



# Citrix Cloud Government

## Contents

<b>What's new in Citrix Cloud Government</b>	<b>3</b>
<b>How to Get Help and Support</b>	<b>5</b>
<b>Secure Deployment Guide for Citrix Cloud Government</b>	<b>10</b>
<b>Service trials for Citrix Cloud Government</b>	<b>15</b>
<b>Sign up for Citrix Cloud Government</b>	<b>18</b>
<b>Connectivity requirements for Citrix Cloud Government</b>	<b>28</b>
<b>Citrix Cloud Connector requirements</b>	<b>31</b>
<b>Create a resource location</b>	<b>39</b>
<b>Install Cloud Connectors from the command line</b>	<b>43</b>
<b>Citrix Cloud Connector proxy and firewall configuration</b>	<b>46</b>
<b>Set up DaaS</b>	<b>47</b>
<b>Set up workspaces for users</b>	<b>49</b>
<b>Citrix Networking</b>	<b>50</b>
<b>Identity and access management for Citrix Cloud Government</b>	<b>51</b>
<b>Connect Active Directory to Citrix Cloud Government</b>	<b>52</b>
<b>Connect Azure Active Directory to Citrix Cloud Government</b>	<b>53</b>
<b>Connect an on-premises Citrix Gateway as an identity provider to Citrix Cloud Government</b>	<b>56</b>
<b>Connect Okta as an identity provider to Citrix Cloud Government</b>	<b>64</b>
<b>Connect SAML as an identity provider to Citrix Cloud Government</b>	<b>71</b>
<b>Manage Citrix Cloud Government</b>	<b>81</b>
<b>Manage Citrix Cloud Government administrators</b>	<b>83</b>
<b>System Log</b>	<b>90</b>
<b>SDKs</b>	<b>93</b>

<b>Citrix Cloud Government platform</b>	<b>95</b>
<b>Workspace Service for Citrix Cloud Government</b>	<b>95</b>

## What's new in Citrix Cloud Government

December 14, 2023

### September 2023

Support for Endpoint Management in Citrix Cloud Government has been deprecated and later removed. For more information, see [Deprecation](#) in the Endpoint Management service documentation.

### August 2022

**Improved administrator management interface:** Citrix Cloud Government 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 Government from AD](#)

**SAML authentication for administrators preview:** Citrix Cloud Government now supports using SAML authentication for administrator groups in AD. For more information, see [Connect SAML as an identity provider to Citrix Cloud Government](#).

### May 2022

**FedRAMP Moderate status:** Citrix DaaS and Citrix Cloud Government have been assigned FedRAMP Moderate. FedRAMP is a program that promotes security standards for cloud services used by US government organizations. US government organizations can deploy virtual apps and desktops in Citrix Cloud Government with Citrix DaaS on Microsoft Azure Government, meeting FedRAMP Moderate status requirements. For more information, see [FedRAMP Moderate status](#).

### 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 Government. View events up to the last 90 days and export events to meet regulatory compliance or for security analysis. For more information, see [System Log](#).

## February 2022

**SAML as identity provider:** Citrix Cloud Government now supports using SAML as an identity provider to authenticate subscribers signing in to their workspaces. For more information, see [Connect Okta as an identity provider to Citrix Cloud Government](#).

## November 2021

**Add administrators in Azure Active Directory groups:** Citrix Cloud Government now supports adding administrators to your Citrix Cloud Government account using Azure AD groups. For more information, see [Manage administrator groups](#).

## September 2021

**Okta as identity provider:** Citrix Cloud Government now supports using Okta as an identity provider to authenticate subscribers signing in to their workspaces. For more information, see [Connect Okta as an identity provider to Citrix Cloud Government](#).

## July 2021

**Citrix Gateway as identity provider:** Citrix Cloud Government now supports using an on-premises Citrix Gateway as an identity provider to authenticate subscribers signing in to their workspaces. For more information, see [Connect an on-premises Citrix Gateway as an identity provider to Citrix Cloud Government](#).

**Multifactor authentication:** Citrix Cloud Government now requires administrators to sign in using multifactor authentication. For more information, see [Enroll in multifactor authentication](#) and [Add administrators to a Citrix Cloud Government account](#).

## June 2021

**System Log preview:** Citrix Cloud Government now includes the System Log preview feature which displays a timestamped list of events that occurred in Citrix Cloud Government. 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](#).

## October 2020

**FedRAMP Ready:** Citrix Workspace is FedRAMP Ready when deployed in Citrix Cloud Government. FedRAMP is a program that promotes security standards for cloud services used by US government

organizations. US government organizations that require FedRAMP Ready cloud services can now use Citrix Workspace and Citrix DaaS (formerly Citrix Virtual Apps and Desktops service) to deliver virtual apps and desktops.

## How to Get Help and Support

December 14, 2023

### Signing in to your account

← → ↻ 🏠 <https://citrix.cloud.us>

# Citrix Cloud Government

## Move Faster, Work Better, Lower IT Costs

A single place to simplify delivery of Citrix technologies. Provide secure access to apps, data and IT tools. Deploy on any cloud or infrastructure.

Enter your Citrix Cloud Government credentials

  
  
  
 Remember me      [Forgot username or password?](#)

Sign in with my organization credentials

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

- Verify you're signing in at <https://citrix.cloud.us> and the sign-in page displays the Citrix Cloud Government logo. Citrix Cloud Government's sign-in URL uses the `.us` top-level domain, not the `.com` top-level domain.

- Make sure you sign in with the **email address** 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 Government](#).
- If your organization allows users to sign in to Citrix Cloud Government using their organization credentials instead of a Citrix Cloud Government account, 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 Government 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 to Citrix Cloud Government](#).

## Changing your password

If you've forgotten or need to reset your Citrix Cloud Government account password, click **Forgot username or password?** and you can enter your account email address. You receive an email to reset your password.

Citrix Cloud Government prompts you to reset your password if your current password is more than 60 days old.

The password you select is case-sensitive and must meet the following requirements:

- At least 12 characters long
- Includes at least one upper-case letter
- Includes at least one lower-case letter
- Includes at least one number
- Includes at least one special character: ! @ # \$ % ^ \* ? + = -

**Important:**

- At least one character in your password must be changed. You cannot use your existing password as your new password.
- You cannot reuse your previous 24 passwords.
- Your new password must be in effect for at least one day before you can change it again.

## Cloud service health

The Citrix Cloud Health Dashboard provides an overview of real-time availability of the Citrix Cloud platform and services in each geographical region. If you experience any issues with Citrix Cloud,

check the Cloud Health Dashboard to verify that Citrix Cloud or specific services are operating normally.

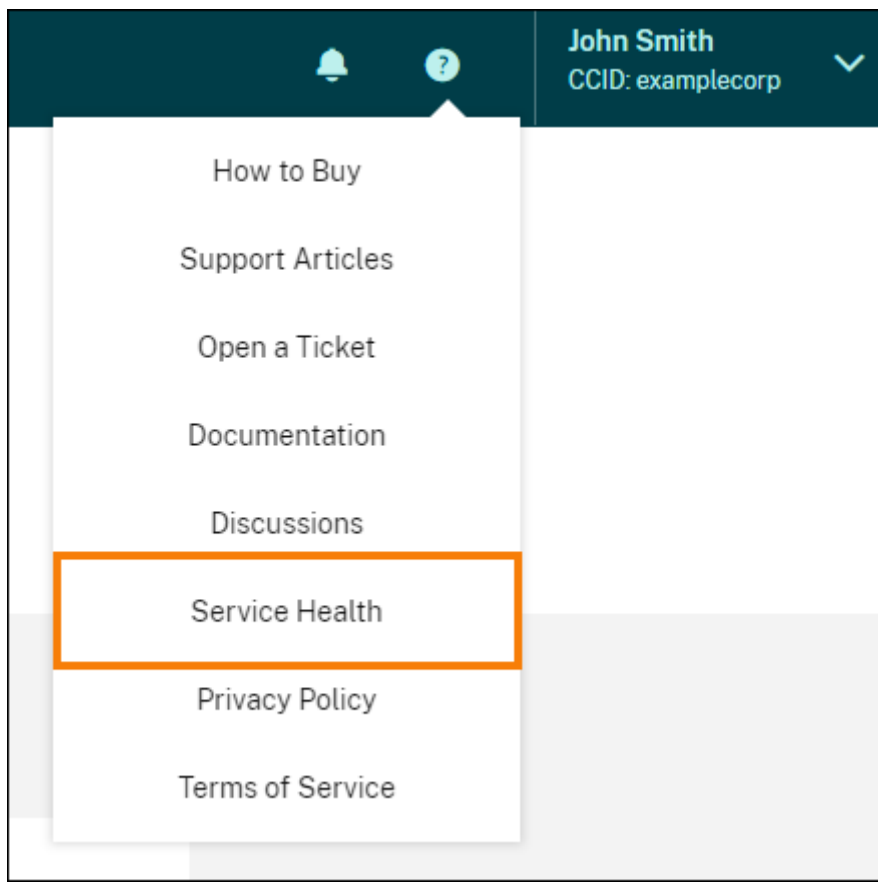
The screenshot shows the Citrix Cloud Health Dashboard. At the top left, it says 'citrix | Cloud Health Dashboard'. On the top right, there is a dropdown menu set to 'EDT' and a 'SUBSCRIBE' button. The main dashboard area has a dark purple background. On the left, there are three white cards: 'UP' with a green circle and the number 54, 'AFFECTED' with a grey circle and the number 0, and 'DOWN' with a grey circle and the number 0. On the right, there is a white panel with 'CURRENT' and 'PLANNED' tabs. Under 'PLANNED', there are two maintenance events for Citrix Analytics Service (CAS) in the EU and APS regions, both scheduled for 04/28/2021. Below the dashboard, there are navigation tabs for 'CURRENT STATUS', 'LIST', and 'CALENDAR'. A legend indicates: green circle for 'Service is operating normally', yellow circle for 'Performance issues', red circle for 'Service disruption', and grey circle for 'N/A'. Below the legend is a table titled 'Citrix Cloud Services'.

SERVICE NAME	AP-S	E.U.	JAPAN	U.S.	US-GOV
Analytics	●	●	●	●	●
Application Delivery Management	●	●	●	●	●

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

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





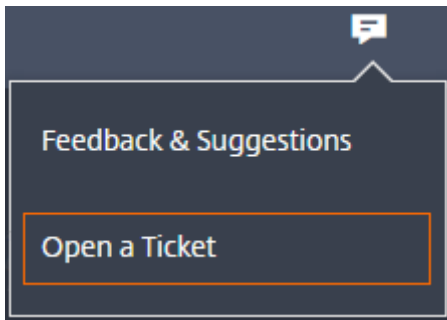
Use the dashboard to learn more about the following conditions:

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

You can also subscribe to notifications about events like maintenance windows and service incidents. For more information about Cloud service health, see [Citrix Cloud service health](#).

## Technical Support

If you're experiencing an issue that requires technical help, click the **Feedback and Support** icon near the top-right of the screen, and then select **Open a Ticket**.



You can then enter the details of the issue in the form that appears. Citrix Technical Support follows up with you to resolve the issue.

### New Support Ticket ✕

---

**Severity**

**High** - There is a critical loss of service that needs immediate attention.

**Medium** - There is a loss of service; operations continue to function in a diminished state.

**Low** - There is a partial, non-critical loss of functionality.

---

You will be contacted within 2 business hours. [Call Support](#) during weekends.

---

**Service**

Select ▼

---

**Subject**

Concise description of the issue. 255

---

**Description**

Provide detailed information about the error message, problem behavior, environment details like Azure, AWS etc...

---

[Submit Ticket](#)

## Secure Deployment Guide for Citrix Cloud Government

December 14, 2023

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

The [Citrix DaaS Technical Security Overview](#) provides similar information for Citrix DaaS (formerly Citrix Virtual Apps and Desktops service).

### Note:

In this article, the term *customer* refers to government agencies and customers in the United States who use Citrix Cloud Government.

## Control Plane

### Guidance for administrators

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

### Password compliance

Citrix Cloud Government prompts administrators to change their passwords if their current password is more than 60 days old. New passwords must meet all the following criteria:

- At least 12 characters long
- Include at least one upper-case and lower-case letter
- Include at least one number
- Include at least one special character: ! @ # \$ % ^ \* ? + = -

Rules for changing passwords:

- At least one character in the current password must be changed. The current password can't be used as a new password.

- The previous 24 passwords can't be reused.
- The new password must be in effect for at least one day before Citrix Cloud Government allows it to be changed again.

## **Encryption and key management**

The control plane does not store sensitive customer information. Instead, Citrix Cloud Government 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 Government is hosted on the Citrix-owned [cloud.us](https://cloud.us) domain. To access Citrix Cloud Government, customers must use a browser capable of TLS 1.2 with strong cipher suites.

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 the 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 Government control plane is hosted in the United States. Customers can't change the host location.

The customer owns and manages the resource locations that they use with Citrix Cloud Government. 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 are stored in resource locations and are under customer control.

## **Audit and change control**

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

Citrix has extensive internal auditing information. If a customer has a concern, they are advised to contact Citrix within 30 days. Citrix reviews the audit logs to determine the administrator who per-

formed an operation. Reviews also the date on which it was performed, the IP address associated with the action.

## **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, the machines on which the Cloud Connector software is installed must be inside the customer's private network and not in the DMZ. For network and system requirements and instructions for installing the Cloud Connector, see [Create a resource location](#).

### **Configuration**

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

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

In the customer's Active Directory (AD), the Cloud Connector's machine account must be restricted to read-only access. In Active Directory it's the default configuration. Also, the customer can enable AD logging and auditing on the Cloud Connector's machine account to monitor any AD access activity.

### **Logging on to the machine hosting the Cloud Connector**

The Cloud Connector contains sensitive security information such as administrative passwords. Only the most privileged administrators are able to log on to the machines hosting the Cloud Connector (for example, to perform maintenance operations). In general, there is no need for an administrator to log on to these machines to manage any Citrix product. The Cloud Connector is self-managing in that respect.

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

### **Installing more 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 more possible security attack vectors and might reduce the security of the overall Citrix Cloud Government solution.

### **Inbound and outbound ports configuration**

The Cloud Connector requires outbound port 443 to be open with access to the internet. The Cloud Connector with 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 more outbound ports with access to the Internet. The Cloud Connector negotiates across a wide range of ports to optimize network bandwidth and performance if more ports are available.

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

---

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

---

Each of the services used within Citrix Cloud Government extends the list of open ports required. For more information, consult [Connectivity requirements for Citrix Cloud Government](#).

### **Monitoring outbound communication**

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

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

During normal operation, the Cloud Connector communicates only with domain controllers in domains that are listed as **Use for subscriptions** on the **Identity and Access Management** page in the Citrix Cloud Government user interface.

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

Each service within Citrix Cloud Government extends the list of servers and internal resources that the Cloud Connector might contact during normal operations. Also, customers cannot control the data that the Cloud Connector sends to Citrix. For more information about services' internal resources and data sent to Citrix, consult [Connectivity Requirements](#).

### Viewing Cloud Connector logs

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

View the 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\Logos.

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

### SSL/TLS Configuration

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

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

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

## Connector updates

When Citrix software updates are available, the Cloud Connector self-manages. Do not disable reboots or put other restrictions on the Cloud Connector. These actions prevent the Cloud Connector from updating itself when there is a critical update.

The customer is not required to take any other action to react to security issues. The Cloud Connector automatically applies any security fixes and updates for Citrix software.

## Guidance for handling compromised accounts

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

## Service trials for Citrix Cloud Government

December 14, 2023

Trials for individual Citrix Cloud Government services are delivered through the Citrix Cloud Government 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.

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

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

## Fast facts about service trials



	Citrix Cloud Government Trial
Number of subscribers allowed	25
Maximum Length	60 calendar days. You can request a trial for the service only once.
Availability	Restricted availability
Resource location	Customer provided and configured
User session length	Unlimited
Local Microsoft Active Directory integration	Yes
Choice of resource locations	Yes
Deploy to on-premises	Yes
Citrix DaaS (formerly Citrix Virtual Apps and Desktops service)	Full feature set
Workspace	Full feature set
Customizable	Yes

## Request a service trial

To request a service trial, you need to speak to a Citrix sales representative and provide your Organization ID (OrgID). The sales representative ensures 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 Government 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 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 some partici-

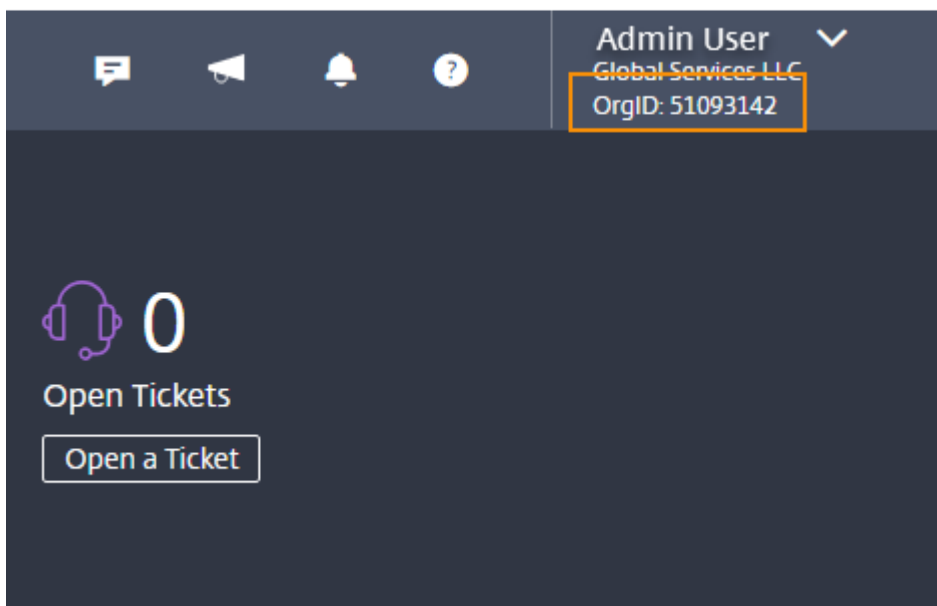
pants at any given time.

## Purchase services

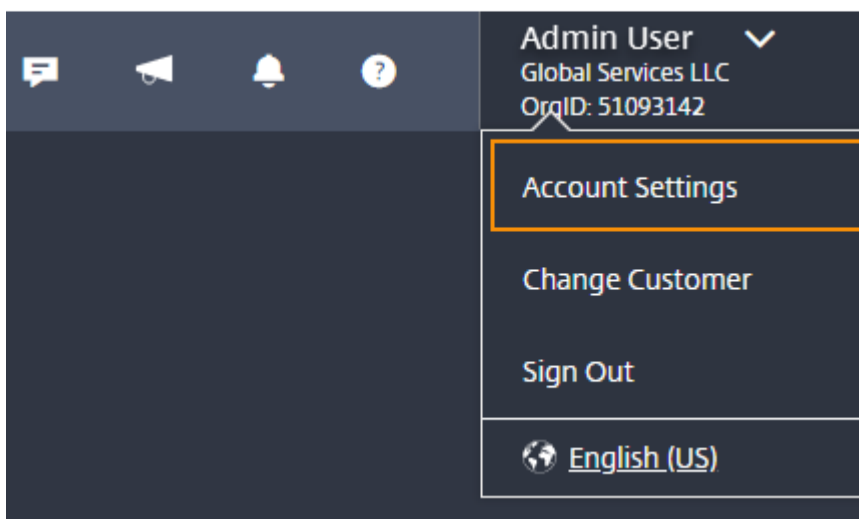
When you're ready to convert your trial to a production service, contact a Citrix sales representative.

To complete the purchase, you need your OrgID, available in the Citrix Cloud Government 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.

The screenshot shows the Citrix Cloud interface. At the top, there is a dark blue header with a hamburger menu icon and the text "Citrix Cloud". Below this is a breadcrumb trail: "← Account Settings". Underneath, there are three tabs: "Company Account" (which is selected and underlined), "My Profile", and "Orders". The main content area displays account details in a light blue box. It includes the following fields:

- Account Name:** Global Services LLC | Edit
- Address:** [Redacted]
- Phone:** [Redacted]
- Organization ID:** 51093142 (This field is highlighted with an orange border)
- Region:** Citrix Cloud US

**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.

## Sign up for Citrix Cloud Government

December 4, 2023

This article walks you through the process of signing up for Citrix Cloud Government 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 Government account. Your OrgID is associated with a physical site address, typically your company's business address. Organizations usually have a single OrgID. If you have different branch offices or have different departments that manage your assets separately, Citrix allows an organization to have multiple OrgIDs.

## What is a Citrix Cloud Government account?

A Citrix Cloud Government account enables you to use one or more Citrix Cloud Government services to securely deliver your apps and data. Citrix Cloud Government creates a uniquely identified OrgID account. It's important to use the right Citrix Cloud Government account, based on how your organization has set up OrgIDs. Your purchases and administrator access can continue on the same OrgIDs.

## Multifactor authentication requirements

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

## Try Citrix Cloud Government

### Complete the sign-up form

Visit <https://onboarding.cloud.us> and complete the sign-up form.

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

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

### Accept the terms of service

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

Agree to the Terms of Service and then click **Continue**. Citrix Cloud Government 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 Government confirmation page in your browser.

### **Create a password and sign in**

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

The password you select is case-sensitive and must include the following criteria:

- At least 12 characters long
- At least one upper-case letter
- At least one lower-case letter
- At least one number
- At least one special character: ! @ # \$ % ^ \* ? + = -

You can then sign in to [Citrix Cloud Government](#) using the email address and password you chose earlier.

## **Purchase Citrix Cloud Government**

### **Order Citrix Cloud Government**

To order Citrix Cloud Government 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 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 Government setup page displays in a browser window, showing your order details. Click **Continue**.

## Create a password

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

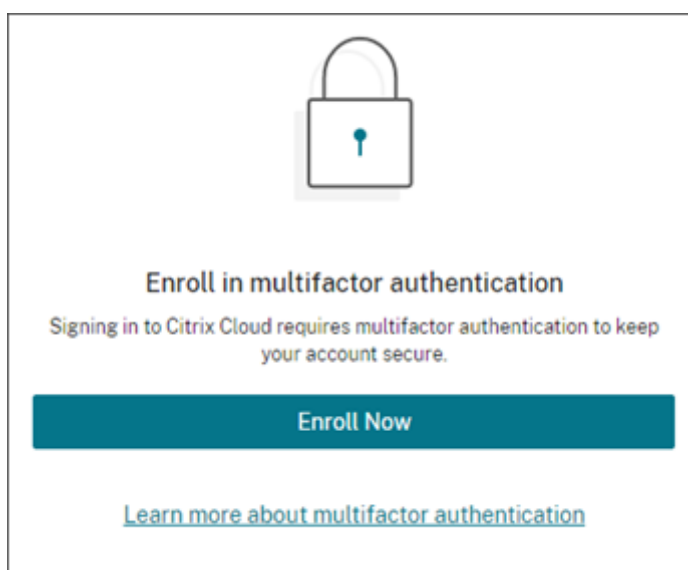
## Sign in with your Citrix Cloud Government credentials

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

## Enroll in multifactor authentication

To keep your administrator account safe and secure, Citrix Cloud Government 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 the account is safe and secure.

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



During enrollment, Citrix Cloud Government presents a QR code and a key. Depending on your authenticator app, you either scan the QR code or enter the key to register your device.

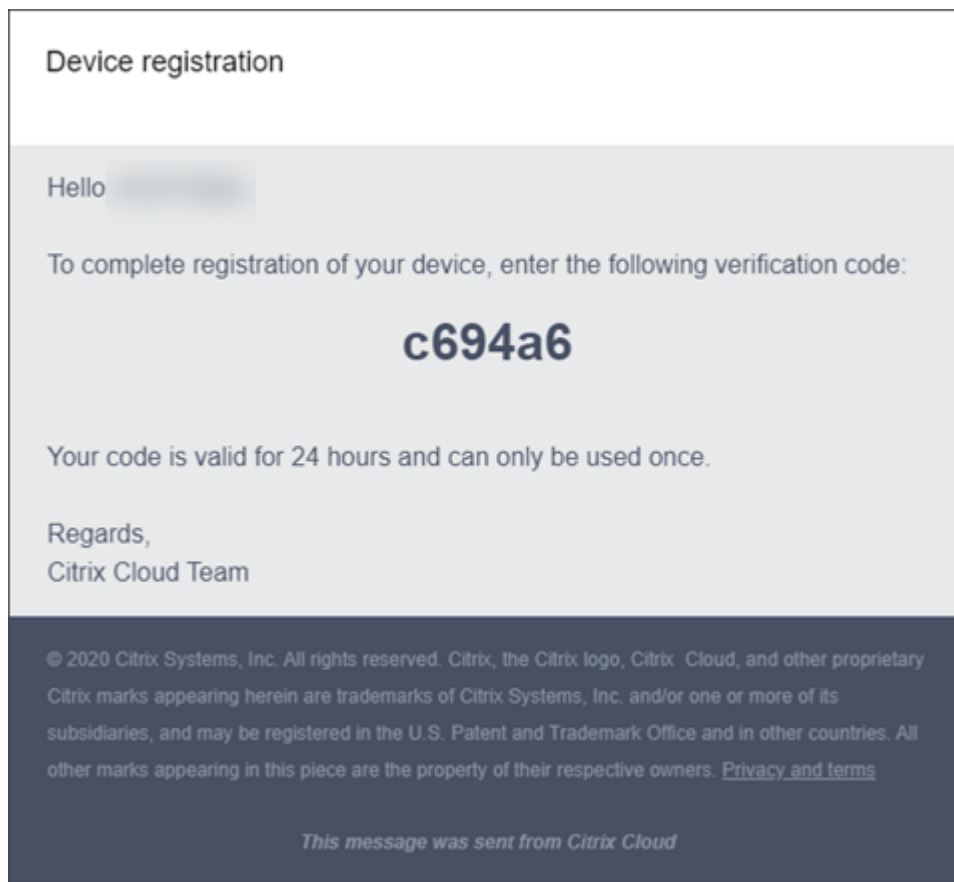
For a smooth enrollment process, Citrix recommends downloading and installing this app on your device beforehand. Citrix Cloud Government also generates one-time use backup codes. The back-up codes are used to access your account in the event you lose your device or when you can't use your authenticator app.

**Notes:**

- When signing in to Citrix Cloud Government, verify that you're viewing the Citrix Cloud Government sign-in page at <https://citrix.cloud.us>. If you sign in to Citrix Cloud Government using a different URL, enrollment in multifactor authentication fails.
- After you enroll, multifactor authentication is used for all customer organizations that you belong to in Citrix Cloud Government. 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 Government deletes the current device enrollment and replaces it with the new device. For more information, see [Change your device for multifactor authentication](#).

To enroll your device in multifactor authentication:


1. Go to Citrix Cloud Government at <https://citrix.cloud.us> and verify that the URL redirects to <https://citrix.cloud.us>. Sign in using your Citrix Cloud Government credentials. Citrix Cloud Government sends you an email with a verification code.



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



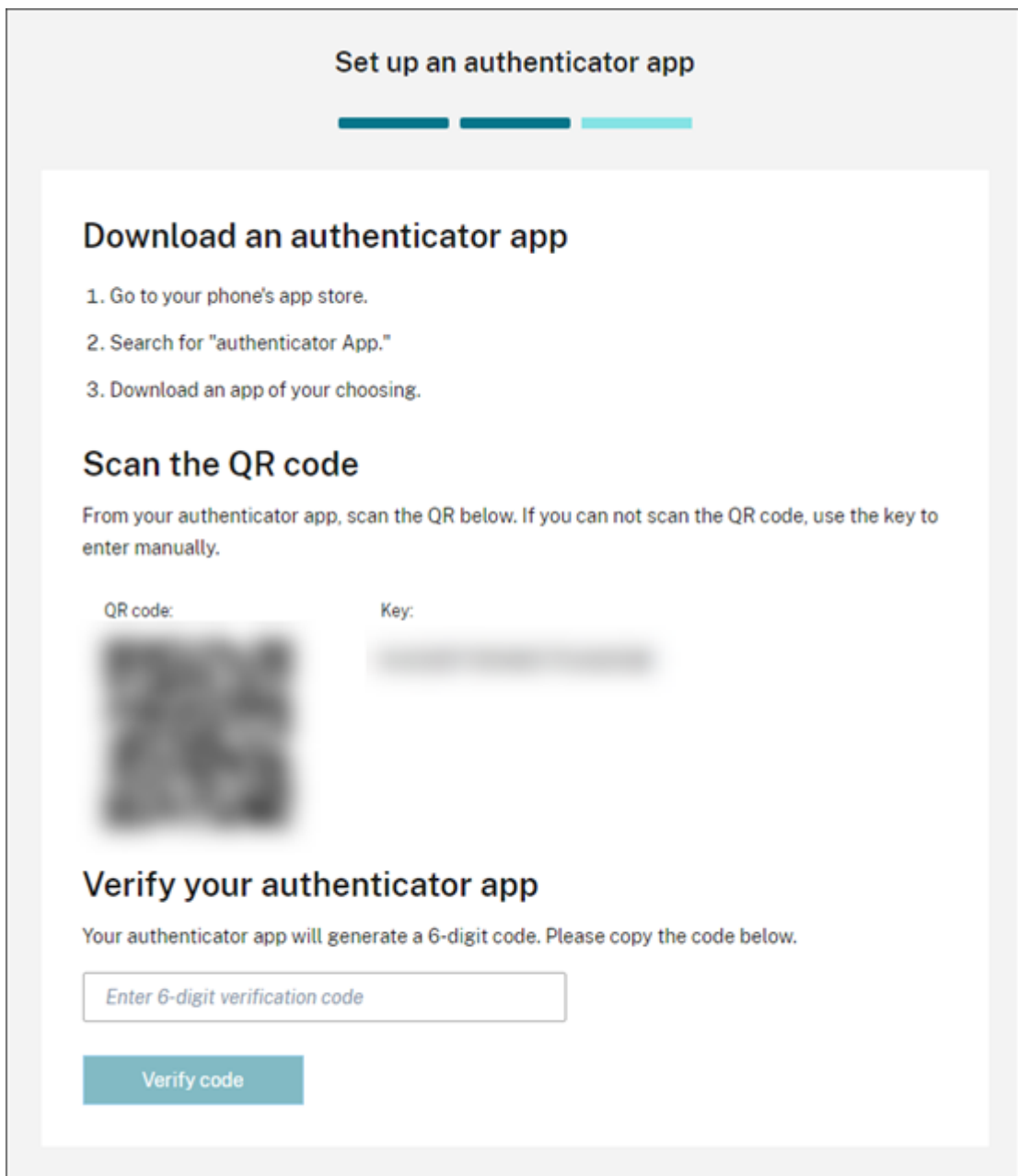
## Set up an authenticator app



### First, we need to verify your account

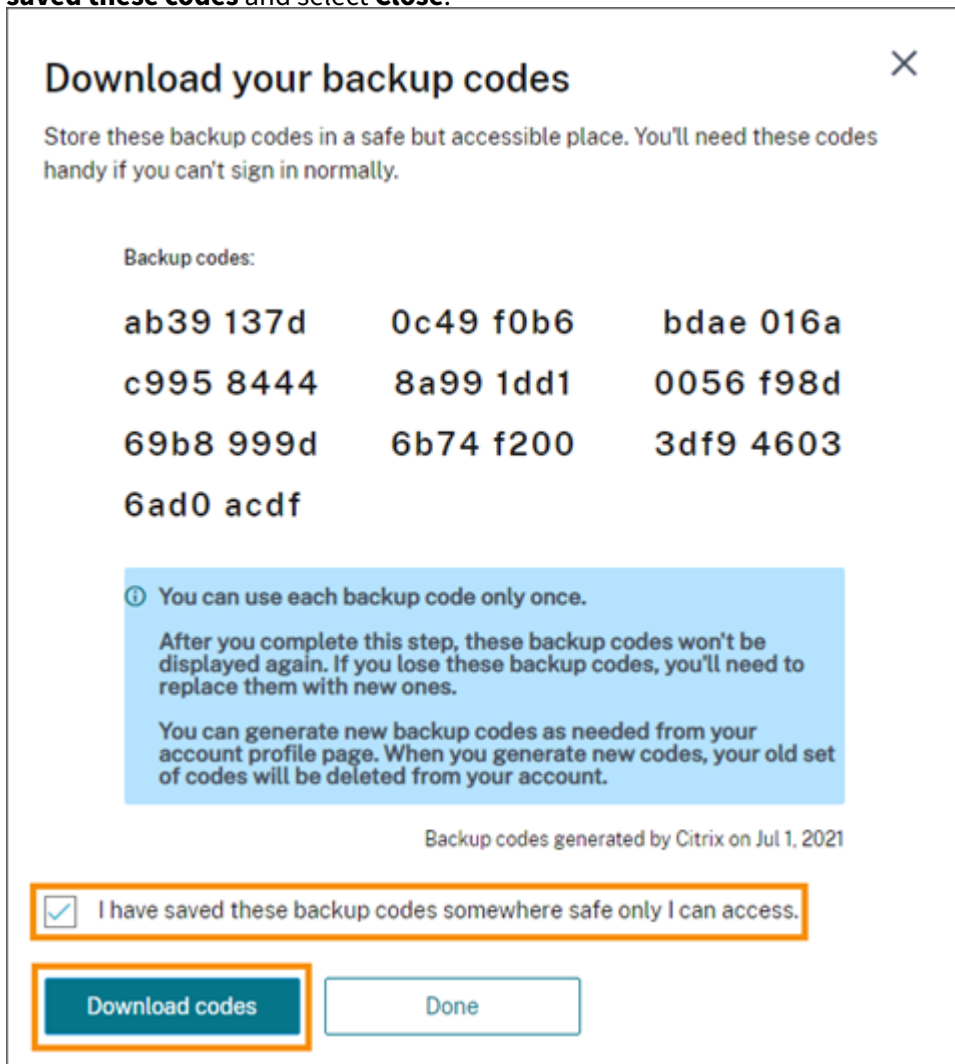
We sent an email to    
Please check your inbox for an email from donotreplynotifications@citrix.com and enter the 6-digit verification code below, followed by your Citrix account password.

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



4. Under **Verify your authenticator app**, enter the code from your authenticator app and select **Verify code**.
5. Configure the following account recovery methods in case 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 code as a text file. Then, select **I've saved these codes** and select **Close**.



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

When your enrollment is completed, the Citrix Cloud console appears. From the top-right menu, select **My Profile**. After successful enrollment, the **Authenticator app** section displays a green check mark and the My Profile page displays your configured recovery methods.

## My profile


### Personal info

Name

Email

### Login security


**Authenticator app**

 An authenticator app is set up on your device. [Change device](#)

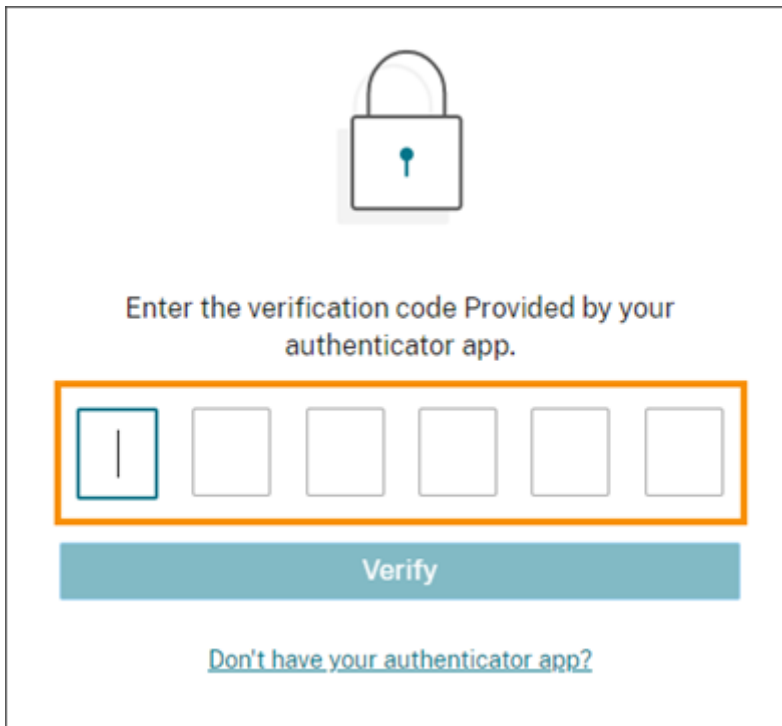
### Verification methods

If you can't sign in using your account password and authenticator app, you can use the methods below to help us verify your identity and recover access to your account.

**Backup codes**

 10 one-time use codes were generated. [Replace backup codes](#)

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



Enter the verification code Provided by your authenticator app.

Verify

[Don't have your authenticator app?](#)

After you enroll in multifactor authentication, signing in to your Citrix Cloud Government account brings you to the Citrix Cloud console page. If you need to register a different device, generate more backup codes. Update your recovery phone number later, so that you can perform these tasks from your My Profile page.

For more instructions, see [Manage your primary MFA method](#) in the Citrix Cloud product documentation.

## Connectivity requirements for Citrix Cloud Government

May 13, 2024

Citrix Cloud Government 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 the customer's resources and Citrix Cloud Government.

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.

## Transport Layer Security requirements

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

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

## Citrix Cloud Government management console

The Citrix Cloud Government management console is a web-based console that you can access after signing in to <https://citrix.cloud.us>. The console's webpages requires more Internet resources when signing in or performing specific operations.

## Configurable inactivity timeout for console

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

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

When the feature is disabled, there is no inactivity timer, and administrators will be logged out only when the 12-hour session limit is reached.

### Note:

- This feature is enabled by default.
- The configurable inactivity timeout is 10 minutes to 1 hour.
- The default inactivity timeout is 15 minutes.

## Proxy configuration

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

## Firewall configuration

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

## Citrix Cloud Connector

The Citrix Cloud Connector is a software package that deploys a set of services that run on Microsoft Windows servers. The machine hosting the Cloud Connector resides within the network where the resources that you use with Citrix Cloud Government reside. The Cloud Connector connects to Citrix Cloud Government, 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 more access requirements depending on the Citrix Cloud Government service with which it is being used.

## 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 available at <https://fqdnallowlists.blob.core.windows.net/fqdnallowlist-gov/allowlist.json>. The list is categorized by the 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**.

## Citrix DaaS service connectivity

Citrix resource location / Cloud Connector:

- [https://\\*.citrixworkspacesapi.us](https://*.citrixworkspacesapi.us)
- [https://\\*.cloud.us](https://*.cloud.us)
- [https://\\*.apps.cloud.us](https://*.apps.cloud.us)
- [https://\\*.blob.core.usgovcloudapi.net](https://*.blob.core.usgovcloudapi.net)
- [https://\\*.servicebus.usgovcloudapi.net](https://*.servicebus.usgovcloudapi.net)
- [https://\\*.xendesktop.us](https://*.xendesktop.us)

Administration console:

- [https://\\*.citrixworkspacesapi.us](https://*.citrixworkspacesapi.us)
- [https://\\*.cloud.us](https://*.cloud.us)
- [https://\\*.blob.core.usgovcloudapi.net](https://*.blob.core.usgovcloudapi.net)
- [https://\\*.xendesktop.us](https://*.xendesktop.us)

## Citrix Cloud Connector requirements

June 18, 2024

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

See also our best practice recommendations for Cloud Connector machine configuration for Citrix DaaS (formerly Citrix Virtual Apps and Desktops service): [Scale and size considerations for Cloud Connectors](#).

### Operating systems

The following operating systems are supported:

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

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

### .NET requirements

Microsoft .NET Framework 4.7.2 or later is required.

### Server requirements

- 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.



## Windows Update guidance

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

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

### Note:

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

## Certificate validation requirements

Cloud Connector binaries and endpoints that the Cloud Connector contacts are protected by X.509 certificates issued by widely respected enterprise certificate authorities (CAs). Certificate verification in Public Key Infrastructure (PKI) includes the Certificate Revocation List (CRL).

When a client receives a certificate, the client checks whether it trusts the CA that issued the certificate. Also, checks whether the certificate is on a CRL. If the certificate is on a CRL, the certificate is revoked and can't 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. Ensure that the Cloud Connector software can be installed successfully.

Citrix Cloud endpoints are protected by certificates issued by DigiCert or by one of the Root Certificate Authorities which is 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 website.
  - <http://cacerts.digicert.com/>
  - <http://dl.cacerts.digicert.com/>
  - <http://crl3.digicert.com>
  - <http://crl4.digicert.com>
  - <http://ocsp.digicert.com>
  - <http://www.d-trust.net>
  - <http://root-c3-ca2-2009.ocsp.d-trust.net>
  - <http://crl.microsoft.com>
  - <http://oneocsp.microsoft.com>
  - <http://ocsp.msocsp.com>
- Communication with the following addresses is enabled:
  - [https://\\*.digicert.com](https://*.digicert.com)
- The following root certificates are installed:
  - <https://cacerts.digicert.com/DigiCertAssuredIDRootCA.crt>
  - <https://cacerts.digicert.com/DigiCertGlobalRootG2.crt>
  - <https://cacerts.digicert.com/DigiCertGlobalRootCA.crt>
  - <https://cacerts.digicert.com/DigiCertTrustedRootG4.crt>
  - <https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt>
  - [https://www.d-trust.net/cgi-bin/D-TRUST\\_Root\\_Class\\_3\\_CA\\_2\\_2009.crt](https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_2009.crt)
  - <https://www.microsoft.com/pkiops/certs/Microsoft%20RSA%20Root%20Certificate%20Authority%202017.crt>
  - <https://www.microsoft.com/pkiops/certs/Microsoft%20EV%20ECC%20Root%20Certificate%20Authority%202017.crt>
  - <https://www.microsoft.com/pkiops/certs/Microsoft%20ECC%20Root%20Certificate%20Authority%202017.crt>

- The following intermediate certificates are installed:
  - <https://cacerts.digicert.com/DigiCertTrustedG4CodeSigningRSA4096SHA384.crt>
  - <https://cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA.crt>

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

For complete instructions for downloading and installing the certificates, see [CTX223828](#).

### Active Directory requirements

- Joined to an Active Directory domain that contains the resources and users that you use to create offerings for your users. For multi-domain environments, see [Deployment scenarios for Cloud Connectors in Active Directory](#) in this article.
- Each Active Directory forest that you plan to use with Citrix Cloud Government must be reachable by two Cloud Connectors always.
- The Cloud Connector must be able to reach the parent (root) domain controllers and the child domain controllers in the Active Directory infrastructure. In order, 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 use in your resource location. For more information, see [Cloud Connector Proxy and Firewall Configuration](#).
- Connected to the Internet. For more information, see [Internet Connectivity Requirements](#).

### Supported Active Directory functional levels

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

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

### Federal Information Processing Standard (FIPS) support

The Cloud Connector currently supports the FIPS-validated cryptographic algorithms that are used on FIPS-enabled machines. Only the latest version of the Cloud Connector software available in Citrix Cloud Government 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:

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 Government 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](#).

## Deployment scenarios for Cloud Connectors in Active Directory

If you have a single domain in a single forest, installing Cloud Connectors in that domain is all you need to establish a resource location. However, if you have multiple domains in your environment, you need to consider where to install the Cloud Connectors. For users to access the resources you make available through Citrix Cloud Government.

### Note:

The resource locations mentioned form a blueprint that needs to be repeated in other physical locations that depend on where your resources are hosted.

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

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

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

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

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

- Trust relationship: Parent/child domain trust

- Domains listed in **Identity and Access Management**: forest1.local, user.forest1.local
- User logons to Citrix Workspace: Supported for all users
- User logons to an on-premises StoreFront: Supported for all users

**Note:**

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

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

In this scenario, one forest (forest1.local) contains your resource domain and one forest (forest2.local) contains your user domain. A trust exists between these forests that allows users to log on to resources. One set of Cloud Connectors is deployed in a single resource location and joined to the forest1.local domain.

- Trust relationship: Forest trust
- Domains listed in **Identity and Access Management**: forest1.local
- User logons to Citrix Workspace: Supported for forest1.local users only
- User logons to an on-premises StoreFront: Supported for all users

**Note:**

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

Because Cloud Connectors can't traverse forest-level trusts, the forest2.local domain is not displayed on the **Identity and Access Management** page in the Citrix Cloud Government console. The console carries the following limitations:

- Resources are published only to users and groups available in forest1.local in Citrix Cloud Government. However, forest2.local users are nested into forest1.local security groups to mitigate this issue.
- Citrix Workspace cannot authenticate users from the forest2.local domain.

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

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

In this scenario, one forest (forest1.local) contains your resource domain and one forest (forest2.local) contains your user domain. A trust exists between these forests that allows users to log on to resources.

One set of Cloud Connectors is deployed within the forest1.local domain and a second set is deployed within the forest2.local domain.

- Trust relationship: Forest trust
- Domains listed in **Identity and Access Management**: forest1.local, forest2.local
- User logons to Citrix Workspace: Supported for all users
- User logons to an on-premises StoreFront: Supported for all users

### **Installation requirements**

- Download the Cloud Connector software only from Citrix Cloud Government and install it on prepared machines. By default the Cloud Connector installer attempts to connect with the control plane from which it is downloaded. So, if you attempt to install the software downloaded from a commercial Citrix Cloud account, the installer doesn't connect with Citrix Cloud Government.
- Because the Cloud Connector software is downloaded, your browser must allow downloading executable files.

### **Important usage considerations**

- Keep all Cloud Connectors powered on always to ensure an always-on connection to Citrix Cloud Government.
- 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. The two connectors installed ensure the connection between Citrix Cloud Government and your resource location remains intact in the event any single Cloud Connector becomes unavailable.
- Each Active Directory forest that you plan to use with Citrix Cloud Government is reachable by two Cloud Connectors always.
- After installation, do not move the machine hosting the Cloud Connector into a different domain. If the machine must be joined to be a different domain, uninstall the Cloud Connector. Reinstall it after the machine is joined to the different domain.

### **View the health of the Cloud Connector**

The Resource Locations page in Citrix Cloud Government displays the health status of all the Cloud Connectors in your resource locations.

## Troubleshoot the Cloud Connector

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

There seems to be a connectivity issue between Citrix Government and the Cloud Connector, as the status is "disconnected". Although the event logs don't indicate any connectivity issues between the Cloud Connector and Citrix Government, contact support for assistance [Contact Citrix Support](#).

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. The issue persists, contact Citrix Support.

To troubleshoot common issues with installing or using the Cloud Connector, refer to [CTX221535](#).

### Event messages

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)

### Event logs

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

## Create a resource location

December 5, 2023

After you sign up for Citrix Cloud Government, 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 Citrix 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 that host the applications and desktops. You might want to deliver 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.
- A Citrix Gateway to enable external users to access applications and desktops securely.

## Default resource locations

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

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

## Task 1: Prepare machines

1. Review [Citrix Cloud Connector requirements](#) for 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. Make sure port 443 (HTTPS) is open for outbound connections.
3. Ensure that the required addresses can be contacted so that you can operate and consume Citrix Cloud Government services.
4. Review [Citrix Cloud Connector proxy and firewall configuration](#) for information about using the Cloud Connector with a web proxy.

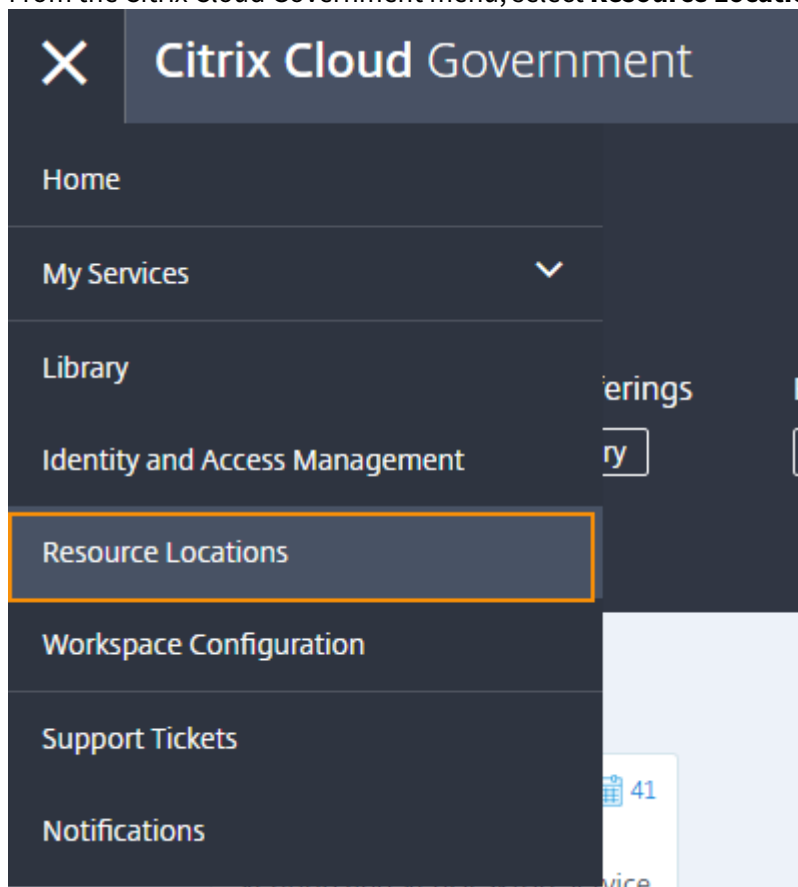
### Task 3: Install Cloud Connectors

**Note:**

Connector Appliance is not available for Citrix Cloud Government.

During installation, the Cloud Connector requires access to the cloud to authenticate the user to perform the installation. Validates the installer's permissions, download, and configure the services that the Cloud Connector provides. The installation occurs with the privileges of the user who initiates the install.

1. From the Citrix Cloud Government menu, select **Resource Locations**.



2. Click **Download** to download the Cloud Connector installer.

3. Double-click the installer. Citrix Cloud Government performs an initial connectivity check and prompts you for your Citrix Cloud Government administrator user name and password.
4. Follow the wizard to install and configure the Cloud Connector. When the installation finishes, Citrix Cloud Government performs a final connectivity check to verify that the Cloud Connector can communicate with Citrix Cloud Government.

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

**Notes:**

- If you're an administrator for multiple organization accounts, Citrix Cloud Government prompts you to select the account you want to associate with the Cloud Connector.
- Use of the same Cloud Connector installer for repeated installations over a period isn't recommended.
- Download a new Cloud Connector from the Resource Locations page in the Citrix Cloud Government console.

### Configure connectivity for users

Provide internal or external access to the services that you make available in the resource location. Secure access for external users requires an existing Citrix Gateway in your environment.

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

**Configure Connectivity** ✕

Connectivity Type

Traditional Gateway

Gateway Service

Internal Only | No external connectivity is set up

2. To configure secure access for external users using an on-premises Gateway:
  - a) Select **Traditional Gateway**.
  - b) Enter the external FQDN of the Citrix Gateway. Example: mynsg.my-domain.com

3. To use the Citrix Gateway service to provide secure access to applications and desktops for external users, select **Gateway Service**
4. To configure internal-only access, select **Internal only**.
5. Click **Save**.

### Create more resource locations

1. From the Citrix Cloud Government management console, click the menu button and select **Resource Locations**.
2. Click **Resource Location** and enter a friendly name.
3. Click **Save**. Citrix Cloud Government displays a tile for the new resource location.
4. Click **Cloud Connectors** and then click **Download** to acquire the Cloud Connector software.
5. On each prepared machine, install the Cloud Connector software using either the installation wizard or the [command-line installation](#). Citrix Cloud Government prompts you to select the resource location you want to associate with the Cloud Connector.

### Cloud Connector installation logs

Cloud Connector installation logs are located at `%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup`.

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

## Install Cloud Connectors from the command line

December 4, 2023

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

During installation, the Cloud Connector requires access to the cloud to authenticate the user installation. Validate the installer's permissions, download, and configure the services the Cloud Connector provides. The installation occurs with the privileges of the user who initiates the install.

#### **Important:**

Using the same installer for repeated installations over a period isn't recommended. Download a new Cloud Connector from the Resource Locations page in the Citrix Cloud Government console.

## Requirements

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

- The customer ID of the Citrix Cloud Government account for which you're 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 that your access to the Citrix Cloud API is secured appropriately. When you create a secure client, the client operates as much with administrator permissions that you have.
- To install a Cloud Connector, you must use a secure client with a Full Access administrator also a full access permission.
- 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 Government uses the ID of the default resource location.

## Create a secure client

When creating a secure client, Citrix Cloud Government generates a unique client ID and secret. You must supply these values when API calls through the command line.

1. From the Citrix Cloud Government 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 Government 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. You can also select **Copy** to manually acquire each value. When finished, select **Close** to return to the console.

## Supported parameters

Make sure 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 Government console.
- **clientId** Required. The secure client ID that an administrator can create, available on the API Access page.
- **clientSecret** Required. The secure client secret that can be downloaded after the secure client is created. Available 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:

```
1 {
2
3 "customerName": "*CustomerID*",
4 "clientId": "*ClientID*",
5 "clientSecret": "*ClientSecret*",
6 "resourceLocationId": "*ResourceLocationId*",
7 "acceptTermsOfService": "true",
8 }
9
10 <!--NeedCopy-->
```

A sample command line that installs using the parameter file:

```
1 CWCCconnector.exe /q /ParametersFilePath:c:\cwccconnector_install_params.
  json
2 <!--NeedCopy-->
```

Use **Start /Wait CWCCconnector.exe /ParametersFilePath:value** to examine a potential error code if there's a failure. You can use the standard mechanism of running **echo %ErrorLevel%** after the installation completes.

## Troubleshooting

### Installation Logs

Installation logs are available at **%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup**. Also, logs are added to **%ProgramData%\Citrix\WorkspaceCloud\InstallLogs** after installation.

### Exit codes

- 1603 - An unexpected error occurred.

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

## Considerations for cloned machines

Each machine hosting the Cloud Connector must have a unique SID and connector ID so that Citrix Cloud Government 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 don't run and the machine cannot connect to Citrix Cloud Government.

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.

## Citrix Cloud Connector proxy and firewall configuration

December 5, 2023

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 Government. 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 Government. For more information about resolving this issue, see [CTX221535](#).

## Installer

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

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 doesn't use the settings defined for the user as described previously. You need to import the setting from the browser.

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

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

After running 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 aren't supported.

## Set up DaaS

November 23, 2023

This article provides an overview of the tasks required to set up Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). For a list of service features that aren't available in Citrix Cloud Government, see [Citrix DaaS for Citrix Cloud Government](#).

## Request a service trial

If you don't have a subscription to Citrix DaaS, you can request a trial. Service trials last for 60 days and have all the same functionality as the production service. To request a trial, follow the steps described in [Request a service trial](#).



## Prepare a master image and install the VDA

Prepare one or more virtual machines with the desktop configuration or applications that you want to deliver to users. Afterward, install the Virtual Delivery Agent (VDA) software on each machine. Join each machine to your domain before installing the VDA.

For instructions, [Install VDAs](#)

## Configure Citrix DaaS

To configure Citrix DaaS, complete the following tasks:

- [Create a host connection](#). A host connection enables Citrix DaaS to provision and manage the machines in your hypervisor or cloud environment.
- [Create Machine Catalogs](#). Machine Catalogs are collections of identically configured machines that are created from the VDAs you prepared earlier.
- Users access the applications or desktops on these machines through their workspaces.
- [Create Delivery Groups](#). Delivery Groups allow you to define which users or user groups can access certain applications or desktops.
  - When users access their workspace, the Delivery Groups govern the applications or desktops to which those users belong.

## Citrix Gateway service

Citrix Gateway service is available for Citrix DaaS. Citrix Gateway service is hosted only on Citrix Cloud Government clouds and is separate from the commercial clouds. The Citrix Gateway service on government clouds is presently available in the United States in the following three regions.

- Arizona
- Texas
- Virginia

## Configure the Citrix Gateway service

Configuring the Citrix Gateway service for Cloud Government is similar to configuring the Citrix Gateway service for commercial clouds. You must enable the Citrix Gateway service to configure connectivity for users. For details, see [Configure connectivity for users](#).

## Citrix Gateway

Citrix Gateway provides users with secure access to Citrix DaaS applications across a range of devices. If you have an existing on-premises Gateway, you can use it with Citrix DaaS to ensure external users can access their applications securely. Also if you need to create a Gateway deployment to use with Citrix DaaS, refer to [Deploy a Citrix ADC VPX instance](#).

## Other features

To learn more about using the other features in Citrix DaaS, refer to the following articles:

- [Printing](#)
- [HDX technologies](#)
- [Policies](#)
- [Managing resources and users](#)
- [Monitoring](#)

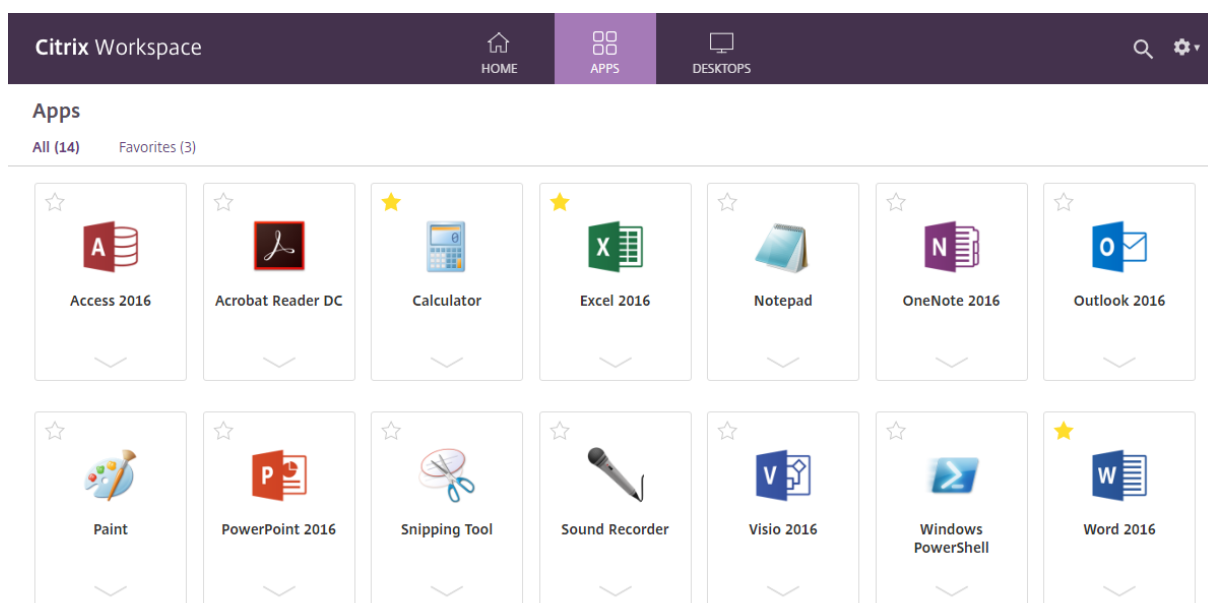
## Next steps

After you set up Citrix DaaS, [configure workspaces](#) for your users. Through workspaces, your users can access the applications and desktops that you make available to them.

## Set up workspaces for users

December 5, 2023

Workspace allows you to deliver access to applications and desktops from any device. Workspaces provide access to resources based on the Delivery Groups that you configure in Citrix DaaS (formerly Citrix Virtual Apps and Desktops service).



Before you set up workspaces for your users, review the features that aren't available in Citrix Cloud Government. See [Workspace Service for Citrix Cloud Government](#).

When you're ready to set up workspaces, consult [Workspace configuration](#).

## Citrix Networking

December 4, 2023

Provide for external users a secure access to applications and desktops, an on-premises Citrix ADC, VPX, or MPX appliance is required. Using smart cards with Citrix Gateway is a common access scenario for Citrix Cloud Government customers.

This article describes Citrix recommendations for using smart cards with Citrix Gateway.

1. Create a primary Gateway virtual server for authenticating users. Select the **Client Authentication** setting and set it to **Mandatory**. The **Mandatory** option enforces the need for smart cards by disallowing any SSL handshake that doesn't include a client certificate.
2. Create a secondary Gateway virtual server that only handles ICA Proxy.

This Gateway isn't configured to prompt for Client Authentication. So the SSL ICA connection doesn't prompt the user again for a PIN. In StoreFront, use this virtual server to route connections to resources.

The virtual server allows users to log on to the primary Gateway, which handles the initial authentication, and access resources through the secondary Gateway.

3. Create a third Gateway virtual server to provide the callback URL for StoreFront. Only StoreFront uses this Gateway to verify requests from the Gateway appliance and doesn't need to be publicly accessible. This virtual server is required when client certificate authentication is mandatory. StoreFront can't present a certificate to authenticate.

### **Additional information**

For more information about creating Citrix Gateway virtual servers, see [Creating Virtual Servers](#).

For more information about configuring smart card authentication in StoreFront, see [Configure smart card authentication](#).

## **Identity and access management for Citrix Cloud Government**

December 14, 2023

Identity and access management includes the identity providers and accounts used for Citrix Cloud Government administrators and workspace subscribers.

### **Identity providers**

The Citrix Cloud Government identity provider is the default identity provider. The identity information is managed for all administrators in Citrix Cloud Government account. You can change the provider to a different identity provider to authenticate administrators, workspace subscribers, or both.

Citrix Cloud Government supports the following identity providers:

- [Azure Active Directory](#): For authenticating Citrix Cloud Government administrators and workspace subscribers.
- [Active Directory](#): For authenticating workspace subscribers.
- [Citrix Gateway](#): For authenticating workspace subscribers.
- [Okta](#): For authenticating workspace subscribers.
- [SAML 2.0](#): For authenticating administrators (preview) and workspace subscribers.

### **Administrators**

Administrators use their identity to access Citrix Cloud Government, perform management activities, and install the Citrix Cloud Connector.

Citrix Cloud Government identity provider authenticates administrators using an email address and password. Administrators can also use their My Citrix credentials to sign in to Citrix Cloud Government.

## Subscribers

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

Administrators can control which domains are used to provide these identities on the **Domains** tab. If you plan to use domains from multiple forests, install at least two Cloud Connectors in each forest. Citrix recommends at least two Cloud Connectors to maintain a high availability environment.

### Note:

- Disabling domains prevents new identities only from being selected. It does not prevent subscribers from using identities that are already assigned.
- Each Cloud Connector list and use all the domains from the single forest in which it is installed.

For more information, see the following articles in the Citrix Cloud product documentation:

- [Assign users and groups to service offerings using Library](#)
- [Deployment scenarios for Cloud Connectors in Active Directory](#)

## Connect Active Directory to Citrix Cloud Government

November 20, 2023

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

Connecting your on-premises Active Directory to Citrix Cloud Government 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

1. From the Citrix Cloud Government menu, select **Identity and Access Management**.
2. From the **Authentication** tab in **Active Directory**, click the ellipsis menu and select **Connect**.
3. Click **Install Connector** to download the Cloud Connector software.
4. Launch the Cloud Connector installer and follow the installation wizard.
5. From the **Connect to Active Directory** page, click **Detect**. After verification, Citrix Cloud displays a message that your Active Directory is connected.
6. Click **Return to Authentication**. The **Active Directory** entry is marked **Enabled** on the **Authentication** tab.

## Connect Azure Active Directory to Citrix Cloud Government

November 20, 2023

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

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

- Use your own Active Directory, so you can control auditing, password policies, and easily disable accounts when needed.
- Configure multifactor authentication for a higher level of security against the possibility of stolen sign-in credentials.
- Use a branded sign-in page, so your users know they are signing in at the right place.
- Use federation to an identity provider of your choice including ADFS, Okta, and Ping, among others.

## Prepare your Active Directory and Azure AD

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

- **Your Azure AD infrastructure is hosted in an Azure Government instance.** You can't federate Azure AD hosted in a commercial Azure instance to Citrix Cloud Government. If you attempt to use Azure AD in a commercial Azure instance with Citrix Cloud Government, Azure AD does not work. If you don't have an Azure Government account, sign up at <https://azure.microsoft.com/en-us/global-infrastructure/government/request/>.
- **Administrator accounts have their "mail" property configured in Azure AD.** To configure, 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 that the Active Directory accounts have the Email user property configured:
  - a) Open Active Directory Users and Computers.
  - b) In the **Users** folder, locate the account you want to check, right-click, and select **Properties**. On the **General** tab, verify the **Email** field has a valid entry. Citrix Cloud requires that administrators added from 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 website.

### Connect Citrix Cloud Government to Azure AD

When connecting your Citrix Cloud Government account to your Azure AD, Citrix Cloud Government needs permission to access your user profile (or the profile of the signed-in user). Along with 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). Or the users can be and add as administrators later.

1. Sign in to Citrix Cloud Government at <https://citrix.cloud.us>.
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 Government.
5. When prompted, sign in to the Azure account with which you want to connect. Azure shows you the permissions that Citrix Cloud Government must access the account and acquire the information required for the connection.
6. Click **Accept** to accept the permission request.

### Add administrators to Citrix Cloud Government from Azure AD

1. From the Citrix Cloud Government 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 that 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 Government sends an invitation to the user you specified and adds the administrator to the list.

After clicking the email link, you can sign in to the company's Azure Active Directory. You can verify the user's email address and completes the connection between the Azure AD user account and Citrix Cloud Government.

### **Add Azure AD administrator groups to Citrix Cloud Government**

You can add administrators to your Citrix Cloud Government 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 users only with Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). Administrators in the group don't have access to manage any other services in the Citrix Cloud Government account.

For more information, see [Manage administrator groups](#).

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

After the Azure AD user accounts are connected, users can sign in to Citrix Cloud Government 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.cloud.us/go/myorganization>
- From the Citrix Cloud Government sign-in page, click **Sign in with my organization credentials**, type the identifier you created when you initially connected Azure AD, and click **Continue**.

### **Enable advanced Azure AD capabilities**

Azure AD provides advanced multifactor authentication, world-class security features. Federation to 20 different identity providers. Self-service password change and reset, among many other features. Turning these features on for your Azure AD users enables Citrix Cloud Government to use those capabilities automatically.



## Connect an on-premises Citrix Gateway as an identity provider to Citrix Cloud Government

November 20, 2023

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

By using Citrix Gateway authentication, you can:

- Continue authenticating users through your existing Citrix Gateway so they can access the resources in your on-premises Citrix 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, and federation. Many other features providing your users access to the resources they need through 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 Technical Details](#).
- Does not have any other Citrix components installed, isn't an Active Directory domain controller, and isn't a machine critical to your resource location infrastructure.
- Joined to the domain where your Site resides. If users access your Site's applications in numerous 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 [Citrix Cloud Connector requirements](#).
- Citrix recommends two servers for Cloud Connector high availability. After installation, the Cloud Connectors allow Citrix Cloud Government to locate and communicate with your Site.

For more information about installing the Cloud Connector, see [Install Cloud Connectors from the command line](#) and [Citrix Cloud Connector proxy and firewall configuration](#).

## Active Directory

Before enabling Citrix Gateway authentication, perform the following tasks:

- Verify that your workspace subscribers have user accounts in the Active Directory (AD). Subscribers with only AD accounts can sign in to their workspaces successfully.
- Ensure that the user properties in your subscribers' AD accounts are populated. Citrix Cloud Government 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 Government 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 Government to communicate with your on-premises environment. For instructions, see [Connect Active Directory to Citrix Cloud Government](#).
- If you are performing federation with Citrix Gateway authentication, synchronize your AD users to the federation provider. Citrix Cloud Government 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 because of deprecation of classic policies. Advanced policies support multifactor authentication for

Citrix Cloud Government, 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 Government. 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 Government and Gateway confirm to the OIDC protocol, which involves digitally signing tokens.

You must configure a certificate for signing these tokens. This certificate must be issued from a public Certificate Authority (CA). Use of a certificate issued by a private CA is supported only to provide Citrix Cloud Government with the private root CA certificate.

So, the certificate chain of trust can't 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 Government assumes that tokens are stale when checking their validity.

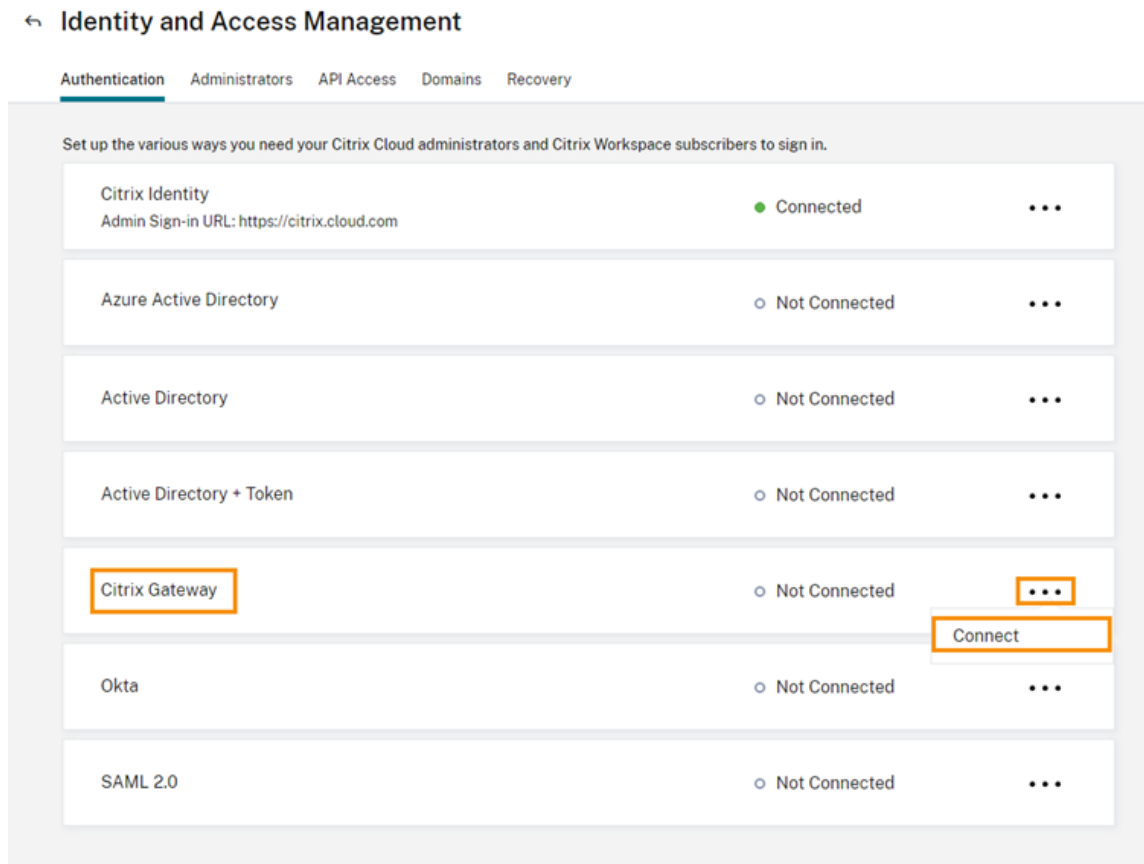
### **Task overview**

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 information generated from Citrix Cloud Government. The OAuth IdP advanced policy enables Citrix Cloud Government 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.

## To enable Citrix Gateway authentication for workspace subscribers

1. From the Citrix Cloud Government 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**.



## Configure your On-Premises Gateway as an Identity Provider for Workspace

Enter your FQDN to help us locate your On-Premises Gateway

Please enter the Fully Qualified Domain Name (FQDN) configured for your on-premises Gateway. The FQDN will help us identify your Gateway to establish a connection to Citrix Cloud.




FQDN:

After Citrix Cloud Government 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 Government displays.

**Create a connection with Citrix Gateway**

 → 
  → 
 

Copy the Client ID and Secret and Redirect URL     
 Go to your On-Premises Citrix Gateway and input your ID, Secret, and URL to establish the connection. [Learn more](#)     
 When configuration is completed, test your Gateway connection to enable this identity provider.

---

**Client ID:** [Redacted] Copy

**Secret:** [Redacted] Copy

**Redirect URL:** https://accounts.cloud.us/core/login-cip Copy

You will not have access to the client ID and secret later. You will have to generate a new pair if you lose track of the original. Download the key to save your ID and secret.

Test and Finish

Also, download a copy of this information and save it securely offline for your reference. This information isn't available in Citrix Cloud Government 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 Government. 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 Government verifies that your Gateway is reachable and configured correctly.
5. Enable Citrix Gateway authentication for workspaces:
- a) From the Citrix Cloud Government menu, select **Workspace Configuration**.
  - b) From the **Authentication** tab select **Citrix Gateway**.
  - c) 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 Government and your on-premises Gateway, verify the following items:

- The FQDN Gateway is reachable from the Internet.
- You have entered the Gateway FQDN correctly in Citrix Cloud Government.
- You have entered the Gateway URL correctly in the `-issuer` parameter of the OAuth IdP policy. Example: `-issuer https://GatewayFQDN.com`. The `issuer` parameter is case sensitive.
- The client ID, secret, and redirect URL values from Citrix Cloud Government 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 that 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 are. NETBIOS names aren't replicated on global catalog servers.

If you use global catalog servers in your AD environment, LDAP actions configured on these servers don't go with Citrix Cloud Government. 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 done with the third-party servers. To configure these policies, you add a second authentication factor to your existing login schema profile by following the tasks:

1. Create an LDAP authentication server that does 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 the 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 checkbox. This checkbox must be cleared because this authentication server is only for extracting user attributes and groups from Active Directory, not authentication.
  - c) Under **Other Settings**, enter the following information:
    - In **Server Logon Name Attribute**, enter **UserPrincipalName**.
    - In **Group Attribute**, select **memberOf**.
    - In **Sub Attribute Name**, select **cn**.
2. Create the LDAP advanced authentication policy:
  - a) Select **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Policy > Add**.
  - b) On the **Create Authentication Policy** page, enter the following information:
    - In **Name**, enter a friendly name for the policy.
    - In **Action Type**, select **LDAP**.
    - In **Action**, select the LDAP authentication server you created earlier.
    - In **Expression**, enter **TRUE**.
  - c) Click **Create** to save the configuration.
3. Create the Authentication Policy Label:



- a) Select **Security > AAA –Application Traffic > Policies > Authentication > Advanced Policies > Policy Label > Add**.
  - b) In **Name**, enter a friendly name for the authentication policy label.
  - c) In Login Schema, select **LSCHEMA\_INT**.
  - d) Under **Policy Binding**, in **Select Policy**, select the LDAP advanced authentication policy you created earlier.
  - e) In **GoTo Expression**, select **END**.
  - f) Click **Bind** to finish the configuration.
4. Define the LDAP Authentication Policy Label as the next factor, after the primary identity provider:
- a) Select **System > Security > AAA - Application Traffic > Virtual Servers**.
  - b) Select the virtual server that has 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 Government 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 Government. Enable **SSOCredentials** on the login schema corresponding to the LDAP factor.

## Connect Okta as an identity provider to Citrix Cloud Government

November 20, 2023

Citrix Cloud Government supports using Okta as an identity provider to authenticate subscribers signing in to their workspaces. By connecting your Okta organization to Citrix Cloud Government, 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 a federated sign-in, not a single sign-on. Sub-

scribers sign in to workspaces from an Okta sign-in page. They might have to authenticate a second time when opening an app or desktop from Citrix DaaS (formerly Citrix Virtual Apps and Desktops service).

## Prerequisites

### Cloud Connectors

You need at least two (2) servers in your Active Directory domain on which to install the Citrix Cloud Connector software. Cloud Connectors are required for enabling communication between Citrix Cloud Government 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 Technical Details](#).
- Does not have any other Citrix components installed, isn't an Active Directory domain controller. This isn't machine critical to your resource location infrastructure.
- Joined to your Active Directory (AD) domain. If your workspace resources and users are in different 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 [Citrix Cloud Connector requirements](#).

For more information about installing Cloud Connectors, see [Install Cloud Connectors from the command line](#) and [Citrix Cloud Connector proxy and firewall configuration](#).

### Okta domain

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

- [okta.com](#)
- [okta-eu.com](#)
- [oktapreview.com](#)

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

To create and configure this application, see the following sections in this article:

- Create an Okta OIDC web application
- Configure the Okta OIDC web application

## Workspace URL

When creating the Okta application, you must supply your Workspace URL from Citrix Cloud Government. To locate the Workspace URL, select **Workspace Configuration** from the Citrix Cloud Government 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 logging off from their workspace.

## Okta API token

Using Okta as an identity provider with Citrix Cloud Government requires an API token for your Okta organization. Create this token using a Read-Only Administrator account in your Okta organization. This token can 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 Government 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 following values associated with your AD accounts:

- Email
- SID
- UPN
- OID

**Note:**

If you're 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 application

1. From the Okta management console, under **Applications**, select **Applications**.
2. Select **Create App Integration**.
3. In **Sign in method**, select **OIDC - OpenID Connect**.
4. In **Application Type**, select **Web Application**. Select **Next**.
5. In **App Integration Name**, enter a friendly name for the app integration.
6. In **Grant type**, select the following options:
  - Authorization Code
  - Implicit (Hybrid)
7. In **Sign-in redirect URIs**, enter `https://accounts.cloud.us/core/login-okta`.
8. In **Sign-out redirect URIs**, enter your Workspace URL from Citrix Cloud.
9. Under **Assignments**, in **Controlled access**, select whether to assign the app integration to everyone in your organization, only groups that you specify, or to assign access later.

10. Select **Save**. After you save the app integration, the console displays the application configuration page.
11. In the **Client Credentials** section, copy the **Client ID** and **Client Secret** values. You use these values when you connect Citrix Cloud Government 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 Government. Citrix Cloud Government requires these settings to authenticate your subscribers through Okta when they sign in to their workspaces.

1. (Optional) Update client permissions for the implicit grant type. You might choose to perform this step if you prefer to allow the least amount of privilege for this grant type.
  - a) From the Okta application configuration page, under **General Settings**, select **Edit**.
  - b) In the **Application** section, under **Client acting on behalf of user**, clear the **Allow Access Token with implicit grant type**.
  - c) Select **Save**.
2. Add application attributes. These attributes are case-sensitive.
  - a) From the Okta console menu, select **Directory > Profile Editor**.
  - b) Select the Okta **User (default)** profile. Okta displays the **User** profile page.
  - c) Under **Attributes**, select **Add attribute**.
  - d) Enter the following information:
    - Display name: cip\_email
    - Variable name: cip\_email
    - Description: AD User Email
    - Attribute Length: Greater than 1
    - Attribute Required: Yes
  - e) Select **Save and Add Another**.
  - f) Enter the following information:
    - Display Name: cip\_sid
    - Variable Name: cip\_sid
    - Description: AD User Security Identifier
    - Attribute Length: Greater than 1
    - Attribute Required: Yes
  - g) Select **Save and Add Another**.
  - h) Enter the following information:
    - Display Name: cip\_upn
    - Variable Name: cip\_upn

- Description: AD User Principal Name
  - Attribute Length: Greater than 1
  - Attribute Required: Yes
- i) Select **Save and Add Another**.
  - j) Enter the following information:
    - Display Name: cip\_oid
    - Variable Name: cip\_oid
    - Description: AD User GUID
    - Attribute Length: Greater than 1
    - Attribute Required: Yes
  - k) Select **Save**.
3. Edit attribute mappings for the application:
- a) From the Okta console, select **Directory > Profile Editor**.
  - b) Locate the **active\_directory** profile for your AD. This profile might be labeled using the format `myDomain User`, where `myDomain` is the name of your integrated AD domain.
  - c) Select **Mappings**. The User Profile Mappings page for your AD domain appears and the tab for mapping your AD to Okta User is selected.
  - d) In the **Okta User Profile** column, locate the attributes you created in Step 2 and map as follows:
    - For `cip_email`, select `email` from the User Profile column for your domain. When selected, the mapping appears as `appuser.email`.
    - For `cip_sid`, select `objectSid` from the User Profile column for your domain. When selected, the mapping appears as `appuser.objectSid`.
    - For `cip_upn`, select `userName` from the User Profile column for your domain. When selected, the mapping appears as `appuser.userName`.
    - For `cip_oid`, select `externalId` from the User Profile column for your domain. When selected, the mapping appears as `appuser.externalId`.
  - e) Select **Save Mappings**.
  - f) Select **Apply updates now**. Okta starts a job to apply the mappings.
  - g) Sync Okta with your AD.
    - i. From the Okta console, select **Directory > Directory Integrations**.
    - ii. Select your integrated AD.
    - iii. Select the **Provisioning** tab.
    - iv. Under **Settings**, select **To Okta**.
    - v. Scroll to the **Okta Attribute Mappings** section and then select **Force Sync**.

## Create an Okta API token

1. Sign in to the Okta console using a Read-Only Administrator account.
2. From the Okta console menu, select **Security > API**.
3. Select the **Tokens** tab and then select **Create Token**.
4. Enter a name for the token.
5. Select **Create Token**.
6. Copy the token value. You supply this value when you connect your Okta organization to Citrix Cloud.

## Connect Citrix Cloud Government to your Okta organization

1. Sign in to Citrix Cloud Government at <https://citrix.cloud.us>.
2. From the Citrix Cloud Government menu, select **Identity and Access Management**.
3. Locate **Okta** and select **Connect** from the ellipsis menu.
4. In **Okta URL**, enter your Okta domain.
5. In **Okta API Token**, enter the API token for your Okta organization.
6. In **Client ID** and **Client Secret**, enter the client ID and secret from the OIDC web app integration you created earlier. To copy these values from the Okta console, select **Applications** and locate your Okta application. Under **Client Credentials**, use the **Copy to Clipboard** button for each value.
7. Click **Test and Finish**. Citrix Cloud Government verifies your Okta details and tests the connection.

After the connection is verified successfully, you can enable Okta authentication for workspace subscribers.

## Enable Okta authentication for workspaces

1. From the Citrix Cloud Government menu, select **Workspace Configuration > Authentication**.
2. Select **Okta**.
3. When prompted, select **I understand the impact on the subscriber experience**.
4. Select **Save**.

After switching to Okta authentication, Citrix Cloud temporarily disables workspaces for a few minutes. When workspaces are re-enabled, your subscribers can sign in using Okta.

## Connect SAML as an identity provider to Citrix Cloud Government

November 20, 2023

Citrix Cloud Government supports using SAML (Security Assertion Markup Language) as an identity provider to authenticate administrators (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).

### Prerequisites

Using SAML authentication with Citrix Cloud Government 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 Government 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, isn't an AD domain controller, and isn't a machine critical to your resource location infrastructure.
- Joined to the domain where your resources are. If users access resources in numerous domains, you must install at least two Cloud Connectors in each domain.
- Connected to a network that can contact the resources that subscribers access through Citrix Workspace.
- Connected to the Internet. For more information, see [Connectivity requirements for Citrix Cloud Government](#).

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 with only 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 Government 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 Government account by deploying Cloud Connectors in your on-premises AD.
- Synchronize your AD users to the SAML provider. Citrix Cloud Government 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 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 earlier. 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 Government.

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 Government administrators is in technical preview. We recommend using preview features only in non-production environments.

### **AD groups**

You can add administrators to Citrix Cloud Government 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 Government. This URL uses the format <https://citrix.cloud.us/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 Government 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 Government.

### **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 aren't 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 Government as described in [Connect Active Directory to Citrix Cloud Government](#).
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 Government. This task involves configuring your SAML provider with the SAML metadata from Citrix Cloud Government. Then configuring Citrix Cloud Government 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 Government 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 the actions that you perform in your SAML provider's administration console. The specific commands that you use to perform these actions might vary from the commands described in this section, depending on your chosen SAML provider. The SAML provider commands in this section are provided as examples only. Refer to your SAML provider's documentation for 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 Government. For example, depending on your SAML provider's console, you might select **Users > Directories**.
  4. Select the option for adding directory attributes. For example, depending on your SAML provider's console, you might select **Directory Attributes**.
  5. Select the option for adding attributes and map the following AD attributes to the custom user attributes you created in Step 2:
    - Select `objectSid` and map to the `cip_sid` attribute.
    - Select `userPrincipalName` and map to the `cip_upn` attribute.
    - Select `ObjectGUID` and map to the `cip_oid` attribute.
    - Select `mail` and map to the `cip_email` attribute.

### Configure the administrator sign-in URL

1. Sign in to Citrix Cloud at <https://citrix.cloud.us>.
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. Go to the next section to configure the SAML connection to Citrix Cloud Government.

### Configure the SAML provider metadata

In this task, you create a connector application using SAML metadata from Citrix Cloud Government. After you configure the SAML application, you use the SAML metadata from your connector application to configure the SAML connection to Citrix Cloud Government.

#### Note:

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

### Create a SAML connector application

1. Sign in to Citrix Cloud Government at <https://citrix.cloud.us>.
2. From the Citrix Cloud menu, select **Identity and Access Management**.
3. Locate **SAML 2.0** and select **Connect** from the ellipsis menu. The **Configure SAML** screen appears.
4. 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)**.
5. If applicable, enter a display name and save the app.
6. From the **Configure SAML** screen in Citrix Cloud Government, in **SAML Metadata** select **Download**. The metadata XML file appears in another browser tab.
7. Enter the following details for the connector application:
  - In the **Audience** field, enter <https://saml.cloud.us>.
  - In the **Recipient** field, enter <https://saml.cloud.us/saml/acs>.
  - In the field for ACS URL validator, enter <https://saml.cloud.us/saml/acs>.
  - In the field for ACS URL, enter <https://saml.cloud.us/saml/acs>.
  - In the field for a single logout URL, enter <https://saml.cloud.us/saml/logout/callback>.
8. Add your custom SAML attributes as parameter values in the application:

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

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

### Add SAML provider metadata to Citrix Cloud Government

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

```

<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="
https://app. .com/saml/metadata/8c733cbd-c579-41d4-b4e1-4ff034893d19">
  <IDPSSODescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" protocolSupportEnumeration=
"urn:oasis:names:tc:SAML:2.0:protocol">
    <KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIID2DCCA
          +w3PpA==</ds:X509Certificate>
        </ds:X509Data>
      </ds:KeyInfo>
    </KeyDescriptor>
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
https://citrixidentity-dev. .com/trust/saml2/http-redirect/slo/1097253"/>
      <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
https://citrixidentity-dev. .com/trust/saml2/http-redirect/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="
https://citrixidentity-dev. .com/trust/saml2/http-post/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
    <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP" Location="
https://citrixidentity-dev. .com/trust/saml2/soap/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
  </IDPSSODescriptor>
</EntityDescriptor>

```

2. In the **Configure SAML** screen in Citrix Cloud Government, 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.

```

<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="
https://app. .com/saml/metadata/8c733cbd-c579-41d4-b4e1-4ff034893d19"

```

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

```

<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="
https://citrixidentity-dev. .com/trust/saml2/http-redirect/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>
<SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="
https://citrixidentity-dev. .com/trust/saml2/http-post/sso/8c733cbd-c579-41d4-b4e1-4ff034893d19"/>

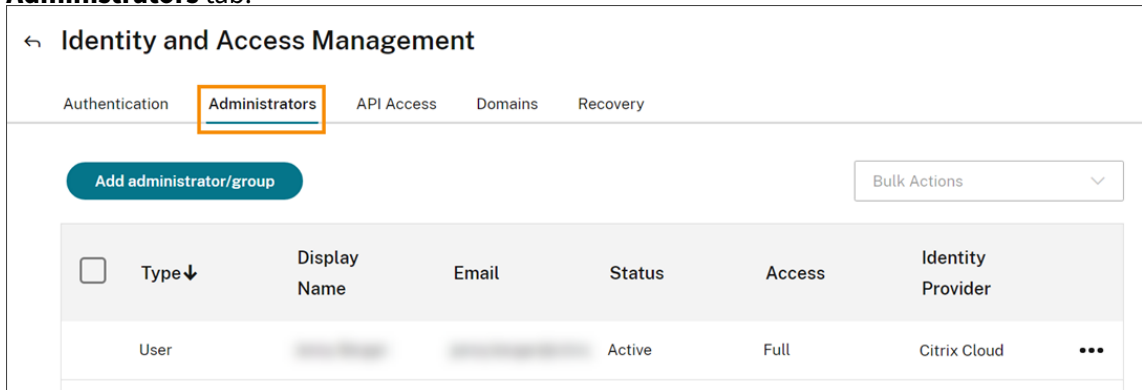
```

- In **Binding Mechanism**, select the mechanism that matches the binding for the SSO Service URL you chose from the metadata file.

- In **SAML Response**, select the signing method your SAML provider uses for the SAML Response and SAML Assertion. By default, Citrix Cloud Government 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 Government, 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 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.
  8. Verify the following default name attribute values in Citrix Cloud Government 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 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, 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 Government from AD

1. In Citrix Cloud Government, 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 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**.

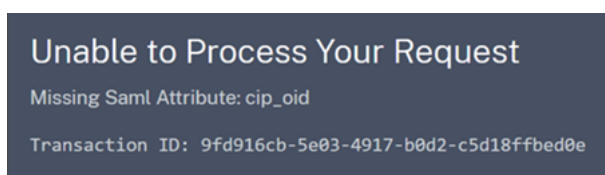
## Enable SAML authentication for workspaces

1. From the Citrix Cloud 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 aren't encoded correctly. When an attribute error occurs, Citrix Cloud Government displays an error message that includes the faulty attribute.





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

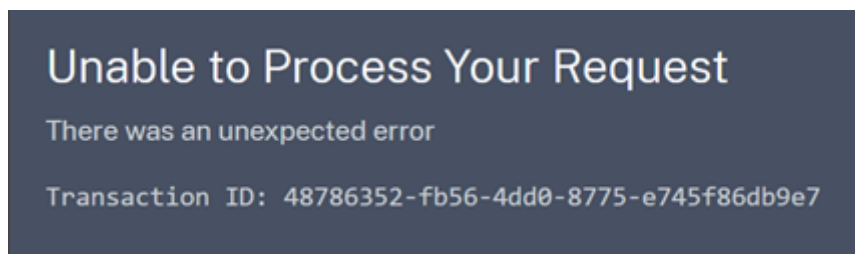
Attribute	Encoding
cip_email	Must be in String format ( <code>user@domain</code> )
cip_oid	Must be in Base64 or String format
cip_sid	Must be in Base64 or String format
cip_upn	Must be String format ( <code>user@domain</code> )

### Unexpected errors

Citrix Cloud Government might experience an unexpected error when:

- A user starts 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.cloud.us`).
- The SAML certificate is invalid or has expired.
- The authentication context is invalid.
- SAML assertion and response signature are mismatched.

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



If this error results from navigating to Citrix Cloud Government 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.cloud.us`).
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 another password prompts.

## Manage Citrix Cloud Government

December 5, 2023

Citrix Cloud Government includes the following administrative features:

- Inviting administrators and delegating access to cloud services
- Assigning a primary resource location
- Assigning users to service offerings in the Library
- Monitoring service notifications
- View the System Log of events that occurred in Citrix Cloud Government

### Administrators

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

### Add administrators and modify permissions

To invite other administrators and fine-tune their access to Citrix Cloud Government, see [Add administrators to a Citrix Cloud Government account](#).

### Remove administrators

You can remove administrators from your Citrix Cloud Government account on the **Administrators** tab. When you remove an administrator, they can no longer sign in to Citrix Cloud Government. If an administrator is logged in when you remove the account, the administrator stays active for a one minute. Eventually, access to Citrix Cloud Government is denied.

**Note:**

- If there's only one administrator in the account, you can't remove that administrator. Citrix Cloud Government requires at least one administrator for each customer account.
- Cloud Connectors aren't linked to administrator accounts. So, Cloud Connectors continue operating even if you remove the administrator who installed it.

## Subscribers

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

The process for assigning users to Library offerings is the same for Citrix Cloud Government and commercial Citrix Cloud. For instructions, see [Assign users and groups to service offerings using Library](#).

### Important:

If you're using an on-premises StoreFront with Citrix DaaS, don't use a Library to assign resources when creating delivery groups. Instead, use Studio to assign resources to users. If you use a 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**).

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 document on the [Citrix Product Documentation](#) website.

## Primary resource locations

A primary resource location is a resource location that you choose as "most preferred" for communications between your domain and Citrix Cloud Government. The resource location that you select as "primary" has Cloud Connectors that have the best performance and connectivity to your domain. The resource location enables your users to log on quickly to Citrix Cloud Government.

The process for selecting a primary resource location is the same for Citrix Cloud Government and commercial Citrix Cloud. For more information, see [Select a primary resource location](#).

## Notifications

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

Managing notifications is the same in Citrix Cloud Government and commercial Citrix Cloud. For more information about notifications, see [Notifications](#).

## System Log

The System Log displays a timestamped list of events that occurred in Citrix Cloud Government. 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 Government and commercial Citrix Cloud, with some important limitations. For more information, see [System Log](#)

## Manage Citrix Cloud Government administrators

December 5, 2023

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

All administrators are required to use tokens as a second factor of authentication when signing in to Citrix Cloud. After you add an administrator, they can enroll their device in multifactor authentication. Also, generate tokens using any app that follows the [Time-Based One-Time Password](#) standard, such as Citrix SSO.

By default, new administrators have Full Access permissions to all functions in the Citrix Cloud Government account. See [Configure administrator permissions](#) in this article you learn how to delegate account administration.

### Add new administrators

Citrix Cloud supports the following identity providers for authenticating administrators:

- Citrix identity provider: The default identity provider in Citrix Cloud. Supports adding individual administrators only.
- Azure AD: Supports adding administrators individually and through AAD groups. Administrators in AAD groups are limited to accessing Citrix DaaS only. For more information, see [Manage administrator groups](#).
- SAML 2.0: Supports adding administrators through AD groups only. For more information, see [Connect SAML as an identity provider to Citrix Cloud](#).

Adding new administrators uses the following workflow:

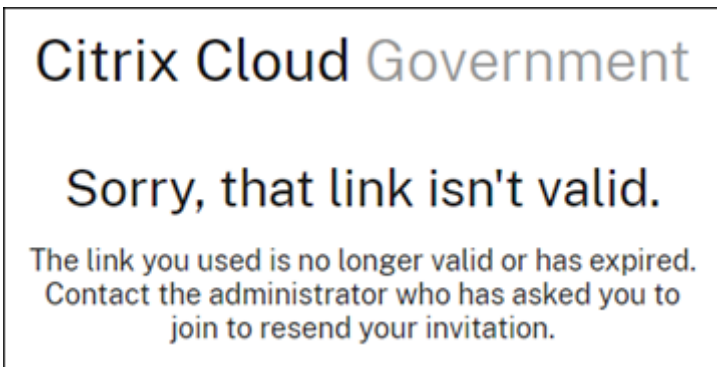
1. Select the identity provider that you want to use for authenticating administrators.
2. Depending on the identity provider, invite individual administrators or select the groups that the administrators belong to.

3. Specify the access permissions that align with the administrators' roles in your organization. For more information, see [configure administrator permissions](#) in this article.

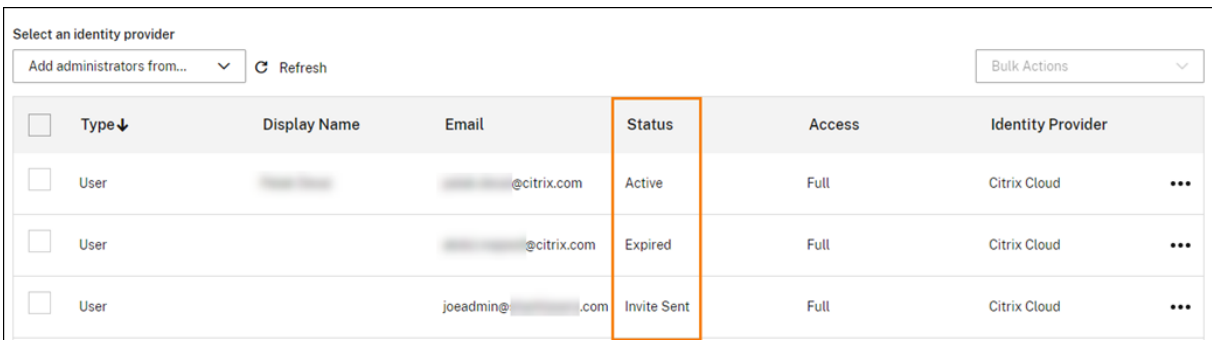
### Invite individual administrators

Adding individual administrators involves inviting them to join your Citrix Cloud Government 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](mailto:cloud@citrix.com) and explain how to access the account. The email is valid for five consecutive days from the day that you send it. After five days have elapsed, the invitation link expires. If the invited administrator uses the expired link, Citrix Cloud Government displays a message indicating the link is not valid.



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



<input type="checkbox"/>	Type ↓	Display Name	Email	Status	Access	Identity Provider	
<input type="checkbox"/>	User		@citrix.com	Active	Full	Citrix Cloud	...
<input type="checkbox"/>	User		@citrix.com	Expired	Full	Citrix Cloud	...
<input type="checkbox"/>	User		joeadmin@.com	Invite Sent	Full	Citrix Cloud	...

### To invite an administrator

1. After signing in to [Citrix Cloud Government](#), select **Identity and Access Management** from the menu.

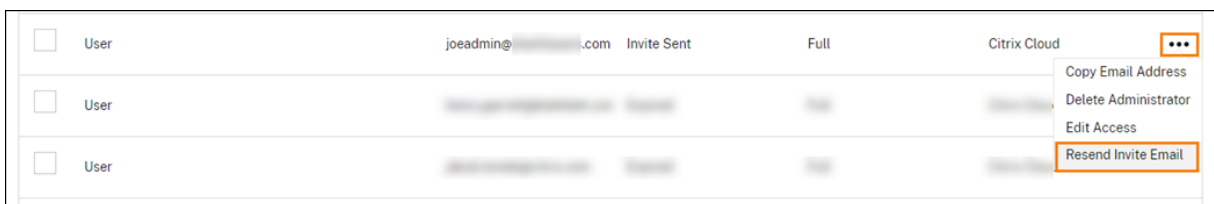
2. On the **Identity and Access Management** page, select **Administrators**. The console shows all the current administrators in the account.
3. Select **Add administrator/group**.
4. In **Administrator details**, select the identity provider you want to use. If using Azure AD, Citrix Cloud might prompt 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 Government functions and subscribed services. **Custom access** allows control of the functions and services that you select.
8. Review the administrator details. Select **Back** to make any changes.
9. Select **Send invitation**. Citrix Cloud sends an invitation to the user you specified and adds the administrator to the list.

### Resend an invitation

To resend the invitation, select **Resend Invite Email** from the ellipsis menu at the far-right of the console. Resending an invitation doesn’t affect the five-day time limit before the invitation expires.

### 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 Government and then invite them again.



### Accept an invitation

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

To accept the invitation, click **Sign In**. Afterwards, a browser window opens. If you don’t already have a Citrix Cloud Government account, the browser displays a page where you can create your password. If you already have an account, Citrix Cloud Government 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). These administrators can only manage Citrix DaaS (formerly Citrix Virtual Apps and Desktops service). For more information, see the following articles:

- [Manage administrator groups](#)
- [Connect SAML as an identity provider to Citrix Cloud Government](#)

## Configure administrator permissions

When you add administrators to your Citrix Cloud Government 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 Government functions such as Library or Resource Locations

With delegated administration in Citrix Cloud Government, you can configure the access permissions to all of your administrators. The permissions in accordance with their role in your organization.

## Console permissions

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

- **Authentication:** Grants access to the **Identity and Access Management > Authentication** tab. Administrators can create and remove identity provider connections and change the administrator sign-in URL, if applicable.  
To manage other aspects of identity providers, such as workspace authentication, more permissions are required.
- **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.
- **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. 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](#).
- **System Log:** Grant access to the **System Log** console page. Administrators can [view System Log events](#) and export events to a CSV file.
- **Workspace Configuration:** Grants access to the **Workspace Configuration** console page. Administrators can change authentication methods, customize workspace appearance and behavior, enable and disable services, and configure site aggregation. For more information, see the [Citrix Workspace](#) product documentation.

### To change existing permissions

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

1. Sign in to Citrix Cloud Government at <https://citrix.cloud.us>.
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 that 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 Government. Reset your authenticator app, you can re-enroll in multifactor authentication.

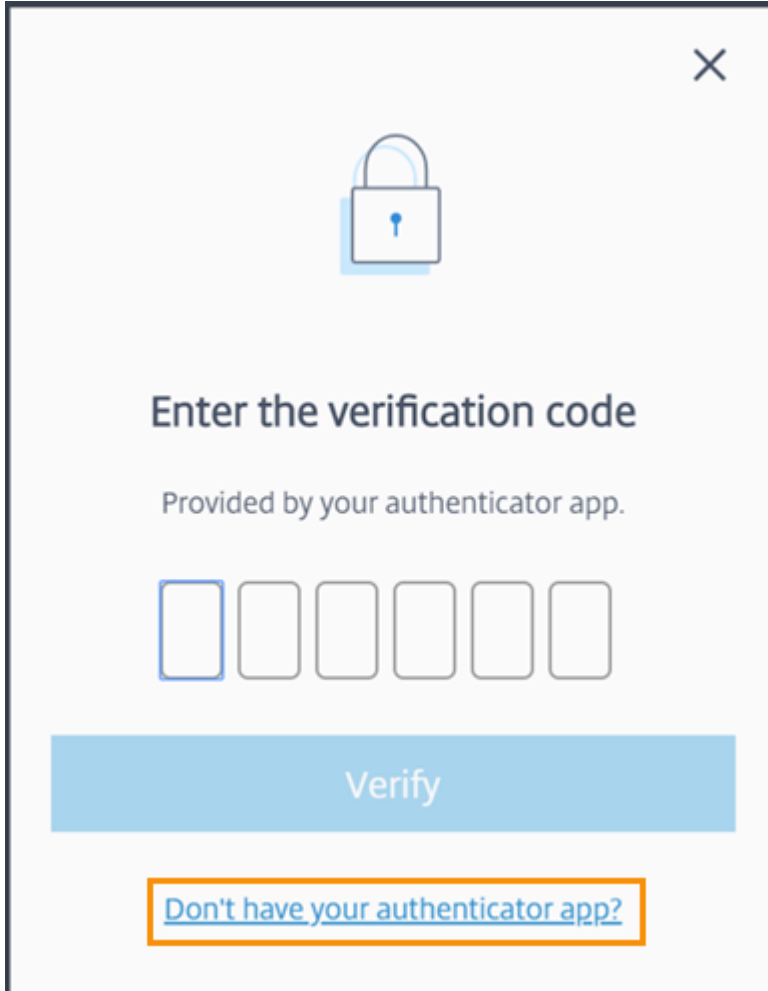
#### Notes

- 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 Government 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 Government entries with differing codes. These entries can cause confusion when signing in to Citrix Cloud Government.
- 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 Government and enter the code from your authenticator app.



The screenshot shows a verification screen with a padlock icon at the top. Below the icon, the text reads "Enter the verification code" and "Provided by your authenticator app." There are six empty input boxes for entering the code. A blue "Verify" button is positioned below the input boxes. At the bottom, a link "Don't have your authenticator app?" is highlighted with an orange border.

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**.

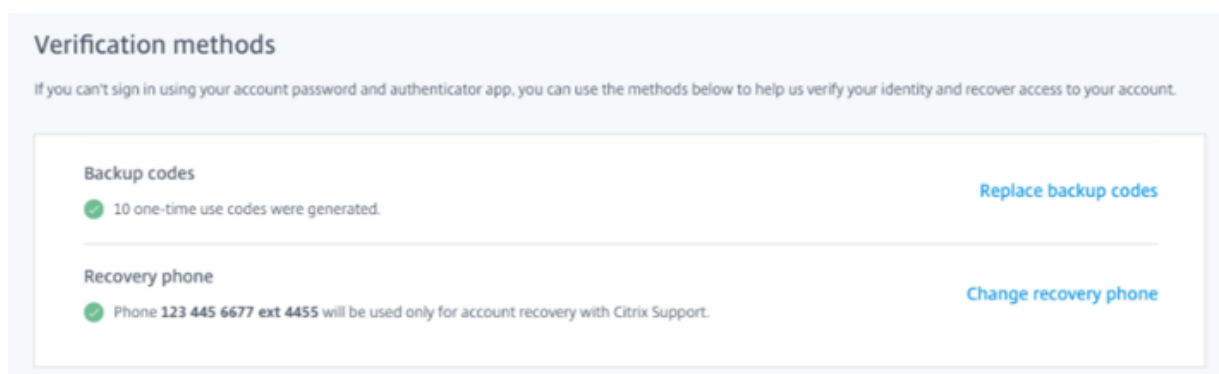


5. When prompted to confirm changing your device, select **Yes, change device**.
6. Verify your identity by entering a verification code from your authenticator app. If you don't have an authenticator app, select **Don't have your authenticator app?** and select a recovery method. Depending on the recovery 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 Government 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 that your Citrix Cloud Government 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 Government 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 code, select **Yes, replace**. Citrix Cloud Government 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

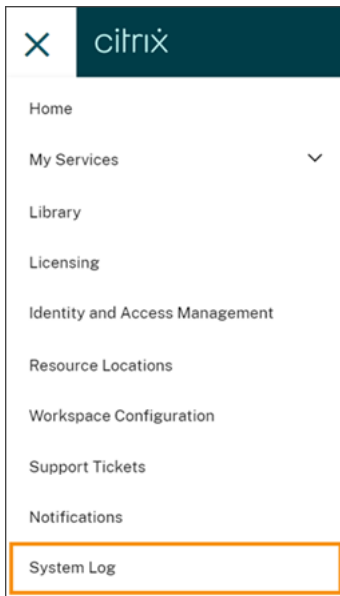
1. Sign in to Citrix Cloud Government and enter the code from your authenticator app.
2. If you are an administrator for multiple customer organizations, select the customer organization from which you originally enrolled in multifactor authentication.
3. From the top-right menu, select **My Profile**.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

## System Log

January 25, 2023

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

To view the system log, select **System Log** from the Citrix Cloud Government 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 Government and commercial Citrix Cloud, the following items are not available for use with Citrix Cloud Government:

- [SystemLog API](#)
- [Splunk add-on for the system log](#)

## Logged events

The system log captures events for certain Citrix Cloud Government 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 commercial Citrix Cloud. The events that are generated in Citrix Cloud Government are a subset of the events that are generated in commercial Citrix Cloud. For notifications about new events that are supported in Citrix Cloud Government, see [What's new in Citrix Cloud Government](#).

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.

← System Log

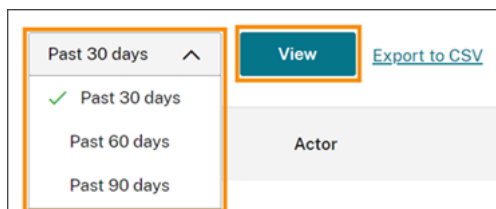
Past 30 days [View](#) [Export to CSV](#) < 1-32 of 32 >

Date & Time	Actor	Event	Target
Feb 20, 2021 02:47:35 UTC	CwcSystem - administrator	Administrator roles or permissions updated	[redacted]@citrix.com - administrator
Feb 19, 2021 11:49:51 UTC	[redacted]@citrix.com - system	Secure client created	MSBL_Schedule - service
Feb 18, 2021 12:52:27 UTC	[redacted]@citrix.com - administrator	'Full' Administrator invitation sent	[redacted]@citrix.com - administrator
Feb 17, 2021 09:40:55 UTC	[redacted]@citrix.com - system	Administrator created	[redacted]@citrix.com - administrator
Feb 03, 2021 11:12:27 UTC	[redacted]@citrix.com - administrator	Administrator access type updated, from 'Full' to 'Custom'	[redacted]@citrix.com - administrator
Feb 02, 2021 07:29:29 UTC	[redacted]@citrix.com - administrator	Administrator deleted	[redacted]@citrix.com - administrator

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 Government 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.

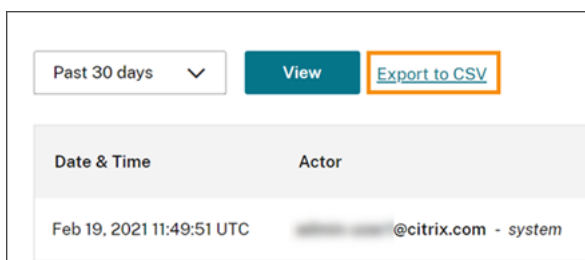
To view events that occurred up to 90 days in the past, filter the list by selecting the time period you want to view and select **View**.



## 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 Government 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 Government 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.

## SDKs

December 5, 2023

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

## Requirements

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 Government:

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

**Note:**

Alternatively, you can run the SDK installer and follow the dialogs to complete the installation. However, you must specify the Citrix Cloud Government environment when you authenticate using the `Get-XdAuthentication` cmdlet. See [To run the Remote PowerShell SDK](#) in this article.

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

To uninstall the Remote PowerShell SDK:

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

### To run the Remote PowerShell SDK

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

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

## Citrix Cloud Government platform

December 14, 2023

The Citrix Cloud Government platform has the following differences, compared to the Citrix Cloud (commercial) platform.

- Use Azure Active Directory with Citrix Cloud Government, your Azure AD infrastructure must be hosted in an Azure Government instance.  
Azure AD hosted in commercial Azure instances can't federate to Citrix Cloud Government.
- Self-service guides that provide walkthroughs of certain aspects of the platform are not available.
- Cloud license usage functions and active usage reports are not available.
- The [System Log API](#) and the [Citrix System Log Add-on for Splunk](#) are not available for use with Citrix Cloud Government.

## Workspace Service for Citrix Cloud Government

January 5, 2021

The Workspace Experience and Site aggregation are generally available to Citrix Cloud Government customers.





© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).