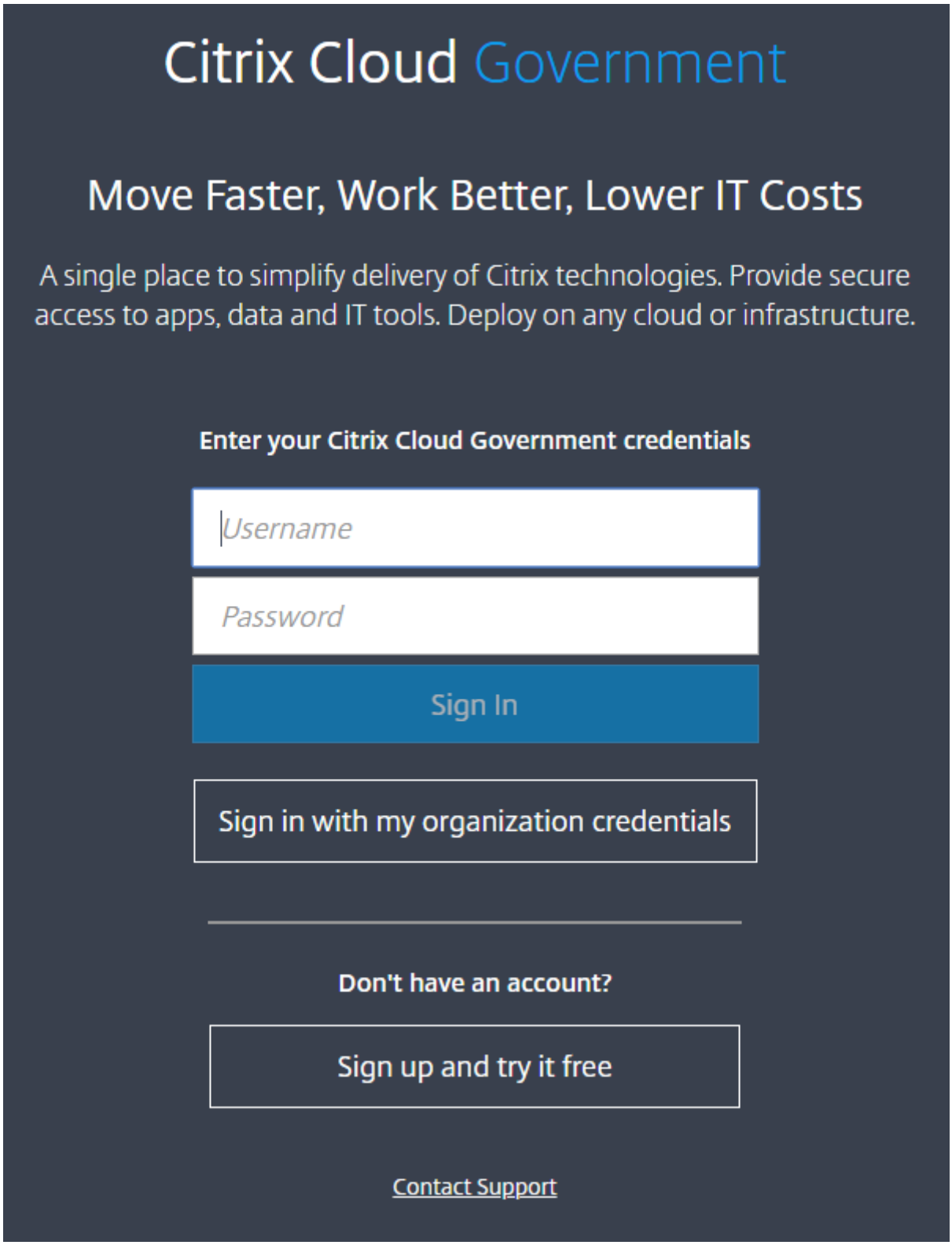
Citrix Cloud Government

Contents

How to Get Help and Support

July 5, 2018

Signing in to your account



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

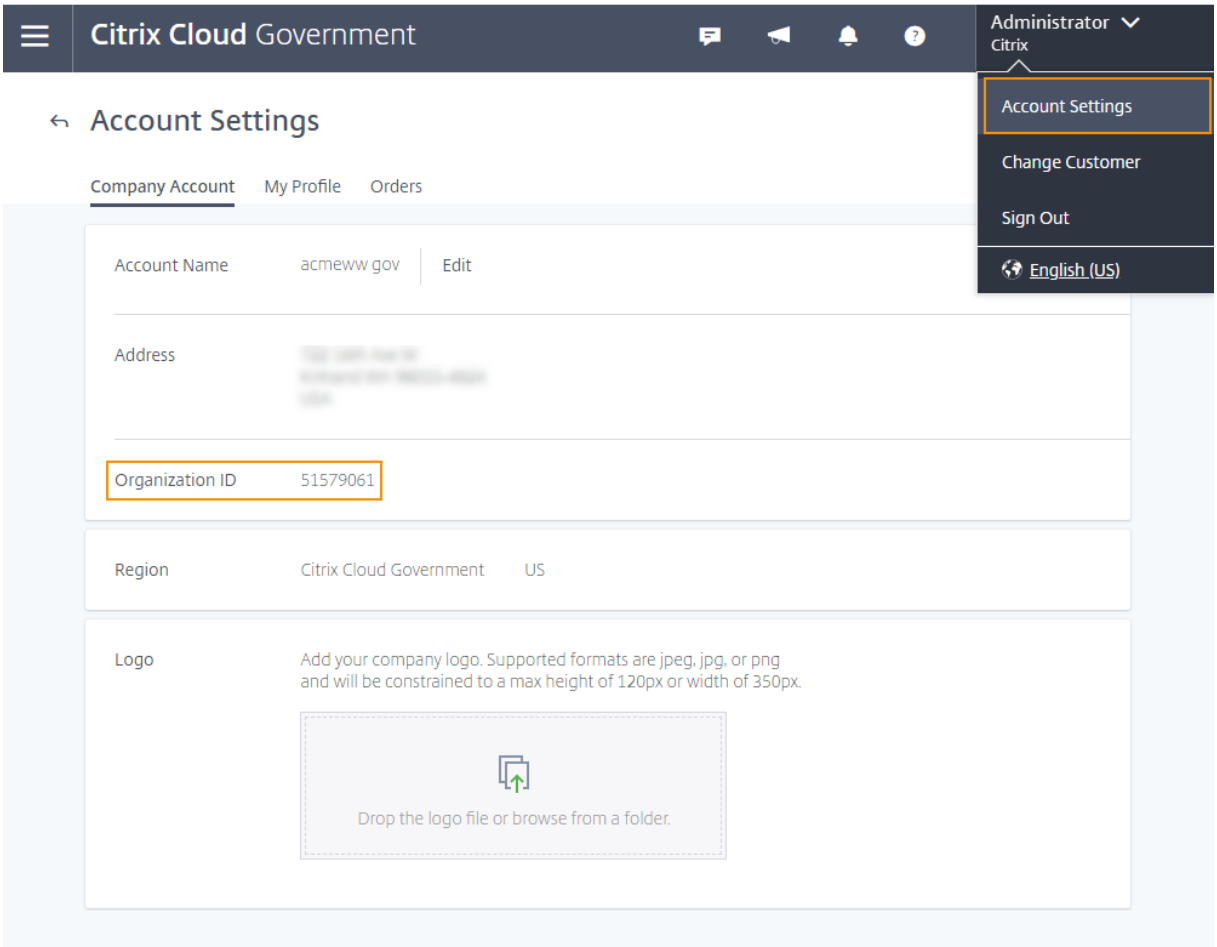
- Make sure you sign in with the **email address** and password you provided when you signed up for your account.
- If your organization allows users to sign in to Citrix Cloud Government using their organization credentials instead of a Citrix Cloud Government account, click **Sign in with my organization credentials** and enter your organization's sign-in URL. You can then enter your organization credentials to access your organization's Citrix Cloud Government account. If you don't know your organization's sign-in URL, contact your organization's administrator for assistance.

> **Note:** You can sign in with your organization credentials if Azure Active Directory is enabled as the identity provider for your account. For more information about using Azure Active Directory as your identity provider, see Connect Azure Active Directory to Citrix Cloud Government.

Purchasing services

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

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



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

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

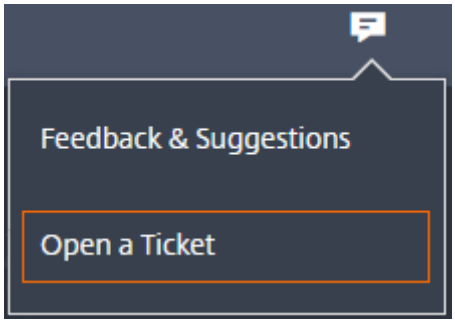
- The service is blocked to administrators and users 30 days after the service expires.
- The service is terminated 90 days after the service expires and Citrix deletes any remaining data.

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

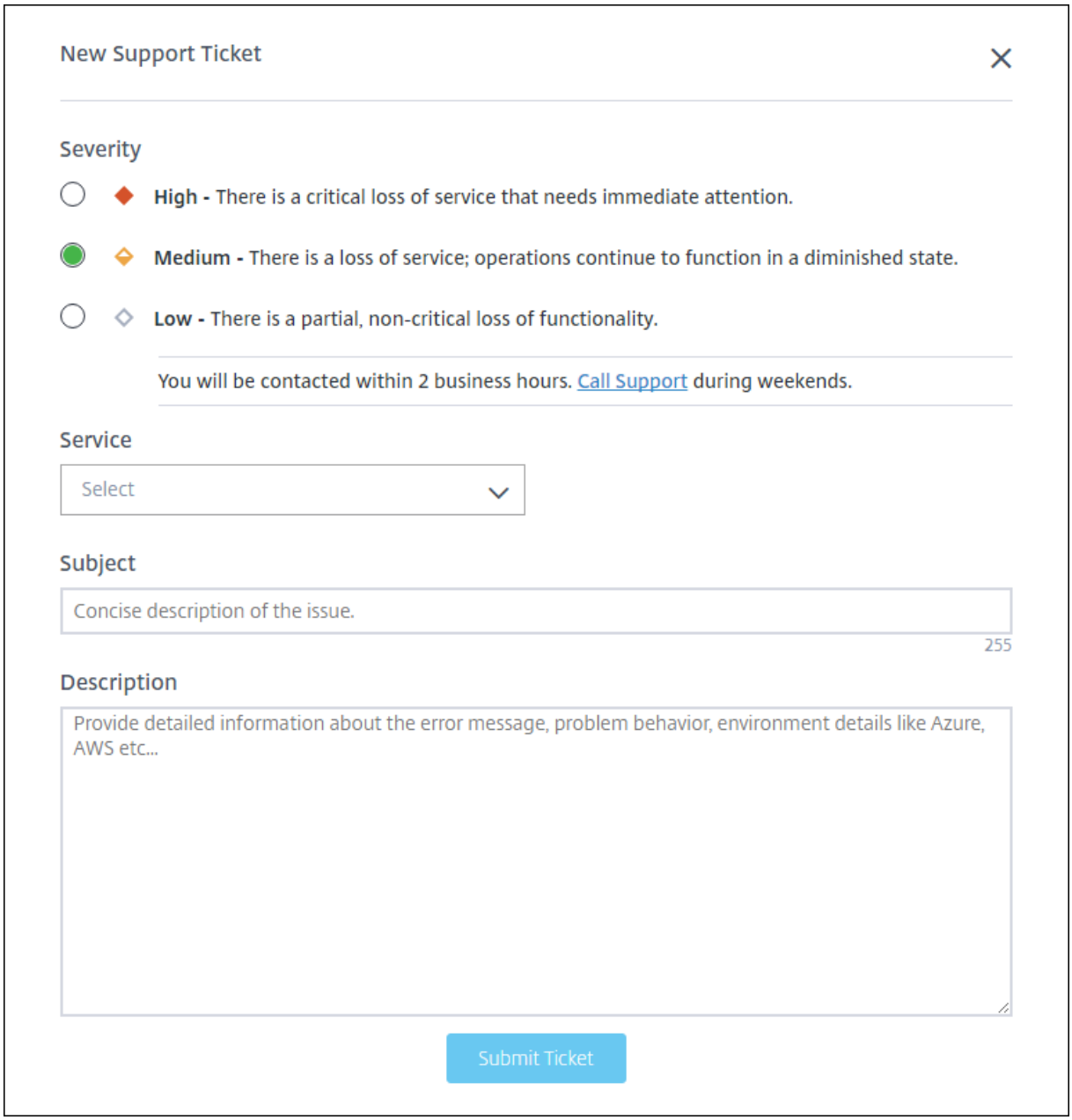
If you need additional assistance renewing or extending your subscription, contact Citrix Customer Service.

Technical Support

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



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



Secure Deployment Guide for Citrix Cloud Government

October 19, 2018

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

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

Control Plane

Guidance for administrators

- Use strong passwords and regularly change your passwords.
- All administrators within a customer account can add and remove other administrators. Ensure that only trusted administrators have access to Citrix Cloud Government.
- Administrators of a customer have, by default, full access to all services. Some services provide a capability to restrict the access of an administrator. Consult the per-service documentation for more information.
- Two-factor authentication for administrators is achieved using Citrix Cloud Government's integration with Azure Active Directory.

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 1.0 and TLS 1.2 with the strongest cipher suites. Customers cannot control the TLS certificate in use, as Citrix Cloud Government is hosted on the Citrix-owned cloud.us domain. To access Citrix Cloud Government, customers must use a browser capable of TLS 1.0 and TLS 1.2 with strong cipher suites.

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

Data sovereignty

The Citrix Cloud Government control plane is hosted in the United States. Customers do not have control over this.

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, and so on) are stored in resource locations and are under customer control.

Audit and change control

There is currently 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 will review the audit logs to determine the administrator who performed an operation, the date on which it was performed, the IP address associated with the action, and so on.

Citrix Cloud Connector

Installation

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

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

Configuration

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

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

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

can enable AD logging and auditing on the Cloud Connector's machine account to monitor any AD access activity.

Logging on to the machine hosting the Cloud Connector

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

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

Installing additional software on Cloud Connector machines

Customers can install antivirus software and hypervisor tools (if installed on a virtual machine) on the machines where the Cloud Connector is installed. However, Citrix recommends that customers do not install any other software on these machines. Other software creates additional possible security attack vectors and might reduce the security of the overall Citrix Cloud Government solution.

Inbound and outbound ports configuration

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

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

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

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

Client Port(s)	Server Port	Service
49152 -65535/UDP	123/UDP	W32Time
49152 -65535/TCP	135/TCP	RPC Endpoint Mapper
49152 -65535/TCP	464/TCP/UDP	Kerberos password change

Client Port(s)	Server Port	Service
49152 -65535/TCP	49152-65535/TCP	RPC for LSA, SAM, Netlogon (*)
49152 -65535/TCP/UDP	389/TCP/UDP	LDAP
49152 -65535/TCP	636/TCP	LDAP SSL
49152 -65535/TCP	3268/TCP	LDAP GC
49152 -65535/TCP	3269/TCP	LDAP GC SSL
53, 49152 -65535/TCP/UDP	53/TCP/UDP	DNS
49152 -65535/TCP	49152 -65535/TCP	FRS RPC (*)
49152 -65535/TCP/UDP	88/TCP/UDP	Kerberos
49152 -65535/TCP/UDP	445/TCP	SMB

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

Monitoring outbound communication

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

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

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

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

Each service within Citrix Cloud Government extends the list of servers and internal resources that the Cloud Connector might contact in the course of normal operations. Additionally, customers cannot control the data that the Cloud Connector sends to Citrix. For more information about services' internal resources and data sent to Citrix, consult Connectivity Requirements.

Viewing Cloud Connector logs

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

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

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

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

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

SSL/TLS Configuration

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

The Cloud Connector must trust the certification authority (CA) used by Citrix Cloud 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 will always use CAs that are part of the standard Windows Trusted Publisher list.

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

Connector updates

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

The customer is not required to take any other action to react to security issues. The Cloud Connector automatically applies any security fixes.

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 will continue to function normally. The old authorization secrets will become invalid in 2-4 weeks. Monitor the Cloud Connector during this time to ensure that there are no unexpected operations.
- **Ongoing high risk:** Citrix can revoke all old secrets. The existing Cloud Connectors will no longer function. To resume normal operation, the customer must uninstall and reinstall the Cloud Connector on all applicable machines.

Service trials for Citrix Cloud Government

September 6, 2018

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.

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

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

Fast facts about service trials

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

Request a service trial

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

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

1. Sign in to your Citrix Cloud 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'll receive an email notification. You have 60 days to complete the trial.

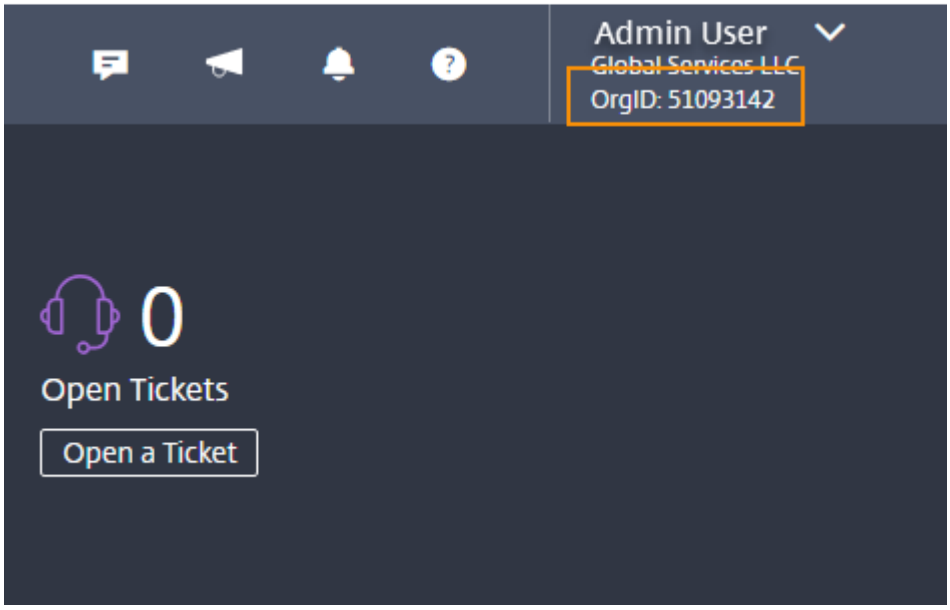
Note: To ensure the best customer experience, Citrix reserves the right to limit trials to a certain number of participants at any given time.

Purchase services

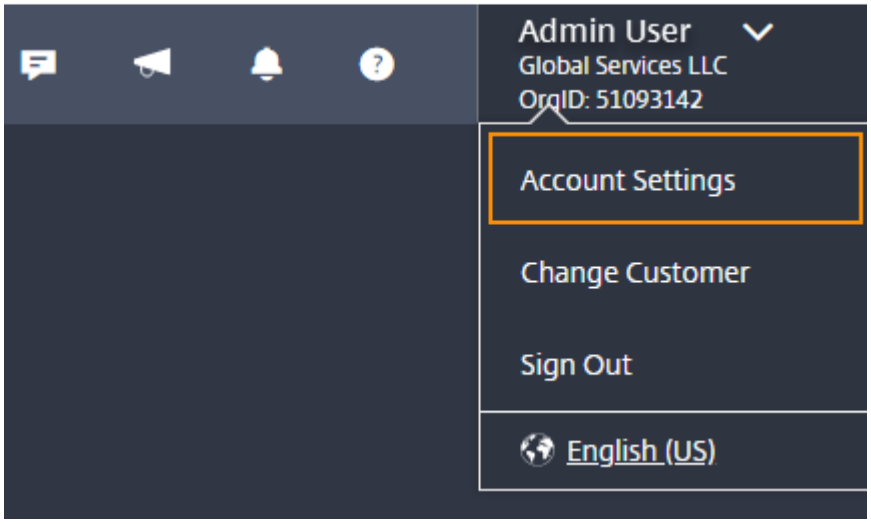
When you're ready to convert your trial to a production service, visit https://www.citrix.com/products/citrix-cloud/buy.html.

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

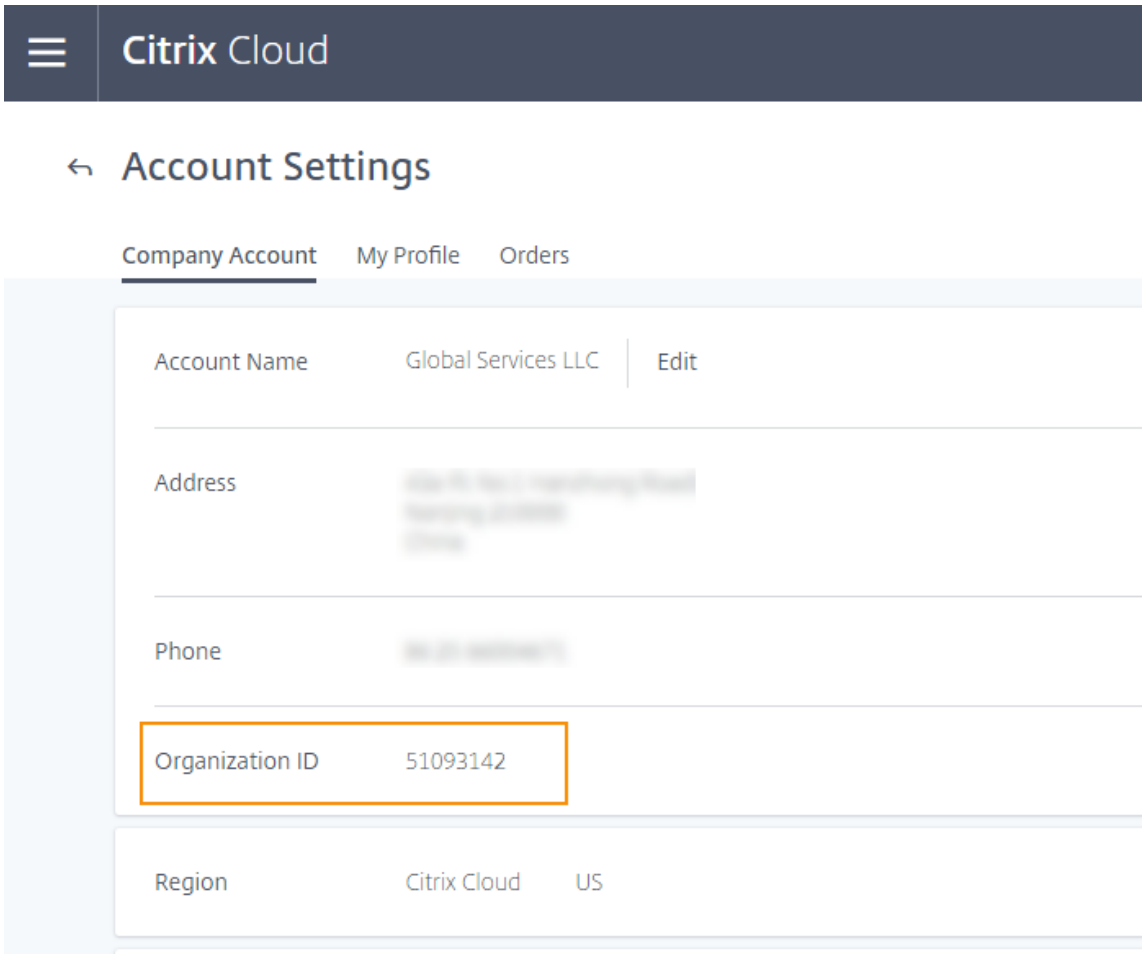
- In the top-right corner of the management console, your OrgID is displayed beneath your account name.



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



Your OrgID is shown in the Organization ID field.



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

October 9, 2018

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. So, organizations usually have a single OrgID. However, in some cases, such as having different branch offices or having different departments managing their assets separately, Citrix may allow an organization to have multiple OrgIDs.

What is a Citrix Cloud 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. A Citrix Cloud Government account is also uniquely identified by an OrgID. It's important to use the right Citrix Cloud Government account, based on how your organization has set up OrgIDs, so that your purchases and administrator access can continue on the same OrgIDs.

Try Citrix Cloud Government

Sign up for Citrix Cloud Government

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

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

- **The email address must be different than others you might have already used with commercial Citrix Cloud.** For example, if you're an administrator on a commercial Citrix Cloud account, Citrix Cloud has a record of that email address. If you sign up for Citrix Cloud Government with that same email address, Citrix Cloud Government does not accept it.

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

Accept the terms of service

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

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

Confirm your email address

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

Create a password and sign in

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

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

Purchase Citrix Cloud Government

Order Citrix Cloud Government

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

Review your order

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

Create a password

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

Sign in with your Citrix Cloud Government credentials

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

Connectivity requirements for Citrix Cloud Government

September 6, 2018

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.

Required addresses

Virtual Apps and Desktops service

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

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 web pages that make up the console might require other resources on the Internet, either when signing in or at a later point when carrying out specific operations.

Proxy configuration

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

Firewall configuration

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

Citrix Cloud Connector

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

Citrix Cloud Connector requirements

September 20, 2018

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

System requirements

The machine hosting the Cloud Connector must meet the following requirements:

- Microsoft .NET Framework 4.5.1 or later installed
- Joined to an Active Directory domain that contains the resources and users that you will use to create offerings for your users.
- Connected to a network that can contact the resources you will use in your resource location. For more information, see Cloud Connector Proxy and Firewall Configuration.
- Connected to the Internet. For more information, see Connectivity requirements.
- Server clock is set to the correct UTC time.

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 will not connect with Citrix Cloud Government.
- Because the Cloud Connector software is downloaded, your browser must allow downloading executable files.
- Install the Cloud Connector on domain-joined machine. If the machine is not joined to a domain, the Cloud Connector installer prevents the installation.
- The machine where you are installing the Cloud Connector must be in sync with UTC time.
- Turn off Internet Explorer Enhanced Security Configuration (IE ESC). If this is turned on, the Cloud Connector might not be able to establish connectivity with Citrix Cloud.
- Ensure you've met the Connectivity requirements for all machines where you install the Cloud Connector.
- If you're installing the Cloud Connector in an environment that has a web proxy or strict firewall rules, see Citrix Cloud Connector proxy and firewall configuration for requirements before continuing the installation.
- Ensure FIPS is not enabled on the machine you are installing the Cloud Connector. The Cloud Connector isn't supported for use with FIPS-enabled machines. If you attempt to install the Cloud Connector on a FIPS-enabled machine, the installation fails.

Important installation considerations

- Do not install the Cloud Connector on an Active Directory domain controller or any other machine critical to your resource location infrastructure. Regular maintenance on the Cloud Connector will perform machine operations that will cause an outage to these additional resources.
- Do not download or install other Citrix products on the machines hosting the Cloud Connector.
- Do not download or install the Cloud Connector on machines that are part of other Citrix product deployments (for example, Delivery Controllers in a XenDesktop deployment).

Important usage considerations

- Keep all Cloud Connectors powered on at all times 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. This ensures 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 you plan to use with Citrix Cloud Government should be reachable by two Cloud Connectors at all times.
- After installation, do not move the machine hosting the Cloud Connector into a different domain. If the machine needs to be joined to be a different domain, uninstall the Cloud Connector and then re-install it after the machine is joined to the different domain.## 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.

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

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

If the Cloud Connector is "disconnected" and the event logs don't indicate why a connection can't be established between the Cloud Connector and Citrix Cloud, 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. If the issue persists, contact Citrix Support.

To troubleshoot commmon issues with installing or using the Cloud Connector, refer to CTX221535.

Event messages

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

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

Event logs

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

Create a resource location

August 27, 2018

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

What is a resource location?

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

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

Task 1: Prepare machines

1. Review Citrix Cloud Connector requirements for requirements, important considerations, supported Active Directory functional levels, and troubleshooting information.

2. Prepare machines that meet the configuration requirements.
3. Join the prepared machines to your domain.

Task 2: Verify connectivity

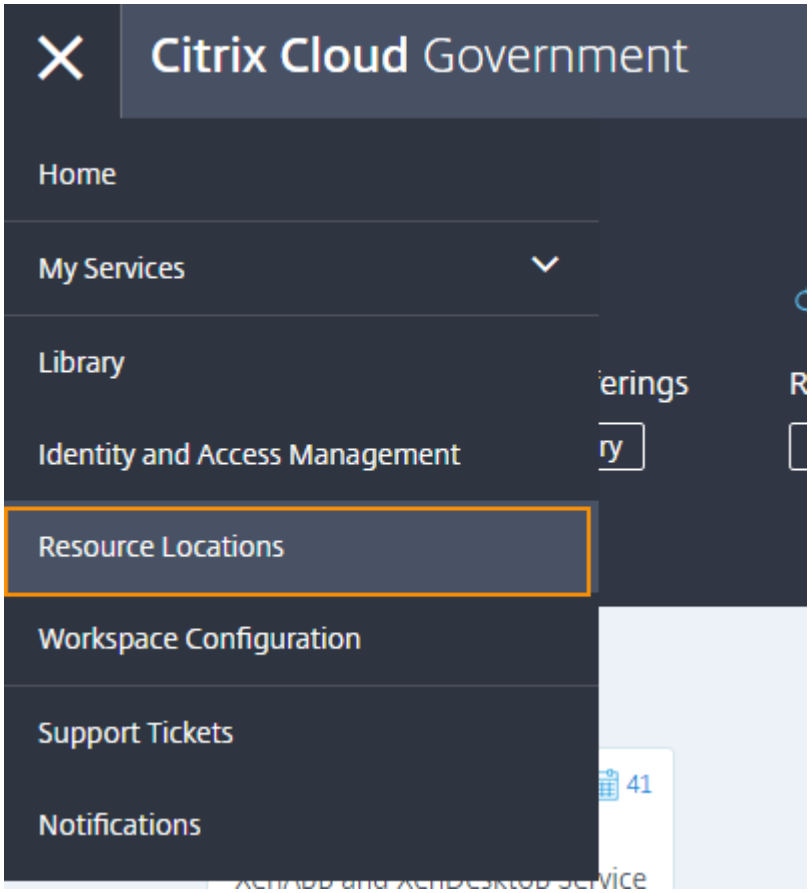
Connecting to the Internet from your data centers requires opening port 443 to outbound connections. However, to operate within environments containing an Internet proxy server or firewall restrictions, further configuration might be needed.

1. Review Connectivity requirements for a list of contactable addresses for available services.
2. Ensure port 443 (HTTPS) is open for outbound connections.
3. Ensure the required addresses can be contacted so you can operate and consume 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: Create your first resource location

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

1. From the Citrix Cloud Government management console, click the menu button in the top-left corner and select **Resource Locations**.



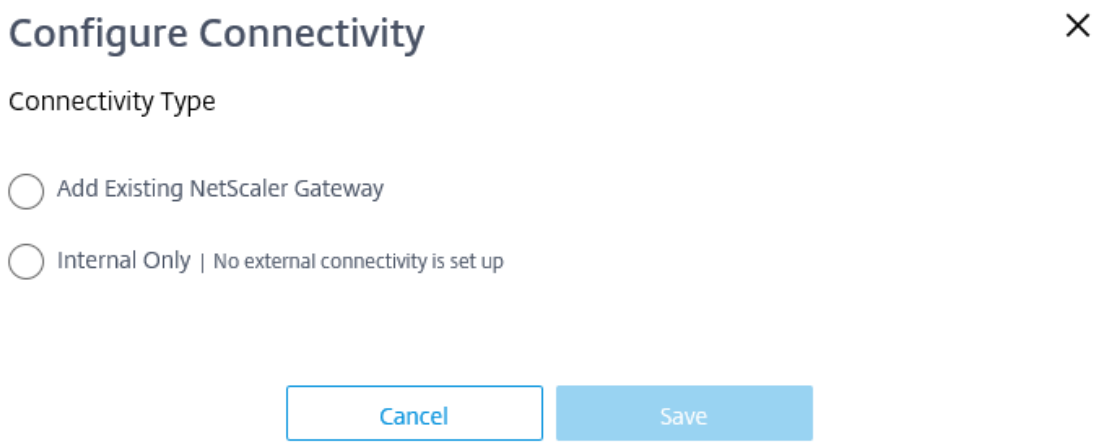
2. Click **Download** to download the Cloud Connector installer.
3. Double-click the installer. Citrix Cloud Government performs an initial connectivity check and prompts you for your Citrix Cloud Government administrator user name and password.
4. Follow the wizard to install and configure the Cloud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

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

Configure connectivity for users

Provide internal or external access to the services 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 internal-only access, select **Internal only**.
3. To configure secure access for external users:
   a) Select **Add existing Gateway**.
   b) Enter the external FQDN of the Citrix Gateway. Example: mynsg.my-domain.com
4. Click **Save**.

Create additional resource locations

After you create your first resource location, use the following steps to create others as needed.

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.

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.

If your organization account has multiple resource locations already, Citrix Cloud Government prompts you to select the resource location you want to associate with the Cloud Connector.

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

Cloud Connector installation logs

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

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

Install Cloud Connectors from the command line

August 27, 2018

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 performing the installation, validate the installer's permission(s), and download and configure the services the Cloud Connector provides. The installation occurs with the privileges of the user who initiates the install.

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

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

Supported parameters

You can retrieve a list of supported parameters by running **CWCConnector /?**.

- **/Customer:** Required. The customer ID shown on the API Access page in the Citrix Cloud Government console (within Identity and Access Management).
- **/ClientId:** Required. The secure client ID an administrator can create, located on the API Access page.
- **/ClientSecret:** Required. The secure client secret that can be downloaded after the secure client is created. Located on the API Access page.
- **/ResourceLocationId:** Required. The unique identifier for an existing resource location. To retrieve the ID, click the **ID** button for the resource location on the Resource Locations page in the Citrix Cloud Government console. If no value is specified, Citrix Cloud Government uses the ID of the first resource location in the account.
- **/AcceptTermsOfService:** Required. Default value is **Yes**.

A sample command line with all required parameters:

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

Exit codes

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

Installation Logs

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

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

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 will not 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

July 6, 2018

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 will use the settings configured for Internet connections. If you can browse the Internet from the machine then the installer should also function.

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

Services at Runtime

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

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

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

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

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

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

Set up the Virtual Apps and Desktops service

September 20, 2018

This article provides an overview of the tasks required to set up the Virtual Apps and Desktops service. For a list of service features that are not available in Citrix Cloud Government, see Virtual Apps and Desktops service for Citrix Cloud Goverment.

Request a service trial

If you don't have a subscription to the Virtual Apps and Desktops service, 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 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 the service

To configure the Virtual Apps and Desktops service, complete the following tasks:

- Create a host connection. A host connection enables the Virtual Apps and Desktops service 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 applications or desktops that appear are governed by the Delivery Groups to which those users belong.

Citrix Gateway

Citrix Gateway provides users with secure access to Virtual Apps and Desktops applications across a range of devices. If you have an existing on-premises Gateway, you can use it with the Virtual Apps and Desktops service to ensure external users can access their applications securely. If you need to create a new Gateway deployment to use with the Virtual Apps and Desktops service, refer to Deploy a Citrix ADC VPX instance.

Additional features

To learn more about using the other features in the Virtual Apps and Desktops service, refer to the following articles:

- Printing

- HDX technologies
- Policies
- Managing resources and users
- Monitoring

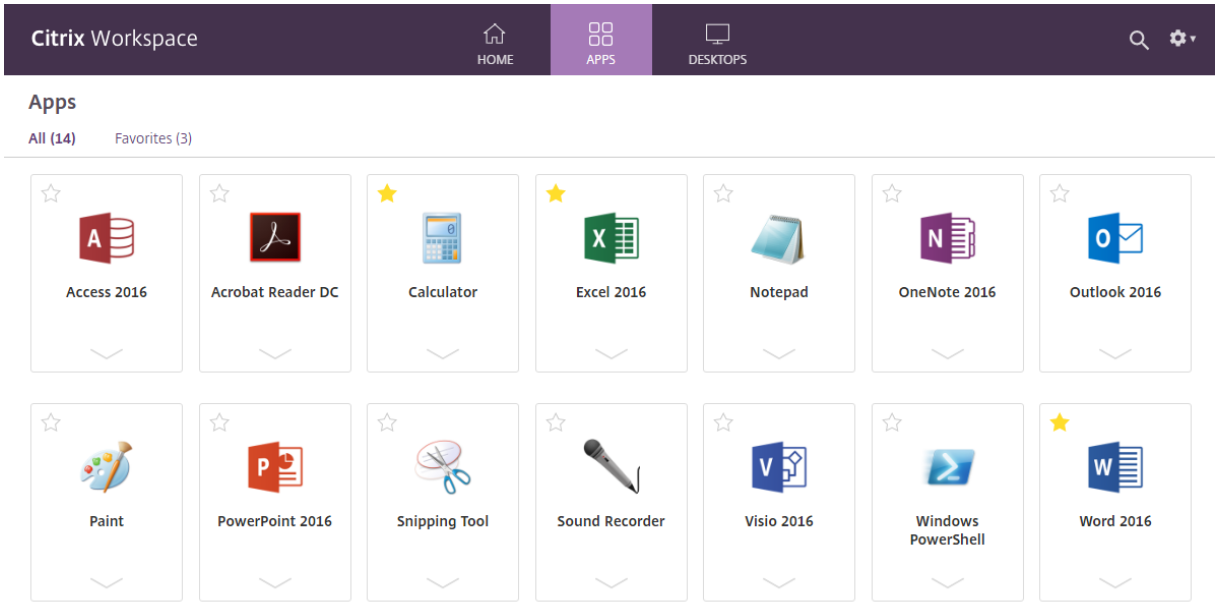
Next steps

After you set up the Virtual Apps and Desktops service, 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

August 27, 2018

A workspace allows you to deliver access to applications and desktops from any device. Workspaces provide access to resources based on the Delivery Groups you configure in the Virtual Apps and Desktops service.



Before you set up workspaces for your users, review the features that are not 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

September 6, 2018

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

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

Manage Citrix Cloud Government

September 6, 2018

Citrix Cloud Government includes the following administrative features:

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

Identity providers

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 this to use Azure Active Directory or your on-premises Active Directory instead.

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

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

Administrators

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

A Citrix identity mechanism provides authentication for administrators using an email address and password. Administrators can also use their My Citrix credentials to sign in to Citrix Cloud Government.

Add new administrators

During the account onboarding process, an initial administrator is created. The administrator can then invite other administrators to join Citrix Cloud Government. These new administrators can 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. This allows you to define access that's aligned with the administrator's role in your organization.

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

Change your password

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

Remove administrators

You can remove administrators from your Citrix Cloud 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 will stay active for a maximum of one minute. Afterward, 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 are not linked to administrator accounts. So, Cloud Connectors will continue operating even if you remove the administrator who installed it.

Subscribers

A subscriber's identity defines the services to which they have access in Citrix Cloud 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.

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.

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

Manage subscriber usage

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

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

Primary resource locations

A primary resource location is a resource location that you designate as "most preferred" for communications between your domain and Citrix Cloud Government. The resource location you select as

"primary" should have Cloud Connectors that have the best performance and connectivity to your domain. This enables your users to log on quickly to Citrix Cloud 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 or 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.

Connect Active Directory to Citrix Cloud Government

September 6, 2018

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 this to use Active Directory (AD) instead.

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

To connect your Active Directory to Citrix Cloud

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

Connect Azure Active Directory to Citrix Cloud Government

September 6, 2018

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 this to use Azure Active Directory (AD) instead.

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

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

Prepare your Active Directory and Azure AD

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

- **Your Azure AD infrastructure is hosted in an Azure Government instance.** You cannot federate Azure AD hosted in a commercial Azure instance to Citrix Cloud Government. If you attempt to use Azure AD in a commercial Azure instance with Citrix Cloud Government, Azure AD does not work. If you don't have an Azure Government account, sign up at https://azure.microsoft.com/en-us/global-infrastructure/government/request/.
- **Administrator accounts have their "mail" property configured in Azure AD.** To do this, you can sync accounts from your on-premises Active Directory into Azure AD using Microsoft's Azure AD Connect tool. Alternatively, you can configure non-synced Azure AD accounts with Office 365 email.

Sync accounts with Azure AD Connect

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

Connect Citrix Cloud Government to Azure AD

When connecting your Citrix Cloud Government account to your Azure AD, Citrix Cloud Government will need permission to access your user profile (or the profile of the signed-in user) as well as the basic profiles of the users in your Azure AD. Citrix requests this permission so it can acquire your name and email address (as the administrator) and enable you to browse for other users and add them as administrators later.

1. Sign in to Citrix Cloud Government at https://citrix.cloud.us.
2. Click the menu button in the top-left corner of the page and select **Identity and Access Management**.
3. Locate **Azure Active Directory**, click the ellipsis button, and then select **Connect**.
4. When prompted, enter a short, URL-friendly identifier for your company and click **Connect**. The identifier you choose must be globally unique within Citrix Cloud Government.
5. When prompted, sign in to the Azure account with which you want to connect. Azure shows you the permissions that Citrix Cloud Government needs to access the account and acquire the information required for connection.
6. Click **Accept** to accept the permissions request.

Add administrators to Citrix Cloud Government from Azure AD

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

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

Sign in to Citrix Cloud using Azure AD

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

- Navigate to the administrator sign-in URL that you configured when you initially connected the Azure AD identity provider for your company. Example: `https://citrix.cloud.us/go/myorganization`

- From the Citrix Cloud Government sign-in page, click **Sign in with my organization credentials**, type the identifier you created when you initially connected Azure AD, and click **Continue**.

Enable advanced Azure AD capabilities

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

Add administrators to a Citrix Cloud Government account

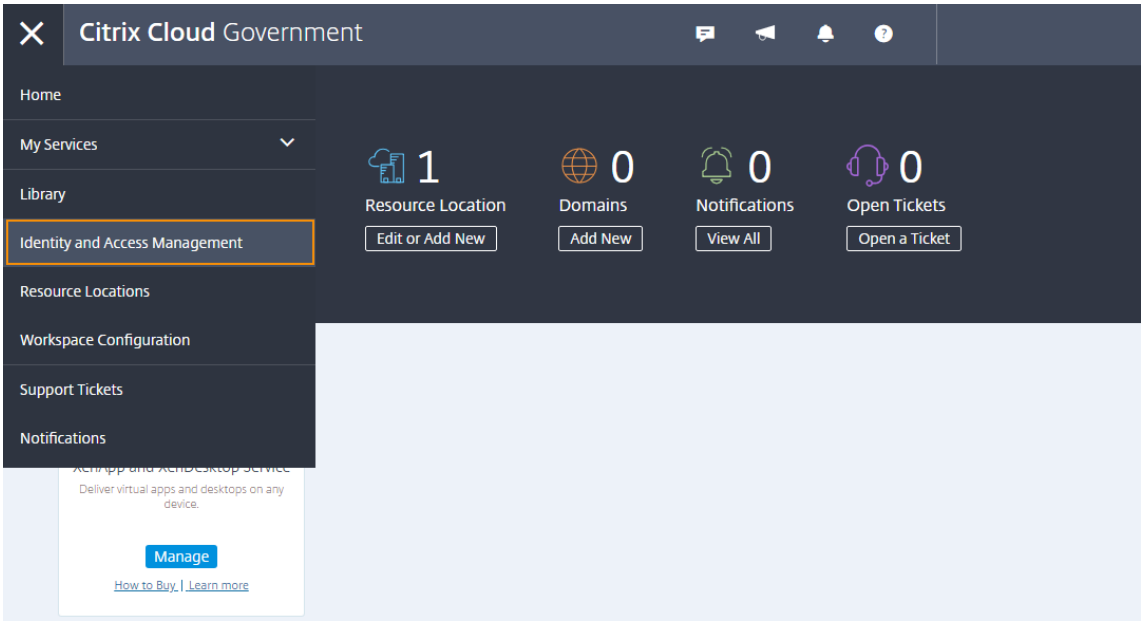
August 27, 2018

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

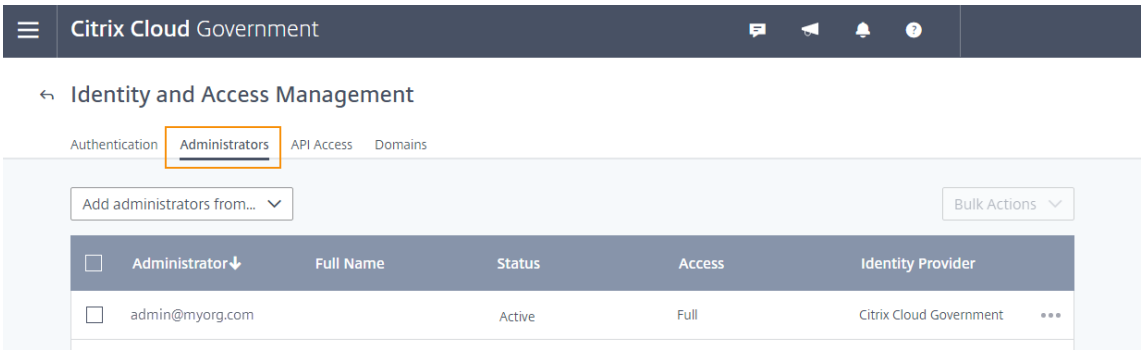
By default, new administrators have Full Access permissions to all functions in the Citrix Cloud Government account. See Configure administrator permissions in this article to learn how to delegate account administration.

Invite new administrators

1. After signing in to Citrix Cloud Government, select **Identity and Access Management** from the menu.



2. On the **Identity and Access Management** page, click **Administrators**. The console shows all the current administrators in the account.



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

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

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

Configure administrator permissions

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

- Help desk access for Virtual Apps and Desktops service
- Access to manage one or more specific cloud services
- Access to manage specific Citrix Cloud Government functions such as Library or Resource Locations

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

To define access permissions

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

1. Sign in to Citrix Cloud 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 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**.

Citrix Cloud Government platform

August 27, 2018

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

- To use Azure Active Directory with Citrix Cloud Government, your Azure AD infrastructure must be hosted in an Azure Government instance. Azure AD hosted in commercial Azure instances cannot federate to Citrix Cloud Government.

- Using the Citrix Gateway service to provide external connectivity to resources is not available. Connectivity options are limited to internal-only access or secure access through an existing on-premises Citrix Gateway.
- Self-service guides that provide walkthroughs of certain aspects of the platform are not available.
- The option to register feedback or suggestions about the platform is not available.
- Cloud license usage functions and active usage reports are not available.

Virtual Apps and Desktops service for Citrix Cloud Government

August 27, 2018

Virtual Apps and Desktops service is generally available to Citrix Cloud Government customers.

Differences

Using the Citrix Gateway service to provide secure access to applications and desktops for external users is not available. To provide external connectivity, an on-premises Citrix Gateway is required.

Workspace Service for Citrix Cloud Government

August 27, 2018

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

Differences

Features not currently available in Workspace Service for Citrix Cloud Government are:

- Using the Citrix Gateway Service to provide secure access to Workspace resources for external users is not available. To provide external connectivity, an on-premises Citrix Gateway is required.
- Specifying the Citrix Gateway service as an external connectivity option when adding an on-premises Virtual Apps and Desktops Site to Workspace. To provide external connectivity, an on-premises Gateway is required.

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