Citrix Cloud Japan
Manage Citrix Cloud Japan administrators 89
System Log 98
Citrix Cloud Japan for Partners 101
SDKs 102
Citrix Gateway service for Citrix Cloud Japan 103
Citrix Cloud Japan

August 16, 2022

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)

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.

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.

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

Configurable console time-outs: Citrix Cloud Japan now includes the ability to specify the length of time that management console sessions can remain idle before they are automatically terminated. For more information, see Console inactivity time-outs.

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.

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 Azure Active Directory groups:** Citrix Cloud Japan now supports adding administrators to your Citrix Cloud Japan account using Azure AD groups. For more information, see Add Azure AD 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 Cloud Japan

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

For more information, see Feature availability for services.

**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**

**August 11, 2022**

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 Gateway**

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
- Contextual access

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

**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.

**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 a complete digital workspace solution that delivers 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 Workspace is generally available to Citrix Cloud Japan customers. The following service features are not available:

- Custom appearance themes for Citrix Workspace app
- Caching to enhance performance for users accessing Workspace through a web browser
- Reauthentication periods to govern the length of time users can stay signed in to Workspace app before needing to sign in again.
- Microapps
- Microsoft Teams integration with Workspace
- Activity feeds in Workspace

For more information, see the Citrix Workspace documentation.
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. The service requires Citrix Cloud Connector version 6.29.0.58841 or later. 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.

Secure Deployment Guide for Citrix Cloud Japan

April 22, 2022

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.
- 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.
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 username.
- 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 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, and must have accepted cipher suites configured.

- If accessing the Citrix Cloud control plane from Windows Server 2016, Windows Server 2019 or Windows Server 2022, the following strong ciphers are recommended: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- If accessing the Citrix Cloud control plane from Windows Server 2012 R2, the strong ciphers are not available, so the following ciphers must be used: TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

For more information about encryption and key management within each cloud service, consult the service’s documentation.
For more information about TLS 1.2 configuration, consult the following articles:

- **CTX245765** Error: “The underlying connection was closed: An unexpected error occurred on a send.” when querying Monitoring Service’s OData endpoint
- Update and configure the .NET Framework to support TLS 1.2 on the Microsoft Docs website.

**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.

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.

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.

<table>
<thead>
<tr>
<th>Client Port(s)</th>
<th>Server Port</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>49152 - 65535/UDP</td>
<td>123/UDP</td>
<td>W32Time</td>
</tr>
</tbody>
</table>
### Citrix Cloud Japan

<table>
<thead>
<tr>
<th>Client Port(s)</th>
<th>Server Port</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>49152-65535/TCP</td>
<td>135/TCP</td>
<td>RPC Endpoint Mapper</td>
</tr>
<tr>
<td>49152-65535/TCP</td>
<td>464/TCP/UDP</td>
<td>Kerberos password change</td>
</tr>
<tr>
<td>49152-65535/TCP</td>
<td>49152-65535/TCP</td>
<td>RPC for LSA, SAM, Netlogon (*)</td>
</tr>
<tr>
<td>49152-65535/TCP/UDP</td>
<td>389/TCP/UDP</td>
<td>LDAP</td>
</tr>
<tr>
<td>49152-65535/TCP</td>
<td>636/TCP</td>
<td>LDAP SSL</td>
</tr>
<tr>
<td>49152-65535/TCP</td>
<td>3268/TCP</td>
<td>LDAP GC</td>
</tr>
<tr>
<td>49152-65535/TCP</td>
<td>3269/TCP</td>
<td>LDAP GC SSL</td>
</tr>
<tr>
<td>53, 49152-65535/TCP/UDP</td>
<td>53/TCP/UDP</td>
<td>DNS</td>
</tr>
<tr>
<td>49152-65535/TCP</td>
<td>49152-65535/TCP</td>
<td>FRS RPC (*)</td>
</tr>
<tr>
<td>49152-65535/TCP/UDP</td>
<td>88/TCP/UDP</td>
<td>Kerberos</td>
</tr>
<tr>
<td>49152-65535/TCP/UDP</td>
<td>445/TCP</td>
<td>SMB</td>
</tr>
</tbody>
</table>

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](https://example.com).

**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](https://example.com) for each service (listed at the beginning of this article)
- [Connectivity Requirements](https://example.com) for supported cloud services
**Viewing Cloud Connector logs**

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

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

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

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

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

**SSL/TLS Configuration**

The Windows Server hosting the Cloud Connector must have the ciphers detailed in [Encryption and key management](#) enabled.

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

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.
- 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

March 30, 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://citrix.citrixcloud.jp/](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](https://www.citrix.com/signup/).
- 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](https://www.citrix.com/support/).

#### Purchasing services

Visit [https://www.citrix.com/buy/](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.

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.

![Support Knowledge Center Menu](image)

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 11, 2022

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 any other Citrix Cloud account, including Citrix Cloud Japan.** For example, if you’re an administrator on a Citrix Cloud account (citrix.cloud.com), 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](https://docs.microsoft.com/en-us/azure/multifactor-authentication/azure-ad-configure-mfa) on the Microsoft website.
- 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](https://docs.microsoft.com/en-us/azure/multifactor-authentication/azure-ad-configure-mfa-change-device).

**To enroll your device in multifactor authentication**

1. Visit [https://citrix.citrixcloud.jp](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.
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 recommends 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://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

April 4, 2022

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

<table>
<thead>
<tr>
<th>Citrix Cloud Japan Trial</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Number of subscribers allowed</strong></td>
</tr>
<tr>
<td><strong>Maximum Length</strong></td>
</tr>
</tbody>
</table>
Citrix Cloud Japan Trial

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>Restricted availability</td>
</tr>
<tr>
<td>Resource location</td>
<td>Customer provided and configured</td>
</tr>
<tr>
<td>User session length</td>
<td>Unlimited</td>
</tr>
<tr>
<td>Local Microsoft Active Directory integration</td>
<td>Yes</td>
</tr>
<tr>
<td>Choice of resource locations</td>
<td>Yes</td>
</tr>
<tr>
<td>Deploy to on-premises</td>
<td>Yes</td>
</tr>
<tr>
<td>Citrix DaaS</td>
<td>Full feature set</td>
</tr>
<tr>
<td>Customizable</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**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/](https://www.citrix.com/buy/).

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

May 4, 2022

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
- 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.

Service connectivity requirements

June 24, 2022
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 address https://citrix-cloud-content.customer.pendo.io/ is contactable.

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

Management console sessions expire based on the inactivity period configured in the Console inactivity time-out setting, located in Account Settings. If a console session becomes idle and the inactivity period elapses, Citrix Cloud automatically terminates the session and prompts the administrator to sign in again. When the session is terminated, any unsaved configuration changes are lost.

For more information, see Console inactivity time-outs in the Citrix Cloud product documentation.

Citrix Cloud Connector

The Citrix Cloud Connector is a software package that deploys a set of services that run on Microsoft Windows servers. The machine hosting the Cloud Connector resides within the network where the resources 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.

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.

<table>
<thead>
<tr>
<th>Required address</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>https://*.citrixworkspacesapi.jp</td>
<td>Provides access to Citrix Cloud APIs that the services use.</td>
</tr>
<tr>
<td>https://*.citrixcloud.jp</td>
<td>Provides access to the Citrix Cloud Japan sign-in interface.</td>
</tr>
<tr>
<td>https://*.blob.core.windows.net</td>
<td>Provides access to Azure Blob Storage, which stores updates for Citrix Cloud Connector.</td>
</tr>
</tbody>
</table>
**Citrix Cloud Japan**

<table>
<thead>
<tr>
<th>Required address</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>https://*.servicebus.windows.net</code></td>
<td>Provides access to Azure Service Bus, which is used by the Active Directory agent and Machine Creation Services.</td>
</tr>
<tr>
<td><code>https://*.cloudapp.net</code></td>
<td>Provides access to Azure Cloud Services, which hosts compute resources and APIs for Citrix Cloud Japan.</td>
</tr>
</tbody>
</table>

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://dlcacerts.digicert.com/DigiCertAssuredIDRootCA.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 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`
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://*.apps.citrixworkspacesapi.net
  - https://*.servicebus.windows.net
- For in-product messages including new features and critical communications: https://citrix-cloud-content.customer.pendo.io/

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

Citrix Workspace

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

Workspace Environment Management service

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

Citrix Cloud Connector requirements

June 30, 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 practice recommendations for configuring Cloud Connector machines for Citrix DaaS (formerly Virtual Apps and Desktops service), see [Scale and size considerations for Cloud Connectors](#).

**Operating systems**

The following operating systems are supported:

- Windows Server 2022
- 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://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
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.
<table>
<thead>
<tr>
<th>Forest Functional Level</th>
<th>Domain Functional Level</th>
<th>Supported Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008 R2</td>
<td>Windows Server 2008 R2</td>
<td>Windows Server 2008 R2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2012,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2012 R2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Windows Server 2008 R2</td>
<td>Windows Server 2012</td>
<td>Windows Server 2012,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2012 R2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Windows Server 2008 R2</td>
<td>Windows Server 2012 R2</td>
<td>Windows Server 2012 R2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Windows Server 2012</td>
<td>Windows Server 2012</td>
<td>Windows Server 2012,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2012 R2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Windows Server 2012</td>
<td>Windows Server 2012 R2</td>
<td>Windows Server 2012 R2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Windows Server 2012 R2</td>
<td>Windows Server 2012 R2</td>
<td>Windows Server 2012 R2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2016</td>
</tr>
</tbody>
</table>

**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 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 located at https://fqdnallowlists.blob.core.windows.net/fqdnallowlist-japan/allowlist.json. This list is grouped by product and includes a change log for each group of FQDNs.

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 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 connection 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 pre-defined set of operations that the Citrix Cloud Agent System can perform.
<table>
<thead>
<tr>
<th>Service Name</th>
<th>Description</th>
<th>Runs As</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Cloud Agent System</td>
<td>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.</td>
<td>Local System</td>
</tr>
<tr>
<td>Citrix Cloud Services Agent WatchDog</td>
<td>Monitors and upgrades the on-premises agents (evergreen).</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Cloud Services Agent Logger</td>
<td>Provides a support logging framework for the Citrix Cloud Connector services.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Cloud Services AD Provider</td>
<td>Enables Citrix Cloud Japan to facilitate management of resources associated with the Active Directory domain accounts in which it is installed.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Cloud Services Agent Discovery</td>
<td>Enables Citrix Cloud Japan to facilitate management of XenApp and XenDesktop legacy on-premises Citrix products.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Cloud Services Credential Provider</td>
<td>Handles storage and retrieval of encrypted data.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Cloud Services WebRelay Provider</td>
<td>Enables HTTP Requests received from WebRelay Cloud service to be forwarded to On-Premises Web Servers.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix CDF Capture Service</td>
<td>Captures CDF traces from all configured products and components.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Config Synchronizer Service</td>
<td>Copies brokering configuration locally for high availability mode.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Service Name</td>
<td>Description</td>
<td>Runs As</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Citrix High Availability Service</td>
<td>Provides continuity of service during outage of central site.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix ITSM Adapter Provider</td>
<td>Automates provisioning and management of virtual apps and desktops.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix NetScaler Cloud Gateway</td>
<td>Provides Internet connectivity to on-premises desktops and applications without the need to open in-bound firewall rules or deploying components in the DMZ.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Remote Broker Provider</td>
<td>Enables communication to a remote Broker service from local VDAs and StoreFront servers.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Remote HCL Server</td>
<td>Proxies communications between the Delivery Controller and the Hypervisor(s).</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Session Manager Proxy</td>
<td>Manages anonymous pre-launched sessions, and uploads session count information to the cloud based Session Manager service.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix WEM Cloud Authentication Service</td>
<td>Provides authentication service for Citrix WEM agents to connect to cloud infrastructure servers.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix WEM Cloud Messaging Service</td>
<td>Provides service for Citrix WEM cloud service to receive messages from cloud infrastructure servers.</td>
<td>Network Service</td>
</tr>
</tbody>
</table>
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 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.

Plan and build your deployment

April 4, 2022

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.

View a video about installing Cloud Connectors:

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

April 4, 2022

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 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) 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.

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

May 25, 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.

Requirements
To use the command line installation 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. To install a Cloud Connector, you must use a secure client which was created by a Full Access administrator, which means the secure client that 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 ensure the security of the secure client details, a JSON configuration file must be provided to the installer. This file must be deleted after the installation has completed. Supported values for the configuration file are:

- **customerName** Required. The customer ID shown on the API Access page in the Citrix Cloud Japan console.
- **clientId** Required. The secure client ID an administrator can create, located on the API Access page.
- **clientSecret** Required. The secure client secret that can be downloaded after the secure client is created. Located on the API Access page.
- **resourceLocationId** Recommended. The unique identifier for an existing resource location. Select the ID button to retrieve the resource location ID on the Resource Locations page in the Citrix Cloud console. If no value is specified, Citrix Cloud uses the ID of the first resource location in the account.
- **acceptTermsOfService** Required. Must be set to `true`.

A sample configuration file:

```json
{
    "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.
Citrix Cloud Japan

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 occurred.
- 2 - A prerequisite check failed.
- 0 - Installation completed successfully.

Citrix Cloud Connector proxy and firewall configuration

March 30, 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:

```
1 netsh winhttp import proxy source =ie
2 <!--NeedCopy-->  
```

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.

Set up workspaces

April 4, 2022

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
- 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.
5. Customize how your end-users launch the apps and desktops that you deliver through your Citrix DaaS deployment.

Identity and access management

July 27, 2022

Identity providers are used for the following purposes:

- Authenticate administrators when they sign in to Citrix Cloud Japan
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.

<table>
<thead>
<tr>
<th>Identity provider</th>
<th>Administrator authentication</th>
<th>Subscriber authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix identity provider</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>(default)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>On-premises Active Directory (AD)</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Azure Active Directory</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>On-premises Citrix Gateway</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Okta</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>SAML 2.0</td>
<td>Yes (AD groups only - preview)</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**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 Azure AD 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 Azure AD 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 Azure AD for administrator authentication, Citrix recommends maintaining at least one full access account under the Citrix identity provider. This ensures that:

- You are not locked out of your Citrix Cloud Japan account in the event you disconnect Azure AD from the management console 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 Azure AD. For example, if Citrix updates the Azure AD application that completes the connection with your Azure AD, you might need to ensure this application is updated in your Citrix Cloud Japan account. Only a full access administrator under the Citrix identity provider can perform this update.
Workspace authentication

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

Prerequisites for identity providers

The following supported identity providers require the Citrix Cloud Connector to be installed in your on-premises environment before connecting with Citrix Cloud Japan:

- 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 delivering applications and desktops through Citrix DaaS (formerly 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
- 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 30, 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.

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 Azure AD authentication is enabled.

Connect Azure Active Directory as an identity provider

August 11, 2022

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) to authenticate Citrix Cloud Japan administrators as well as workspace subscribers.
By using Azure AD with Citrix Cloud Japan, you can:

- 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.

Azure AD applications and permissions

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

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.

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. Select Add administrator/group.
3. In Administrator details, select Azure AD.
4. Type the name of the user you want to add and then click Next. Inviting Azure AD 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 Azure Active Directory. This verifies the user’s email address and completes the connection between the Azure AD user account and Citrix Cloud Japan.

Add Azure AD administrator groups to Citrix Cloud Japan

You can add administrators to your Citrix Cloud Japan account using Azure Active Directory (AD) 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 Add Azure AD administrator groups to Citrix Cloud.

**Sign in to Citrix Cloud Japan using Azure AD**

After the Azure AD 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 Azure AD identity provider for your company. Example: 
  
  [https://citrix.citrixcloud.jp/go/myorganization](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 Azure AD, and click **Continue**.

**Enable Azure AD authentication for workspaces**

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

**Important:**

Before enabling Azure AD workspace authentication, review the [Azure Active Directory](https://azure.microsoft.com/) section for considerations for using Azure AD 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 **Azure Active Directory**.
3. Click **Confirm** to accept the workspace experience changes that will occur when Azure AD authentication is enabled.

**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 use those capabilities automatically.

**Reconnect to Azure AD for the updated app**

In April 2022, the Azure AD 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 Azure AD to Citrix Cloud Japan before April 2022 and you want to use the latest updated app, you need to disconnect your Azure AD 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 Azure AD, verify that you meet the following requirements:

- You must be a Global Admin in Azure AD. When reconnecting your Azure AD, you grant application-level permissions to Citrix Cloud Japan through the Global Admin role in Azure AD. This allows Citrix Cloud Japan to reconnect to Azure AD on your behalf. For more information, see Azure Active Directory 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 Azure AD 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 Azure AD. For instructions, see Invite individual administrators.
- If you are using Azure AD to authenticate workspace subscribers, select a different identity provider temporarily. Citrix Cloud Japan doesn't allow you to disconnect your Azure AD 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 Azure AD

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 Azure Active Directory 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.
6. Select Accept to accept the permissions request.
Azure Active Directory Permissions for Citrix Cloud Japan

June 23, 2022

This article describes the permissions that Citrix Cloud Japan requests when connecting and using Azure Active Directory (AD). Depending on how Azure AD is used with the Citrix Cloud Japan account, one or more enterprise applications might be created in the target Azure AD tenant. You can connect multiple Citrix Cloud Japan accounts to one Azure AD tenant and use the same enterprise applications, without creating a set of applications for each account.

Note:
As of April 2022, the Azure AD app that Citrix Cloud Japan uses to connect your Azure AD was updated to use the GroupMember.Read.All permission instead of the Group.Read.All permission. If you have an existing Azure AD connection (before April 2022) and you want the app to use the new permission, you must disconnect and then reconnect your Azure AD to Citrix Cloud Japan. This action ensures your account is using the latest Azure AD app in Citrix Cloud Japan. For more information, see Reconnect to Azure AD 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 Azure AD enterprise applications that Citrix Cloud Japan uses when connecting and using Azure AD and the purpose for which each application is used.

<table>
<thead>
<tr>
<th>Name</th>
<th>Application ID</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Cloud ProductionJP</td>
<td>f751768a-a91d-4306-af65-448ab59e2c85</td>
<td>Workspace subscriber login</td>
</tr>
<tr>
<td>CC-Directory-ProductionJP</td>
<td>6550e1c7-8970-46bc-82b6-ebd920ff255d</td>
<td>Default connection between Azure AD and Citrix Cloud Japan</td>
</tr>
<tr>
<td>Athena ProductionJP</td>
<td>6464247d-8d40-42b9-a75e-4660db847454</td>
<td>Administrator invitations and logins</td>
</tr>
</tbody>
</table>

Permissions

The permissions in Citrix Cloud Japan’s enterprise applications allow Citrix Cloud Japan to access certain data in your Azure AD tenant. Citrix Cloud Japan uses these data to perform specific functions such as connecting to your Azure AD 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 Azure AD. For more information about Azure AD 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 Azure AD 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 Azure Active Directory. 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 Azure AD.
- **Claim Value:** The string of information that Azure AD 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 Azure AD 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 Azure AD. For example, users from Azure AD can be granted 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 Azure AD. For example, groups from Azure AD can also be granted access to Citrix DaaS applications.
  - **Directory.Read.All:** Citrix Cloud Japan calls List memberOf in Microsoft Graph to get the user’s group membership as Groups.Read.All is not sufficient.

**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 Azure Active Directory resource applications.
### Default connection between Azure AD and Citrix Cloud Japan

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

<table>
<thead>
<tr>
<th>API Name</th>
<th>Claim Value</th>
<th>Permission Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Graph</td>
<td>GroupMember.Read.All</td>
<td>Read all groups</td>
<td>Delegated</td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>User.ReadBasic.All</td>
<td>Read all users’ basic profiles</td>
<td>Delegated</td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>User.Read.All</td>
<td>Read all users’ full profiles</td>
<td>Delegated</td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>User.Read</td>
<td>Sign in and read user profile</td>
<td>Delegated</td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>GroupMember.Read.All</td>
<td>Read all groups</td>
<td>Application</td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>Directory.Read.All</td>
<td>Read directory data</td>
<td>Application</td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>User.Read.All</td>
<td>Read all users’ full profile</td>
<td>Application</td>
</tr>
</tbody>
</table>

### Administrator invitations and logins

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

<table>
<thead>
<tr>
<th>API Name</th>
<th>Claim Value</th>
<th>Permission Name</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Graph</td>
<td>User.Read</td>
<td>Sign in and read user profile</td>
<td>Delegated</td>
</tr>
<tr>
<td>Microsoft Graph</td>
<td>User.ReadBasic.All</td>
<td>Read all users’ basic profiles</td>
<td>Delegated</td>
</tr>
</tbody>
</table>
## Connect an on-premises Citrix Gateway as an identity provider

September 30, 2021

Citrix Cloud Japan supports using an on-premises Citrix Gateway as an identity provider to authenticate subscribers signing into 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
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 Connectors 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.
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:

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.
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.
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**.
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.
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:
   b) On the Create Authentication Policy page, enter the following information:
      • In Name, enter a friendly name for the policy.
      • In Action Type, select LDAP.
      • In Action, select the LDAP authentication server you created earlier.
      • In Expression, enter TRUE.
   c) Click Create to save the configuration.
3. Create the Authentication Policy Label:
   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:
   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 SSO Credentials on the login schema corresponding to the LDAP factor.

Connect Okta as an identity provider

April 4, 2022

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 Connect Citrix Federated Authentication Service to Citrix Cloud.

Tip:
Learn more about supported identity providers with the Introduction to Citrix Identity and Authentication education course. The “Planning Citrix Identity and Access Management” module includes short videos that walk you through connecting this identity provider to Citrix Cloud Japan and enabling authentication for Citrix Workspace.

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
- okta-eu.com
Citrix Cloud Japan

- 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 website. For more information about locating the custom domain for your organization, see Finding Your Okta Domain on the Okta website.

**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 Cloud Japan 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.

**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 website. Afterward, you import your AD users and groups to Okta. When importing, include the SID, UPN, and OID values associated with your AD accounts.

**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.
3. In Sign in method, select OIDC - OpenID Connect and then select Web Application. Select Next.
4. Enter an app integration name.
5. In Grant type, select the following options:
   - Authorization Code
   - Implicit (Hybrid)
7. In Sign-out redirect URIs, enter your Workspace URL from Citrix Cloud Japan.
8. In Assignments, select whether to assign the app integration to everyone in your organization, only groups that you specify, or to assign access later.
9. Select Save.
Citrix Cloud Japan

After you save the app integration, the console displays Client ID and Client Secret values in the Client Credentials sections. 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 itself, 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) Locate the Okta user profile and select Profile. Under Attributes, select Add attribute.
   c) 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
   d) Select Save and Add Another.
   e) 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
   f) Select Save and Add Another.
   g) Enter the following information:
      • Display Name: cip_oid
      • Variable Name: cip_oid
      • Description: AD User GUID
      • Attribute Length: Greater than 1
      • Attribute Required: Yes
   h) Select Save.
3. Edit attribute mappings for the application:
   a) From the Okta console, select Directory > Directory Integrations.
   b) Select the AD you previously integrated. For more information, see Sync accounts with the Okta AD agent.
   c) Select the Provisioning tab and then select Settings > To Okta.
   d) Under Okta Attribute Mappings, map the following attributes. Select Save after modifying each attribute.
      - Select appuser.objectSid and map to the cip_sid attribute.
      - Select appuser.userName and map to the cip_upn attribute.
      - Select appuser.externalId and map to the cip_oid attribute.
   e) 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
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.
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**

August 11, 2022

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. If you want to use SAML authentication with your Azure AD, you have the option to use the Citrix Cloud Japan SAML SSO app from the Azure AD 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: Azure Active Directory single sign-on (SSO) integration with Citrix Cloud SAML SSO on the Azure AD 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 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.
- Joined to the domain where your resources reside. If users access resources in multiple domains, you need to install at least two Cloud Connectors in each domain.
- Connected to a network that can contact the resources that subscribers access through Citrix Workspace.
Citrix Cloud Japan

- 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 can't 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
- Connect your Active Directory (AD) to your Citrix Cloud Japan account by deploying Cloud Connectors in your on-premises AD.
- 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)
- 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 you don’t already have custom attributes that map to the AD user attributes described above, create the custom attributes and map them to 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 have already created custom attributes that map to the required AD user attributes listed earlier in this section, you don’t need to create and map more custom attributes. 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.

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. This task involves configuring your SAML provider with the SAML metadata from Citrix Cloud Japan and then configuring Citrix Cloud Japan with the metadata from your SAML provider to create 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 already have custom attributes for the SID, UPN, OID, and email attributes configured in your SAML provider, you don’t have to perform this task. Proceed to Create a SAML connector application and use your existing custom SAML attributes in Step 8.

**Note:**

The steps in this section describe actions that you perform in your SAML provider’s administration console. The specific commands you use to perform these actions might vary from the commands described in this section, depending on your chosen SAML provider. The SAML provider commands in this section are provided as examples only. Refer to your SAML provider’s documentation for more information about the corresponding commands for your SAML provider.

1. Sign in to the administration console of your SAML provider and select the option for creating custom user attributes. For example, depending on your SAML provider’s console, you might select *Users > Custom User Fields > New User Field*.
2. Add 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

2. From the Citrix Cloud menu, select **Identity and Access Management**.
3. Locate **SAML 2.0** and select **Connect** from the ellipsis menu.
4. When prompted, enter a short, URL-friendly identifier for your company and select **Save and continue**. The **Configure SAML** page appears.
5. Proceed to the next section to configure the SAML connection to Citrix Cloud.

### Configure the SAML provider metadata

In this task, you create a connector application using SAML metadata from Citrix Cloud 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.

**Note:**

Some steps in this section describe actions that you perform in your SAML provider's administration console. The specific commands you use to perform these actions might vary from the commands described in this section, depending on your chosen SAML provider. The SAML provider commands in this section are provided as examples only. Refer to your SAML provider's documentation for more information about the corresponding commands for your SAML provider.

### Create a SAML connector application

1. From your SAML provider's administration console, add an application for an identity provider with attributes and sign response. For example, depending on your provider’s console, you might select **Applications > Applications > Add App** and then select **SAML Test Connector (IdP w/ attr w/ sign response)**.

2. If applicable, enter a display name and save the app.
3. From the **Configure SAML** screen in Citrix Cloud Japan, in **SAML Metadata**, select **Download**. The metadata XML file appears in another browser tab.

   Note:
   If needed, you can also download this file from [https://saml.citrixcloud.jp/saml/metadata.xml](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](https://saml.citrixcloud.jp).
   - In the **Recipient** field, enter [https://saml.citrixcloud.jp/saml/acs](https://saml.citrixcloud.jp/saml/acs).
   - In the field for ACS URL validator, enter [https://saml.citrixcloud.jp/saml/acs](https://saml.citrixcloud.jp/saml/acs).
   - In the field for ACS URL, enter [https://saml.cloud.com/saml/acs](https://saml.cloud.com/saml/acs).

5. Add your custom SAML attributes as parameter values in the application:

<table>
<thead>
<tr>
<th>Create this field</th>
<th>Assign this custom attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>cip_sid</td>
<td>cip_sid or your existing SID attribute</td>
</tr>
<tr>
<td>cip_upn</td>
<td>cip_upn or your existing UPN attribute</td>
</tr>
<tr>
<td>cip_oid</td>
<td>cip_oid or your existing OID attribute</td>
</tr>
<tr>
<td>cip_email</td>
<td>cip_email or your existing email attribute</td>
</tr>
</tbody>
</table>

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 SingleSignOnService 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 Re-
sponse 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.
   - 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 faulty attribute.

To resolve this type of error, ensure 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, the request is made by selecting a tile through the identity provider’s app portal instead of navigating directly to the workspace URL (customer.citrixcloud.jp).
- The SAML certificate is invalid or has expired.
- The authentication context is invalid.
- SAML assertion and response signature is mismatched.

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

![Unable to Process Your Request](https://example.com/error.png)

Transaction ID: 48786352-fb56-4dd9-8775-e745f86db9e7

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).
2. Assign users to both the SAML app and the bookmark app.
3. Change the visibility settings of the SAML app and the bookmark app so that the bookmark app is visible and the SAML app is hidden in the app portal.
4. Disable the Prompt=Login parameter to remove additional password prompts.

**Licensing for Citrix Cloud Japan**

May 4, 2022
Citrix Cloud Japan provides license and usage monitoring for certain cloud services. As well, license and usage monitoring is available for on-premises deployments where Citrix License Server is registered with Citrix Cloud Japan.

All features of license and usage monitoring and license server registration in Citrix Cloud Japan function in the same manner as in Citrix Cloud.

**Licensing for cloud services**

Enterprise customers can monitor license assignments and usage for supported cloud services by selecting **Licensing** from the Citrix Cloud Japan menu.

Currently, license and usage monitoring is available for **Citrix DaaS** only. For more information, see the following articles in the Citrix Cloud documentation:

- Monitor licenses and active usage for Citrix DaaS (User/Device)
- Monitor licenses and peak usage for Citrix DaaS (Concurrent)

**Licensing for on-premises deployments**

Enterprise customers with an on-premises deployment of Citrix Virtual Apps and Desktops can use Citrix Cloud Japan to stay abreast of licenses and usage for both User/Device and Concurrent licensing models. By registering Citrix License Server with Citrix Cloud Japan, customers can use the Licensed Deployments page for the following tasks:

- Monitor the reporting status of registered license servers
- View license assignments and usage trends for deployments that use the User/Device licensing model.
- View peak license usage trends for deployments that use the Concurrent licensing model.

For more information about license and usage monitoring for on-premises Virtual Apps and Desktops deployments, see **Monitor licenses and usage for on-premises deployments** in the Citrix Cloud documentation.

**Licensing for Citrix Service Providers**

Citrix Service Providers (CSP) can use the following tools to understand and report on product licenses and usage:

- License Usage Insights is a free service in Citrix Cloud that collects and aggregates product usage information across single-tenant and multitenant customers. For more information, see **Licensing for Citrix Service Providers** in the Citrix Cloud documentation.
• The Licensing feature in Citrix Cloud enables customers of CSPs to monitor their licenses and usage for Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). CSPs can sign in under their customer’s Citrix Cloud account to view and export this information as well. For more information, see Customer license and usage monitoring for Citrix DaaS in the Citrix Cloud documentation.

Manage Citrix Cloud Japan

April 4, 2022

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.

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 Desktops 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 website.

Primary resource locations

A primary resource location is a resource location that you designate as “most preferred” for communications between your domain and Citrix Cloud 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.

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 organization’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

August 11, 2022
Citrix Cloud Japan

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.
- **Azure AD**: Supports adding administrators individually and through Azure AD groups. Administrators in Azure AD groups are limited to accessing Citrix DaaS only. For more information, see Add Azure AD administrator groups to Citrix Cloud.
- **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.

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.

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 Azure AD, 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 Azure AD is selected, type the name of the user you want to add and then click Next. Inviting Azure AD 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.

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 Azure AD groups (for Azure AD authentication). For more information, see the following articles:

- Add Azure AD administrator groups to Citrix Cloud
- 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. Administrators for Citrix DaaS can use the Library to offer applications and desktops to users instead of using the delivery group wizard. For more information, see Create delivery groups in the Citrix DaaS product documentation.

- **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.

- **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.

- **Secure Client:** Grants access to the Identity and Access Management > API Access > Secure Clients tab. Administrators can create and manage their own secure clients for use with Citrix Cloud APIs. This permission doesn’t include access to the Identity and Access Management > API Access > Product Registrations tab. Only full access administrators can access the Product Registrations tab. For more information, see Monitor licenses and usage for on-premises deployments in the Citrix Cloud product documentation.

- **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.

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**.
Console inactivity time-outs

The **Console inactivity time-out** setting (located in **Account Settings > Company Account**) enables you to specify the length of time that management console sessions can remain idle. When the idle period expires, Citrix Cloud signs out administrators automatically and any unsaved configuration changes are lost.

When enabled, the setting defaults to a minimum idle period of 10 minutes. You can specify a different idle period, up to one hour and 40 minutes.

If the setting is disabled, management console sessions can remain idle for up to 24 hours. Citrix recommends enabling this setting so you can define an idle period that aligns with your organization’s security policies.

This setting functions in the same manner in Citrix Cloud Japan as it does in Citrix Cloud. For more information, see [Console inactivity time-outs](#) in the Citrix Cloud product documentation.

System Log

April 1, 2022

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 organization’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

**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.

<table>
<thead>
<tr>
<th>Date &amp; Time</th>
<th>Actor</th>
<th>Event</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feb 20, 2021 02:47:35 UTC</td>
<td>CwcSystem - administrator</td>
<td>Administrator roles or permissions updated</td>
<td>CwcSystem - administrator</td>
</tr>
<tr>
<td>Feb 19, 2021 11:49:50 UTC</td>
<td>CwcSystem - system</td>
<td>Secure client created</td>
<td>CwcSystem - system</td>
</tr>
<tr>
<td>Feb 18, 2021 02:52:27 UTC</td>
<td>CwcSystem - administrator</td>
<td>TuF Administrator invitation sent</td>
<td>CwcSystem - administrator</td>
</tr>
<tr>
<td>Feb 17, 2021 09:40:55 UTC</td>
<td>CwcSystem - system</td>
<td>Administrator created</td>
<td>CwcSystem - system</td>
</tr>
<tr>
<td>Feb 03, 2021 02:52:27 UTC</td>
<td>CwcSystem - administrator</td>
<td>Administrator access type updated, from 'TuF' to 'Custom'</td>
<td>CwcSystem - administrator</td>
</tr>
<tr>
<td>Feb 02, 2021 07:29:29 UTC</td>
<td>CwcSystem - administrator</td>
<td>Administrator deleted</td>
<td>CwcSystem - administrator</td>
</tr>
</tbody>
</table>

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 secure client. 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 secure client.
- 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.

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 secure client.

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.

Citrix Cloud Japan for Partners

April 29, 2022

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.
Citrix Cloud Japan

SDKs

April 4, 2022

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](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.

   **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.*

© 1999–2022 Citrix Systems, Inc. All rights reserved.
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 `InstallorremovetheRemotePowerShellSDK` 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.

---

**Citrix Gateway service for Citrix Cloud Japan**

April 4, 2022

Citrix Gateway service is generally available for Citrix Cloud Japan. All customers’ traffic passes through dedicated Citrix Cloud Japan POPs only. 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 Virtual 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.

**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.

   ![Configure Connectivity](image)

   Configure Connectivity
   
   Connectivity Type
   
   - Traditional Gateway
   - Gateway Service
   - Internal Only | No external connectivity is set up

   ![Save](image)

   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](#).