validate the installer's permission(s), and download and configure the services 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 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.
> - Using the same Cloud Connector installer for repeated installations over a period of time is not recommended. 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 located at **%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup**.

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

Install Cloud Connectors from the command line

January 7, 2021

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

During installation, the Cloud Connector requires access to the cloud to authenticate the user performing the installation, validate the installer's permission(s), and download and configure the services the Cloud Connector provides. The installation occurs with the privileges of the user who initiates it.

> **Important:**
>
> Using the same installer for repeated installations over a period of time is not recommended. Download a new Cloud Connector from the Resource Locations page in the Citrix Cloud Japan console.

Use **Start /Wait CWCConnector.exe /parameter:value** to examine potential error codes in the case of a failure. This can be done using the standard mechanism of running **echo %ErrorLevel%** after the installation completes.

Requirements

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

- 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 secure client. The client ID and secret ensures your access to the Citrix Cloud API is secured appropriately. When you create a secure client, the client operates with the same level of administrator permissions that you have. For example, if you are a Full Access administrator, the secure client that you create also has 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 secure client

When creating a secure client, 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 **Secure Clients** tab, enter a name for your client and select **Create Client**. Citrix Cloud Japan generates and displays a client ID and secret for the secure client.
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

To retrieve a list of supported parameters, run **CWCConnector /?**.

- **/Customer:** Required. The customer ID appears on the **API Access** page in the Citrix Cloud Japan console.
- **/ClientId:** Required. The client ID of the secure client that you want to use to install the Cloud Connector. The client ID appears in the ID column for the secure client on the API Access page.
- **/ClientSecret:** Required. The client secret for the secure client that you want to use. The client secret is generated when you create the secure client and is not displayed on the API Access page. You can retrieve this value from the CSV file that you downloaded when you created the client.
- **/ResourceLocationId:** Required. The unique identifier for an existing resource location. If you don't specify this value, Citrix Cloud Japan uses the ID of the default resource location.
- **/AcceptTermsOfService:** Required. The default value is **Yes**.

Sample command line with all required parameters

```
CWCConnector.exe /q /Customer:*Customer*  /ClientId:*ClientId*  /
    ClientSecret:*ClientSecret*  /ResourceLocationId:*ResourceLocationId
    *  /AcceptTermsOfService:*true*
```

Troubleshooting

Installation Logs

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

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

Exit codes

- 1603 - An unexpected error occured.
- 2 - A prerequiste check failed.
- 0 - Installation completed successfully.

Citrix Cloud Connector proxy and firewall configuration

January 8, 2021

Port 443 using HTTP traffic, egress only. For full connectivity details, see Connectivity requirements.

Configuring the Cloud Connector to support a web proxy

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.

Installer

The installer will use 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 Internet Explorer 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
```


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.

Connect Active Directory to Citrix Cloud Japan

January 8, 2021

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.

Connect Azure Active Directory as an identity provider

January 8, 2021

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 Azure Active Directory (AD) instead.

By using Azure AD with Citrix Cloud Japan, you can:

- Leverage 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.

Prepare your Active Directory and Azure AD

Before you can use Azure AD, be sure you meet the following requirements:

- You have a Microsoft Azure account. Every Azure account comes with Azure AD 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 Azure AD. This role is required to give Citrix Cloud Japan your consent to connect with Azure AD.
- **Administrator accounts have their "mail" property configured in Azure AD.** To do this, you can sync accounts from your on-premises Active Directory into Azure AD using Microsoft's Azure AD Connect tool. Alternatively, you can configure non-synced Azure AD accounts with Office 365 email.

Sync accounts with Azure AD 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 Azure AD have different email addresses than administrators who sign in using a Citrix-hosted identity.
2. Install and configure Azure AD Connect. For complete instructions, see Integrate your on-premises directories with Azure Active Directory on the Microsoft Azure web site.

Connect Citrix Cloud Japan to Azure AD

When connecting your Citrix Cloud Japan account to your Azure AD, 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 Azure AD. 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://citrixcloud.jp.

2. Click the menu button in the top-left corner of the page and select **Identity and Access Management**.
3. Locate **Azure Active Directory**, 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 Azure AD

1. From the Citrix Cloud Japan management console, from the **Identity and Access Management** page, click the **Administrators** tab.
2. From the **Add administrators from** menu, select the Azure AD option.
3. In the search box, start typing the name of the user you want to add and invite them to the account as described in Add administrators to a Citrix Cloud Japan account. Citrix Cloud Japan sends the user an email containing a link to accept the invitation.

After clicking the email link, the user signs in to the company's Azure Active Directory. This verifies the user's email address and completes the connection between the Azure AD user account and Citrix Cloud Japan.

Sign in to Citrix Cloud Japan using Azure AD

After the Azure AD user accounts are connected, users 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 Azure AD identity provider for your company. Example: `https://https://citrixcloud.jp/go/myorganization`
- From the Citrix Cloud Japan sign-in page, click **Sign in with my organization credentials**, type the identifier you created when you initially connected Azure AD, and click **Continue**.

Enable advanced Azure AD capabilities

Azure AD 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 Azure AD users enables Citrix Cloud Japan to leverage those capabilities automatically.

Manage Citrix Cloud Japan

January 8, 2021

Citrix Cloud Japan includes the following administrative features:

- Inviting administrators and delegating access to cloud services
- Connecting Azure Active Directory to Citrix Cloud Japan
- Assigning a primary resource location
- Assigning users to service offerings in the Library
- Monitoring service notifications

Identity providers

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 Azure Active Directory or your on-premises Active Directory instead.

For more information, see Connect Azure Active Directory to Citrix Cloud Japan.

For more information, see Connect Active Directory to 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.

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. 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 commercial Citrix Cloud. 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 commercial Citrix Cloud. For more information, see Select a primary resource location.

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 commercial Citrix Cloud. For more information about notifications, see Notifications.

Add administrators to a Citrix Cloud Japan account

January 8, 2021

Administrators are managed from the Citrix Cloud Japan console. If you want to be added as an administrator to an existing Citrix Cloud Japan account, you must be invited by an existing administrator of the account.

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.

Invite new administrators

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

3. To select administrators using the default identity provider:
   a) From the **Add administrators from…** menu, select **Citrix Identity**.
   b) Enter the email address of the person you want to invite.
4. To select administrators using Azure Active Directory:
   a) From the **Add administrators from…** menu, select **Azure AD**.
   b) Click **Sign In** and provide your credentials for your Azure AD instance.
   c) Type the user name of the person you want to invite. The email address associated with the user name appears.
5. Click **Invite**. Citrix Cloud Japan sends an invitation to the email address you specified and adds the administrator to the list with the status **Invite Sent.** The email is sent from cloud@citrix.com and explains how to access the account.

When the administrator receives the email, they click the **Sign In** link to accept the invitation. Also, a browser window opens, displaying a page where they can create their password.

If the administrator already has an account, Citrix Cloud Japan prompts them to use their existing password and sign in. After accepting the invitation, the administrator receives a welcome email and the Administrators tab shows the administrator as “Active” in the console.

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 Virtual Apps and Desktops service
- 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 in Citrix Cloud Japan, you can configure the access permissions all of your administrators need in accordance with their role in your organization.

To define access permissions

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

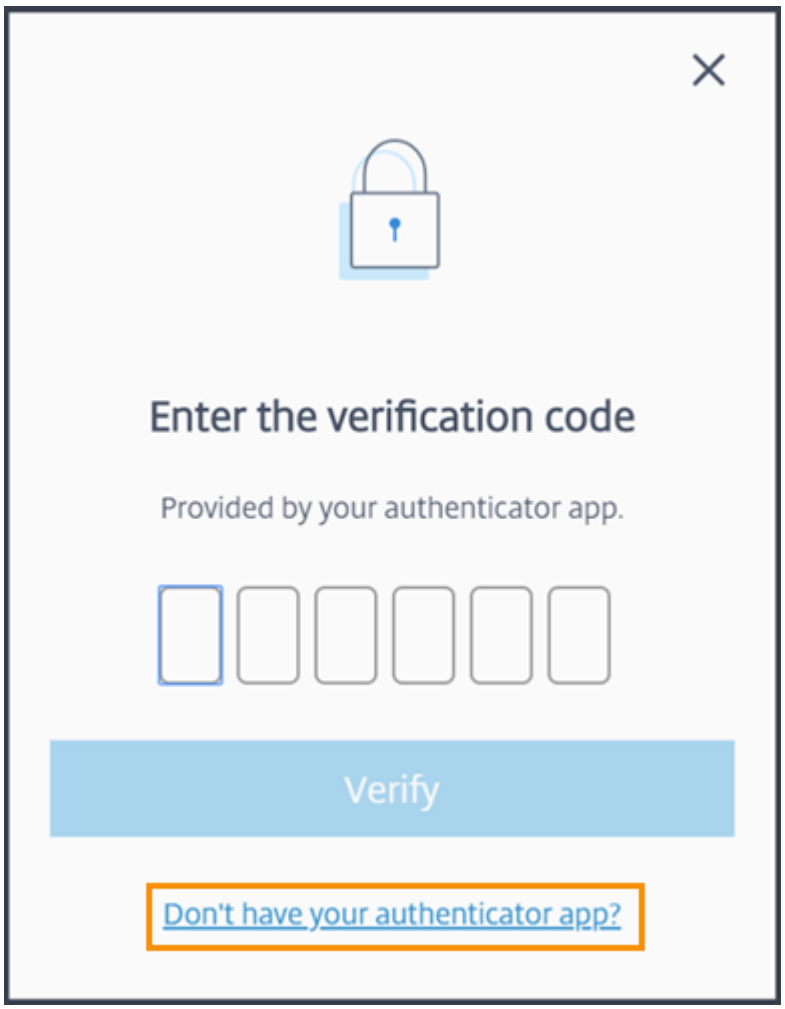
1. Sign in to Citrix Cloud Japan at https://citrixcloud.jp.
2. Click the menu button in the top-left corner of the page and select **Identity and Access Management**.
3. Click the **Administrators** tab.
4. Locate the administrator you want to manage, click the ellipsis button, and select **Edit access**.
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.

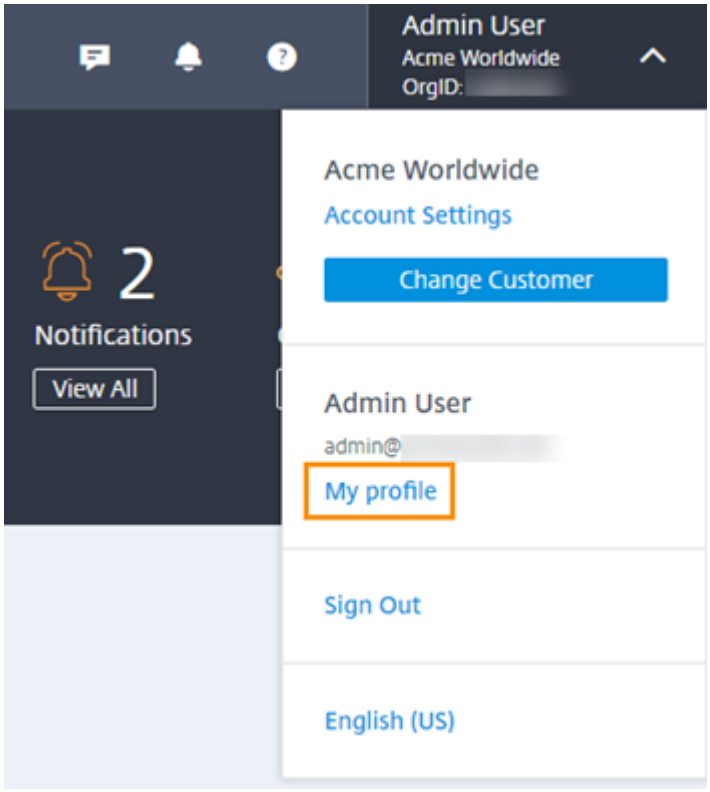
> **Notes**
>
> - Changing your device deletes the current device enrollment and generates a new authenticator app key.
> - If you are re-enrolling with the same authenticator app from your original enrollment, delete the Citrix Cloud Japan entry from your authenticator app before you re-enroll. The 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 recommends 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.

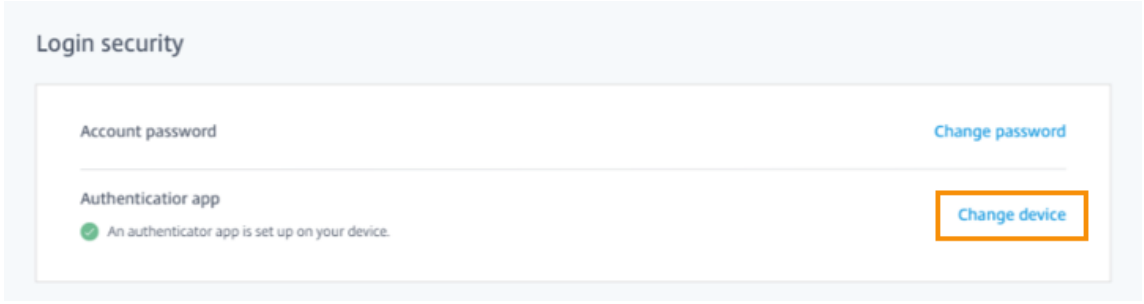


If you don’t have your authenticator app, click **Don’t have your authenticator app?** and select a recovery method to help you sign in. Depending on the recovery method selected, enter the recovery code you received or an unused backup code and select **Verify**.

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



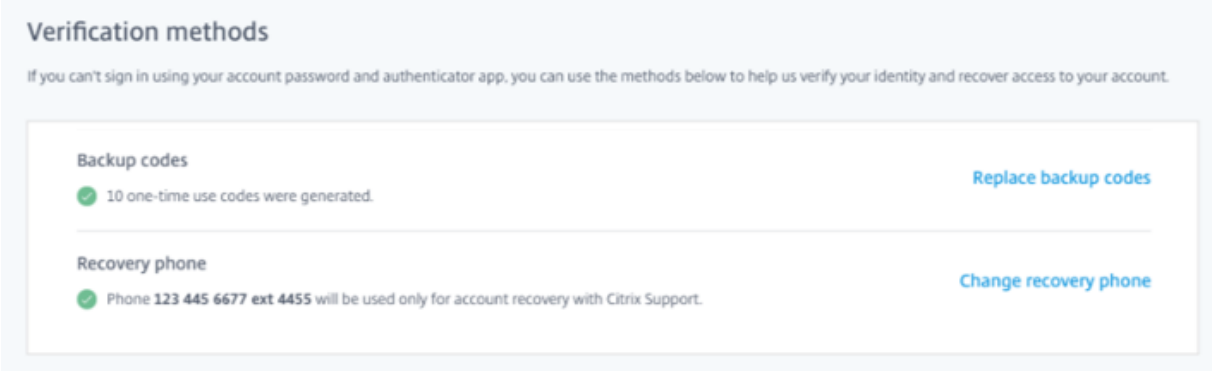
4. In **Authenticator app**, select **Change device**.



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**.

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

SDKs

January 8, 2021

The **Citrix Virtual Apps and Desktops Remote PowerShell SDK** automates complex and repetitive tasks. It provides the mechanism to set up and manage the Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop) 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=CitrixCloudJapan`. This command enables the SDK to run in the context of Citrix Cloud Japan by default.

> 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 Virtual Apps and Desktops 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 snapins: `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 CitrixCloudJapan` 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 Virtual Apps and Desktops service documentation.

> Notes:
>
> - Once authenticated, remote access remains valid in the current PowerShell session for 24 hours. After this time, you must enter your credentials.
> - The Set-XdCredentials cmdlet cannot be used with Citrix Cloud Japan to define credentials. Only the Get-XdAuthentication cmdlet is supported with Citrix Cloud Japan.
> - 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 Limitations in the Virtual Apps and Desktops service documentation.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States