Citrix Cloud™ Government

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

Contents

What's new in Citrix Cloud™ Government 3

Service Level Agreement 5

How to Get Help and Support 7

Secure Deployment Guide for Citrix Cloud™ Government 12

Service trials for Citrix Cloud™ Government 17

Sign up for Citrix Cloud™ Government 20

Connectivity requirements for Citrix Cloud™ Government 29

Citrix Cloud Connector™ requirements 32

Create a resource location 40

Install Cloud Connectors from the command line 44

Citrix Cloud Connector™ proxy and firewall configuration 47

Set up DaaS 48

Set up workspaces for users 50

Citrix Networking 50

License Activation Service 51

Identity and access management for Citrix Cloud™ Government 52

Connect Active Directory to Citrix Cloud™ Government 53

Connect Microsoft Entra ID to Citrix Cloud™ Government 53

Connect an on-premises Citrix Gateway as an identity provider to Citrix Cloud™ Government 56

Connect Okta as an identity provider to Citrix Cloud™ Government 64

Connect SAML as an identity provider to Citrix Cloud™ Government 70

Manage Citrix Cloud™ Government 81

Manage Citrix Cloud™ Government administrators 83

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

System Log **90**

SDKs **93**

Citrix Cloud™ Government platform **94**

Workspace Service for Citrix Cloud™ Government **95**

Connector Appliance for Cloud Services **95**

Active Directory with Connector Appliance **124**

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

What's new in Citrix Cloud™ Government

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

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

Connect Okta as an identity provider to Citrix Cloud Government.

November 2021

Add administrators in Microsoft Entra ID groups: Citrix Cloud Government now supports adding administrators to your Citrix Cloud Government account using Microsoft Entra ID 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.

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

Service Level Agreement

Effective date: November 1st, 2024

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

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

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

- Regularly scheduled maintenance windows.
- Customer's failure to follow configuration requirements for the Service as documented on Citrix Product documentation, or abusive behavior, or faulty input.
- Customer's use of a Service after Citrix® advised Customer to modify Customer's use of the Service, if Customer did not modify use.
- Caused by any component not managed by Citrix including, but not limited to, Customer controlled physical and virtual machines, Customer installed and maintained operating systems, Customer installed and controlled software, networking equipment or other hardware; Customer defined and controlled security settings, group policies and other configuration policies; public cloud provider failures, Internet Service Provider failures; or other Customer support factors external to Citrix'control.
- Customer's employees, agents, contractors, or vendors, or anyone gaining access by means of Customer's passwords or equipment, or otherwise resulting from Customer's failure to follow appropriate security practices.
- Customer's attempts to perform operations that exceed Service entitlements.
- Service disruption due to Force Majeure, including, but not limited to, natural disasters, war or acts of terrorism, or government actions.

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

Citrix offers Service Commitments to customers that:

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

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

Per Service Availability Measures

The following table lists the uptime measures in the SLA metrics for the various services supported in Citrix Cloud Government:

Citrix Cloud Government Service	Measure for monthly uptime
Citrix Gateway Service for HDX™ Proxy	Time users can access their app or desktop session through the Service.
Citrix DaaS™	Time users can access their app or desktop session through the Service.
Citrix Workspace™	Same as above for component services, but includes availability for each. Credits may be prorated if a claim relates to less than all components.

Service Commitment and Remedies

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

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

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

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

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

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

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

How to Get Help and Support

Signing in to your account



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

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

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 Microsoft Entra ID is enabled as the identity provider for your account. For more information about using Microsoft Entra ID as your identity provider, see Connect Microsoft Entra ID 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:

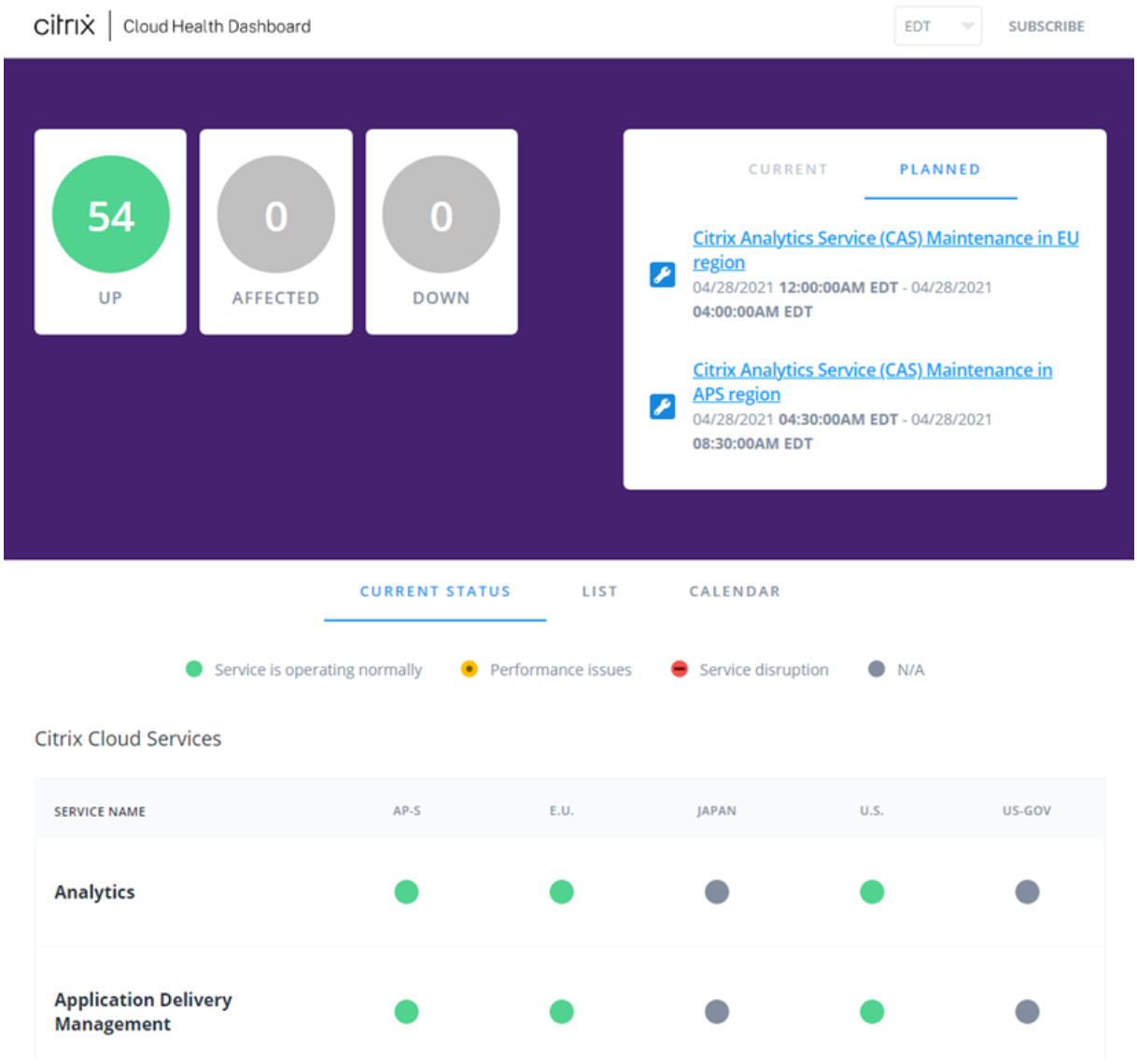
- At least 12 characters long
- Includes at least one upper-case letter
- Includes at least one lower-case letter
- Includes at least one number
- Includes at least one special character: `! @ # $ % ^ * ? + = -`

> **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.

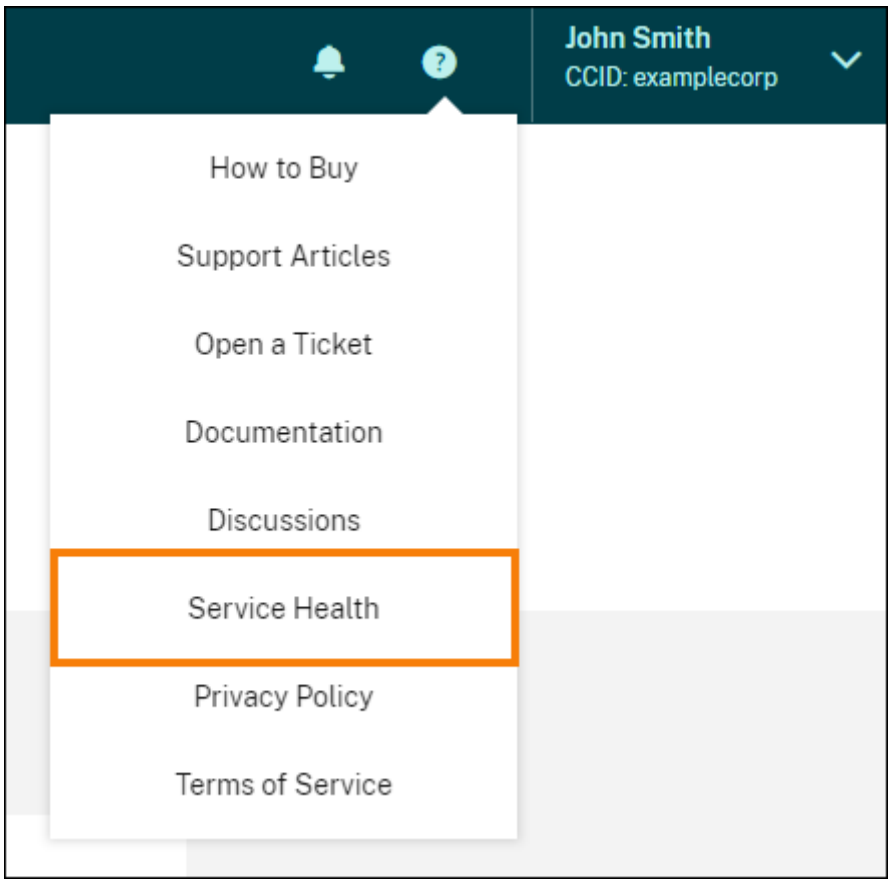
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

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

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



Use the dashboard to learn more about the following conditions:

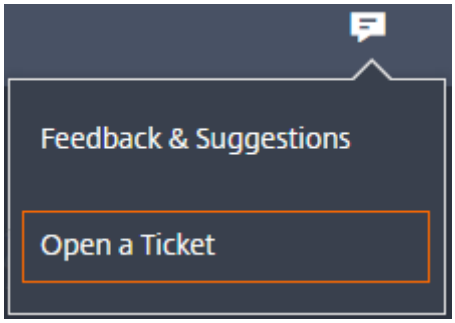
- The current health status of all Citrix Cloud services, grouped by geographical region
- The health history of each service for the last seven days
- Maintenance windows for specific services

You can also subscribe to notifications about events like maintenance windows and service incidents. For more information about Cloud serice health, see Citrix Cloud service health.

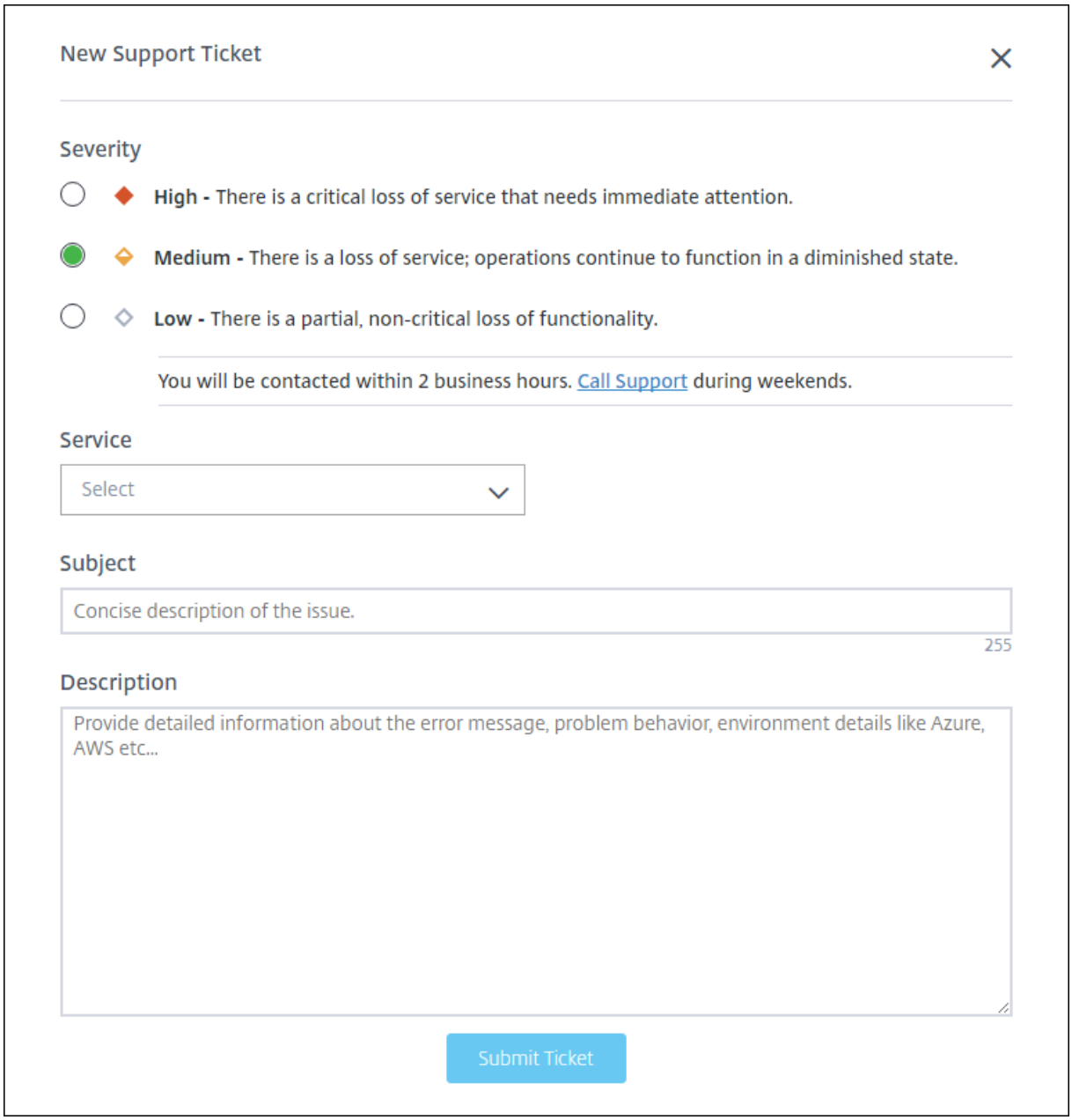
Technical Support

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.**

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



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.



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

Secure Deployment Guide for Citrix Cloud™ Government

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 Microsoft Entra ID.

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.

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

- 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 or higher 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` domain. To access Citrix Cloud Government, customers must use a browser capable of TLS 1.2 or higher with strong cipher suites.

The following strong ciphers are recommended: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

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

Data sovereignty

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

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

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.

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

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.

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

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\Logs.

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

SSL/TLS Configuration

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

The Cloud Connector must trust the certification authority (CA) used by Citrix Cloud 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).

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

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

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

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

		Citrix Cloud Government Trial
	Maximum Length	60 calendar days. You can request a trial for the service only once.
	Availability	Restricted availability
	Resource location	Customer provided and configured
	User session length	Unlimited
	Local Microsoft Active Directory integration	Yes
	Choice of resource locations	Yes
	Deploy to on-premises	Yes
	Citrix DaaS (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 participants at any given time.

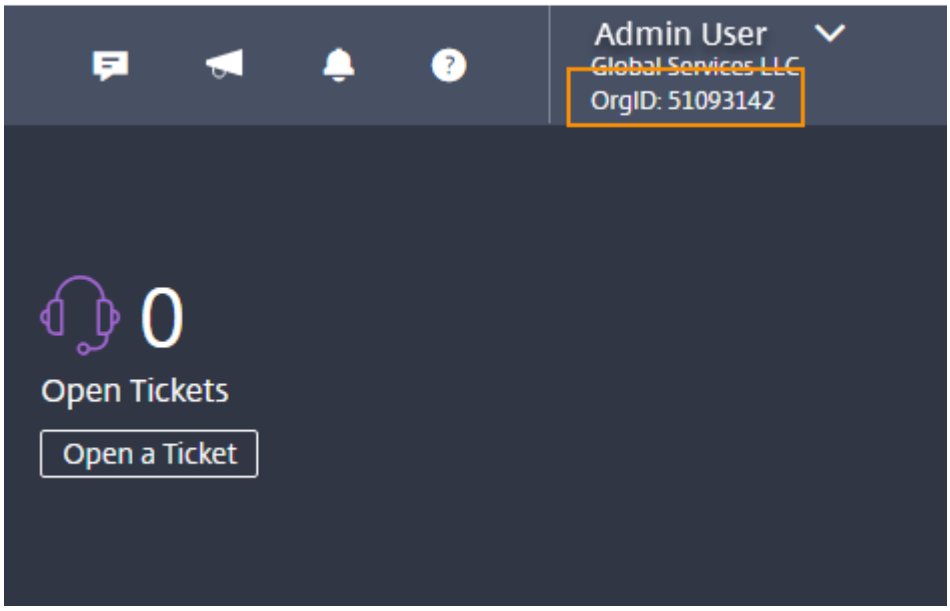
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Purchase services

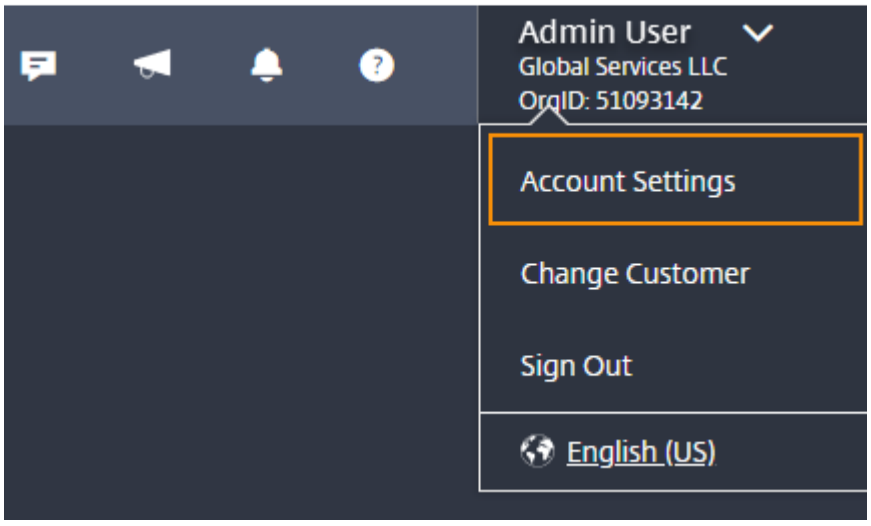
When you're ready to convert your trial to a production service, contact a Citrix sales representative.

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.

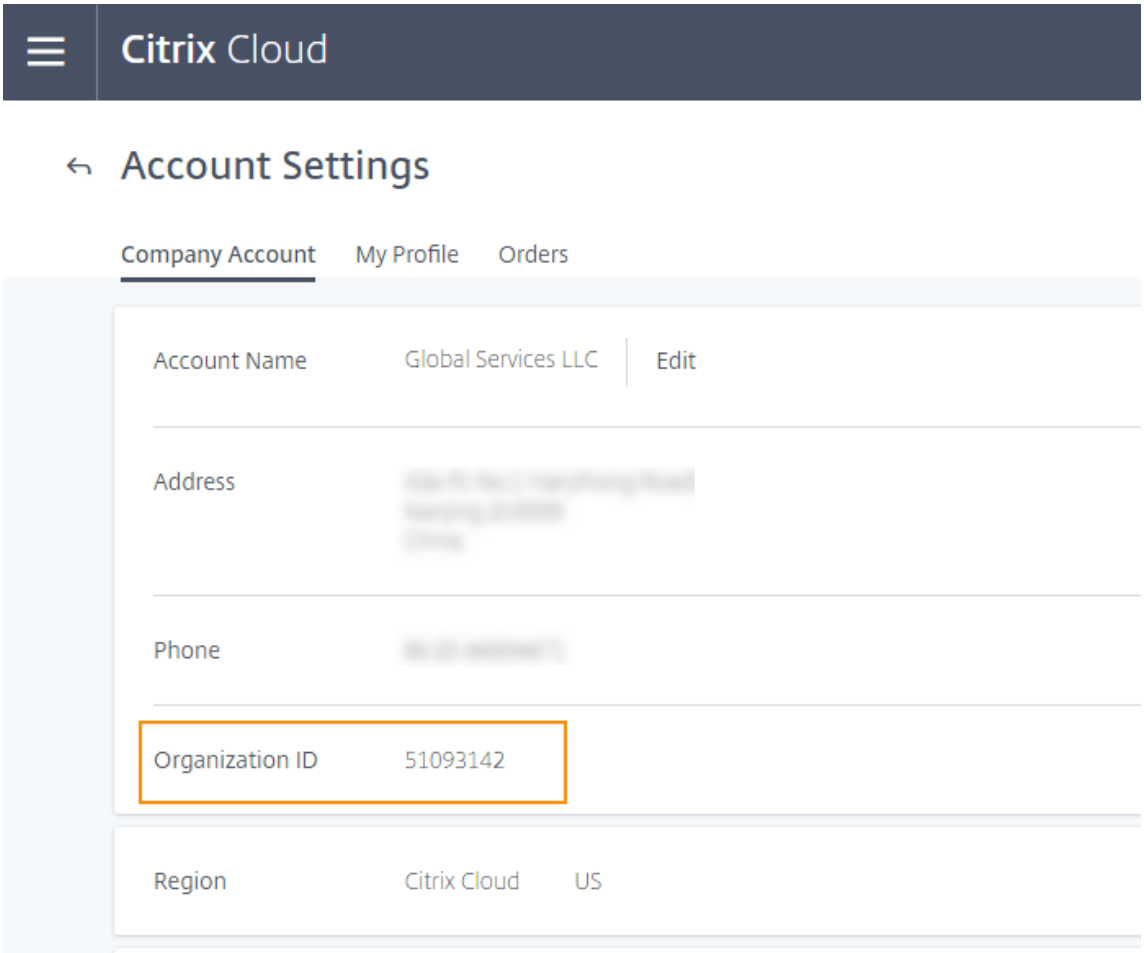


- From the top-right menu, click **Account Settings**.



  Your OrgID is shown in the Organization ID field.

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



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

Sign up for Citrix Cloud™ Government

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

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

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.

Onboard your Citrix Cloud account

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

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**.

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

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.

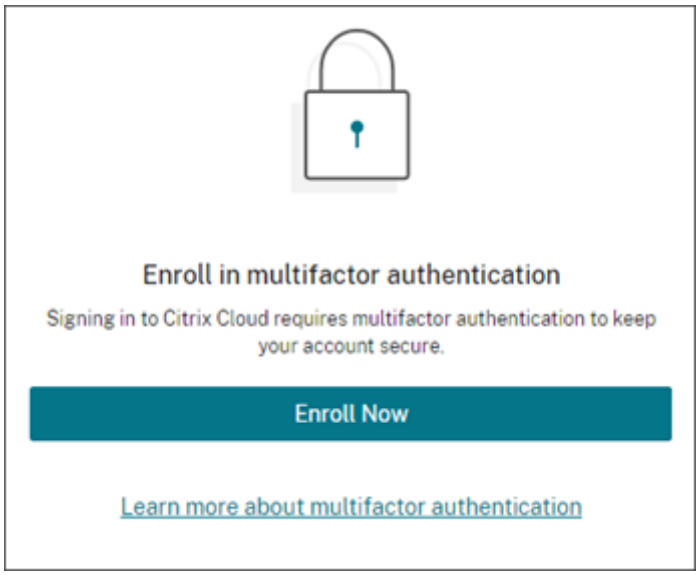
Sign in with your Citrix Cloud Government credentials

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.



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

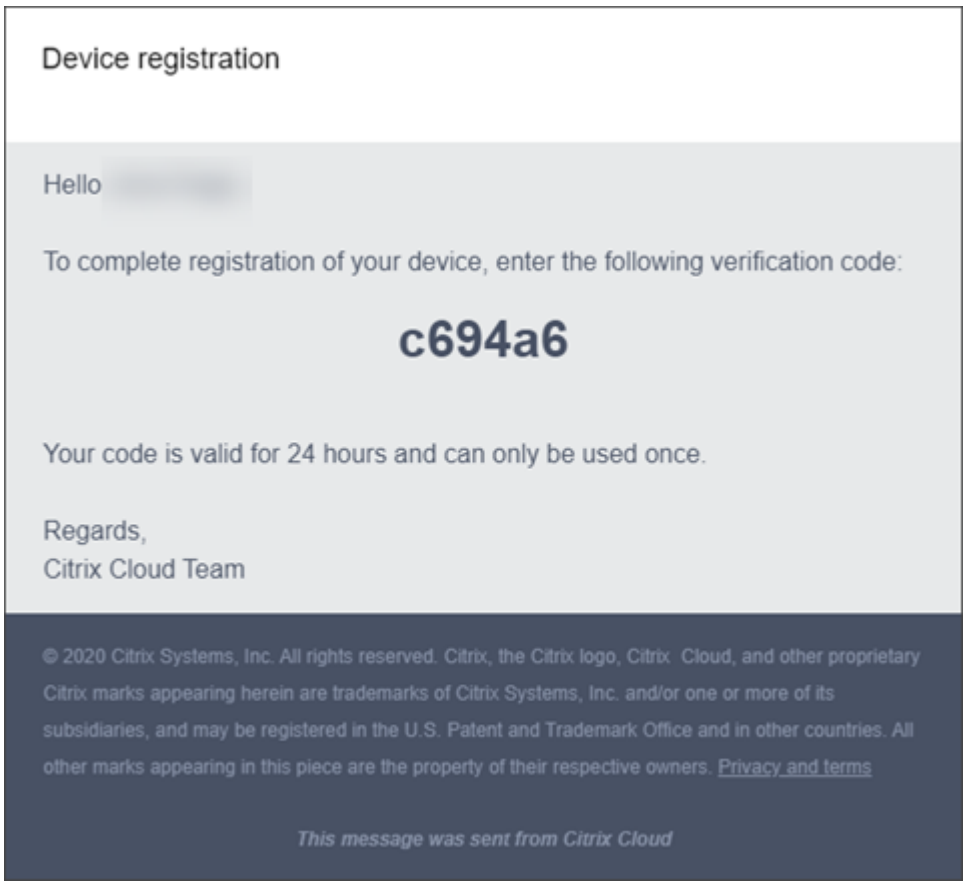
During enrollment, Citrix Cloud Government presents a QR code and a key. Depending on your authenticator app, you either scan the QR code or enter the key to register your device.
For a smooth enrollment process, Citrix recommends downloading and installing this app on your device beforehand. Citrix 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 your'e 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:

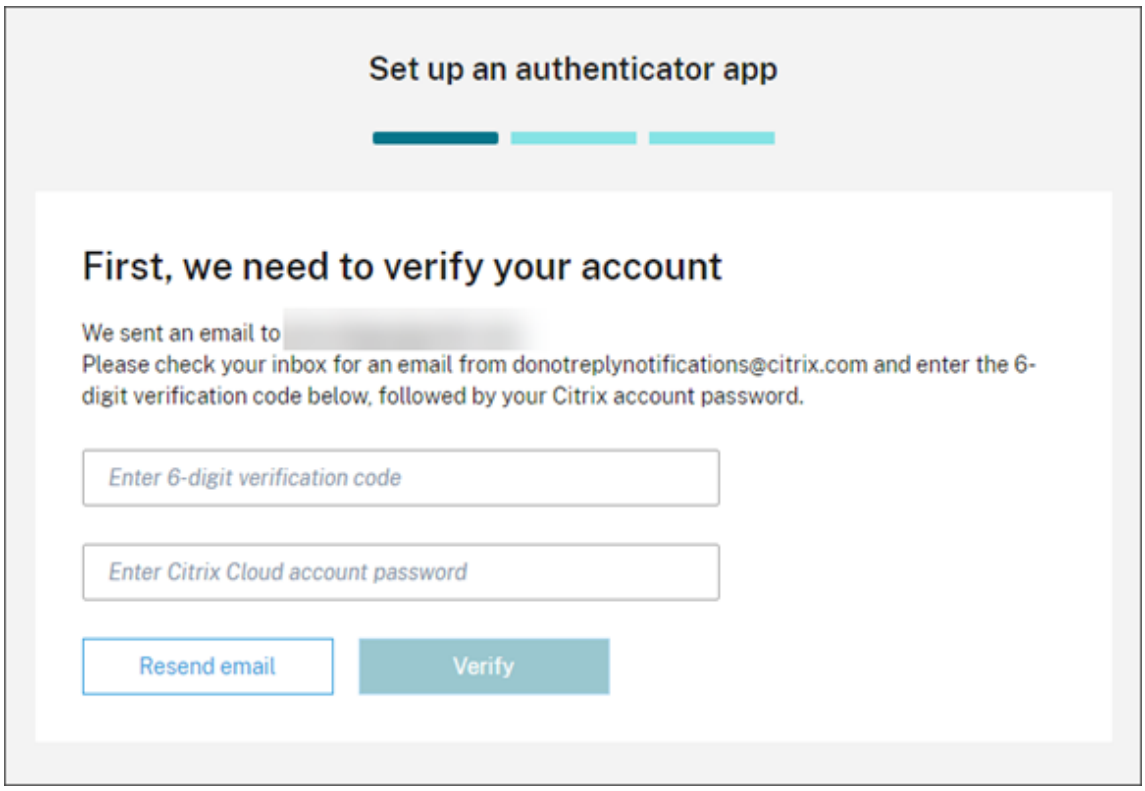
1. Go to Citrix Cloud Government at https://citrix.cloud.us and verify that the URL redirects to https://citrix.cloud.us. Sign in using your Citrix Cloud Government credentials.
   Citrix Cloud Government sends you an email with a verification code.

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



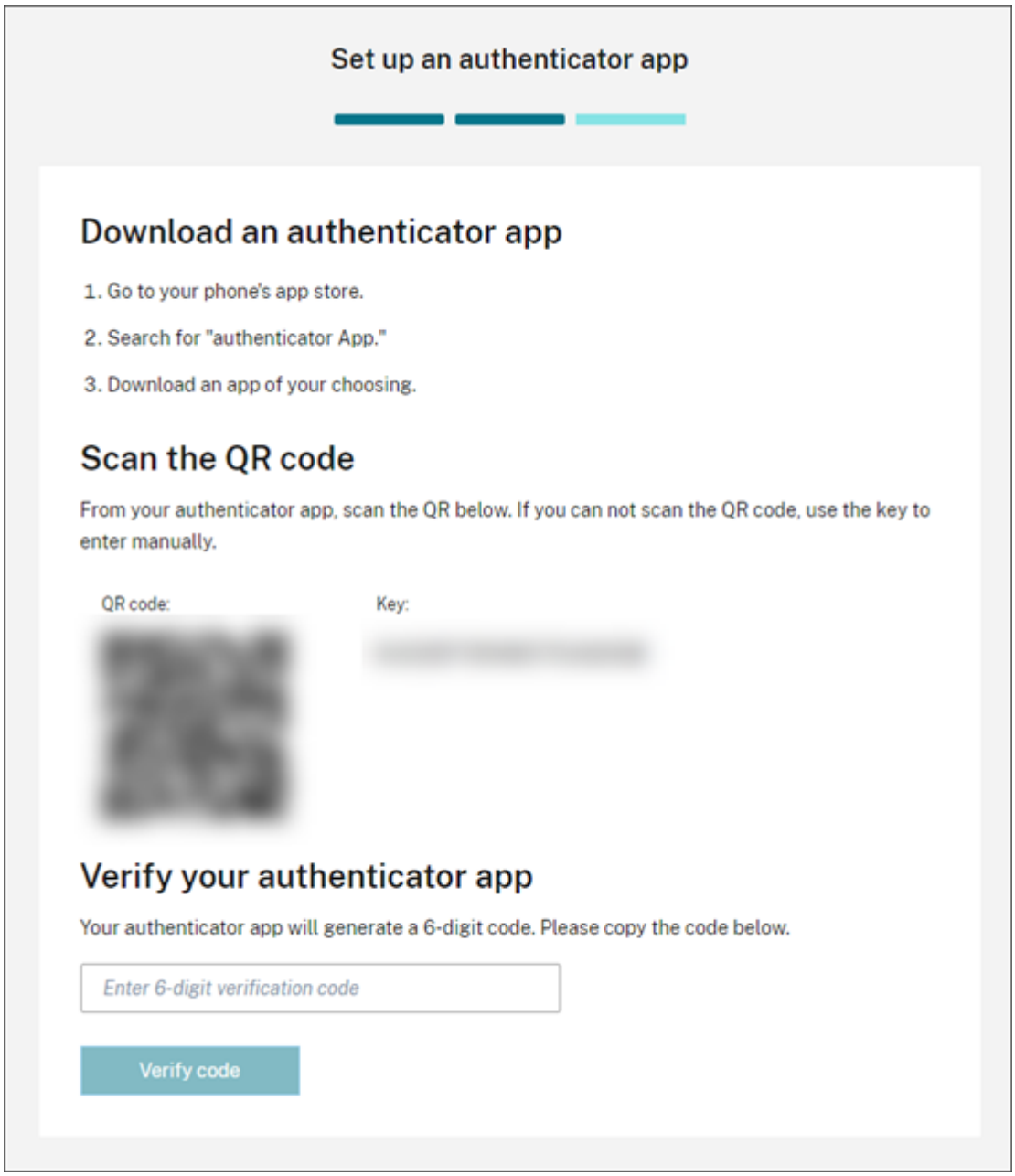
2. After you receive the email, enter the 6-digit verification code and your Citrix Cloud Government password and select **Verify**.

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



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.

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

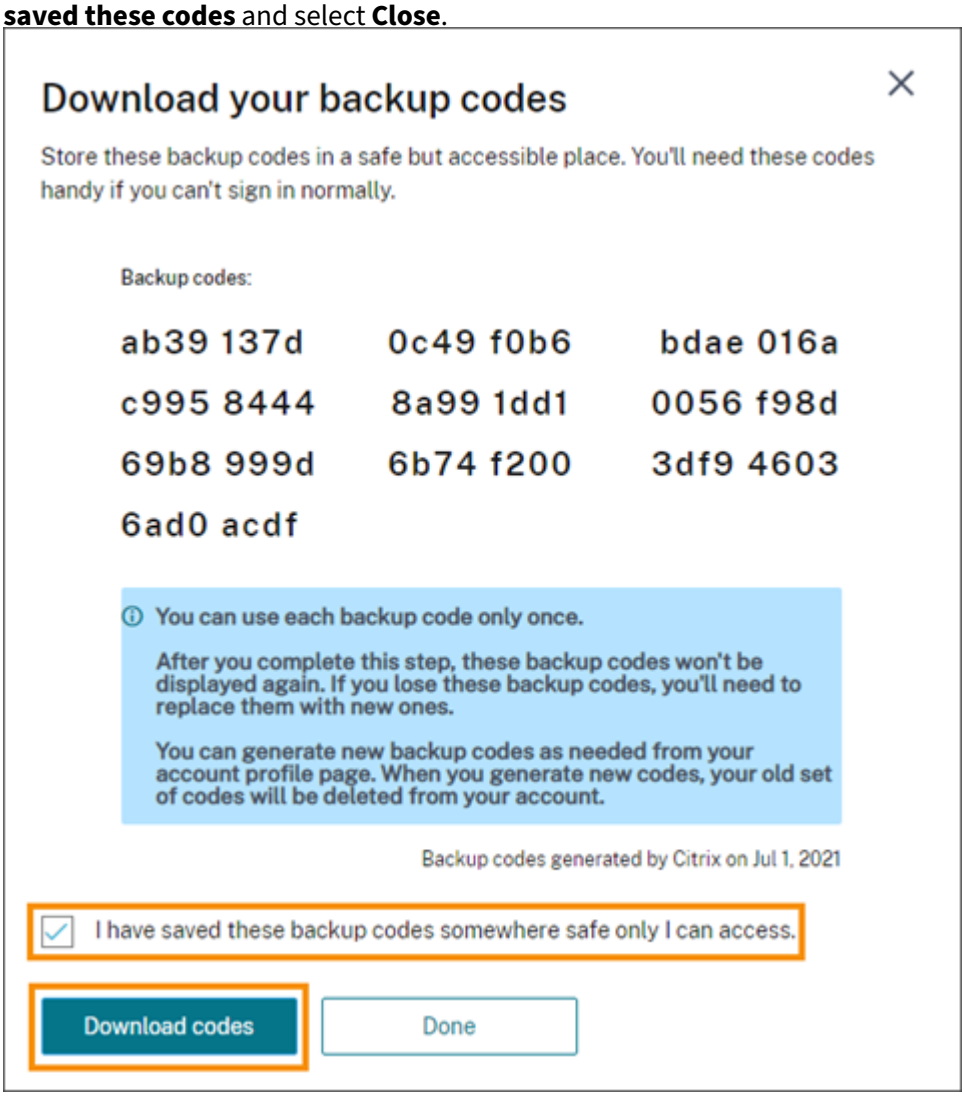


4. Under **Verify your authenticator app**, enter the code from your authenticator app and select **Verify code**.
5. Configure the following account recovery methods in case you lose your device or can't use your authenticator app:

    - 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

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

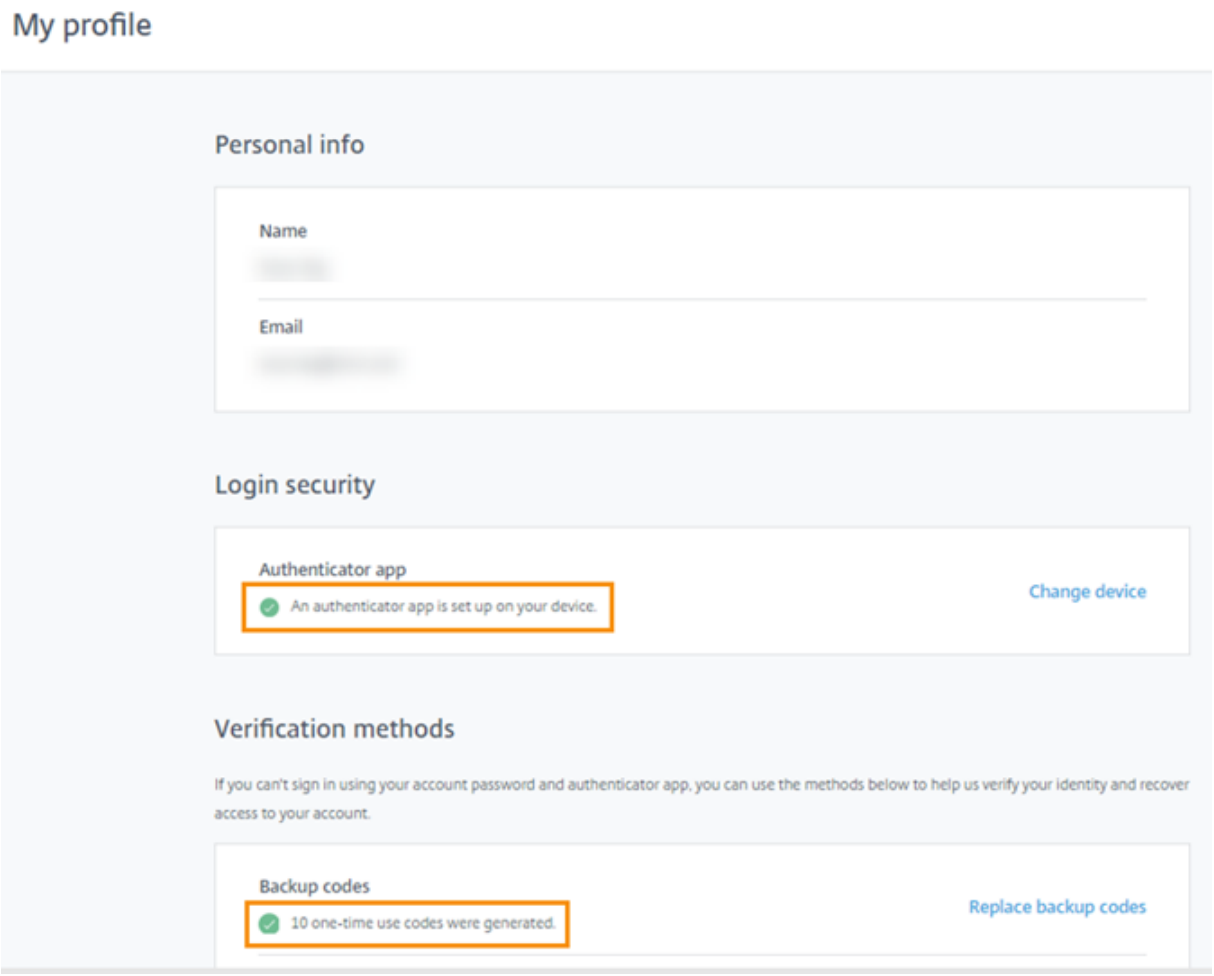
backup codes to help you sign in if you can't use your authenticator app. When prompted, select **Download codes** to download your backup code as a text file. Then, select **I've saved these codes** and select **Close**.



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

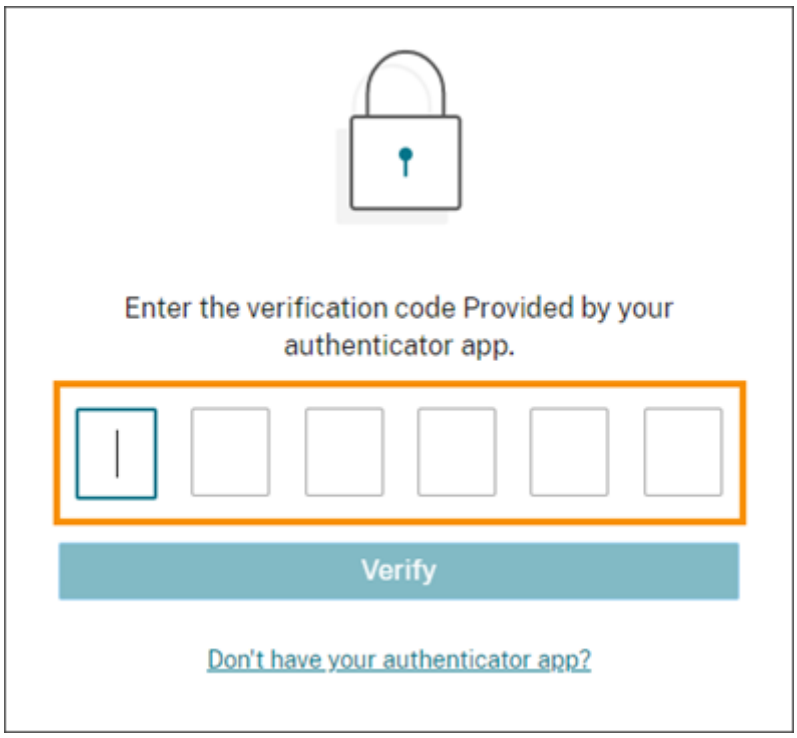
When your enrollment is completed, the Citrix Cloud console appears. From the top-right menu, select **My Profile**. After successful enrollment, the **Authenticator app** section displays a green check mark and the My Profile page displays your configured recovery methods.

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



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.

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



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

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.

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

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.

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

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://fqdnallowlistsa.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://*.cloud.us
- https://*.apps.cloud.us
- https://*.blob.core.usgovcloudapi.net
- https://*.servicebus.usgovcloudapi.net
- https://*.xendesktop.us

Administration console:

- https://*.citrixworkspacesapi.us
- https://*.cloud.us
- https://*.blob.core.usgovcloudapi.net
- https://*.xendesktop.us

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

Citrix DaaS Remote PowerShell SDK

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

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

Citrix Cloud Connector™ requirements

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

System requirements

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

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

.NET requirements

Microsoft .NET Framework 4.7.2 or later is required.

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

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

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

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`
- The following root certificates are installed:
  - `https://cacerts.digicert.com/DigiCertGlobalRootG3.crt`
  - `https://cacerts.digicert.com/DigiCertGlobalRootG2.crt`
  - `https://cacerts.digicert.com/DigiCertGlobalRootCA.crt`
  - `https://cacerts.digicert.com/DigiCertTrustedRootG4.crt`

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

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

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

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

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

Active Directory requirements

- Joined to an Active Directory domain that contains the resources and users that you use to create offerings for your users. 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.

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

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.

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

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 do-

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

main. 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.

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

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.

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

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

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

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

What is a resource location?

A resource location contains the compute and network resources required to deliver services to your users. The resources that your resource location contains depends on the services you want to deliver. For example, if you plan to deliver applications and desktops through Citrix DaaS (formerly 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.

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

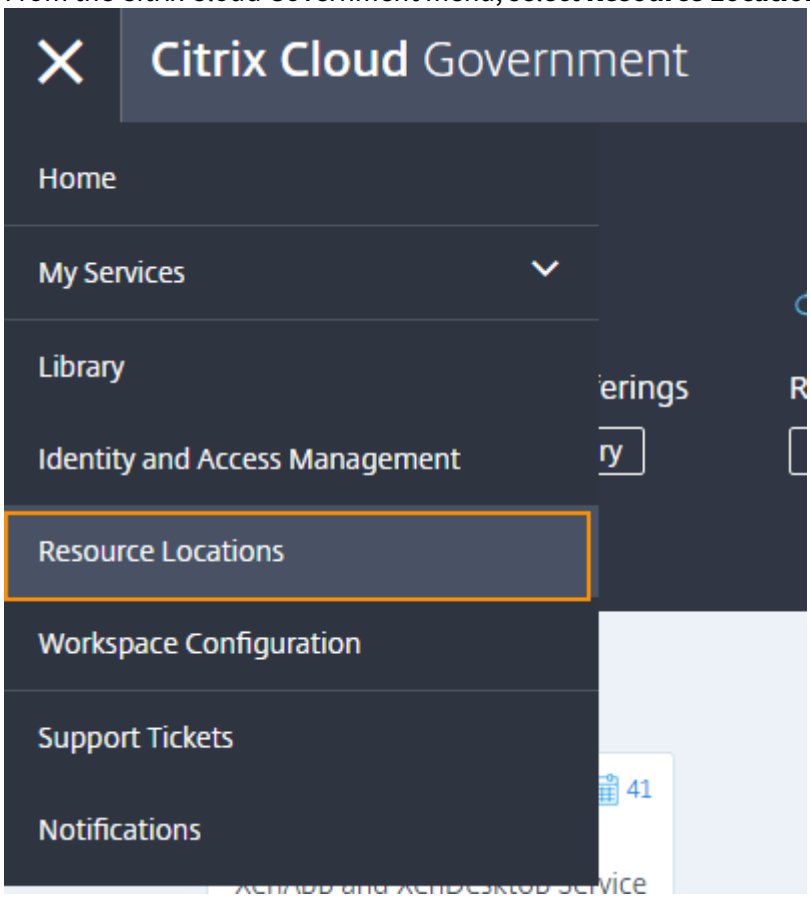
1. Review Connectivity requirements for a list of contactable addresses for available services.
2. Make sure port 443 (HTTPS) is open for outbound connections.
3. Ensure that the required addresses can be contacted so that you can operate and consume Citrix Cloud Government services.
4. Review Citrix 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.

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

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.

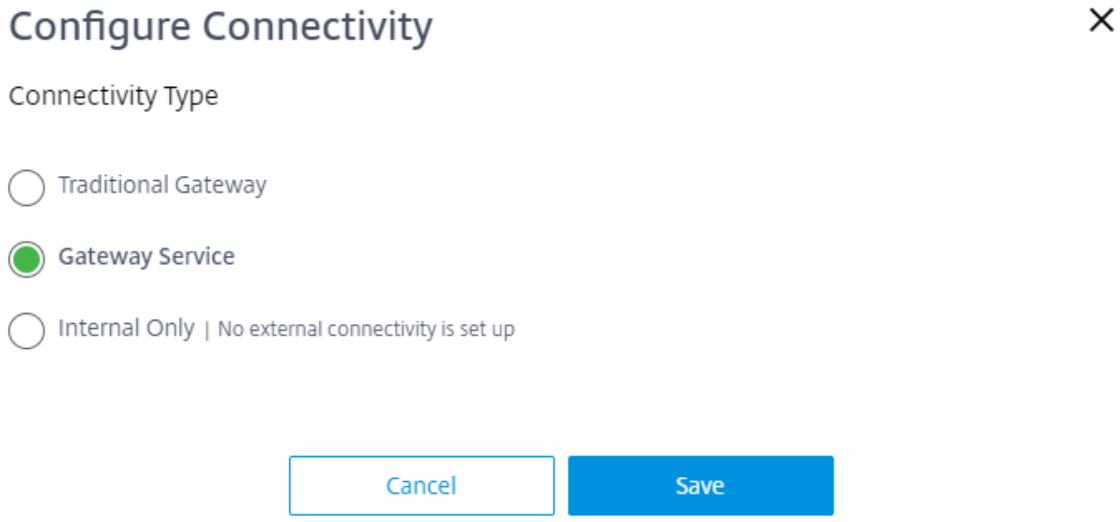
After installation, Citrix Cloud registers your domain in **Identity and Access Management**.

> **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.



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

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

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

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.

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

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 service principal.
    - The client ID and secret ensures that your access to the Citrix Cloud API is secured appropriately. When you create a service principal, the client operates as much with administrator permissions that you have.
- To install a Cloud Connector, you must use a service principal 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 service principal

When creating a service principal, 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 **service principals** tab, enter a name for your client and select **Create Client**. Citrix Cloud Government generates and displays a client ID and secret for the service principal.
3. Select **Download** to download the client ID and secret as a CSV file and store it in a secure location. 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 service principal 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:

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

- **customerName** Required. The customer ID shown on the API Access page in the Citrix Cloud Government console.
- **clientId** Required. The service principal ID that an administrator can create, available on the API Access page.
- **clientSecret** Required. The service principal secret that can be downloaded after the service principal 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:

```
{

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

A sample command line that installs using the parameter file:

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

Use **Start /Wait CWCConnector.exe /ParametersFilePath:value** to examine a potential error code 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.

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

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

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.

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

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:

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

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

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:

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

- 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

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

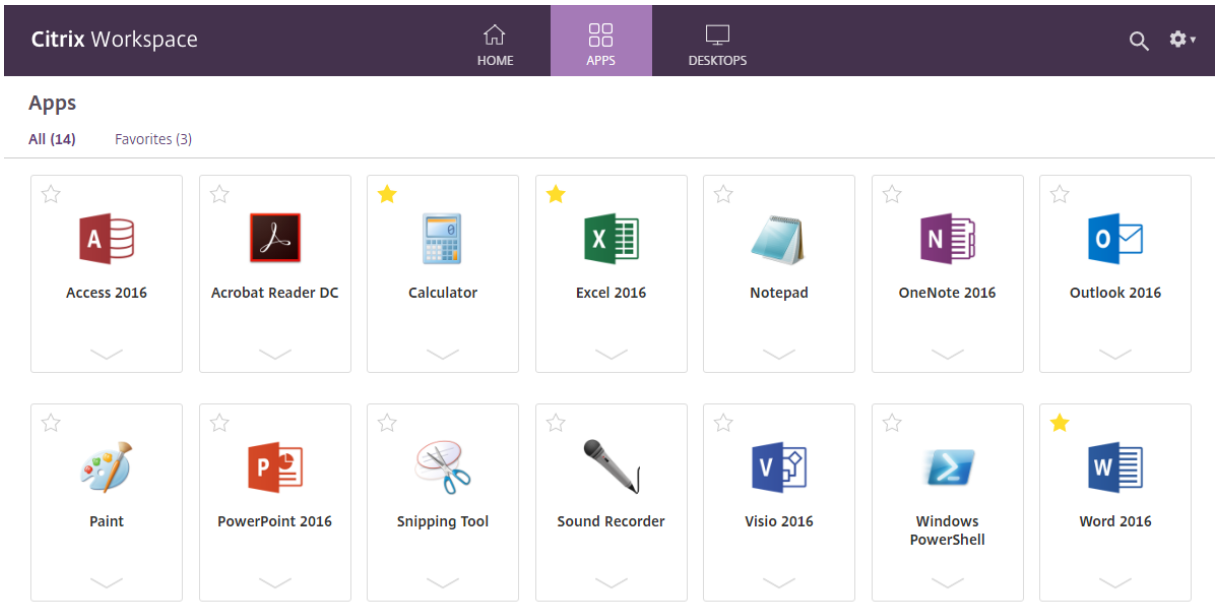
- Policies
- Managing resources and users
- Monitoring

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

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

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

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

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.

License Activation Service

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

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

For more information, see License Activation Service.

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

Identity and access management for Citrix Cloud™ Government

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:

- Microsoft Entra ID: 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.

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

> **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

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 Microsoft Entra ID to Citrix Cloud™ Government

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 Microsoft Entra ID instead.

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

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

- Use your own Active Directory, so you can control auditing, password policies, and easily disable accounts when needed.
- Configure 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 Microsoft Entra ID

Before you can use Microsoft Entra ID, be sure you meet the following requirements:

- **Your Microsoft Entra ID infrastructure is hosted in an Azure Government instance.** You can't federate Microsoft Entra ID hosted in a commercial Azure instance to Citrix Cloud Government. If you attempt to use Microsoft Entra ID in a commercial Azure instance with Citrix Cloud Government, Microsoft Entra ID 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 Microsoft Entra ID.** To configure, you can sync accounts from your on-premises Active Directory into Microsoft Entra ID using Microsoft's Microsoft Entra ID Connect tool. Alternatively, you can configure non-synced Microsoft Entra ID accounts with Office 365 email.

Sync accounts with Microsoft Entra ID Connect

1. Ensure that the Active Directory accounts have the Email user property configured:
    a) Open Active Directory Users and Computers.
    b) In the **Users** folder, locate the account you want to check, right-click, and select **Properties**. On the **General** tab, verify the **Email** field has a valid entry. Citrix Cloud requires that administrators added from Microsoft Entra ID have different email addresses than administrators who sign in using a Citrix-hosted identity.
2. Install and configure Microsoft Entra ID Connect. For complete instructions, see Integrate your on-premises directories with Microsoft Entra ID on the Microsoft Azure website.

Connect Citrix Cloud Government to Microsoft Entra ID

When connecting your Citrix Cloud Government account to your Microsoft Entra ID, 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 Microsoft Entra ID. Citrix requests this permission so it can

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

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 **Microsoft Entra ID**, click the ellipsis button, and then select **Connect**.
4. When prompted, enter a short, URL-friendly identifier for your company and click **Connect**. The identifier you choose must be globally unique within Citrix Cloud 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 Microsoft Entra ID

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 **Microsoft Entra ID**.
4. Type the name of the user that you want to add and then click **Next**.
    - Inviting Microsoft Entra ID guest users is not supported.
5. In **Set access**, configure the appropriate permissions for the administrator.
6. Review the administrator details. Select **Back** to make any changes.
7. Select **Send invitation**. Citrix Cloud 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 Microsoft Entra ID. You can verify the user's email address and completes the connection between the Microsoft Entra ID user account and Citrix Cloud Government.

Add Microsoft Entra ID administrator groups to Citrix Cloud Government

You can add administrators to your Citrix Cloud Government account using Microsoft Entra ID (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.

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

Sign in to Citrix Cloud using Microsoft Entra ID

After the Microsoft Entra ID user accounts are connected, users can sign in to Citrix Cloud Government using one of the following methods:

- Navigate to the administrator sign-in URL that you configured when you initially connected the Microsoft Entra ID identity provider for your company. Example: `https://citrix.cloud.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 Microsoft Entra ID, and click **Continue**.

Enable advanced Microsoft Entra ID capabilities

Microsoft Entra ID 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 Microsoft Entra ID users enables Citrix Cloud Government to use those capabilities automatically.

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

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:

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

- 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

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

- 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.

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

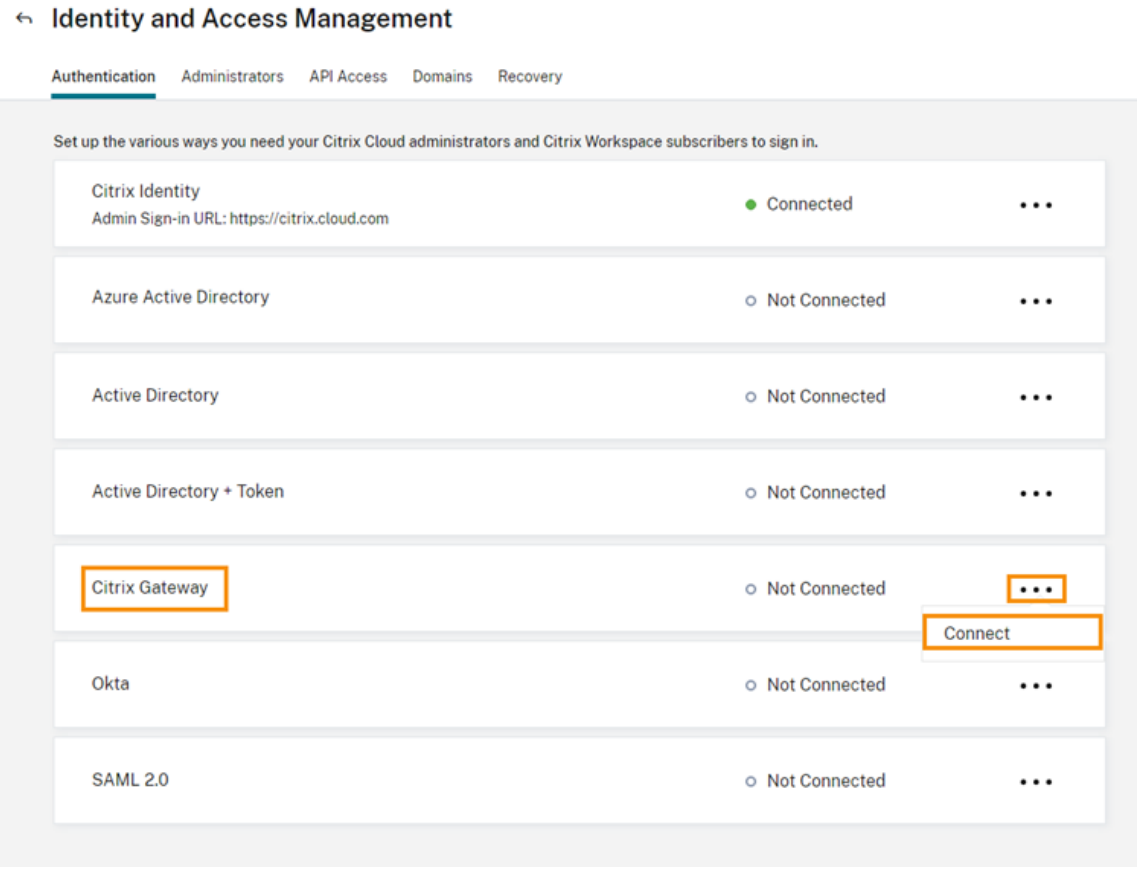
Task overview

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.

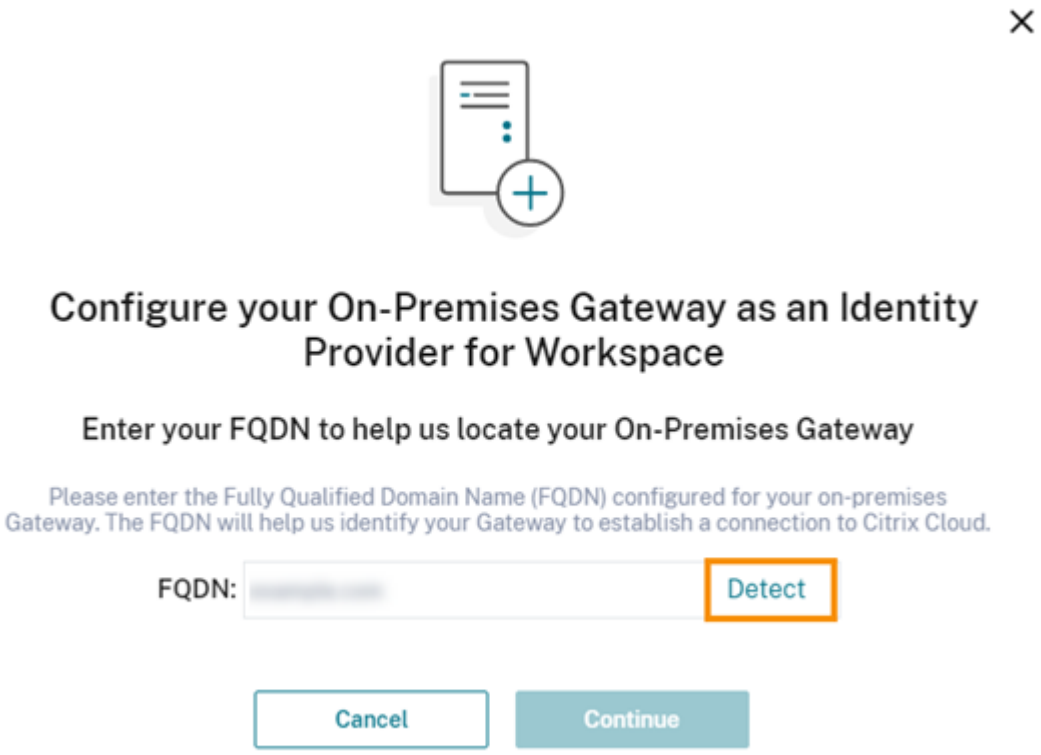
To enable Citrix Gateway authentication for workspace subscribers

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**.



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

3. Enter the FQDN of your on-premises Gateway and click **Detect**.

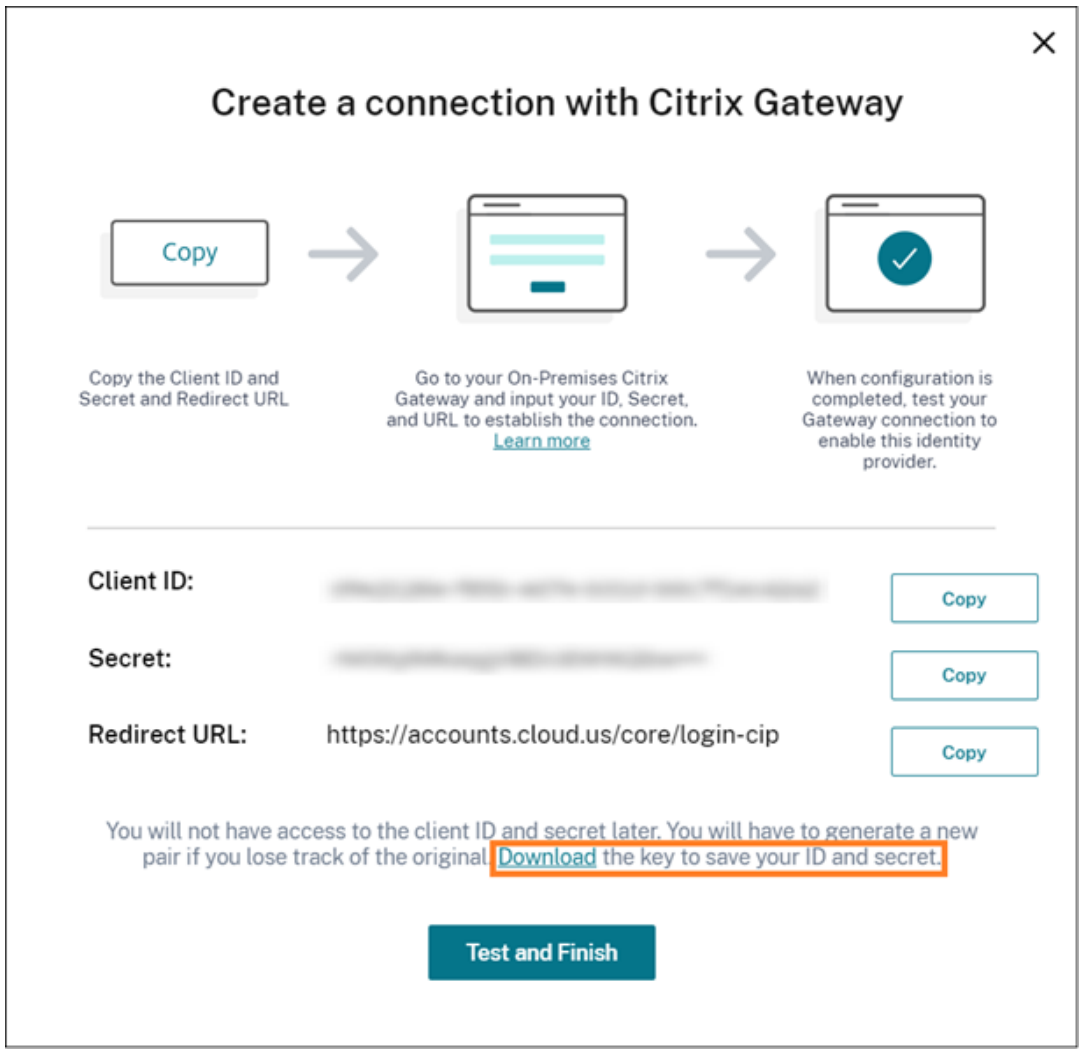


After Citrix Cloud Government detects it successfully, click **Continue**.

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

   a) Copy the Client ID, Secret, and Redirect URL that Citrix Cloud Government displays.

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



Also, download a copy of this information and save it securely offline for your reference. This information 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**.

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

Troubleshooting

As a first step, review the Prerequisites and Requirements sections in this article. Verify you have all the required components in your on-premises environment and that you have made all required configurations. If any of these items are missing or misconfigured, 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

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

user properties and AD configuration properties.

Ensure that you have LDAP policies configured, even if authentication is 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:

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

a) Select **Security > AAA –Application Traffic > Policies > Authentication > Advanced Policies > Policy Label > Add**.
b) In **Name**, enter a friendly name for the authentication policy label.
c) In Login Schema, select **LSCHEMA_INT**.
d) Under **Policy Binding**, in **Select Policy**, select the LDAP advanced authentication policy you created earlier.
e) In **GoTo Expression**, select **END**.
f) Click **Bind** to finish the configuration.

4. Define the LDAP Authentication Policy Label as the next factor, after the primary identity provider:

a) Select **System > Security > AAA - Application Traffic > Virtual Servers**.
b) Select the virtual server that 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

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. Subscribers 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).

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

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,

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

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.

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

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 your'e 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.

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

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

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

- Attribute Required: Yes

i) Select **Save and Add Another**.

j) Enter the following information:

- Display Name: cip_oid
- Variable Name: cip_oid
- Description: AD User GUID
- Attribute Length: 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**.

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

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

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).

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

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

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

  - 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.

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

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.

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

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.

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

- 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.

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

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

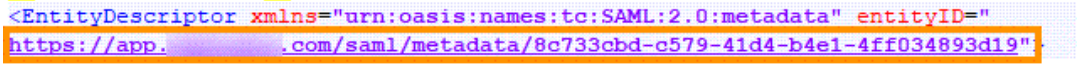
1. Acquire the SAML metadata from your SAML provider. The following image is an example of what this file might look like:

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



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.

   - 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**.

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

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

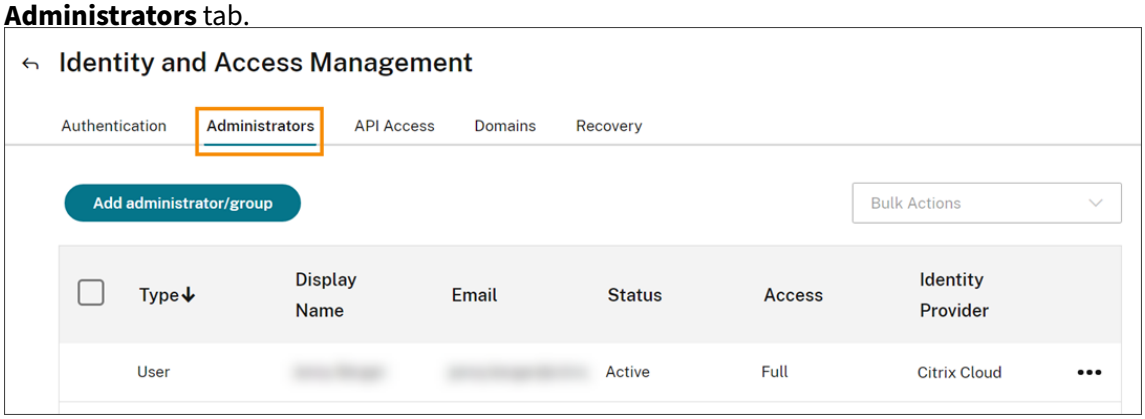
- In **SAML Response**, select the signing method your SAML provider uses for the SAML Response and SAML Assertion. By default, Citrix Cloud Government rejects any responses that aren't signed as specified in this field.

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.

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

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**.

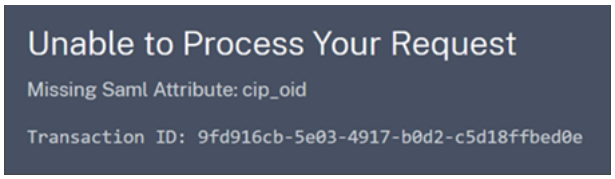
Enable SAML authentication for workspaces

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.



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

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

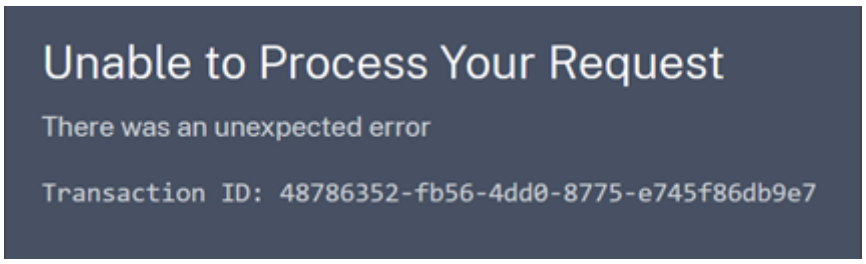
Attribute	Encoding
cip_email	Must be in String format (`user@domain`)
cip_oid	Must be in Base64 or String format
cip_sid	Must be in Base64 or String format
cip_upn	Must be String format (`user@domain`)

Unexpected errors

Citrix Cloud 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.

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

Manage Citrix Cloud™ Government

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

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

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.

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

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

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.
- Microsoft Entra ID: 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:

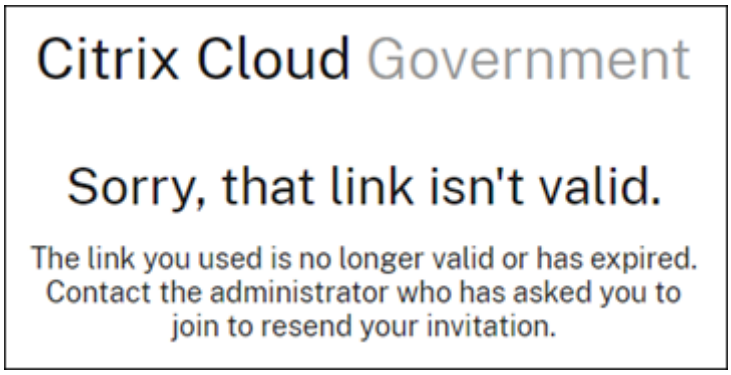
1. Select the identity provider that you want to use for authenticating administrators.
2. Depending on the identity provider, invite individual administrators or select the groups that the administrators belong to.
3. Specify the access permissions that align with the administrators' roles in your organization. For more information, see configure administrator permissions in this article.

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

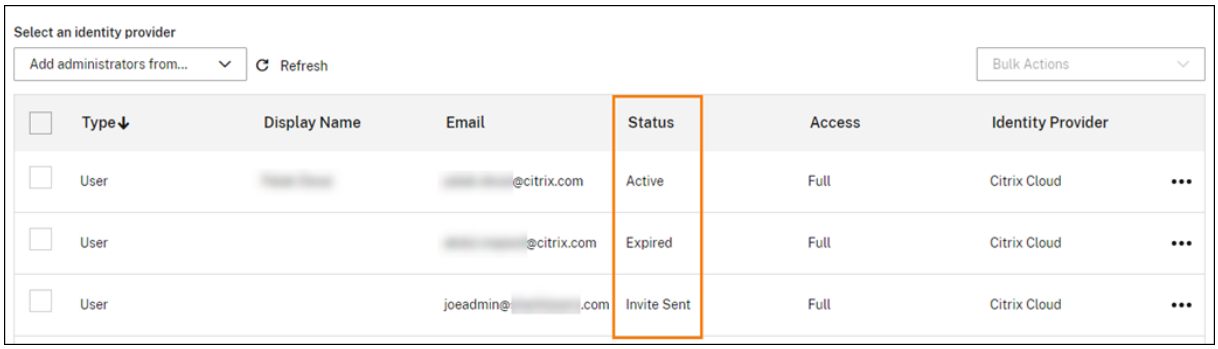
Invite individual administrators

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` 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.



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 Microsoft Entra ID, Citrix Cloud might prompt you to sign in first.

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

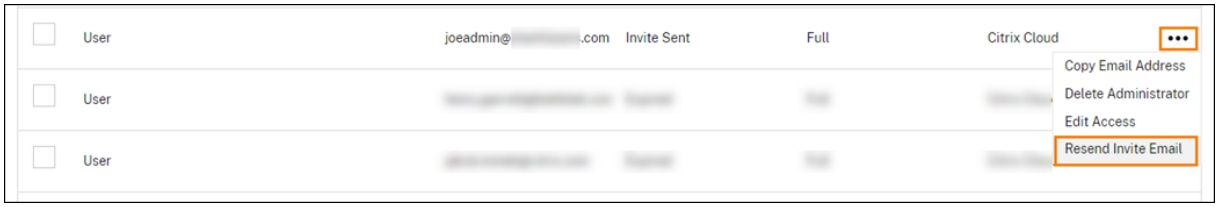
5. If **Citrix Identity** is selected, enter the user's email address and then select **Next**.
6. If **Microsoft Entra ID** is selected, type the name of the user you want to add and then click **Next**. Inviting Microsoft Entra ID guest users is not supported.
7. In **Set access**, configure the appropriate permissions for the administrator. **Full access** (selected by default) allows control of all Citrix Cloud 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 Microsoft Entra ID groups (for Microsoft Entra ID authentication). These administrators can only manage Citrix DaaS (formerly Citrix Virtual Apps and Desktops™ service). For more information, see the following articles:

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

- 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.
- **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.

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

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**.

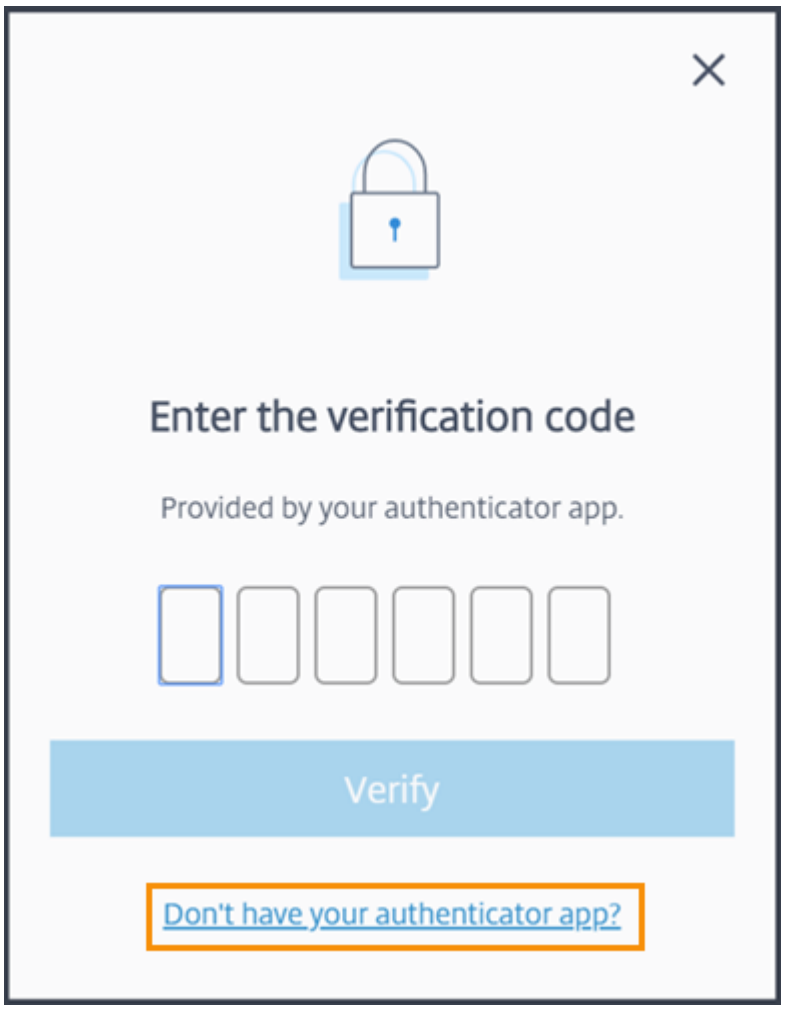
Change your device for multifactor authentication

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.

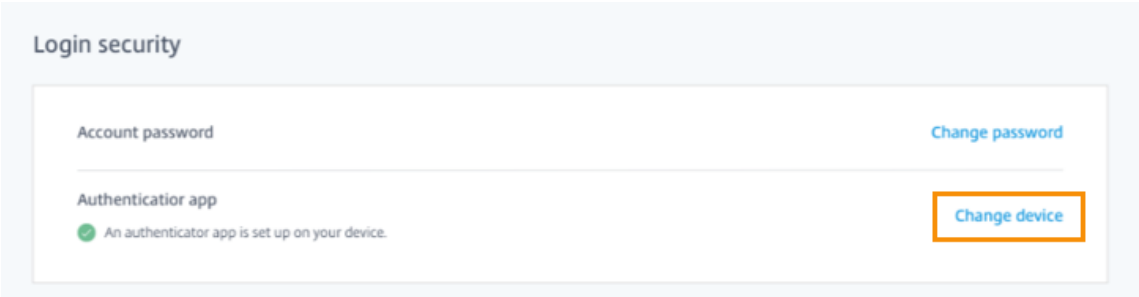
1. Sign in to Citrix Cloud Government and enter the code from your authenticator app.

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



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

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

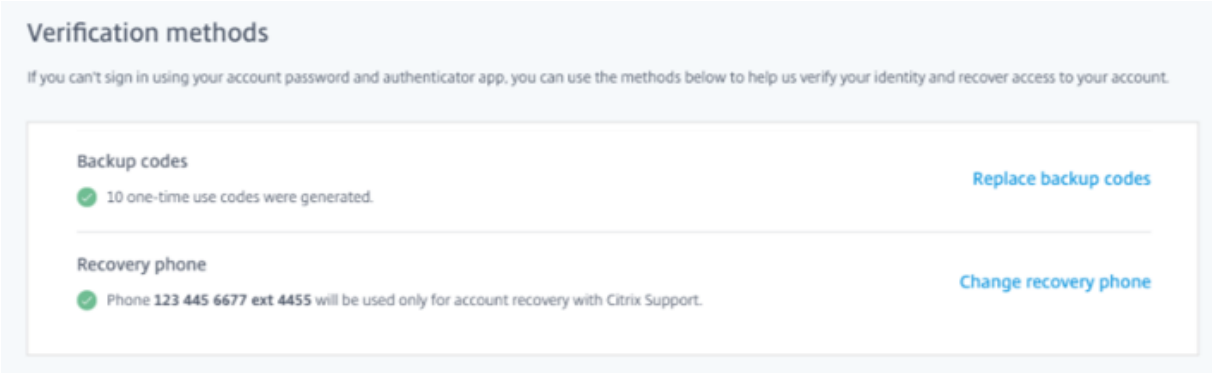


© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**.

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

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**.

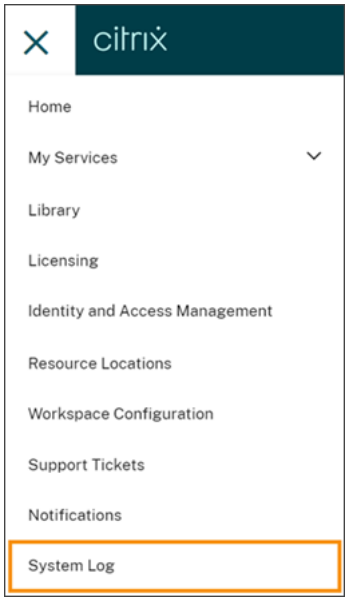
Change your recovery phone number

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

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.

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

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:

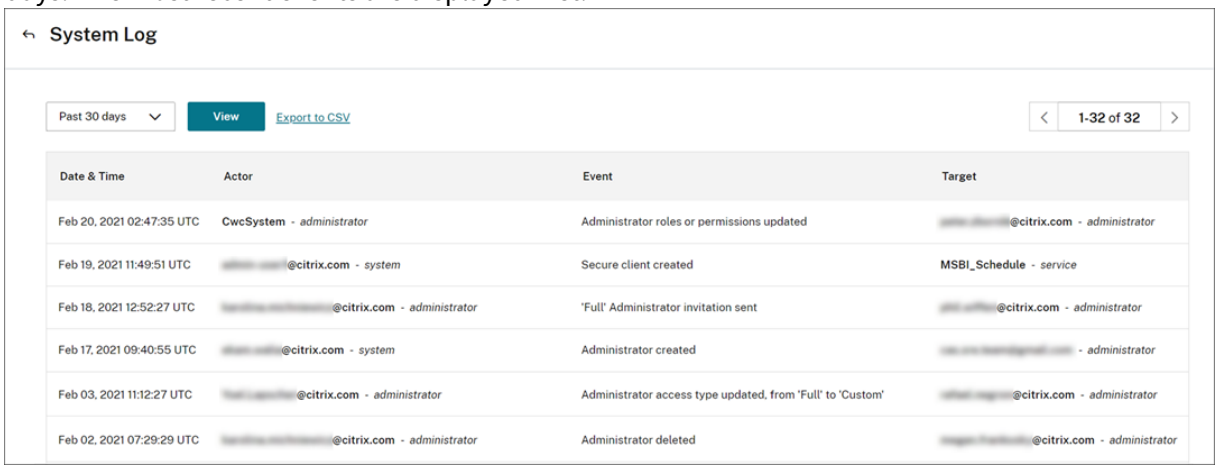
- SystemLog API
- Splunk add-on for the system log

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.



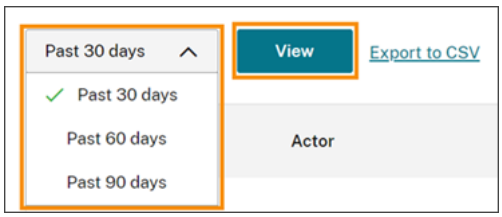
The displayed list includes the following information:

- Date and time (UTC) when the event occurred.
- Actor that initiated the event, such as an administrator or service principal. Entries with the actor **CwcSystem** indicate that Citrix Cloud Government performed the operation.
- Brief description of the event, such as editing an administrator or creating a new service principal.

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

- 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.

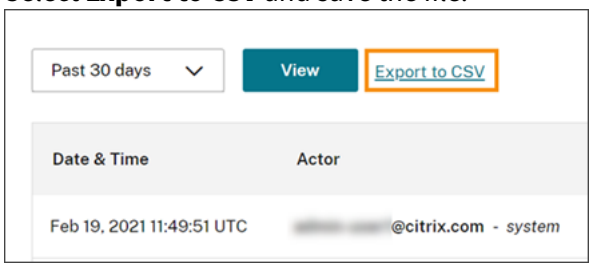
To view events that occurred up to 90 days in the past, filter the list by selecting the time period you want to view and select **View**.



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 service principal.

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.

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

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

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.

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

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

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

- Use Microsoft Entra ID with Citrix Cloud Government, your Microsoft Entra ID infrastructure must be hosted in an Azure Government instance.
  Microsoft Entra ID 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.

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

Workspace Service for Citrix Cloud™ Government

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

Connector Appliance for Cloud Services

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

Connector Appliance functions

- **Connecting Active Directory to Citrix Cloud** enables AD management, allowing the use of AD forests and domains within your resource locations. It removes the need for adding any additional AD trusts. For more information, see Active Directory with Connector Appliance.

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

The Connector Appliance platform is part of Citrix Cloud Platform and Citrix Identity Platform and can process data, including the following information:

- IP addresses or FQDNs
- Device, user, and resource location identifiers
- Timestamps
- Event data
- User and group details from Active Directory (for example, used for authenticating and searching for users and groups)

Details of specific information processed by the Connector Appliance are available in the *Data Collected by Citrix Cloud Platform* table in the Citrix Cloud Services Data Protection Overview.

Connector Appliance availability and load management

For continuous availability and to manage load, install multiple Connector Appliances in each of your resource locations. Citrix recommends at least two Connector Appliances in each resource location. If one Connector Appliance is unavailable for any time, the other Connector Appliances can maintain the connection. Since each Connector Appliance is stateless, the load can be distributed across all

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

available Connector Appliances. There is no need to configure this load balancing function. It is automated. If at least one Connector Appliance is available, there is no loss in communication with Citrix Cloud.

If you have only one connector configured for a resource location, Citrix Cloud shows a warning on both the **Resource Locations** and the **Connectors** page.

Connector Appliance updates

The Connector Appliance is updated automatically. You are not required to take any actions to update your connector.

You can configure your resource location to apply updates either immediately as they become available or during a specific maintenance window.

For more information about configuring updates, see Connector updates

As part of the update, the Connector Appliance becomes temporarily unavailable. Updates are applied to only one Connector Appliance in a resource location at a time. For this reason, register at least two Connector Appliances in each resource location to ensure that at least one Connector Appliance is always available.

Connector Appliance communication

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

The following table lists the ports that the Connector Appliance requires access to:

Service	Port	Supported Domain Protocol	Configuration details
DNS	53	TCP/UDP	This port must be open to the local setup
NTP	123	UDP	This port must be open to the local setup
HTTPS	443	TCP	Connector Appliance requires outbound access to this port

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

To configure the Connector Appliance, IT administrators must be able to access the administration interface on port 443 (HTTPS) of the Connector Appliance.

> **Note:**
>
> You must include `https://` at the start of the IP address.

The Connector Appliance can communicate with both on-premises systems in your resource location and with external systems. If you define one or more web proxies during Connector Appliance registration, only traffic from the Connector Appliance to external systems is routed through this web proxy. If your on-premises system is located in a private address space, traffic from Connector Appliance to this system is not routed through the web proxy.

The Connector Appliance defines private address spaces as the following IPv4 address ranges:

- 10.0.0.0 –10.255.255.255
- 172.16.0.0 –172.31.255.255
- 192.168.0.0 –192.168.255.255

Internet connectivity requirements

Connecting to the Internet from your data centers requires opening port 443 to outbound connections. However, to operate within environments containing an Internet proxy server or firewall restrictions, further configuration might be needed.

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

- `https://*.cloud.us`
- `https://*.citrixworkspacesapi.us`
- `https://*.citrixnetworkapi.us`
- `https://*.nssvc.net`
    - Customers who can't enable all subdomains can use the following addresses instead:
        - `https://*.g.nssvc.net`
        - `https://*.c.nssvc.net`
- `https://*.servicebus.windows.net`
- `https://ctxccopspacrconnappprodgov.azurecr.us`
- `https://ctxccopspacrconnappprodgov.usgovvirginia.data.azurecr.us`

Network requirements

Ensure that your environment has the following configuration:

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

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

System requirements

The Connector Appliance is supported on the following hypervisors:

- Citrix Hypervisor 8.2 CU1 LTSR
- VMware ESXi version 7 update 2
- Hyper-V on Windows Server 2016, Windows Server 2019, or Windows Server 2022.
- Nutanix AHV
- Microsoft Azure
- AWS
- Google Cloud Platform
- XenServer® 9

Your hypervisor must provide the following minimum capabilities:

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

You can host multiple Connector Appliances on the same hypervisor host. The number of Connector Appliances on the same host is only constrained by the hypervisor and hardware limitations.

> **Note:**
>
> Cloning, suspending, and taking snapshots of the Connector Appliance VM are not supported.

Obtain the Connector Appliance

Download the Connector Appliance software from within Citrix Cloud.

1. Sign in to Citrix Cloud.

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

2. From the menu in the top left of the screen, select **Resource Locations**.
3. If you do not already have a resource location, click the plus icon (+) or select **Add a Resource Location**.
4. In the resource location where you want to register the Connector Appliance, click the **Connector Appliances** plus icon (+).

   The **Add a Connector Appliance** task opens.
5. From the **Hypervisor** list in **Step 1**, choose the type of hypervisor or cloud provider that you use to host your Connector Appliance.

   - For on-premises hypervisors and cloud environments, you can download the Connector Appliance within Citrix Cloud:

     a) Click **Download Image**.

     b) Review the Citrix End User Service Agreement and, if you agree, select **Agree and Continue**.

     c) When prompted, save the provided Connector Appliance file.

        The file name extension of the Connector Appliance file depends on the hypervisor that you choose.

   - For some cloud environments, you can get the Connector Appliance from the marketplace:

     - AWS
     - Microsoft Azure
     - Google Cloud
6. Keep the **Install Connector Appliance** task open. After installing the Connector Appliance, you input your registration code into **Step 2**.

You can also get to the **Install Connector Appliance** task from the **Connectors** page. Select the plus icon (+) to add a connector and choose to add a Connector Appliance.

Install Connector Appliance on your hypervisor

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

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

Citrix Hypervisor

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

1. Connect to your Citrix Hypervisor server or pool by using XenCenter on a system that has access to the downloaded Connector Appliance XVA file.
2. Select **File** > **Import**.
3. Specify or browse to the path where the Connector Appliance XVA file is located. Click **Next**.
4. Select the Citrix Hypervisor server where you want to host the Connector Appliance. Alternatively, you can select the pool to host the Connector Appliance in and Citrix Hypervisor chooses a suitable available server. Click **Next**.
5. Specify the storage repository to use for your Connector Appliance. Click **Import**.
6. Click **Add** to add a virtual network interface. From the **Network** list, select the network for the Connector Appliance to use. Click **Next**.
7. Review the options to use to deploy the Connector Appliance. If any are incorrect, use **Previous** to change these options.
8. Ensure that **Start the new VM(s) automatically as soon as the import is complete** is selected. Click **Finish**.

After the Connector Appliance is deployed and has successfully started up, its console displays a landing page that contains the Connector Appliance IP address. Use this IP address to connect to the Connector Appliance administration page and complete the registration process.

By default, the Connector Appliance uses DHCP to set its network configuration. If DHCP is not available in your environment, you must set the network configuration at the Connector Appliance console before you can access the Connector Appliance management console. For more information, see Set the network configuration by using the Connector Appliance console.

Next step: Register your Connector Appliance with Citrix Cloud.

VMware ESXi

This section describes how to deploy Connector Appliance on a VMware ESXi host by using the VMware vSphere Client.

1. Connect to your ESXi host by using the vSphere Client on a system that has access to the downloaded Connector Appliance OVA file.
2. Select **File** > **Deploy OVF Template**….
3. Specify or browse to the path where the Connector Appliance OVA file is located. Click **Next**.
4. Review the template details. Click **Next**.

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

5. You can specify a unique name for your Connector Appliance instance. By default, the name is set to **Connector Appliance**. Ensure that you choose a name that distinguishes this instance of the Connector Appliance from other instances hosted on this ESXi host. Click **Next**.
6. Specify the destination storage for your Connector Appliance. Click **Next**.
7. Choose the format to store the virtual disks in. Click **Next**.
8. Review the options to use to deploy the Connector Appliance. If any are incorrect, use **Back** to change these options.
9. Select **Power on after deployment**. Click **Finish**.

After the Connector Appliance is deployed and has successfully started up, its console displays a landing page that contains the Connector Appliance IP address. Use this IP address to connect to the Connector Appliance administration page and complete the registration process.

By default, the Connector Appliance uses DHCP to set its network configuration. If DHCP is not available in your environment, you must set the network configuration at the Connector Appliance console before you can access the Connector Appliance UI. For more information, see Set the network configuration by using the Connector Appliance console.

Next step: Register your Connector Appliance with Citrix Cloud.

Hyper-V

This section describes how to deploy Connector Appliance on a Hyper-V host. You can deploy the VM by using the Hyper-V Manager or by using the included PowerShell script.

Deploy the Connector Appliance by using the Hyper-V Manager

1. Connect to your Hyper-V host.
2. Copy or download the Connector Appliance ZIP file to the Hyper-V host.
3. Extract the contents of the ZIP file. The ZIP file contains a PowerShell script and the connector-appliance.vhdx file.
4. Copy the VHDX file to where you want to keep your VM disks. For example, `C:\ConnectorApplianceVMs`.
5. Open Hyper-V Manager.
6. Right-click on your server name and select **New > Virtual Machine**.
7. In the **New Virtual Machine Wizard**, on the **Specify Name and Location** panel, enter a unique name to identify your Connector Appliance. Click **Next**.
8. On the **Specify Generation** panel, select **Generation 1**. Click **Next**.
9. On the **Assign Memory** panel, configure the following settings and then click **Next**:

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

a) Assign 4 GB of RAM.
b) Disable dynamic memory.

10. On the **Configure Networking** panel, select a switch from the list (for example, Default Switch). Click **Next**.
11. On the **Connect Virtual Hard Disk** panel, select **Use an existing virtual hard disk**.
12. Browse to the location of the connector-appliance.vhdx file and select it. Click **Next**.
13. On the **Summary** panel, review the values you have chosen and click **Finish** to create the VM.
14. On the **Virtual Machines** panel, right-click on the Connector Appliance VM and select **Settings**.
15. In the **Settings** window, select **Hardware > Processors** and perform the following actions:

    a) In **Number of virtual processors**, change the value to **2**.
    b) Click **Apply**.
    c) Click **OK**.

16. On the **Virtual Machines** panel, right-click on the Connector Appliance VM and select **Start**.
17. Right-click on the Connector Appliance VM and select **Connect** to open the console.

After the Connector Appliance is deployed and has successfully started up, connect to the console using the Hyper-V Manager. The console displays a landing page that contains the Connector Appliance IP address. Use this IP address to connect to the Connector Appliance administration page and complete the registration process.

By default, the Connector Appliance uses DHCP to set its network configuration. If DHCP is not available in your environment, you must set the network configuration at the Connector Appliance console before you can access the Connector Appliance UI. For more information, see Set the network configuration by using the Connector Appliance console.

Next step: Register your Connector Appliance with Citrix Cloud.

Deploy the Connector Appliance by using a PowerShell script The connector-appliance.zip file contains a PowerShell script that creates and starts a new VM.

> **Note:**
>
> To run this unsigned PowerShell script, you might have to change the execution policies on the Hyper-V system. For more information, see https://go.microsoft.com/fwlink/?LinkID=135170. Alternatively, you can use the provided script as the basis to create or amend your own local script.

1. Connect to your Hyper-V host.
2. Copy or download the Connector Appliance ZIP file to the Hyper-V host.

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

3. Extract the contents of the ZIP file: A PowerShell script and a VHDX file.
4. In a PowerShell console, change the current directory to where the ZIP file contents are located and run the following command:

```
.\connector-appliance-install.ps1
```

5. When prompted, type a name for your VM or select **Enter** to accept the default value of **Connector Appliance**.
6. When prompted, type a destination for the root disk or press Enter to use the system default directory for VHDs.
7. When prompted, type a file name for the root disk or select **Enter** to accept the default value of connector-appliance.vhdx.
8. When prompted, select the switch to use. Select **Enter**.
9. Review the summary of the VM import information. If the information is correct, select **Enter** to continue. The script creates and starts the Connector Appliance VM.

After the Connector Appliance is deployed and has successfully started up, its console displays a landing page that contains the Connector Appliance IP address. Use this IP address to connect to the Connector Appliance and complete the registration process.

Next step: Register your Connector Appliance with Citrix Cloud.

Nutanix AHV

This section describes how to deploy Connector Appliance from the `connector-appliance.vhdx` file onto a Nutanix AHV host by using the Nutanix Prism web console.

1. On the main menu of the Nutanix Prism web console, select the **Storage** view.
2. Click **+ Storage Container** to create a storage container to hold the Connector Appliance image file. Alternatively, you can use an existing storage container.
3. Upload the `connector-appliance.vhdx` file to your storage container.
    a) On the main menu of the web console, select **Settings**.
    b) Select the **Image Configuration** tab and click **+ Upload Image**
    c) In **Create Image**, specify a **Name** for your image.
    d) From the **Image Type** list, select **DISK**.
    e) From the **Storage Container** list, select the storage container you created.
    f) Select **Upload a file**.
    g) Click **Choose file** and navigate to the `connector-appliance.vhdx` file on your local system.

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

h) Click **Save**.

4. Wait until the image is created and its state shows as **ACTIVE** in the **Image Configuration** page.
5. Select the **Network Configuration** tab.
6. Click **+ Create Network** to create a network for the Connector Appliance to use.
7. In the **Create Network** page, specify the following information:
   - The network name.
   - The network VLAN ID.
8. On the main menu of the web console, select the **VM** view.
9. Click **+ Create VM** to create a Connector Appliance instance.
10. In **Create VM**, specify the following information:
    - The VM name
    - The number of vCPUs
    - The amount of memory in GiB
11. Select to use **Legacy BIOS**.
12. Click **+ Add New Disk** to add a disk to the VM.
13. In **Add Disk**, complete the following information:
    a) For **Type**, select **DISK**.
    b) For **Operation**, select **Clone from Image Service**.
    c) For **Bus Type**, select **SCSI**
    d) For **Image**, select the image you created when you uploaded the Connector Appliance file.
14. Click **Add** to finish adding the disk.
15. In **Create VM**, click **+ Add New NIC**.
16. In **Create NIC**, select the network to add the VM to.
17. For **Network Connection State**, select **Connected**.
18. Click **Add** to finish adding the NIC.
19. Click **Save** to create the VM.

    By default, the new VM is powered off.
20. In the **VM** view, select the VM and click **Power on**.
21. Wait for the VM to start up. This process can take several minutes.

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

After the Connector Appliance is deployed and has successfully started up, you can find the Connector Appliance IP address in one of the following places:

- In the **VM** view of the Nutanix Prism web console.
- In the Connector Appliance console.

Use this IP address to connect to the Connector Appliance administration page and complete the registration process.

Next step: Register your Connector Appliance with Citrix Cloud.

Microsoft Azure

This section describes how to deploy Connector Appliance in Microsoft Azure. You can deploy the Connector Appliance from the Azure Marketplace or from the downloaded disk image by using the included PowerShell script.

Deploy the Connector Appliance from the Azure Marketplace To deploy the Connector Appliance from the Azure Marketplace complete the following steps:

1. Go to the Connector Appliance in the Azure Marketplace. (Azure Marketplace)

   Alternatively, you can search for "Connector Appliance for Cloud Services"in the marketplace search.

2. Click **Get It Now** and then **Create**.
3. On the **Create Citrix Connector™ Appliance for Cloud Services** page, complete the following information:

   - Select the **Subscription** to use.
   - Select the **Resource group** to use.
   - Select the **Region** to locate the Connector Appliance in.
   - Specify a **VM name**.
   - Select a **Virtual network** to add the Connector Appliance to. This network is used to access Citrix Cloud, the local resources, and the Connector Appliance administration page. This network cannot be changed later.
   - Specify a value for **Subnet**.

   Click **Next : Tags >**.

4. On the **Tags** tab, add required tags if needed.

   Click **Next : Review + create >**.

5. After you have reviewed the deployment details, click **Create**.

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

After the Connector Appliance is deployed and has successfully started up, its console displays a landing page that contains the Connector Appliance IP address. Use this IP address to connect to the Connector Appliance administration page and complete the registration process.

Next step: Register your Connector Appliance with Citrix Cloud.

Deploy the Connector Appliance VM by using a PowerShell script The `connector-appliance-azure.zip` file contains a PowerShell script that creates and starts a new VM. You can use the provided script as the basis to create or amend your own local script.

Before running the script ensure that you have the following prerequisites:

- Install the Az PowerShell module into your local PowerShell environment.
- Run the PowerShell script in the directory where the VHD file is located.

Complete the following steps:

1. Copy or download the Connector Appliance ZIP file to your Windows system.
2. Extract the contents of the ZIP file: A PowerShell script and a VHD file.
3. Open a PowerShell console as Administrator.
4. Change the current directory to where the ZIP file contents are located and run the following command:

   ```
   .\connector-appliance-upload-Azure.ps1
   ```

5. A dialog appears, prompting you to log into Microsoft Azure. Enter your credentials.
6. When prompted by the PowerShell script, select the subscription to use. Press Enter.
7. Follow the prompts in the script, which guide you through uploading the image and creating a virtual machine.
8. After you have created the first VM, the script asks if you want to create another VM from the uploaded image.

   - Type `y` to create another VM.
   - Type `n` to exit the script.

After the Connector Appliance is deployed and has successfully started up, its console displays a landing page that contains the Connector Appliance IP address. Use this IP address to connect to the Connector Appliance administration page and complete the registration process.

Next step: Register your Connector Appliance with Citrix Cloud.

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

AWS

This section describes how to deploy Connector Appliance in AWS. Connector Appliance is available as an AMI in the AWS marketplace and we recommend that you install the Connector Appliance from the AMI. Alternatively, you can deploy a downloaded disk image by using the AWS UI or by using the included PowerShell script.

Networking prerequisites To deploy the Connector Appliance on AWS, ensure that you have access to Citrix Cloud from the subnet in which the Connector Appliance is created.

We recommend using a private IP address for the appliance, which requires specific configuration to provide access to Citrix Cloud. To achieve this configuration, complete the following steps in the **AWSManagement Console**:

1. Create the NAT gateway.
    a) In the top navigation bar, select **Services > VPC > NAT Gateways**.
    b) On the top right, click **Create NAT Gateway**. Enter the following information:
        - Enter **Name**.
        - Select **subnet** from the list.
        - Set **Connectivity type** as **Public**.
        - Select an **Elastic IP allocation ID** from the list. If there is no available Elastic IP, click **Allocate Elastic IP** and follow the instructions to create one.
    c) Click **Create NAT Gateway**.
2. Create a route table entry including the NAT gateway.
    a) In the top navigation bar, select **Services > VPC > Route Tables**.
    b) On the top right, click **Create route table**. Enter the following information:
        - Enter **Name**.
        - From the list, select the VPC that contains the subnet you selected when creating the NAT gateway.
    c) Click **Create route table**.
    d) In the **Routes** tab of the route table you created, click **Edit routes > Add route**.
    e) Input the **Destination** and **Target** for the new route entry.
        - Set the destination as 0.0.0.0/0.
        - For the target, select the **NAT Gateway** you created from the list.
    f) Click **Save change**.

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

3. Attach the subnet to be used for the Connector Appliance to this route table.

    a) In the top navigation bar, **Select Services > VPC > Route Tables**.
    b) Select the route table that contains the NAT gateway.
    c) In the display page, go to the **Subnet Associations** tab.
    d) Click **Edit subnet associations**.
    e) Select the subnet or subnets to attach to the route table.
    f) Click **Save Associations**.

Deploy the Connector Appliance from the AWS Marketplace Before beginning, ensure you meet the following prerequisites:

- You have permissions to operate EC2 resources.
- You have completed the configuration in Networking prerequisites.
- (Optional) You can create a security group that restricts which IP addresses are permitted to access your Connector Appliance.

Complete the following steps:

1. Log in to the **AWSManagement Console**.
2. Find the Connector Appliance AMI in the AWS marketplace. You can do this in one of the following ways:

    - Follow the marketplace link provided in Citrix Cloud. (AWS Marketplace)
    - Search for the AMI in the AWS Management Console:

        a) Go to **Services > Compute > EC2 > AMIs**
        b) Ensure that you are in the US East (Ohio) region.
        c) In **Public images**, search for "Citrix Connector Appliance"or for the AMI ID "ami-026eaf9b3b232577f".

3. Verify that you have the correct AMI by checking the AMI ID (ami-026eaf9b3b232577f) and owner ID (414337923189).
4. Copy the AMI to your subscription:

    a) Go to **Actions > Copy AMI**.
    b) In the **Copy AMI** dialog, you can select the **Destination Region** that you require.
    c) Click **Copy AMI**

5. From your copied AMI summary page, click **Launch instance from AMI**.
6. In the **Launch an instance** dialog, complete the following steps:

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

a) Select the number of instances to create. For resiliency, we recommend that you have two or more Connector Appliances in each resource location.
b) Specify a name for the instance.
c) For the **Instance type**, select **t2.medium**. The instance type must have at least 4 GB and 2 CPUs.
d) For the **Key pair (login)**, select **Proceed without a key pair**. SSH login to the Connector Appliance is not permitted, so a key pair is not needed.
e) For the **Network settings**, in the **Firewall (security group)** section, configure the following settings:
    i. Choose whether to **Create security group** or **Select existing security group**.
    ii. Deselect **Allow SSH traffic from the internet**
    iii. Select **Allow HTTPs traffic from the internet**
    iv. Select **Allow HTTP traffic from the internet**

Click **Launch instance**.

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

   Alternatively, you can click the **View All Instances** button on this page or go to **Services > EC2 >Instances** in the AWS Management Console to see a list of your instances.

8. When your **Instance state** has changed to **Running**, go into the instance details and use the **Private IPv4 address** to connect to the Connector Appliance administration page and complete the registration process.

You might need to use a bastion host to go to the Connector Appliance administration page at the internal IP address from your browser and complete the registration process.

By default, the Connector Appliance uses DHCP to set its network configuration. You can edit this network configuration using the Connector Appliance web interface. For more information, see Configuring network settings on the Connector Appliance administration page.

Next step: Register your Connector Appliance with Citrix Cloud.

Deploy the Connector Appliance by using the AWS UI Before beginning, ensure you meet the following prerequisites:

- You have permissions to operate S3 and EC2 resources.
- You have created a service role and policy that has VM import access. For more information, see https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role.

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

> **Note:**
>
> To create a service role, you must create an S3 bucket. When creating the policy, set the S3 bucket you have created with VM import access.

- You have access to AWS CloudShell. It is only available in certain regions. For the list of regions where AWS CloudShell is supported, see https://docs.aws.amazon.com/cloudshell/latest/userguide/supported-aws-regions.html.
- You have completed the configuration in Networking prerequisites.

Complete the following steps:

1. On your local system, extract the contents of `connector-appliance-aws.zip`.
2. Log in to the **AWSManagement Console**.
3. Create a storage bucket by completing the following steps. (Alternatively, you can skip these steps and use an existing storage bucket.)
   a) In the top navigation bar, select **Services** > **S3** > **Create bucket**.
   b) Enter a unique name for your bucket. For naming conventions for buckets in Amazon S3, see https://docs.aws.amazon.com/AmazonS3/latest/userguide/bucketnamingrules.html.
   c) Select the region for your bucket. Ensure that you choose the same region as your AWS Region, because you cannot use the files in the bucket if these regions are different.
   d) Keep the remaining settings set to the defaults, then click **Create bucket**.
4. Click the name of the bucket that you have created. Click **Upload** > **Add files**, then select the `connector-appliance.vhd` file. Keep the remaining settings set to the defaults then click **Upload**.
5. Click the file you uploaded. Click **Copy S3 URI**.
6. Click the **AWS CloudShell icon** in the top navigation bar and run the following commands:
   a) Create a task to convert your VHD file to a snapshot:

```
aws ec2 import-snapshot --disk-container Format=VHD,Url="<S3_URI>"
```

   Replace the placeholder value with your S3 URI that you copied from the previous step. For example, `aws ec2 import-snapshot --disk-container Format=VHD,Url="s3://my-aws-bucket/connector-appliance.vhd"`.

   This command is complete when the following command returns a JSON string containing `"Status": "completed"`. Make note of the `ImportTaskId` value in the JSON output.

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

b) Run the following command:

```
aws ec2 describe-import-snapshot-tasks --import-task-ids <
    ImportTaskId>
```

Replace the placeholder value with the `ImportTaskId` copied from the previous step. For example, `aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-0273h2836153itg5`.

7. On the **AWSManagement Console**, in the top navigation bar, select **Services** > **EC2**.
8. From the menu on the left of the screen, click **Snapshots**.
9. Right-click on the snapshot that you created and click **Create Image**.
10. In the pane that opens, complete the following steps:

    a) Enter a name for your AMI.
    b) Select **Hardware-assisted virtualization**.

    Click **Create**.
11. From the menu on the left of the screen, click **AMIs**.
12. Right-click on the AMI that you created and click **Launch**.
13. In the pane that opens, complete the following steps:

    a) Choose the instance type.
    b) (Optional) Customize the network on the **Configure Instance** tab.
    c) (Optional) Attach another volume on the **Add Storage** tab.
    d) Set security group rules on the **Configure Security Group** tab.

    After you have reviewed the instance launch, click **Review and Launch**.

After the Connector Appliance is deployed and has successfully started up, go to **Services** > **EC2** > **Instances** and select the instance you have created. Use the **Private IPv4 address** to connect to the Connector Appliance administration page and complete the registration process. You might need to use a bastion host to go to the Connector Appliance administration page at the internal IP address from your browser to continue the installation process.

By default, the Connector Appliance uses DHCP to set its network configuration. You can edit this network configuration using the Connector Appliance web interface. For more information, see Configuring network settings on the Connector Appliance administration page.

Next step: Register your Connector Appliance with Citrix Cloud.

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

Deploy the Connector Appliance by using a PowerShell script The `connector-appliance-aws.zip` file contains a PowerShell script that creates and starts a new VM. Before running the script ensure that you have the following prerequisites:

- You have either AWS.Tools, AWSPowerShell.NetCore or AWSPowerShell installed on your system. For more information, see https://docs.aws.amazon.com/powershell/latest/userguide/pstools-getting-set-up.html.
- You have created a service role and policy that has VM import access. Both the service role and the policy must be named `vmimport` for this PowerShell script to work. For more information, see https://docs.aws.amazon.com/vm-import/latest/userguide/required-permissions.html#vmimport-role.

  > **Note:**
  >
  > To create a service role, you must create an S3 bucket. When creating the policy, set the S3 bucket you have created with VM import access.

- You have created an Amazon EC2 security group.
- You have S3 permissions and API access.
- You have completed the configuration in Networking prerequisites.

Complete the following steps:

1. On your local system, extract the contents of `connector-appliance-aws.zip` to a folder.
2. In PowerShell, run the following commands:

   a) To be able to run an AWS cmdlet in your local environment, run the following command to add a new profile to the AWS SDK store:

   ```
   Set-AWSCredential -AccessKey <access_key_ID> -SecretKey <
       secret_key> -StoreAs MyProfile
   ```

   Replace the placeholder values with your access key and secret key. Provide a unique profile name. In the example we have provided, it is `MyProfile`.

   b) Set the profile to the default:

   ```
   Initialize-AWSDefaultConfiguration -ProfileName MyProfile
   ```

   c) Change the current directory to the folder where the extracted files are located and run the following command:

   ```
   .\connector-appliance-upload-aws.ps1
   ```

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

3. Follow the prompts in the script, which guide you through selecting the region for your Connector Appliance deployment, uploading the image to your chosen bucket, and entering a name for your VM.

    - You must use the bucket with VM import access that you created earlier.
    - When asked to select the VPC to use, select the VPC where the NAT gateway and route tables are configured.
    - When asked to select the subnet to use, select the subnet attached to the route table containing the NAT gateway.

    For more information, see Networking prerequisites.

After the Connector Appliance is deployed and has successfully started up, the script displays the private IP address of the Connector Appliance. You might need to use a bastion host to go to the Connector Appliance administration page at the internal IP address from your browser and complete the registration process.

By default, the Connector Appliance uses DHCP to set its network configuration. You can edit this network configuration using the Connector Appliance web interface. For more information, see Configuring network settings on the Connector Appliance administration page.

Next step: Register your Connector Appliance with Citrix Cloud.

Google Cloud Platform

This section describes how to deploy Connector Appliance on the Google Cloud Platform. You can install the Connector Appliance from the Google Cloud Marketplace. Alternatively, you can deploy a downloaded disk image by using the Google Cloud Platform Console or by using the included PowerShell script.

The file `connector-appliance-gcp.zip` contains:

- `connector-appliance.tar.gz`, which is a disk image of the Connector Appliance
- `connector-appliance-upload-gcp.ps1`, which is a PowerShell script that can be used to automatically deploy the Connector Appliance

Deploy the Connector Appliance from the Google Cloud marketplace

1. Log in to your Google account.
2. Follow the marketplace link provided in Citrix Cloud. (Google Cloud Marketplace)

    Alternatively, you can search for "Connector Appliance for Cloud Services"in the marketplace search.

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

3. Click **Launch**.
4. On the **New Citrix Connector Appliance for Cloud Services deployment** page, complete the following information:

   - Specify a **Deployment name** for the deployment job.
   - Select the **Zone** to locate the Connector Appliance in.
   - Select the **Machine family**, **Series**, and **Machine type** to use.
   - Select the **Boot disk type** and **Boot disk size in GB** to use.
   - In the **Networking** section, specify the networking interface to be used by the Connector Appliance. If you want to be able to connect to the administration page from a public network, specify an **External IP**.

   Click **Deploy**. You are directed to the **Deployment Manager** page.

   > **Note:**
   >
   > After the Connector Appliance is deployed and has successfully started up, you receive an email to confirm that the Connector Appliance is deployed on Google Cloud Platform.

5. On the **Deployment Manager** page, click on the instance name. Alternatively, you can search for the Connector Appliance instance that you created in the **Compute Engine**.
6. If you previously specified an **External IP** when setting up the networking interface for your Connector Appliance, copy the **External IP address** in the **Network interfaces** section in the **Details** tab. Use this IP address to connect to the Connector Appliance administration page and complete the registration process. Alternatively, you can use the **Primary internal IP address** to visit the Connector Appliance administration page from another machine that is in the same subnet as your Connector Appliance.

Next step: Register your Connector Appliance with Citrix Cloud.

Deploy the Connector Appliance by using the Google Cloud Platform console

1. On your local system, extract the contents of `connector-appliance-gcp.zip`.
2. In your Google Cloud Platform project, create a storage bucket. (Alternatively, you can use an existing storage bucket.)

   a) From the main menu, select **Cloud Storage**.
   b) On the main pane, select **Create bucket**.
   c) Specify a name for your bucket.
   d) Configure the data storage and access settings that you require. You can leave these settings as the defaults.
   e) Click **Create**.

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

3. Inside your storage bucket, select **Upload files** and choose the file `connector-appliance.tar.gz`. Wait while the file uploads.
4. Select the uploaded file to view its details. Copy the value of **gsutil URI** to the clipboard.
5. Open the Cloud Shell by clicking the **Activate Cloud Shell** icon in the header bar.
6. In your Cloud Shell, run the following command to create an image:

```
gcloud compute images create "Image name" --guest-os-features=
    MULTI_IP_SUBNET --source-uri="gsutil URI of uploaded connector-
    appliance.tar.gz file"
```

7. From the main menu, select **Compute Engine** > **VM Instances**.
8. Select **Create Instance**. In the pane that opens, specify the following information:

   a) In the **Name** field, specify a name for the Connector Appliance instance.
   b) Choose a region to locate the Connector Appliance in.
   c) Choose the machine configuration.
   d) In the **Boot disk** section, click **Change**.
   e) In the section that opens, go to the **Custom images** tab.
   f) From the **Image** list, select the image you created.
   g) Click **Select**.
   h) In the **Firewall** section, enable HTTPS traffic to allow access to the Connector Appliance administration page.
   i) Specify any additional configuration required. For example, you might not want to use the default networking configuration.

   Click **Create**.
9. In the **VM Instances** section, select your newly created VM to view its details.

After the Connector Appliance is deployed and has successfully started up, the **VM Instances** section displays the Connector Appliance IP addresses.

If the Connector Appliance has an external IP address, you can use this IP address to go to the Connector Appliance administration page from your browser and complete the registration process.

If the Connector Appliance has only an internal IP address, use a bastion host to go to the Connector Appliance administration page from your browser and complete the registration process. For more information, see https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host.

Next step: Register your Connector Appliance with Citrix Cloud.

Deploy the Connector Appliance by using a PowerShell script To use the provided PowerShell script to deploy the Connector Appliance, you must have the Google Cloud SDK installed on your system.

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

1. On your local system, extract the contents of `connector-appliance-gcp.zip` to a folder.
2. In PowerShell, change the directory to the folder where the extracted files are located.
3. Run the command `.\connector-appliance-upload-GCP.ps1`.
4. In the browser window that opens, authenticate with the Google Cloud SDK with an account that has access to the project you want to deploy the Connector Appliance to.
5. In Google Cloud Tools for PowerShell, when prompted by the PowerShell script, select the project to use. Press Enter.
6. Follow the prompts in the script, which guide you through uploading the disk, creating an image, and creating a virtual machine.
7. After you have created the first VM, the script asks if you want to create another VM from the uploaded image.
    - Type `y` to create another VM.
    - Type `n` to exit the script.

After the Connector Appliance is deployed and has successfully started up, the script displays the internal IP address of the Connector Appliance. Alternatively, you can go to the Google Cloud Platform console to find the Connector Appliance internal IP address. The **Compute Engine** > **VM Instances** section displays the Connector Appliance IP address.

Use a bastion host to go to the Connector Appliance administration page at the internal IP address from your browser and complete the registration process. For more information, see https://cloud.google.com/compute/docs/connect/ssh-using-bastion-host.

Next step: Register your Connector Appliance with Citrix Cloud.

Register your Connector Appliance with Citrix Cloud

Register a Connector Appliance with Citrix Cloud to provide a channel for communication between Citrix Cloud and your resource locations.

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

After you install your Connector Appliance on the hypervisor and start it, the console displays the IP address of the Connector Appliance. The console also displays an SSL fingerprint that you can use to validate your connection to the Connector Appliance UI.

1. Copy the Connector Appliance IP address to your browser address bar.

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

> **Note:**
>
> You may have to include `https://` at the start of the IP address. For Citrix Cloud Government, append `?deployment=productiongov` to the end of the web address.

The Connector Appliance UI uses a self-signed certificate, which is valid for five years. As a result, you might see a message about the connection not being secure. To verify the connection to your Connector Appliance, you can compare the SSL fingerprint in the console with the fingerprint the browser receives from the webpage.

For example, in the Google Chrome browser, complete the following steps:

a) Click the **Not Secure** marker next to the address bar.

b) Select **Certificate**. The **Certificate** window opens.

c) Go to the **Details** tab and find the **Thumbprint** field.

If the value of the **Thumbprint** field and the SSL fingerprint provided in the console match, you can confirm that your browser is connecting directly to the Connector Appliance UI.

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

2. If your browser requires an extra step to confirm that you want to continue to the site, complete this step now.

   The **Create new password** webpage opens.

3. Create a password for your Connector Appliance UI and click **Set password**.

   The password you set must meet the following requirements:

   - 8 or more characters long
   - Contains both upper and lower case letters
   - Contains at least one non-alphabetic character

   Ensure that you store this password in a safe place for future use.

4. Sign in with the password you set. The **Connector administration** page opens.

5. (Optional) If you use one or more web proxies, you can add the proxy addresses in the **Proxy servers** section. Both unauthenticated and authenticated proxies are supported. To add an unauthenticated proxy, provide a valid **Proxy IP Address and Port**. To add an authenticated proxy, provide a valid **Username** and **Password** as well.

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

> **Note:**
>
> Only basic proxy authentication is supported. Other forms of authentication are not supported.

Only traffic to external systems is routed through the web proxy. For more information, see Connector Appliance communication.

6. (Optional) If your network uses TLS intercepting web proxies to access the internet you may require your Connector to trust its Root Certificate Authority to successfully communicate with the cloud.

   a) Under **Root certificate authorities**, select **Add certificate**.

   b) Copy the contents of the certificate in PEM format:

   ```
   -----BEGIN CERTIFICATE-----
   <certificate-base64-bytes>
   -----END CERTIFICATE-----
   ```

   c) In **Full Certificate Details**, paste the certificate contents.

   d) Select **Add Certificate**.

   To add a RootCA using the Connector Appliance APIs, see Managing root certificate authorities in the Citrix Developer documentation.

   > **Note:**
   >
   > Certificates which are expired or will expire in the next 30 days will show a warning.

7. Click **Register Connector** to open the registration task.
8. Choose a name for your Connector Appliance. This name can help you distinguish between the various Connector Appliances that exist in your resource location. After you register your Connector Appliance, the name cannot be changed.

   Enter the name in the **Connector Appliance name** field and click **Next**.

   The webpage provides a code to use to register with Citrix Cloud. This code expires in 15 minutes.
9. Use the **Copy** button to copy the code to the clipboard.
10. Return to the **Resource Locations** webpage.
11. Paste the code into **Step 2** of the **Install Connector Appliance** task. Click **Confirm Details**.

    Citrix Cloud verifies that the Connector Appliance is present and can be contacted. If the registration code has expired, you are prompted to generate a new code.

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

12. Click **Register**.

    The page shows whether the registration was successful. If the registration failed, you are prompted to try again.

13. Click **Close**.

The **Connector Appliance administration page** also enables you to download a diagnostic report for the Connector Appliance. For more information, see Generating a diagnostic report.

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

After registering your Connector Appliance

For each resource location, we advise that you install and register two or more Connector Appliances. This configuration ensures continuous availability and enables the connectors to balance the load.

You cannot directly manage your Connector Appliance.

The Connector Appliance is updated automatically. You are not required to take any actions to update your connector. You can specify the time and day that you want Connector Appliance updates to be applied in your resource location. For more information, see Connector updates.

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

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

Generating a diagnostic report

You can generate and download a diagnostic report from the **Connector Appliance administration page**.

1. From the Connector Appliance console in your hypervisor, copy the IP address to your browser address bar.
2. Enter the password that you set when you registered your Connector Appliance.
3. In the **Diagnostic report** section of the page, click **Download Report**.

The diagnostic reports are provided in a `.zip` file.

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

Verify your network connection

You can check your network connection from the **Connector Appliance administration page** by using the **TCP Capture** diagnostic check.

1. On the **Connector Appliance administration page**, click your account name in the header bar and select **Network Diagnostics**.
2. (Optional) In the **TCP Capture** section, enter the target IP address, host name, or port to restrict the TCP capture.
3. From the **Trace Duration** menu, select the duration for which you want your trace to run.
4. (Optional) Enable **Packet Tracing** to capture the contents of the packets.

   When packet tracing is disabled, the TCP capture functionality uses a best-effort approach to capture the headers for diagnosis. This best-effort approach captures the first 512 bytes of each packet. However, as headers are not a fixed size, this approach might not capture all of the header.
5. Click **Start trace**.
6. Wait until the trace has completed. After the trace has completed, you can download a trace report or start a new trace.

   - Click **Download** to download the trace report. The trace report is provided in a `.pcap` file.
   - Click **Start new trace** to begin another trace.

Connecting Active Directory to Citrix Cloud

You can use Connector Appliance to connect a resource location to forests which do not contain Citrix Virtual Apps and Desktops™ resources. For example, in the case of Citrix Secure Private Access customers or Citrix Virtual Apps and Desktops customers with some forests only used for user authentication.

For more information, see Active Directory with Connector Appliance.

Validating your Kerberos configuration

If you use Kerberos for single sign-on, you can verify that the configuration on your Active Directory controller is correct from the **Connector Appliance administration** page. The **Kerberos validation** feature enables you to validate a Kerberos realm-only mode configuration or a Kerberos Constrained Delegation (KCD) mode configuration.

Validate Kerberos realm-only configuration:

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

1. Go to the **Connector Appliance administration** page.
2. From the Connector Appliance console in your hypervisor, copy the IP address to your browser address bar.
3. Enter the password that you set when you registered your Connector Appliance.
4. To validate your realm-only Kerberos configuration select the **Kerberos Validation Realm-Only** in the **Active Directory domains** section.
5. Specify the **Active Directory Domain**.

    - If you're validating a Kerberos realm-only mode configuration, you can specify any Active Directory domain. This mode doesn't depend on being joined to the domain.

6. Specify the **Service FQDN**. The default service name is assumed to be "https". If you specify "computer.example.com", this value is considered the same as "https://computer.example.com".
7. Specify the **Username**.
8. Specify the **Password**.
9. Click **Test Kerberos**.

Validate Kerberos Contrained Delegation (KCD) configuration:

1. Go to the **Connector Appliance administration** page.
2. To validate **Kerberos Constrained Delegation (KCD)** mode for domains to which the Connector Appliance has been joined, select **Kerberos validation** from the ellipsis menu (...) of the relevant domain.
3. Specify the **Active Directory Domain**.

    - If you're validating a Kerberos Constrained Delegation configuration, you must select from a list of joined domains.

4. Specify the **Service FQDN**. The default service name is assumed to be "https". For example, specify "computer.example.com", this value is considered the same as "https://computer.example.com%E2%80%9D.
5. Specify the **Username**.

    - For the Kerberos Constrained Delegation mode, you can also validate the kerberos setup using service accounts by selecting the **Service Accounts** tab.

6. Click **Test Kerberos**.

If the Kerberos configuration is correct, you see the message "Successfully validated Kerberos setup". If the Kerberos configuration is not correct, you see an error message that provides information about how the validation failed.

For more information about Kerberos, see the Microsoft documentation.

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

Network settings for your Connector Appliance

By default, the IP address and network settings of your Connector Appliance are automatically assigned by using DHCP.

After registering your Connector Appliance by using DHCP, you can edit its network settings in the **Connector Appliance administration page**.

However, if DHCP is not available in your environment or if you do not have access to the **Connector Appliance administration page**, you can set the network configuration directly on the Connector Appliance console.

Configuring network settings on the Connector Appliance administration page

After registering your Connector Appliance by using DHCP, you can edit its network settings in the **Connector Appliance administration page**.

To manually configure your network settings:

1. In the **Connector Summary** section, select **Edit network settings**.
2. In the **Network settings** dialog, choose **Configure your own network settings**.
3. Enter the **IP address**, **Subnet mask**, and **Default gateway**.
4. Add one or more **DNS servers**.
5. Add one or more **NTP servers**.
6. Click **Save**.

When you save changes to your network settings, the Connector Appliance restarts. During the restart, the Connector Appliance is temporarily unavailable. You are logged out of the **Connector Appliance administration page** and the URL of this page changes. You can find the new URL in the Connector Appliance console or by looking at the network information in your hypervisor.

To change your network configuration to use automatically assigned values:

1. In the **Connector Summary** section, select **Edit network settings**.
2. In the **Network settings** dialog, choose **Obtain IP address automatically**.
3. Click **Save**.

When you save changes to your network settings, the Connector Appliance restarts. During the restart, the Connector Appliance is temporarily unavailable. You are logged out of the **Connector Appliance administration page** and the URL of this page changes. You can find the new URL in the Connector Appliance console or by looking at the network information in your hypervisor.

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

Set the network configuration by using the Connector Appliance console

By default, the IP address and network settings of your Connector Appliance are automatically assigned by using DHCP. However, if DHCP is not available in your environment or if you do not have access to the **Connector Appliance administration page**, you can set the network configuration directly on the Connector Appliance console.

To set the network configuration:

1. In your hypervisor, restart the Connector Appliance.
2. While the Connector Appliance starts up, watch the console for the message `Welcome to GRUB!`.
3. When you see this message, press **Esc** to enter the GRUB menu.
4. To edit the boot parameters, press **e**.

   You see a view that looks like the following image:
5. Edit the line that begins with `linux` to include your required network configuration.
   - To specify DHCP networking, append `network=dhcp` to the end of the line.
   - To specify static networking, append the following parameters to the end of the line:

     ```
     network=static:ip=<static_ip_address>:netmask=<netmask>:route
        =<default_gateway>:dns=<dns_server_1>,<dns_server_2>:ntp=<
        ntp_server_1>,<ntp_server_2>
     ```

     Replace the placeholder values with the values for your configuration.
6. Press **Ctrl+X** to start the Connector Appliance with the new configuration.

Change the administrator user password for the Connector Appliance

1. From the user menu in the top-right of the console, select **Change password**.

   The change password page is displayed.
2. Enter your current password and then enter and confirm the new password. The new password you set must meet the following requirements:
   - 8 or more characters long
   - Contains both upper and lower case letters
   - Contains at least one non-alphabetic character
   - Must not be the same as current password
3. Select **Change password** to save your changes.

Citrix Cloud signs you out automatically and redirects you to the sign-in page.

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

Active Directory with Connector Appliance

You can use Connector Appliance to connect a resource location to forests which do not contain Citrix Virtual Apps and Desktops™ resources. For example, in the case of Citrix Secure Private Access customers or Citrix Virtual Apps and Desktops customers with some forests only used for user authentication.

When using multi-domain Active Directory with Connector Appliance, note that the Connector Appliance cannot be used in place of Cloud Connectors in forests that contain VDAs.

Requirements

Active Directory requirements

- Joined to an Active Directory domain that contains the resources and users that you use to create offerings for your users. For more information, see the Deployment scenarios for Connector Appliances in Active Directory article.
- Each Active Directory forest that you plan to use with Citrix Cloud™ must always be reachable by two Connector Appliances.
- The Connector Appliance must be able to reach domain controllers in both the forest root domain and in the domains that you intend to use with Citrix Cloud. For more information, see the following Microsoft support articles:
  - How to configure domains and trusts
  - "Systems services ports"section in Service overview and network port requirements for Windows
- Use universal security groups instead of global security groups. This configuration ensures that user group membership can be obtained from any domain controller in the forest.

Network requirements

- Connected to a network that can contact the resources you use in your resource location.
- Connected to the Internet. For more information, see System and Connectivity Requirements.

In addition to the ports listed in Connector Appliance communication, the Connector Appliance requires an outbound connection to the Active Directory domain via these ports:

Service	Port	Supported Domain Protocol
Kerberos	88	TCP/UDP

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

Service	Port	Supported Domain Protocol
NetBIOS Name Service	137	UDP
NetBIOS Datagram	138	UDP
NetBIOS Session	139	TCP
LDAP	389	TCP/UDP
SMB over TCP	445	TCP
Kerberos kpasswd	464	TCP/UDP
Global Catalog	3268	TCP
Dynamic RPC Ports	49152–65535	TCP

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

Supported Active Directory functional levels

Connector Appliance has been tested and is supported with the following forest and domain functional levels in Active Directory.

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

Other combinations of domain controller, forest functional level, and domain functional level have not been tested with the Connector Appliance. However, these combinations are expected to work and are also supported.

Connect an Active Directory domain to Citrix Cloud by using Connector Appliance

When you connect to the Connector Appliance administration webpage, the Active Directory domains section displays two tabs.

- **Joined Domains** –Used for joining the Connector Appliance to AD Domains by creating a machine account for the appliance in the Domain. Kerberos can be validated by clicking the ellipsis

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

menu on the right-hand side of the joined domain. Machine account presence in the domain is required.

- **Service Accounts** –Used as part of a Secure Private Access solution to achieve Kerberos SSO using a service account instead of the machine account created by joining the domain. Kerberos can be validated by clicking the ellipsis menu on the right-hand side of the service account. Having a specific domain associated with the machine isn't mandatory. However, even if the Connector Appliance isn't connected to the domain, it can still connect to the domain controller.

To configure Active Directory to connect to Citrix Cloud through the Connector Appliance, complete the following steps.

1. Install a Connector Appliance in your resource location.

   You can follow the information in the Connector Appliance product documentation.

2. Connect to the Connector Appliance administration webpage in your browser by using the IP address provided in the Connector Appliance console.
3. In the **Active Directory domains** section, navigate to the **Joined domains** tab.
4. Click **+ Add Active Directory domain**, a new pop-up window displays to enter the domain name.

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

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

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

8. Click **Join**.

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

9. To add more **Active Directory domains**, select **+ Add Active Directory domain** and repeat the preceding steps.
10. Go to the domains page in **Citrix Cloud Console** and select **Connector Appliance** to service your domains.

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

11. If you have not already registered your Connector Appliance, continue with the steps as described in Register your Connector Appliance with Citrix Cloud.

If you receive an error when joining the domain, verify that your environment fulfills the Active Directory requirements and the network requirements.

What's next

- You can add more domains to this Connector Appliance.

  > **Note:**
  >
  > The Connector Appliance is tested with up to 10 forests.

- For resilience, add each domain to more than one Connector Appliance in each resource location.

Viewing your Active Directory configuration

You can view the configuration of the Active Directory domains and Connector Appliances in your resource locations in the following places:

- In Citrix Cloud:

  1. In the menu, go to the **Identity and Access Management** page.
  2. Go to the **Domains** tab.

     Your Active Directory domains are listed with the resource locations that they are part of.

- In the Connector Appliance webpage:

  1. Connect to the Connector Appliance webpage by using the IP address provided in the Connector Appliance console.
  2. Log in with the password you created when you first registered.
  3. In the **Active Directory domains** section of the page, you can see the list of Active Directory domains this Connector Appliance is joined to.

Removing an Active Directory domain from a Connector Appliance

To leave an Active Directory domain, complete the following steps:

1. Connect to the Connector Appliance webpage by using the IP address provided in the Connector Appliance console.

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

2. Log in with the password you created when you first registered.
3. In the **Active Directory domains** section of the page, find the domain you want to leave in the list of joined Active Directory domains.
4. Note the name of the machine account created by your Connector Appliance.
5. Click the delete icon (trashcan) next to the domain. A confirmation dialog appears.
6. Click **Continue** to confirm the action.
7. Go to your Active Directory controller.
8. Delete the machine account created by your Connector Appliance from the controller.

Deployment scenarios for using Connector Appliance with Active Directory

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

For more information about using Cloud Connectors with Active Directory, see Deployment scenarios for Cloud Connectors in Active Directory

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

- You are setting up Secure Private Access. For more information, see Secure Private Access with Connector Appliance.
- You have one or more forests that are only used for user authentication
- You want to reduce the number of connectors required to support multiple forests
- You need a Connector Appliance for other use cases

Only users in one or more forests with a single set of Connector Appliances for all forests

This scenario applies to Workspace Standard customers or customers using Connector Appliance for Secure Private Access.

In this scenario, there are several forests that contain only user objects (`forest1.local`, `forest2.local`). These forests do not contain resources. One set of Connector Appliances is deployed within a resource location and joined to the domains for each of these forests.

- Trust relationship: None
- Domains listed in **Identity and Access Management**: `forest1.local`, `forest2.local`
- User logons to Citrix Workspace™: Supported for all users
- User logons to an on-premises StoreFront™: Supported for all users

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

Users and resources in separate forests (with trust) with a single set of Connector Appliances for all forests

This scenario applies to Citrix Virtual Apps and Desktops customers with multiple forests.

In this scenario, some forests (`resourceforest1.local`, `resourceforest2.local`) contain your resources (for example, VDAs) and some forests (`userforest1.local`, `userforest2.local`) contain only your users. A trust exists between these forests that allows users to log on to resources.

One set of Cloud Connectors is deployed within the `resourceforest1.local` forest. A separate set of Cloud Connectors is deployed within the `resourceforest2.local` forest.

One set of Connector Appliances is deployed within the `userforest1.local` forest and the same set is deployed within the `userforest2.local` forest.

- Trust relationship: Bi-directional forest trust, or uni-directional trust from the resource forests to the user forests
- Domains listed in **Identity and Access Management**: `resourceforest1.local`, `resourceforest2.local`, `userforest1.local`, `userforest2.local`
- User logons to Citrix Workspace: Supported for all users
- User logons to an on-premises StoreFront: Supported for all users

© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at https://www.cloud.com/legal. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (https://www.cloud.com/legal) for more information.