Citrix Cloud

Contents

Citrix Cloud

September 16, 2021

Citrix Cloud is a platform that hosts and administers Citrix cloud services. It connects to your resources through connectors on any cloud or infrastructure you choose (on-premises, public cloud, private cloud, or hybrid cloud). It allows you to create, manage, and deploy workspaces with apps and data to your end-users from a single console.

Try Citrix Cloud

Experience a full production environment in a proof-of-concept for one or more Citrix Cloud services. After signing up for Citrix Cloud, you can request service trials right inside the console. When the trial ends, you can convert to a production environment so you retain all your configurations. For more information, see Citrix Cloud Service Trials.

Citrix Cloud service documentation

Looking for information about setting up or managing Citrix Cloud services? Go to the **Citrix Cloud Services** section in the Table of Contents on the left side of this page. Select the service that you want to go directly to the product documentation for that service.

Architectural and deployment resources

Citrix Tech Zone contains a wealth of information to help you learn more about Citrix Cloud and other Citrix products. Here you'll find reference architectures, diagrams, and technical papers that provide insights for designing, building, and deploying Citrix technologies.

To learn more about key service components in Citrix Cloud, see the following resources:

- Citrix Workspace conceptual diagram: Provides an overview of key areas such as identity, workspace intelligence, and single sign-on.
- Reference Architectures: Provides comprehensive guides for planning your Citrix Workspace implementation, including use cases, recommendations, and related resources.
- Virtual Apps and Desktops Service reference architectures: Provides in-depth guidance for deploying Virtual Apps and Desktops service with related services.

Education resources

The Citrix Cloud Learning Series portal offers education modules to get you up and running with Citrix Cloud and its services. You can view all of the modules sequentially, from overviews through planning and building services. Start your cloud journey with the following courses:

- Fundamentals of Citrix Cloud
- Intro to Citrix Identity and Authentication
- Moving from StoreFront to Workspace

The Citrix Education video library offers online video lessons that walk you through key deployment tasks and troubleshooting the components that you use with Citrix Cloud services. Learn more about tasks like installing Cloud Connectors and registering VDAs, as well as troubleshooting these components.

Service Level Agreement

June 29, 2021

Effective date: October 30, 2020

Citrix Cloud 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 Service availability. This SLA is part of the Citrix end user service agreement (EUSA) 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 https://docs.citrix.com, 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.

Citrix Service Providers (CSPs) are eligible on October 1, 2018.

Per Service Availability Measures

Service	Measure for Monthly Uptime
Citrix Analytics for Performance	Time users can access and improve apps and desktops performance.
Citrix Analytics for Security	Time users can detect and mitigate user access and activity risks.
Citrix Application Delivery Management service	Average time the Service is available across all POPs.
Citrix Content Collaboration	Time users can enumerate files and folders associated with their account or download files that are hosted in Citrix-managed storage zones.
Citrix Endpoint Management	Time users can access their Citrix delivered mobile apps and enrolled devices through the Service.
Citrix Gateway Service for HDX Proxy	Time users can access their app or desktop session through the Service.
Citrix Intelligent Traffic Management	Time users can access traffic management functionality through DNS queries or HTTP API calls.
Citrix SD-WAN Orchestrator	Time users can access their SD-WAN Orchestrator account and manage their SD-WAN network through the Service.
Citrix Secure Workspace Access	Time users can access their SaaS or internal web app through the Service.

Service	Measure for Monthly Uptime
Citrix Virtual Apps service	Time users can access their app or desktop session through the Service.
Citrix Virtual Desktops service	Time users can access their app or desktop session through the Service.
Citrix Virtual Apps and Desktops service	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.
Citrix Wrike	Time users can access and use the service.

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 EUSA 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. Customer 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 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.

Secure Deployment Guide for the Citrix Cloud Platform

June 24, 2021

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

The following articles provide similar information for other services in Citrix Cloud:

- Analytics Technical Security Overview
- Endpoint Management Technical Security Overview
- Secure Browser Technical Security Overview
- ShareFile Technical Security Overview
- Virtual Apps and Desktops technical security overview
- Virtual Apps and Desktops Standard for Azure technical security overview

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.
- 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's integration with Azure Active Directory.
- By default, Citrix Cloud automatically terminates administrator sessions after 60 minutes of inactivity. This 60-minute timeout cannot be changed. *Inactive* means the session is completely idle and the administrator is not interacting with the Citrix Cloud console in any way. *Activity* refers to actions such as navigating the graphical interface, selecting configuration options, saving configuration changes, or waiting for a change to take effect.

Password compliance

Citrix Cloud prompts administrators to change their passwords if their current password is more than 60 days old. New passwords must meet all of 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 cannot be used as a new password.
- The previous 24 passwords cannot be reused.
- The new password must be in effect for at least one day before Citrix Cloud allows it to be changed again.

Encryption and key management

The control plane does not store sensitive customer information. Instead, Citrix Cloud retrieves information such as administrator passwords on-demand (by prompting the administrator explicitly). There is no data-at-rest that is sensitive or encrypted, and thus you do not need to manage any keys.

For data-in-flight, Citrix uses industry standard TLS 1.2 with the strongest cipher suites. Customers cannot control the TLS certificate in use, as Citrix Cloud is hosted on the Citrix-owned cloud.com domain. To access Citrix Cloud, customers must use a browser capable of TLS 1.2, and must have accepted cipher suites configured.

- If the Cloud Connector is installed on Windows Server 2016 or Windows Server 2019, the following strong ciphers are recommended: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- If the Cloud Connector is installed on Windows Server 2012 R2, the strong ciphers are not available, so the following ciphers must be used: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

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

Data sovereignty

The Citrix Cloud control plane is hosted in the United States, the European Union, and Australia. Customers do not have control over this.

The customer owns and manages the resource locations that they use with Citrix Cloud. 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.

For Content Collaboration, consult the following resources for information about controlling where the data resides:

- Content Collaboration service documentation
- ShareFile Security FAQ
- Citrix ShareFile Security and Compliance
- How to Implement Storage Zones for On-Premises Storage

Other services may have an option to store data in different regions. Consult the Geographical Considerations topic or the Technical Security Overviews (listed at the beginning of this article) for each service.

Security issues insight

The website status.cloud.com provides transparency into security issues that have an ongoing impact on the customer. The site logs status and uptime information. There is an option to subscribe for updates to the platform or individual services.

Citrix Cloud Connector

Installing the Cloud Connector

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

Also, Citrix strongly recommends that the machines on which the Cloud Connector software is installed 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 Citrix Cloud Connector.

Configuring the Cloud Connector

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) Citrix strongly recommends that the Cloud Connector's machine account be restricted to read-only access. This is the default configuration in Active Directory.

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 allows sensitive security information to pass through to other platform components in Citrix Cloud services, but also stores the following sensitive information:

- Service keys for communicating with Citrix Cloud
- Hypervisor service credentials for power management in Citrix Virtual Apps and Desktops

This sensitive information is encrypted using the Data Protection API (DPAPI) on the Windows server hosting the Cloud Connector. Citrix strongly recommends allowing only the most privileged administrators to log on to Cloud Connector machines (for example, to perform maintenance operations). In general, there is no need for an administrator to log on to these machines to manage any Citrix product. The Cloud Connector is self-managing in that respect.

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

Installing other 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 possible security attack vectors and might reduce the security of the overall Citrix Cloud solution.

Inbound and outbound ports configuration

The Cloud Connector requires outbound port 443 to be open with access to the internet. Citrix strongly recommends that the Cloud Connector 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 support SSL/TLS encrypted communication.

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

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

Client Port	Server Port	Service
49152 -65535/UDP	123/UDP	W32Time

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

Each of the services used within Citrix Cloud extends the list of open ports required. For more information, consult the following resources:

- Technical Security Overviews for each service (listed at the beginning of this article)
- Internet Connectivity Requirements for Citrix Cloud services
- Application Delivery Management service port requirements
- Endpoint Management port requirements

Monitoring outbound communication

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

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

During normal operation, the Cloud Connector communicates only with domain controllers in domains that are not disabled on the **Identity and Access Management** page in the Citrix Cloud user interface.

Each service within Citrix Cloud 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 the following resources:

- Technical Security Overviews for each service (listed at the beginning of this article)
- Internet Connectivity Requirements for Citrix Cloud services

Viewing Cloud Connector logs

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

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

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

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

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

SSL/TLS Configuration

The 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 SSL/TLS certificates and by Microsoft Azure Service Bus SSL/TLS certificates. Citrix and Microsoft might change certificates and CAs in the future, but always uses CAs that are part of the standard Windows Trusted Publisher list.

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

Security compliance

To ensure security compliance, 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.

Citrix Connector Appliance for Cloud Services

Installing the Connector Appliance

The Connector Appliance is hosted on a hypervisor. This hypervisor must be inside your private network and not in the DMZ.

Ensure that the Connector Appliance is within a firewall that blocks access by default. Use an allow list to allow only expected traffic from the Connector Appliance.

Ensure that the hypervisors that host your Connector Appliances are installed with up-to-date security updates.

For network and system requirements and instructions for installing the Connector Appliance, see Connector Appliance for Cloud Services.

Logging on to the hypervisor hosting a Connector Appliance

The Connector Appliance contains a service key for communicating with Citrix Cloud. Allow only the most privileged administrators to log on to a hypervisor hosting the Connector Appliance (for example, to perform maintenance operations). In general, there is no need for an administrator to log on to these hypervisors to manage any Citrix product. The Connector Appliance is self-managing.

Inbound and outbound ports configuration

The Connector Appliance requires outbound port 443 to be open with access to the internet. Citrix strongly recommends that the Connector Appliance have no inbound ports accessible from the internet.

You can locate the Connector Appliance behind a web proxy for monitoring its outbound internet communications. However, the web proxy must support SSL/TLS encrypted communication.

The Connector Appliance might have other outbound ports with access to the internet. The Connector Appliance negotiates across a wide range of ports to optimize network bandwidth and performance if other ports are available.

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

Connection Direction	Connector Appliance Port	External Port	Service
Inbound	443/TCP	Any	Local Web UI
Outbound	49152-65535/UDP	123/UDP	NTP

Connection Direction	Connector Appliance Port	External Port	Service
Outbound	53, 49152-65535/TCP/UDP	53/TCP/UDP	DNS
Outbound	67/UDP	68/UDP	DHCP and broadcast

Each of the services used within Citrix Cloud extends the list of open ports required. For more information, consult the following resources:

- Technical Security Overviews for each service (listed at the beginning of this article)
- System and Connectivity Requirements for Citrix Cloud services

Monitoring outbound communication

The Connector Appliance communicates outbound to the Internet on port 443 to Citrix Cloud servers.

Each service within Citrix Cloud extends the list of servers and internal resources that the Connector Appliance might contact during normal operations. Also, customers cannot control the data that the Connector Appliance sends to Citrix. For more information about services' internal resources and data sent to Citrix, consult the following resources:

- Technical Security Overviews for each service (listed at the beginning of this article)
- System and Connectivity Requirements for Citrix Cloud services

Viewing Connector Appliance logs

You can download a diagnostic report for your Connector Appliance that includes various log files. For more information about getting this report, see Connector Appliance for Cloud Services.

SSL/TLS Configuration

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

The Connector Appliance trusts the certification authority (CA) used by Citrix Cloud SSL/TLS certificates. Citrix might change certificates and CAs in the future, but always use CAs that the Connector Appliance trusts.

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

Security compliance

To ensure security compliance, the Connector Appliance self-manages and you cannot log in to it through the console.

You are not required to take any other action to react to connector security issues. The Connector Appliance automatically applies any security fixes.

Ensure that the hypervisors that host your Connector Appliances are installed with up-to-date security updates.

Guidance for handling compromised accounts

- Audit the list of administrators in Citrix Cloud 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.

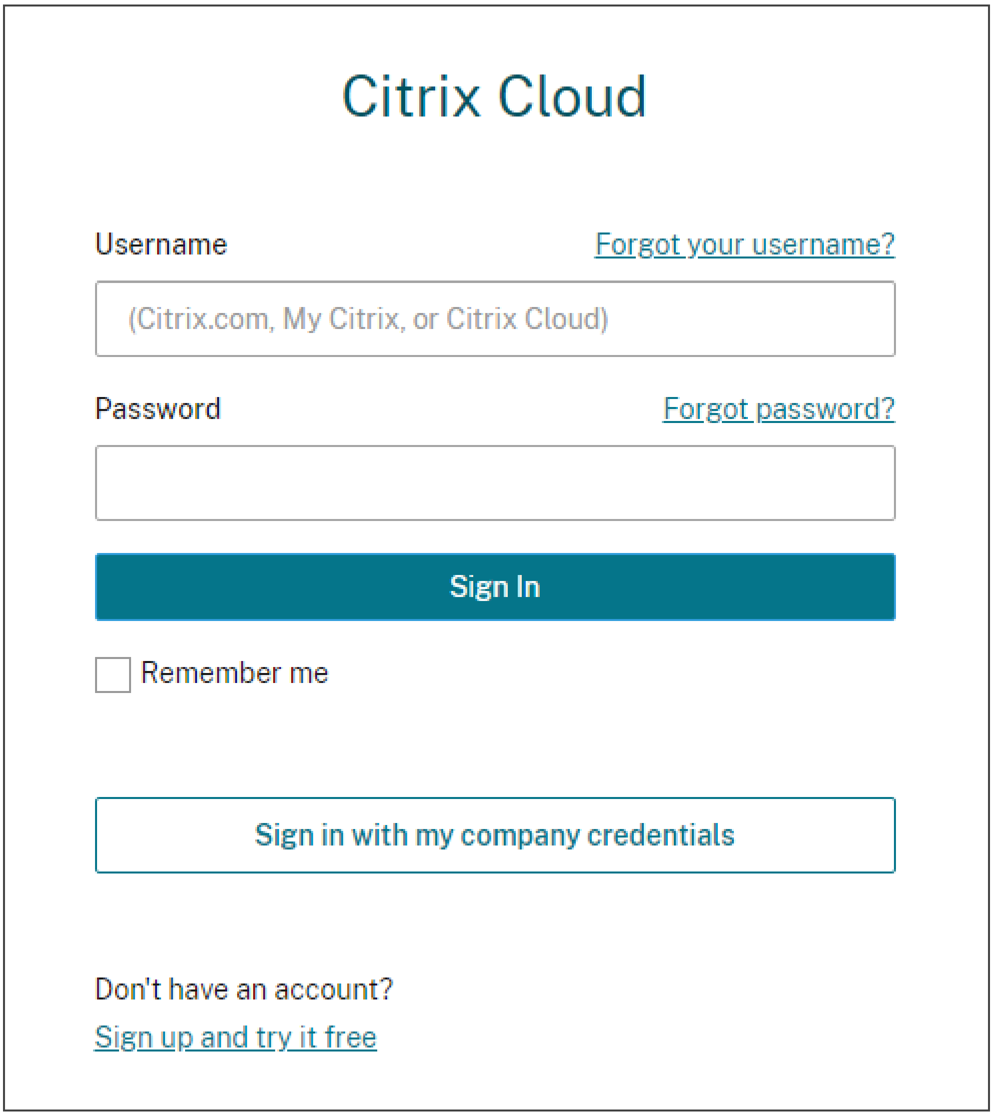
How to Get Help and Support

July 8, 2021

Creating a Citrix Cloud account

If you encounter an error when signing up for a Citrix Cloud account, contact Citrix Technical Support.

Signing in to your account



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

- Make sure you sign in with the email address and password you provided when you signed up for your account.
- If you haven't recently signed in to Citrix Cloud or if your password doesn't meet requirements, you're prompted to reset your password before signing in. For more information, see Changing your password in this article.
- If users access Citrix Cloud using company credentials instead of a Citrix account, select **Sign in with my company credentials** and enter your company's sign-in URL. You can then enter your company credentials to access your company's Citrix Cloud account. If you don't know your company's sign-in URL, contact your company's administrator for assistance.

Changing your password

If you've forgotten your Citrix Cloud account password, select **Forgot your username or password?** and enter your account email address to receive an email to reset your password. If you don't receive the password reset email, or if you need further assistance, contact Citrix Customer Service.

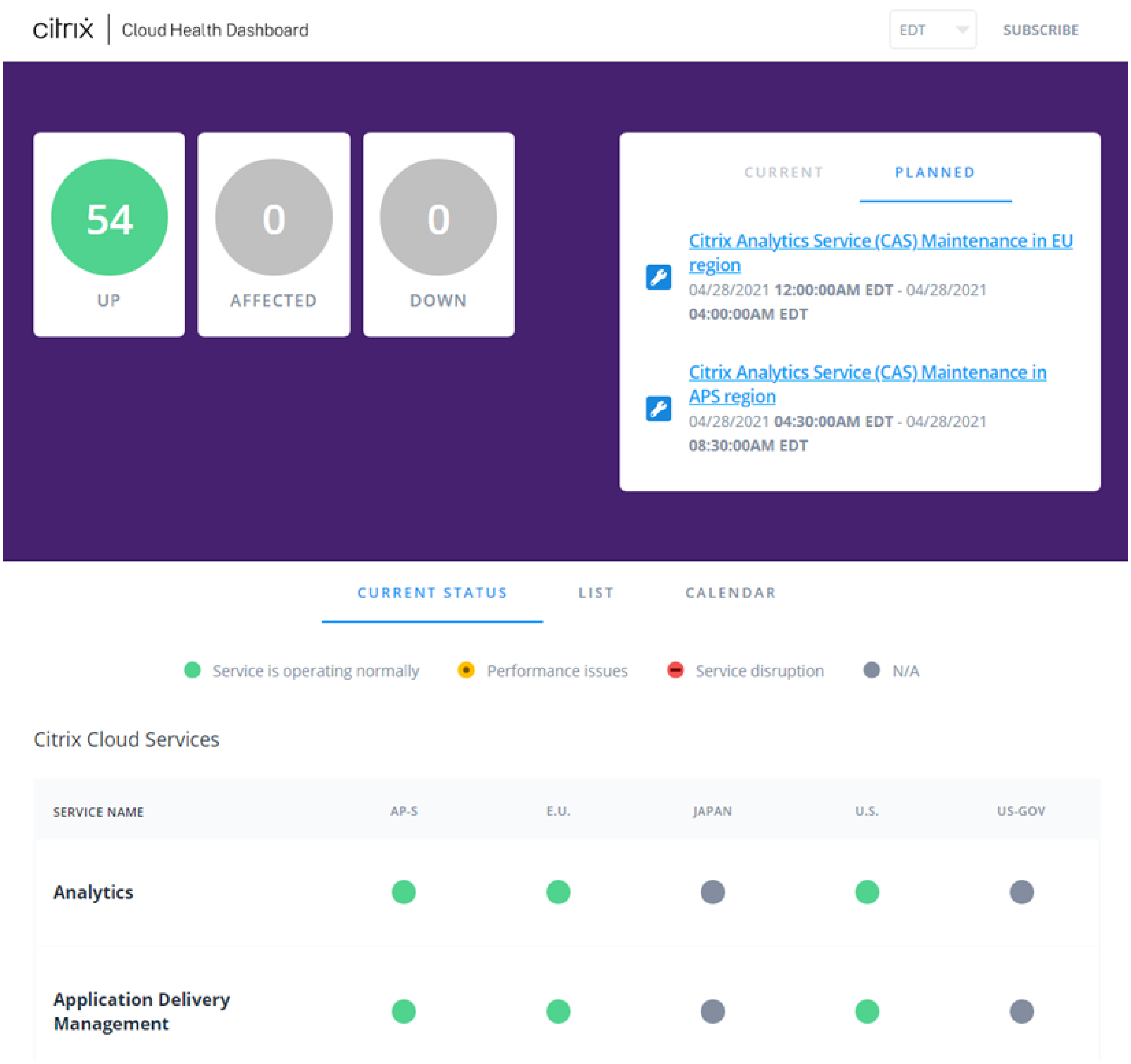
To help keep your account password safe and secure, Citrix Cloud might prompt you to reset your password when you attempt to sign in. This prompt occurs if:

- Your password doesn't meet Citrix Cloud's complexity requirements. Passwords must be at least 8 characters long and include:
  - At least one number
  - At least one upper-case letter
  - At least one symbol: ! @ # $ % ^ * ? + = -
- Your password includes dictionary words.
- Your password is listed in a known database of compromised passwords.
- You haven't signed in to Citrix Cloud in the last six months.

When prompted, select **Reset Password** to create a new strong password for your account.

Cloud Health Dashboard

The Citrix Cloud Health Dashboard (https://status.cloud.com) 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.



Citrix Analytics Service (CAS) Maintenance in EU region
04/28/2021 **12:00:00AM EDT** - 04/28/2021 **04:00:00AM EDT**

Citrix Analytics Service (CAS) Maintenance in APS region
04/28/2021 **04:30:00AM EDT** - 04/28/2021 **08:30:00AM EDT**

🟢 Service is operating normally 🟡 Performance issues 🔴 Service disruption ⚫ N/A

Citrix Cloud Services

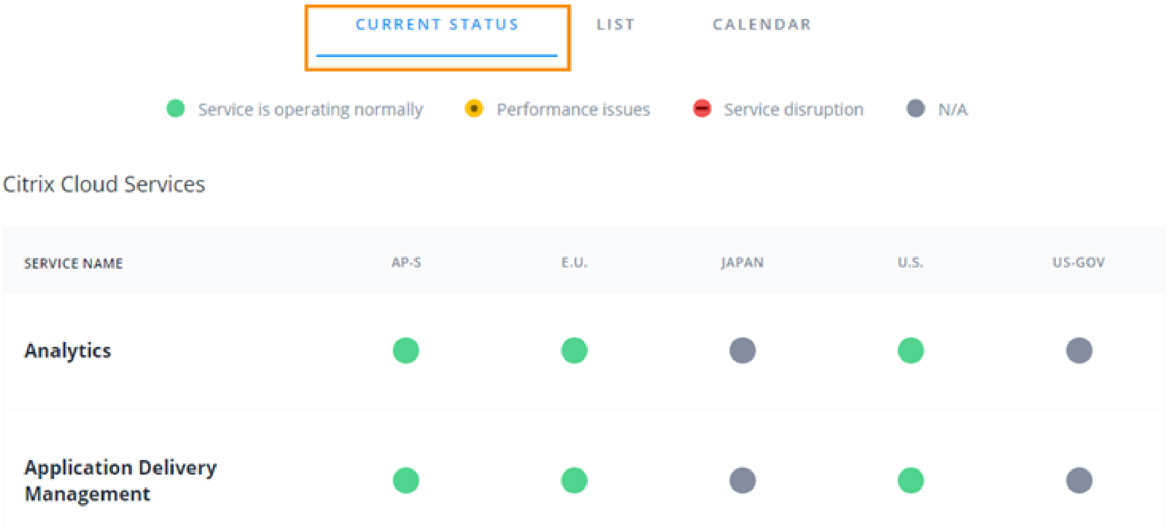
SERVICE NAME	AP-S	E.U.	JAPAN	U.S.	US-GOV
Analytics	🟢	🟢	⚫	🟢	⚫
Application Delivery Management	🟢	🟢	⚫	🟢	⚫

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

View health and maintenance status

Select **Current Status** to display the current health status of all Citrix Cloud services and platform components in each geographical region.

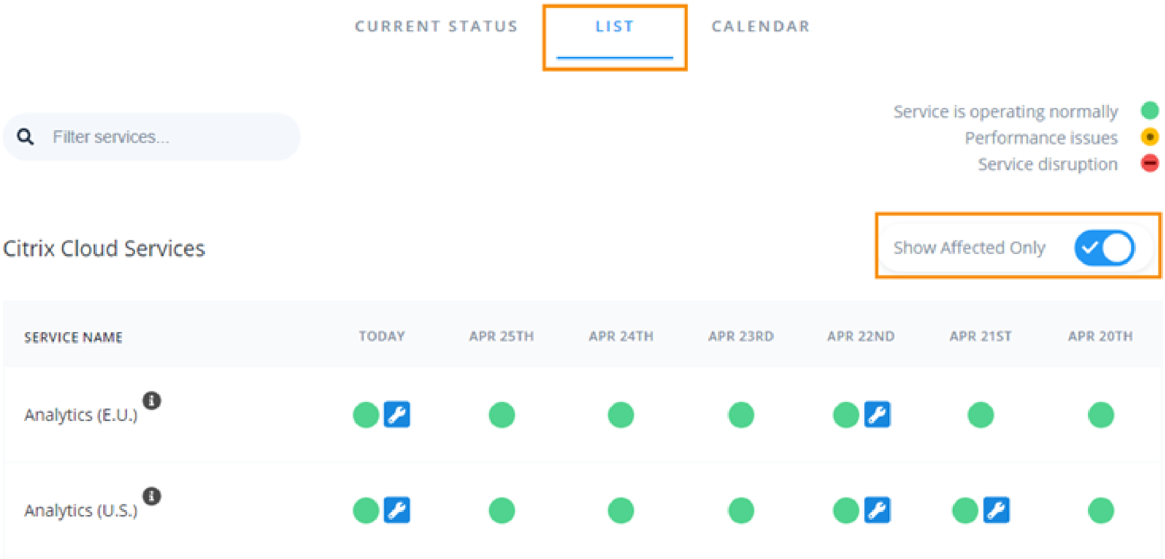


🟢 Service is operating normally 🟡 Performance issues 🔴 Service disruption ⚫ N/A

Citrix Cloud Services

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

Select **List** to display the health status of all Citrix Cloud services and platform components for the last seven days. Select **Show Affected Only** to display only the services that have had maintenance or health events in the last seven days.



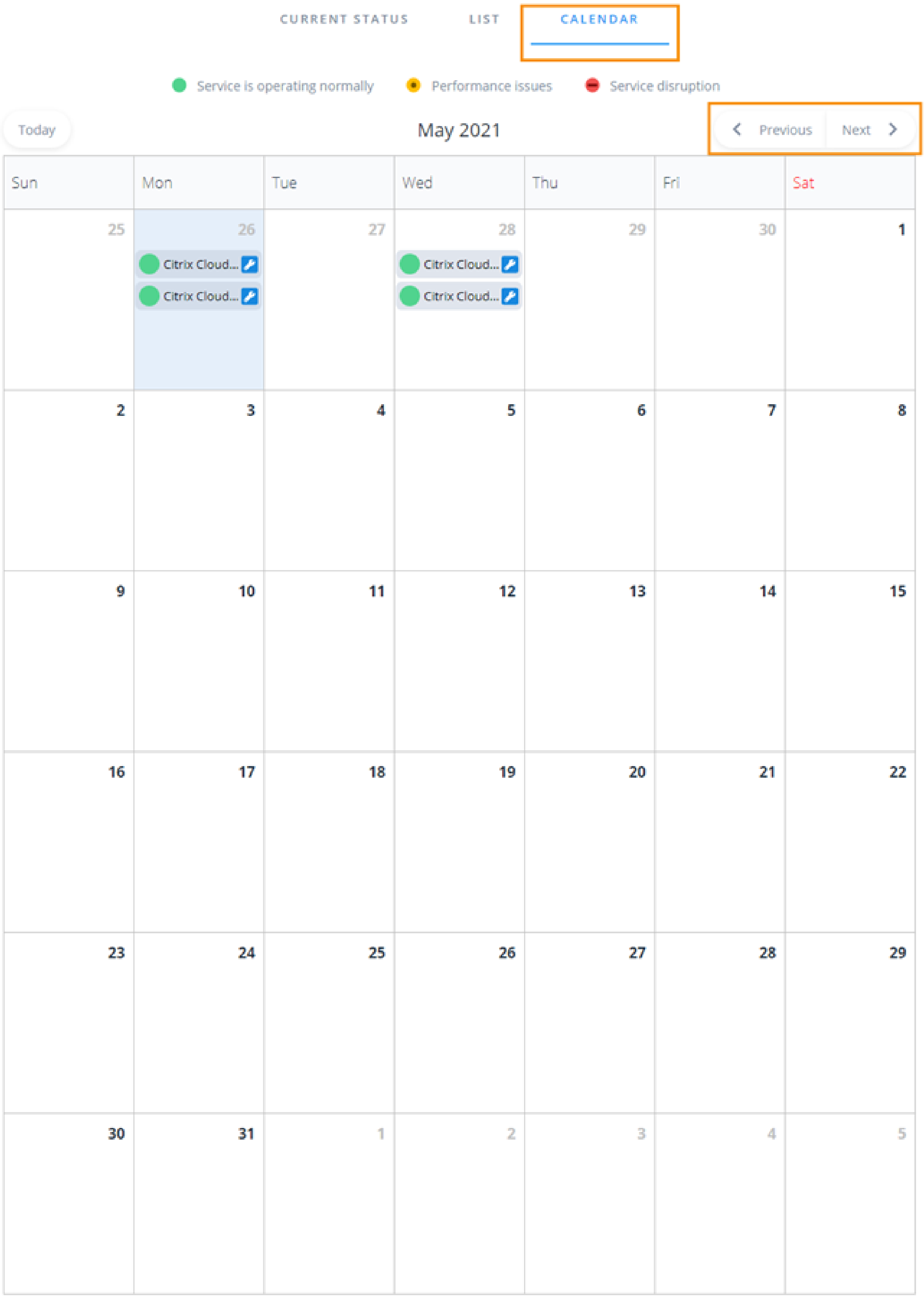
Service is operating normally 🟢
Performance issues 🟡
Service disruption 🔴

Citrix Cloud Services

Show Affected Only ✓

SERVICE NAME	TODAY	APR 25TH	APR 24TH	APR 23RD	APR 22ND	APR 21ST	APR 20TH
Analytics (E.U.) ℹ	🟢 🔧	🟢	🟢	🟢	🟢 🔧	🟢	🟢
Analytics (U.S.) ℹ	🟢 🔧	🟢	🟢	🟢	🟢 🔧	🟢 🔧	🟢

Select **Calendar** to display a calendar view of service maintenance windows. Select **Next** or **Previous** to scroll through the scheduled maintenance events for each month.



● Service is operating normally ● Performance issues ● Service disruption

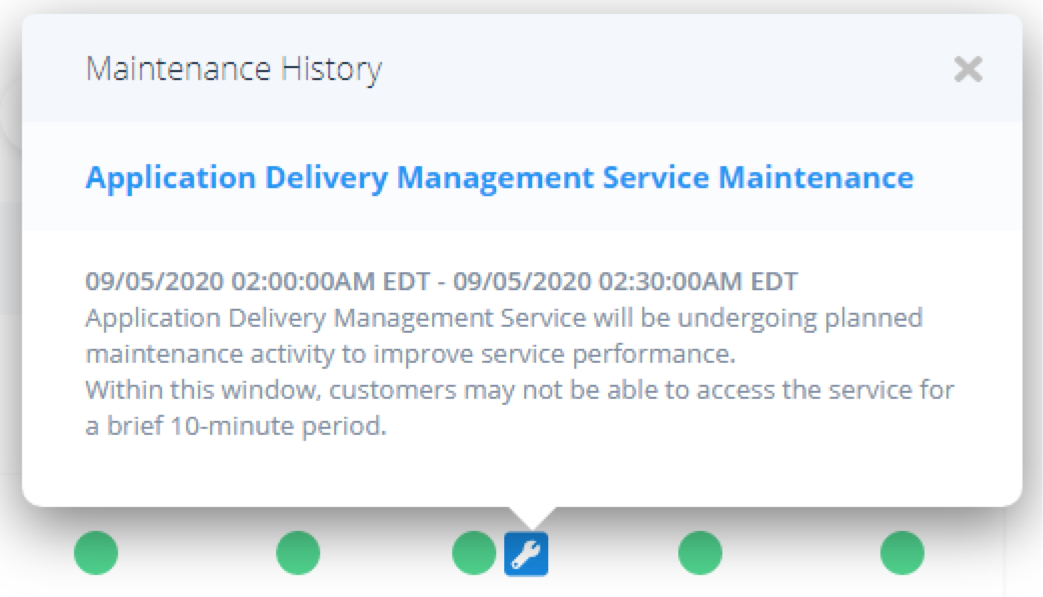
May 2021

Sun	Mon	Tue	Wed	Thu	Fri	Sat
25	26 ● Citrix Cloud... ● Citrix Cloud...	27	28 ● Citrix Cloud... ● Citrix Cloud...	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

View service incident details

To view more detailed information about the service health incident for an affected service:

- From the List view, click the icon next to the service indicator to view more detailed information about the service health incident.

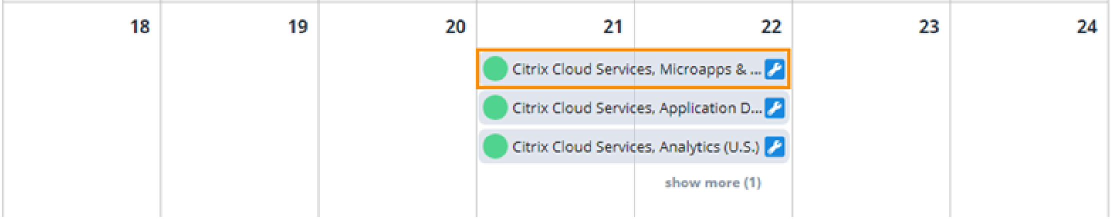


Maintenance History

Application Delivery Management Service Maintenance

09/05/2020 02:00:00AM EDT - 09/05/2020 02:30:00AM EDT
Application Delivery Management Service will be undergoing planned maintenance activity to improve service performance.
Within this window, customers may not be able to access the service for a brief 10-minute period.

- From the Calendar view, click the service entry to view the status page for the scheduled maintenance window.

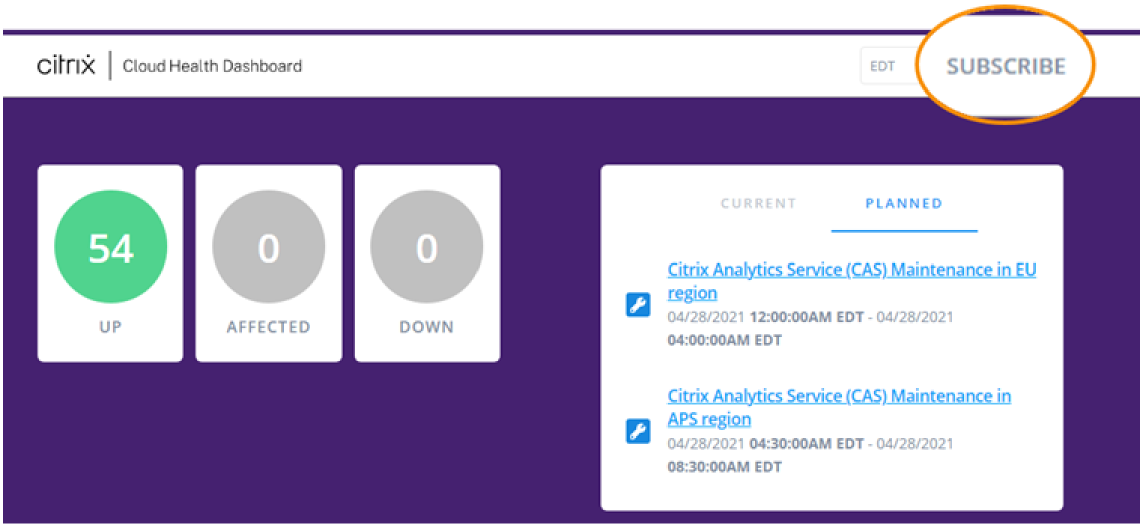


18
19
20
21
22
23
24
Citrix Cloud Services, Microapps & ...
Citrix Cloud Services, Application D...
Citrix Cloud Services, Analytics (U.S.)
show more (1)

Subscribe to notifications

You can receive notifications about service health events using the following methods:

- Select **Subscribe** in the upper-right of the dashboard and select the notification method you want to use. You can select from several methods, including email and phone.



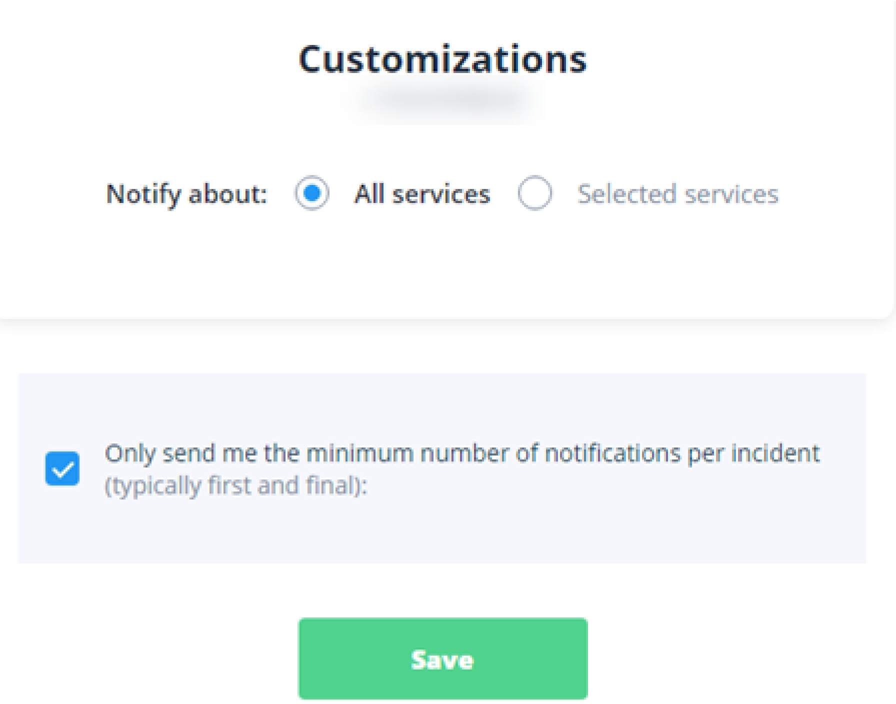
Citrix Analytics Service (CAS) Maintenance in EU region
04/28/2021 12:00:00AM EDT - 04/28/2021 04:00:00AM EDT

Citrix Analytics Service (CAS) Maintenance in APS region
04/28/2021 04:30:00AM EDT - 04/28/2021 08:30:00AM EDT

- Enter the following URLs in your RSS reader to subscribe to the Citrix Cloud Health RSS feed:
  - To receive service incident and maintenance notifications in a single feed, subscribe to `https://status.cloud.com/?format=atom`.
  - To receive only service incident notifications, subscribe to `https://status.cloud.com/atom/incidents`.
  - To receive only maintenance notifications, subscribe to `https://status.cloud.com/atom/maintenances`.

To subscribe to all service notifications in all geographical regions:

1. Select **Subscribe** in the upper-right corner of the dashboard and then select the notification method you want to use.
2. Enter the contact details or URL for the chosen subscription method. Select **Next**.
3. From the **Customizations** page, select **All services** to receive notifications for all services in all geographical regions.
4. To receive only the first and last notifications for each incident, select **Only send me the minimum number of notifications per incident**.
5. Click **Save**.



Customizations

Notify about: ● All services ○ Selected services

☑ Only send me the minimum number of notifications per incident (typically first and final):

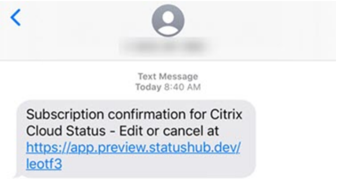
To subscribe to notifications for specific services or regions:

1. Select **Subscribe** in the upper-right corner of the dashboard and then select the notification method you want to use.
2. Enter the contact details or URL for the chosen subscription method. Select **Next**.
3. From the **Customizations** page, select **Selected services**. A multi-page list appears that displays every service in every supported region.
4. Select the services in the geographical regions that you want to be notified about. To be notified about all services in a geographical region, select **Aggregate by groups** and then select the region.
5. To receive only the first and last notifications for each incident, select **Only send me the minimum number of notifications per incident**.
6. Click **Save**.

Unsubscribe from notifications

Depending on the subscription method, links to unsubscribe or change your subscription are included in the confirmation message you receive (for example, when subscribing to phone notifications) or in each notification message (for example, when you subscribe to email notifications). For example:

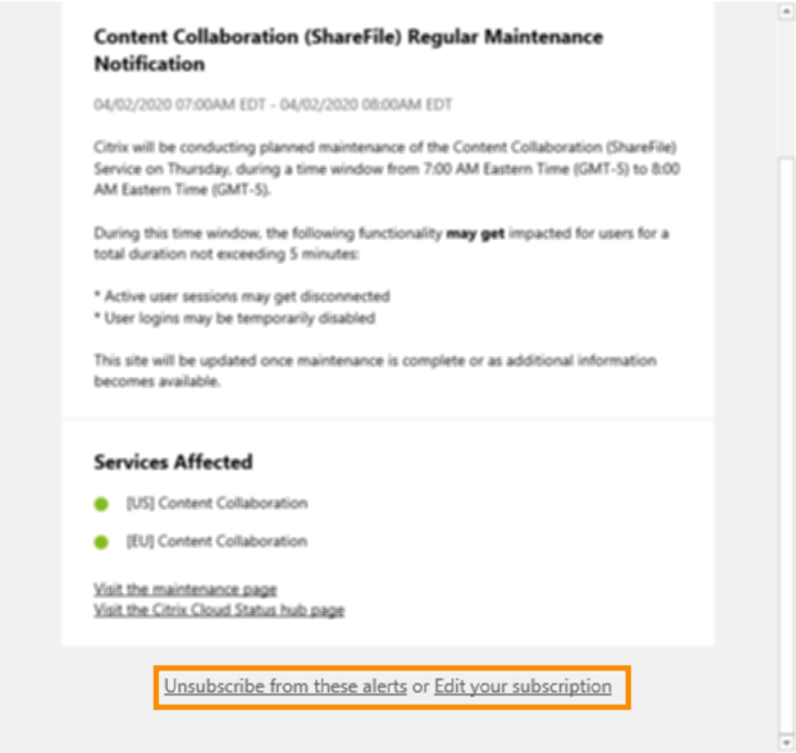
- Phone notification with subscription options:



Text Message
Today 8:40 AM

Subscription confirmation for Citrix Cloud Status - Edit or cancel at https://app.preview.statushub.dev/leotf3

- Notification email with subscription options



Content Collaboration (ShareFile) Regular Maintenance Notification

04/02/2020 07:00AM EDT - 04/02/2020 08:00AM EDT

Citrix will be conducting planned maintenance of the Content Collaboration (ShareFile) Service on Thursday, during a time window from 7:00 AM Eastern Time (GMT-5) to 8:00 AM Eastern Time (GMT-5).

During this time window, the following functionality **may get** impacted for users for a total duration not exceeding 5 minutes:

* Active user sessions may get disconnected
* User logins may be temporarily disabled

This site will be updated once maintenance is complete or as additional information becomes available.

Services Affected

● [US] Content Collaboration

● [EU] Content Collaboration

Visit the maintenance page
Visit the Citrix Cloud Status hub page

Unsubscribe from these alerts or Edit your subscription

To unsubscribe from all notifications and remove all subscription methods:

1. Locate your subscription confirmation message or an existing notification and select the link to unsubscribe. Some subscription methods might provide a single link to edit or cancel your subscription.
2. Depending on your subscription method, use one of the following options on the **Edit Subscriptions** page:
    - Select **Remove all subscriptions**.
    - Select **Unsubscribe**. From the **Unsubscribe methods** page, select **Remove all subscriptions**.

To unsubscribe from all notifications for a specific subscription method:

1. Locate your subscription confirmation message or an existing notification and select the link to unsubscribe. Some subscription methods might provide a single link to edit or cancel your subscription.
2. Depending on your subscription method, use one of the following options on the **Edit Subscriptions** page:

- Select the subscription method you want to remove. Your subscription is removed immediately.
- Select **Unsubscribe**. From the **Unsubscribe methods** page, select the subscription method you want to remove. Your subscription is removed immediately.

Change service notifications

1. Locate your subscription confirmation message or an existing notification and select the link to edit your subscription. Some subscription methods might provide a single link to edit or cancel your subscription.
2. From the **Edit Subscriptions page**, select the subscription method that you want to manage.
3. On the **Customizations** page, select the services you want to be notified about or clear the services you no longer want notifications for, as needed.
4. Select **Save**.

Citrix Cloud support forums

On the Citrix Cloud support forums you can get help, provide feedback and improvement suggestions, view conversations from other users, or start your own topics.

Citrix support staff members track these forums and are ready to answer your questions. Other Citrix Cloud community members can also offer help or join the discussion.

You don't need to sign in to read forum topics. However, you must sign in to post or reply to a topic. To sign in, use your existing Citrix account credentials, or use the email address and password you provided when you created your Citrix Cloud account. To create a new Citrix account, go to Create or request an account.

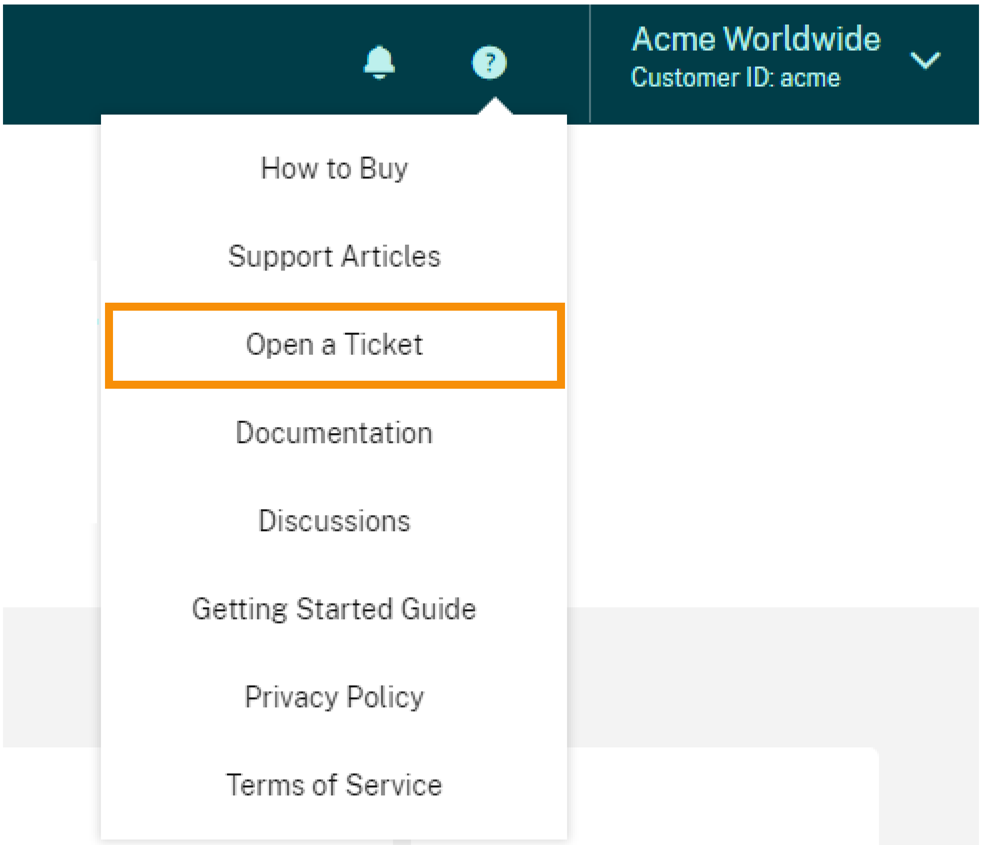
Technical Support

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

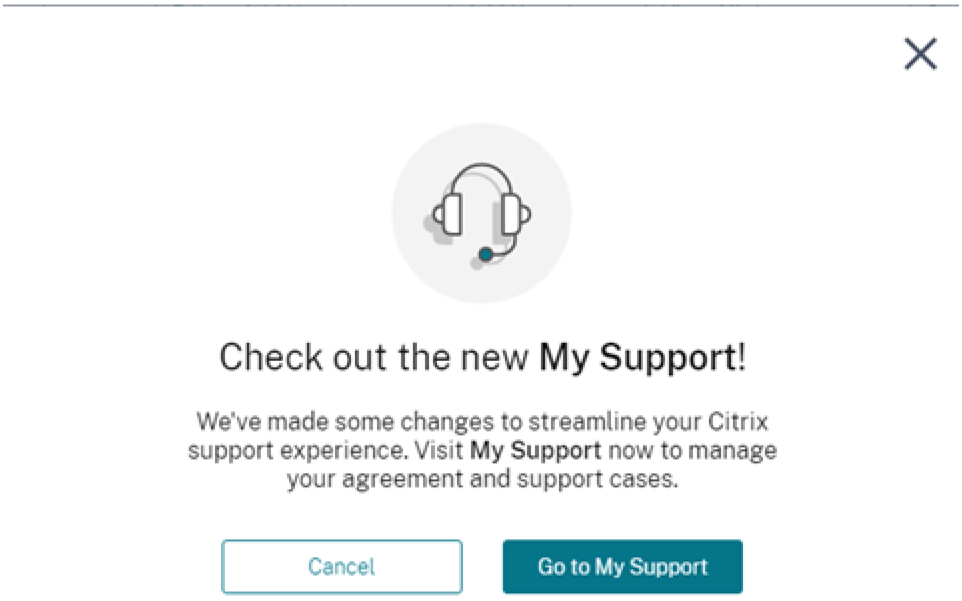
To access the Support Knowledge Center, visit https://support.citrix.com/case/manage.

Alternatively, in Citrix Cloud:

1. Select the **Help** icon near the top-right of the screen

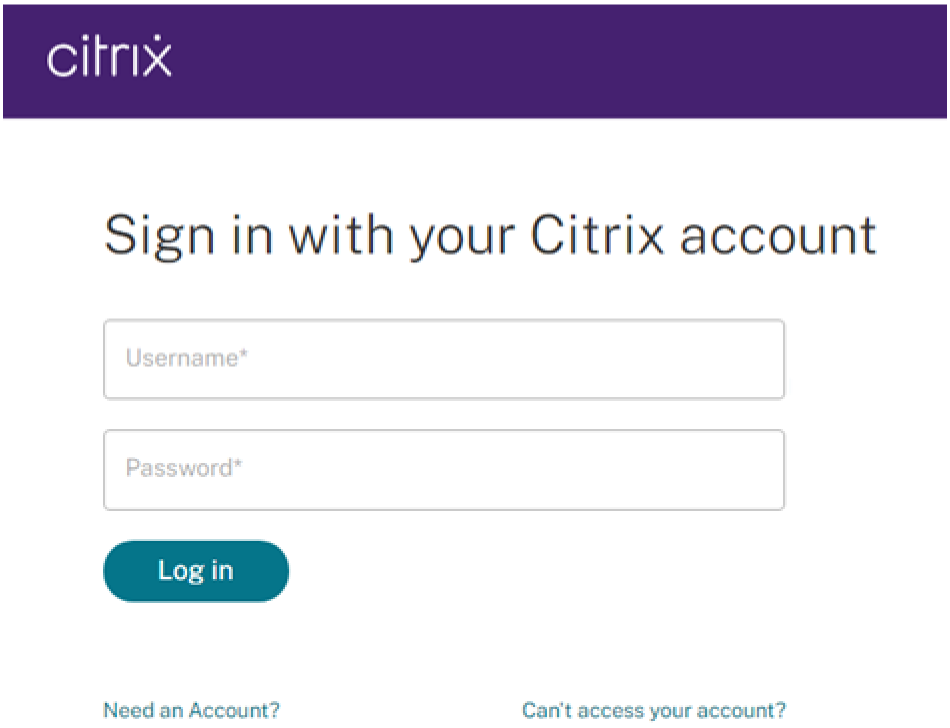


2. Select **Open a Ticket > Go to My Support**


Check out the new **My Support!**

We've made some changes to streamline your Citrix support experience. Visit **My Support** now to manage your agreement and support cases.

3. Sign in with your Citrix account



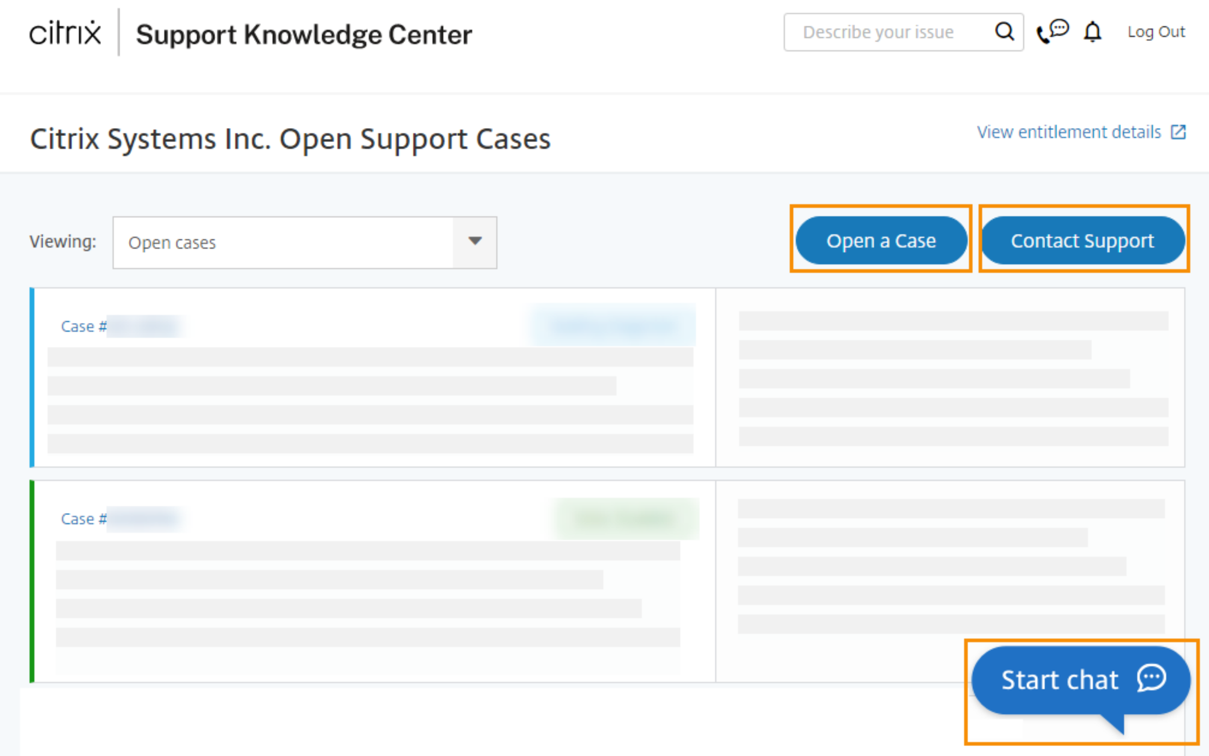
Sign in with your Citrix account

Username*

Password*

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

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



Support articles and documentation

Citrix provides substantial product and support content to help you get the most out of Citrix Cloud and resolve issues you might experience with Citrix products.

Education resources

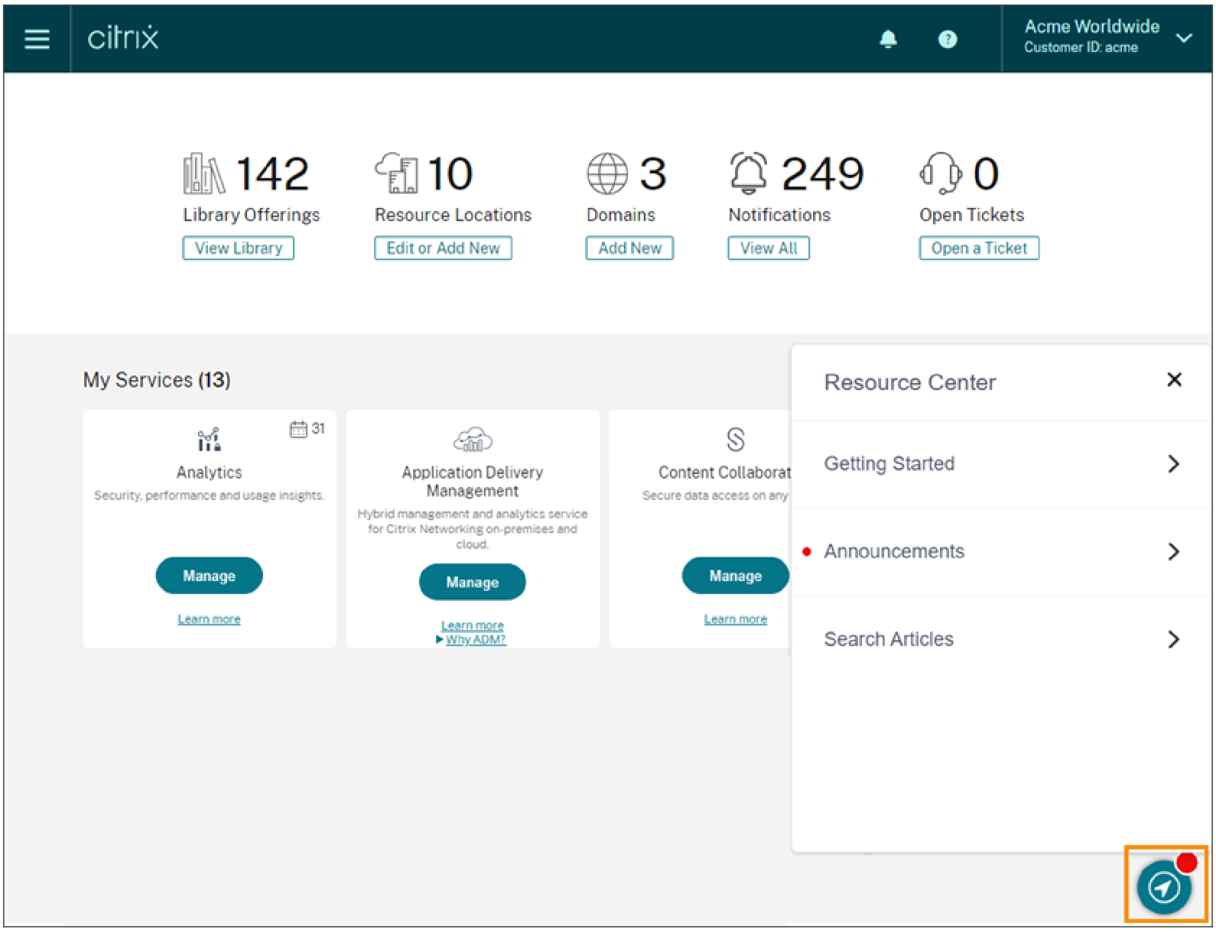
The Citrix Cloud Learning Series portal offers education modules to get you up and running with Citrix Cloud and its services. You can view all of the modules sequentially, from overviews through planning and building services. Start your cloud journey with the following courses:

- Fundamentals of Citrix Cloud
- Intro to Citrix Identity and Authentication
- Moving from StoreFront to Workspace

The Citrix Education video library offers online video lessons that walk you through key deployment tasks and troubleshooting the components that you use with Citrix Cloud services. Learn more about tasks like installing Cloud Connectors and registering VDAs, as well as troubleshooting these components.

Citrix Cloud Resource Center

The Citrix Cloud Resource Center can help you get started with Citrix Cloud, learn more about features, and search to resolve issues. Click the blue compass icon at the bottom right of the page. This feature is available for the Citrix Cloud platform and Virtual Apps and Desktops and Application Delivery Management services.



- **Get Started**: Provides a brief guided walkthrough of key tasks specific to the service you're currently working with. You can also find links to training and onboarding resources to help you learn more about service capabilities and set up your end-users for success.
- **Announcements**: Provides notifications of newly released features and links to essential Citrix communications. Select a feature notification to receive a brief guided walkthrough of the feature.
- **Search Articles**: Provides a list of product documentation and Knowledge Center articles for common tasks and helps you find more articles, without leaving Citrix Cloud. Enter a search query in the **How do I…** box for a filtered list of articles based on the service you're working with. In general, support articles appear first in the list, followed by product documentation articles.

Citrix Tech Zone

Citrix Tech Zone contains a information to help you learn more about Citrix Cloud and other Citrix products. Here, you can find reference architectures, diagrams, videos, and technical papers that provide insights for designing, building, and deploying Citrix technologies.

Third Party Notifications

May 25, 2021

- Citrix Cloud Third Party Notifications (PDF)
- Citrix Analytics Service Third Party Notifications (PDF)
- Virtual Apps and Desktops Third Party Notifications (PDF)
- Virtual Apps and Desktops Standard for Azure Third Party Notifications (PDF)
- Citrix ShareFile Sync for Mac Third Party Notices (PDF)
- Citrix ShareFile Sync for Windows Third Party Notices (PDF)
- Secure Browser Service (PDF)
- Citrix Endpoint Management Third Party Notifications (PDF)
- Citrix Cloud Linux VDA Image Service Third Party Notices (PDF)
- Connector Appliance for Cloud Services Third Party Notices (PDF)
- Citrix Microapps Service Third Party Notices (PDF)

Sign up for Citrix Cloud

September 24, 2021

This article walks you through the process of signing up for Citrix Cloud and performing the required tasks for onboarding your account successfully.

> **Tip:**
>
> The "Getting Started with Citrix Cloud" education module, included in the Fundamentals of Citrix Cloud course, provides short videos that walk you through the tasks described in this article. The full course also gives you a firm foundation for understanding Citrix Cloud, its benefits for your organization, and important use cases that Citrix Cloud services address.

What is a Citrix account?

A Citrix account, also known as a Citrix.com account or My Citrix account, enables you to manage access to the licenses you have purchased. Your Citrix account uses an organization ID (OrgID) as a unique identifier. You can access your Citrix account by logging in at https://www.citrix.com with a username (also known as a web login) or your email address, if one is linked to your account.

> **Important:**
>
> A username maps to a single, unique Citrix account, but an email address can map to multiple Citrix accounts.

What is an OrgID?

An OrgID is the unique identifier assigned to your Citrix account. Your OrgID is associated with a physical site address, typically your company's business address. So, companies 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 a single company to have multiple OrgIDs.

Citrix routinely cleans up certain OrgIDs, merging duplicates in some cases. If your company has OrgIDs that you want to merge with a valid and active OrgID, you can contact Citrix Customer Support with the OrgIDs you want merged.

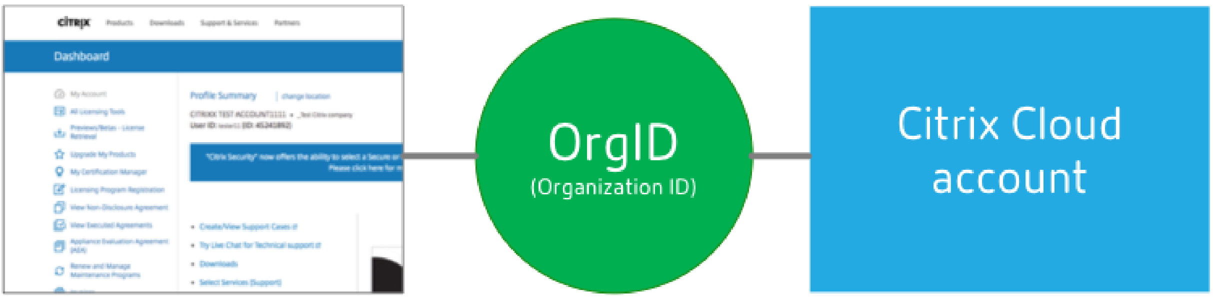
> **Note:**
>
> Companies have already set up OrgIDs based on how they want to manage their assets, so if you don't know what OrgID you need to use or how many OrgIDs you have, contact the IT department or Citrix administrator in your company. If you need help, Citrix Customer Support can also help you locate an OrgID. You can contact Citrix customer support at https://www.citrix.com/contact/support.html.

What is a Citrix Cloud account?

A Citrix Cloud account enables you to use one or more Citrix Cloud services to securely deliver your apps and data. A Citrix Cloud account is also uniquely identified by an OrgID, just like your Citrix account. It's important to use the right Citrix Cloud account, based on how your organization has set up OrgIDs, so that your purchases and administrator access can continue on the same OrgIDs. For example, if a company's design department using OrgID 1234 has been using Virtual Apps and Desktops on-premises and wants to try Citrix Cloud, one of the admins of OrgID 1234 should sign up for Citrix Cloud on that OrgID using a web login or email address associated with that OrgID. So, when the company decides to purchase a Virtual Apps and Desktops subscription, the order can be placed on OrgID 1234 and the transition is smooth.

> **Important:**
>
> Users who have access to a particular Citrix account do not automatically have access to the Citrix Cloud account associated with that Citrix account's OrgID. Because Citrix Cloud access en-

> ables users to potentially impact service, it's important to control who accesses the Citrix Cloud account.



Citrix.com account. This is where you can download traditional on-premises licenses

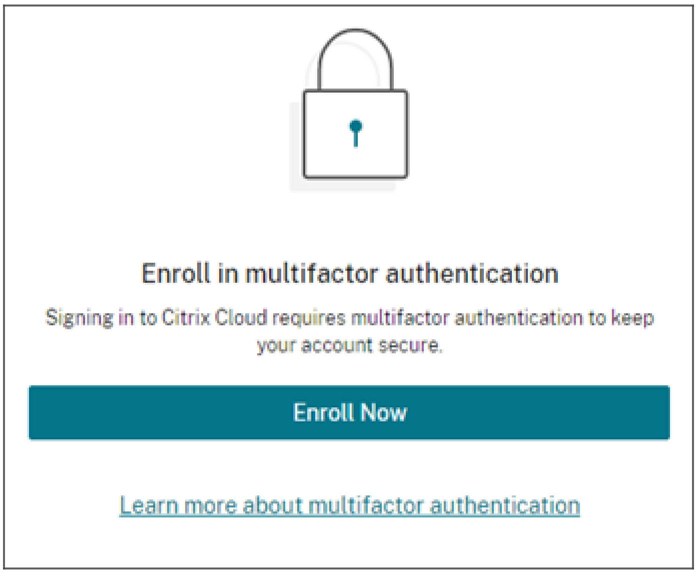
OrgID that you use to place orders against

You will need to place orders against the same OrgID for Citrix Cloud subscriptions for this account

Multifactor authentication requirements

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

If you're an existing Citrix customer, Citrix Cloud prompts you to enroll when you visit the sign-up page and enter the credentials associated with your Citrix.com account. If you're new to Citrix, Citrix Cloud prompts you to enroll after you create a Citrix account during the sign-up process.



Enroll in multifactor authentication

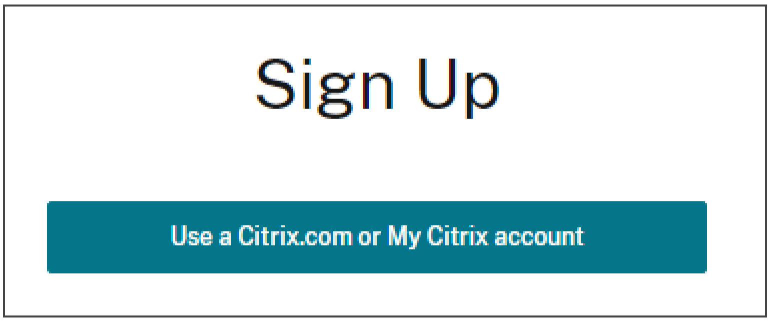
Signing in to Citrix Cloud requires multifactor authentication to keep your account secure.

Step 1: Visit the sign-up page

Using a web browser, visit https://onboarding.cloud.com.

If you're an existing Citrix customer or have a Citrix.com or My Citrix account

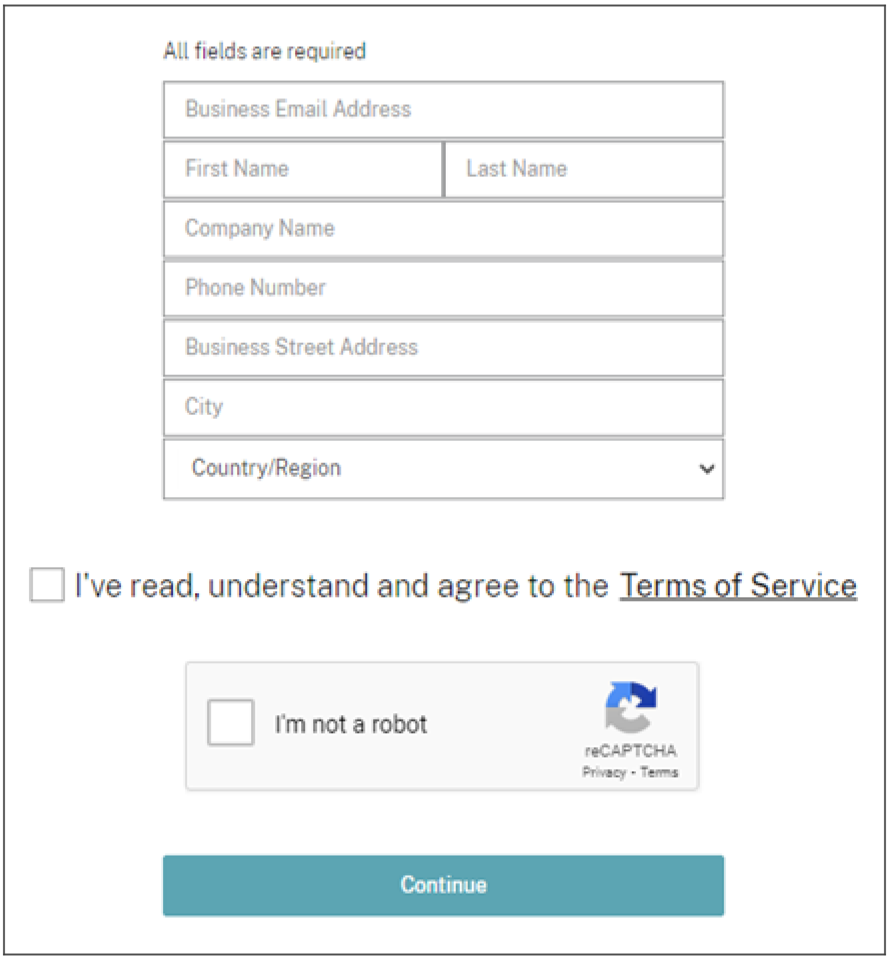
1. Select **Use a Citrix.com or My Citrix account**.



2. Enter your username and password (also known as your web login) or the email address and password associated with your Citrix.com account.
3. When prompted to enroll in multifactor authentication, select **Enroll now**.
4. Complete the enrollment process as described in Step 5: Enroll in multifactor authentication in this article.

If you are new to Citrix and Citrix Cloud

Complete the form fields and select **Continue**.



All fields are required

Business Email Address

First Name

Last Name

Company Name

Phone Number

Business Street Address

City

Country/Region

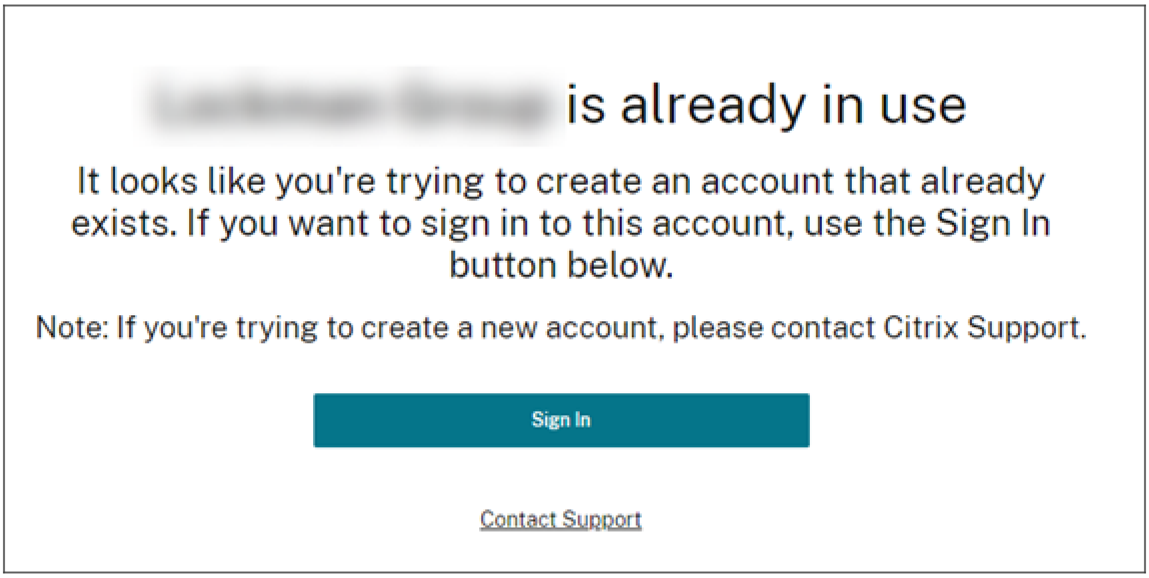
□ I've read, understand and agree to the Terms of Service

□ I'm not a robot

Continue

Remember to use your business email address and business address. Using a personal email address or personal address could result in delays when requesting trials.

What happens if the account is already in use?



[redacted] is already in use

It looks like you're trying to create an account that already exists. If you want to sign in to this account, use the Sign In button below.

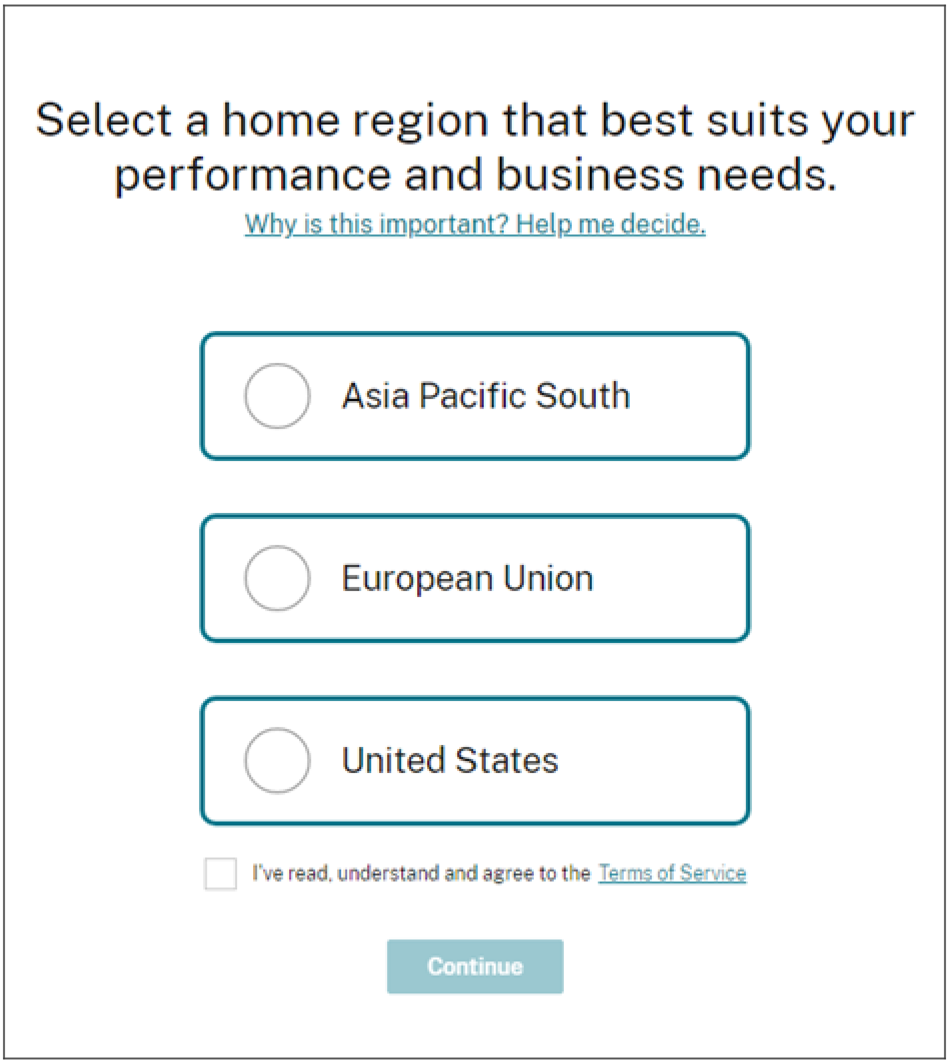
Note: If you're trying to create a new account, please contact Citrix Support.

If you see this message, it means that another administrator from your Citrix account has already created the Citrix Cloud account.

Since a Citrix Cloud account allows administrators much greater control on the service, we expect that the first administrator who creates the Citrix Cloud account has to explicitly give access to another administrator, even if the other administrator is already a member of the Citrix account.

By selecting **Request Approval**, all existing administrators on the account are notified of your request. If the existing administrators are no longer with your organization, please contact Citrix Support.

Step 2: Pick your Citrix Cloud region



Select a home region that best suits your performance and business needs.

Why is this important? Help me decide.

○ Asia Pacific South

○ European Union

○ United States

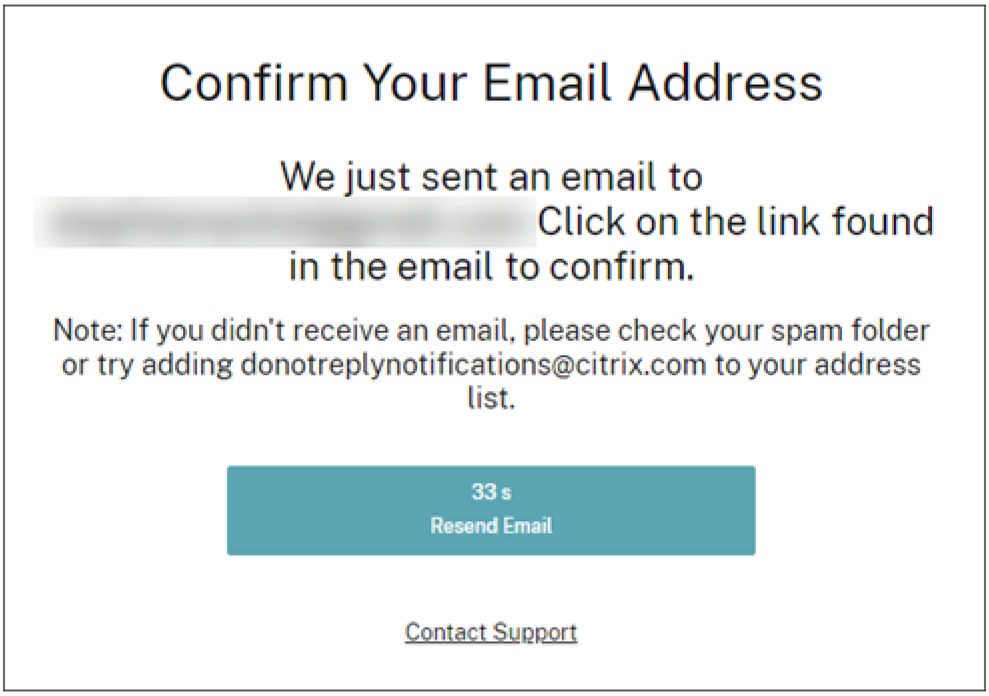
□ I've read, understand and agree to the Terms of Service

A Citrix Cloud region is a geographical boundary within which Citrix operates, stores, and replicates services and data for delivery of Citrix Cloud services. Citrix may use multiple public or private clouds located in one or more countries within the region, including states and provinces, to provide services. For more information about Citrix Cloud regions, refer to Geographical Considerations.

> **Important:**
>
> After you select a region, your selection can't be undone or changed.

Step 3: Verify your email address

If you have not verified your email address, you might be asked to verify it.

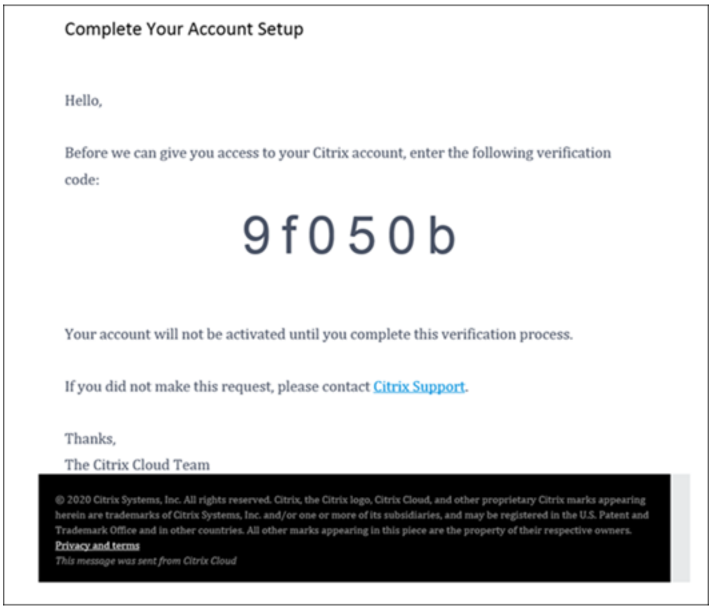


Confirm Your Email Address

We just sent an email to [redacted] Click on the link found in the email to confirm.

Note: If you didn't receive an email, please check your spam folder or try adding donotreplynotifications@citrix.com to your address list.

Citrix Cloud then sends you a verification email. Here's an example of what you'll receive:



Complete Your Account Setup

Hello,

Before we can give you access to your Citrix account, enter the following verification code:

9f050b

Your account will not be activated until you complete this verification process.

If you did not make this request, please contact Citrix Support.

Thanks,
The Citrix Cloud Team

© 2020 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, Citrix Cloud, and other proprietary Citrix marks appearing herein are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries. All other marks appearing in this piece are the property of their respective owners.
Privacy and terms
This message was sent from Citrix Cloud

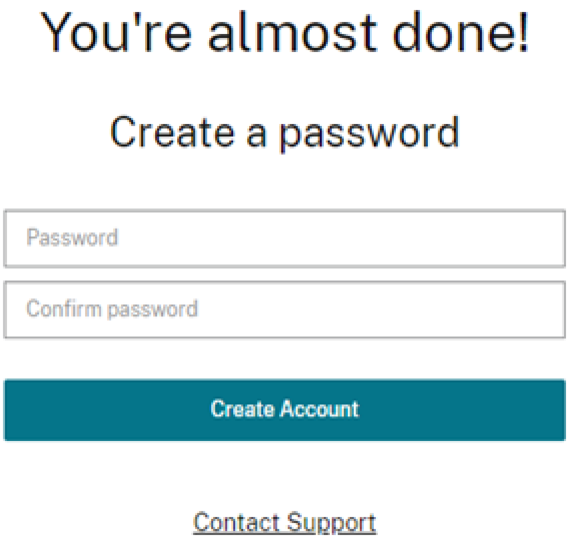
After you receive the verification email and confirm your email address, your Citrix Cloud account is active.

Step 4: Pick a password

> **Note:**
>
> Citrix Cloud prompts you to pick a password only if you are creating a Citrix account for the first

> time.

Type and confirm your Citrix Cloud password to finish creating your account.



You're almost done!

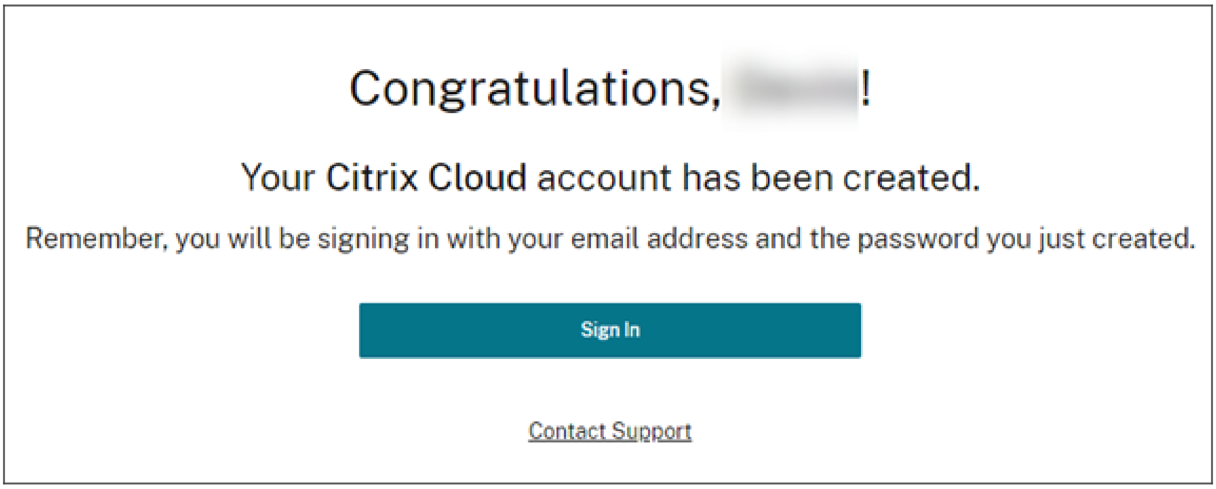
Create a password

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

- At least 8 characters long
- At least one upper-case letter
- At least one number
- One symbol: ! @ # $ % ^ * ? + = -

Valid passwords cannot include dictionary words. If, after picking your password, Citrix determines your password isn't sufficiently complex or is listed in a known database of compromised passwords, Citrix Cloud might prompt you to change it the next time you sign in to Citrix Cloud. For more information, see Changing your password.

After your account is created, you can sign in to Citrix Cloud.



Congratulations, [redacted]!

Your Citrix Cloud account has been created.

Remember, you will be signing in with your email address and the password you just created.

Step 5: Enroll in multifactor authentication

To keep your administrator account safe and secure, Citrix Cloud requires you to use multifactor authentication when you sign in. Enrolling in multifactor authentication prevents unauthorized access to your administrator account and only requires a device, such as a computer or mobile device, with an authenticator app installed that follows the Time-Based One-Time Password standard, such as Citrix SSO.

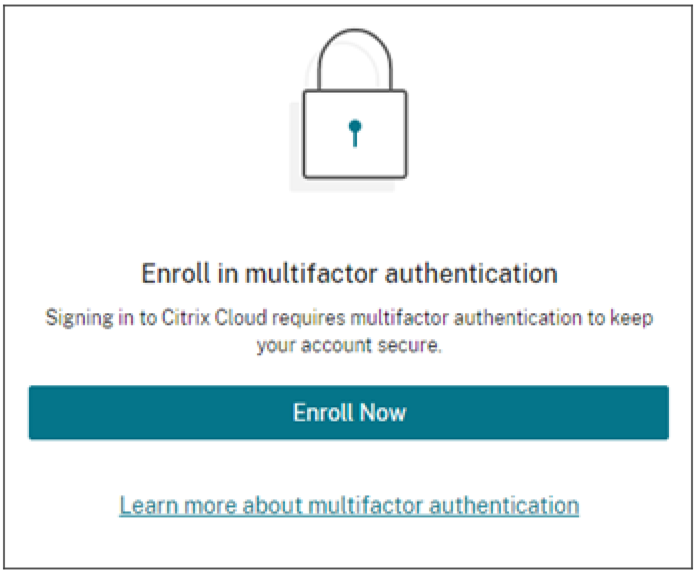
If you're not enrolled in multifactor authentication, Citrix Cloud prompts you to enroll when you sign in.

During enrollment, Citrix Cloud presents a QR code and a key. Depending on your authenticator app, you can either scan the QR code or enter the key to register your device. For a smooth enrollment process, Citrix recommends downloading and installing this app on your device beforehand. Citrix Cloud also generates one-time use backup codes that you can use to access your account in the event you lose your device or can't use your authenticator app.

> **Notes:**
>
> - When signing in to Citrix Cloud, verify that you are viewing the Citrix Cloud sign-in page at https://accounts.cloud.com. If you sign in to Citrix Cloud using a different URL (such as `https://accounts-internal.cloud.com`), enrollment in multifactor authentication fails.
> - Only administrators under the Citrix identity provider can enroll in multifactor authentication through Citrix Cloud. If you use Azure AD to manage Citrix Cloud administrators, you can configure multifactor authentication using the Azure portal. For more information, see Configure Azure Multi-Factor Authentication settings on the Microsoft web site.
> - After you enroll, multifactor authentication is used for all customer organizations that you belong to in Citrix Cloud. 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 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

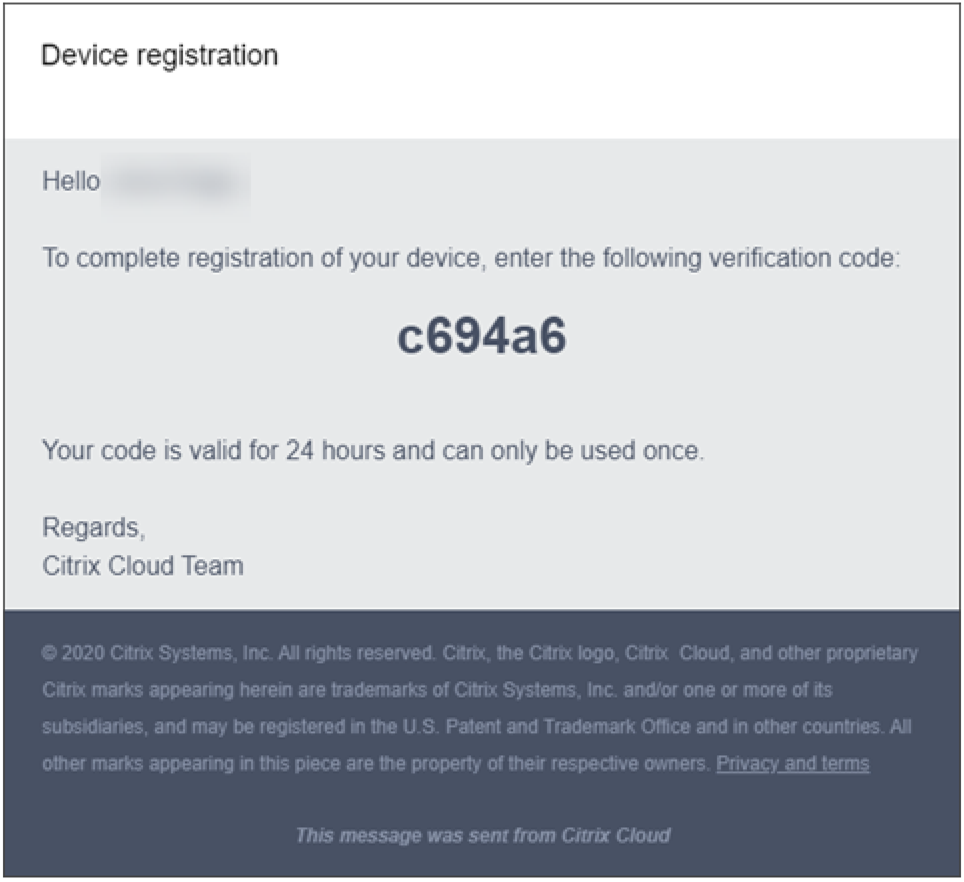
1. Go to https://citrix.cloud.com and verify that the URL redirects to https://accounts.cloud.com. Sign in using your Citrix Cloud credentials.
2. When prompted to enroll in multifactor authentication, select **Enroll Now**.



Enroll in multifactor authentication

Signing in to Citrix Cloud requires multifactor authentication to keep your account secure.

Citrix Cloud sends you an email with a verification code.



Device registration

Hello

To complete registration of your device, enter the following verification code:

c694a6

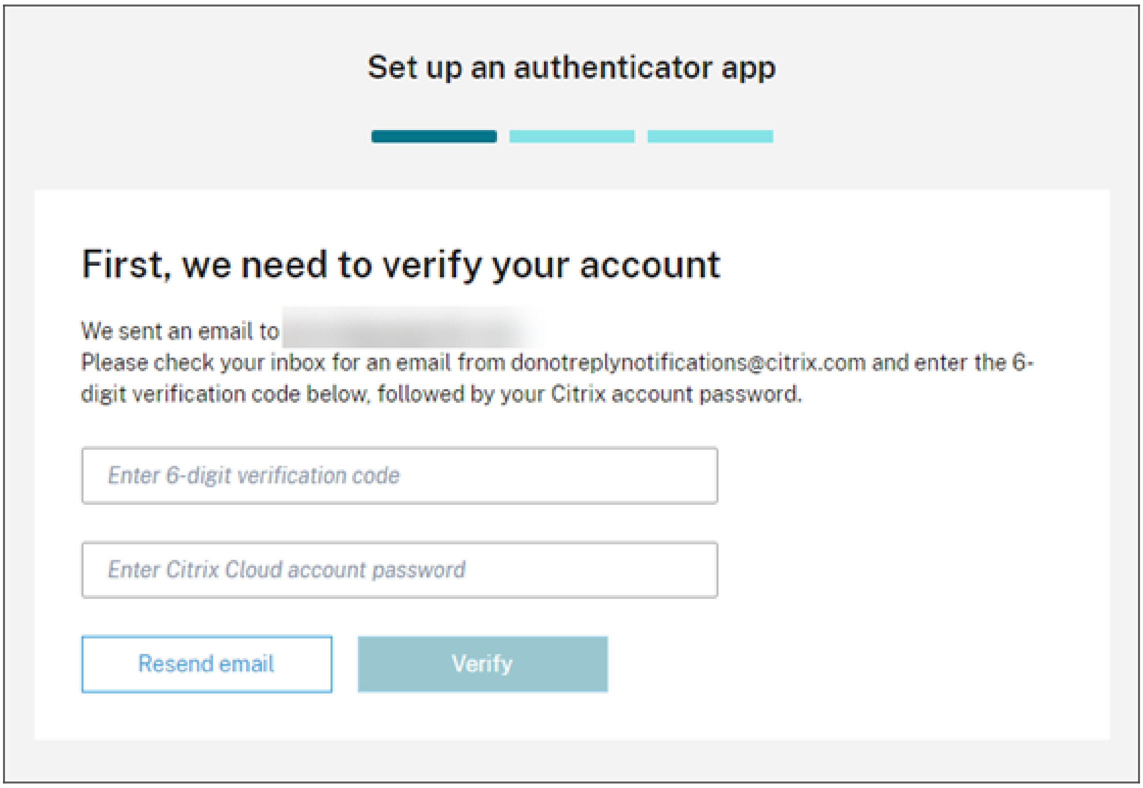
Your code is valid for 24 hours and can only be used once.

Regards,
Citrix Cloud Team

© 2020 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, Citrix Cloud, and other proprietary Citrix marks appearing herein are trademarks of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered in the U.S. Patent and Trademark Office and in other countries. All other marks appearing in this piece are the property of their respective owners. Privacy and terms

This message was sent from Citrix Cloud

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



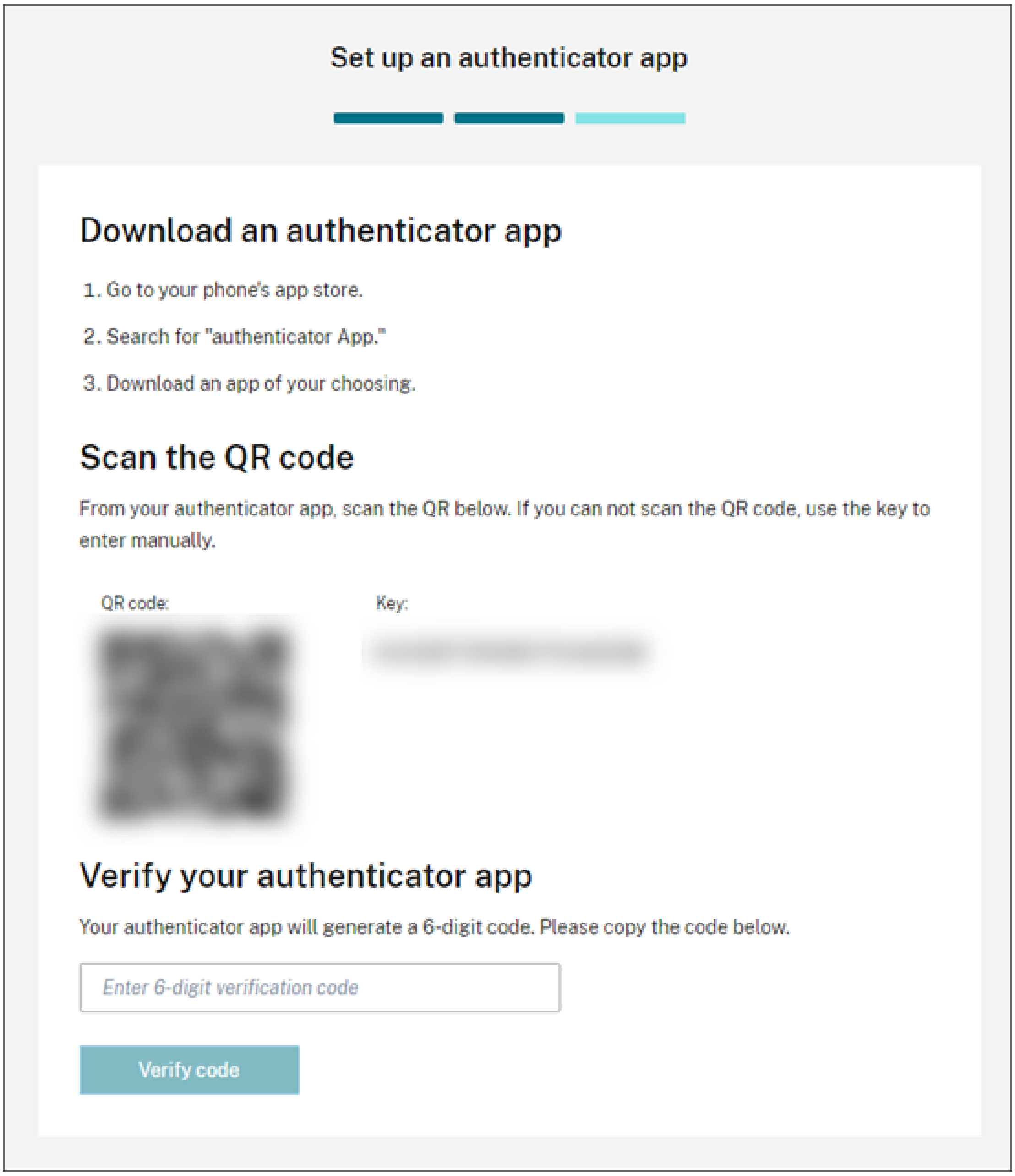
Set up an authenticator app

First, we need to verify your account

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

Enter 6-digit verification code
Enter Citrix Cloud account password
Resend email
Verify

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



Set up an authenticator app

Download an authenticator app

1. Go to your phone's app store.
2. Search for "authenticator App."
3. Download an app of your choosing.

Scan the QR code

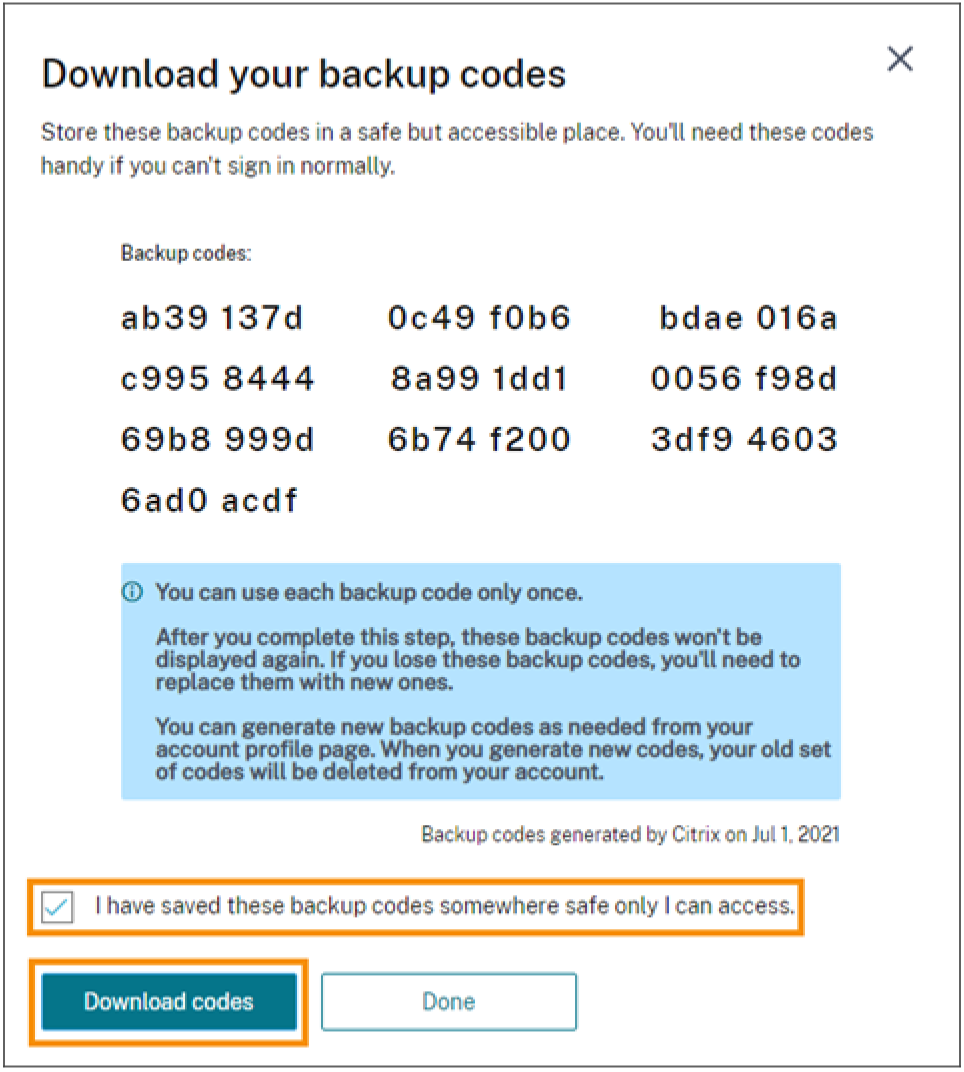
From your authenticator app, scan the QR below. If you can not scan the QR code, use the key to enter manually.

Verify your authenticator app

Your authenticator app will generate a 6-digit code. Please copy the code below.

5. Under **Verify your authenticator app**, enter the code from your authenticator app and select **Verify code**.
6. Configure the following account recovery methods in the event you lose your device or can't use your authenticator app:
   - Recovery phone (required): Select **Add a recovery phone** and enter a phone number that a Citrix Support representative can use to call you and verify your identity. Citrix Support uses this phone number only when you request help to sign in. Citrix recommends using a landline phone number.
   - Backup codes (required): Select **Generate backup codes** to create a set of one-time use

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



Download your backup codes

Store these backup codes in a safe but accessible place. You'll need these codes handy if you can't sign in normally.

Backup codes:

```
ab39 137d    0c49 f0b6    bdae 016a
c995 8444    8a99 1dd1    0056 f98d
69b8 999d    6b74 f200    3df9 4603
6ad0 acdf
```

ⓘ You can use each backup code only once.

After you complete this step, these backup codes won't be displayed again. If you lose these backup codes, you'll need to replace them with new ones.

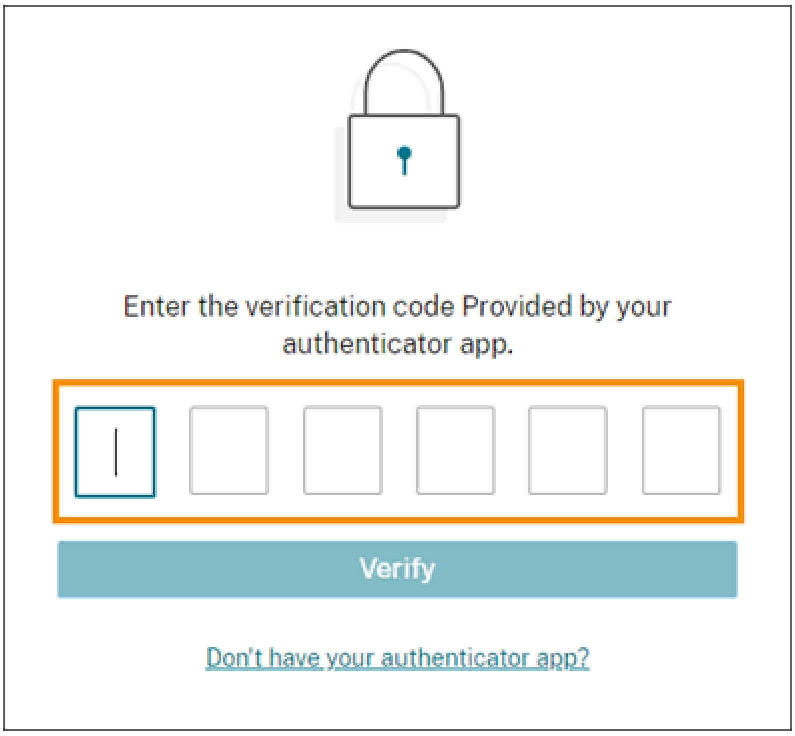
You can generate new backup codes as needed from your account profile page. When you generate new codes, your old set of codes will be deleted from your account.

Backup codes generated by Citrix on Jul 1, 2021

☑ I have saved these backup codes somewhere safe only I can access.

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

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



Enter the verification code Provided by your authenticator app.

Manage your device enrollment

If you need to register a different device, generate more backup codes, or update your recovery phone number later, you can perform these tasks from your My Profile page. For instructions, see the following articles:

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

Step 6: Verify your OrgID and invite administrators

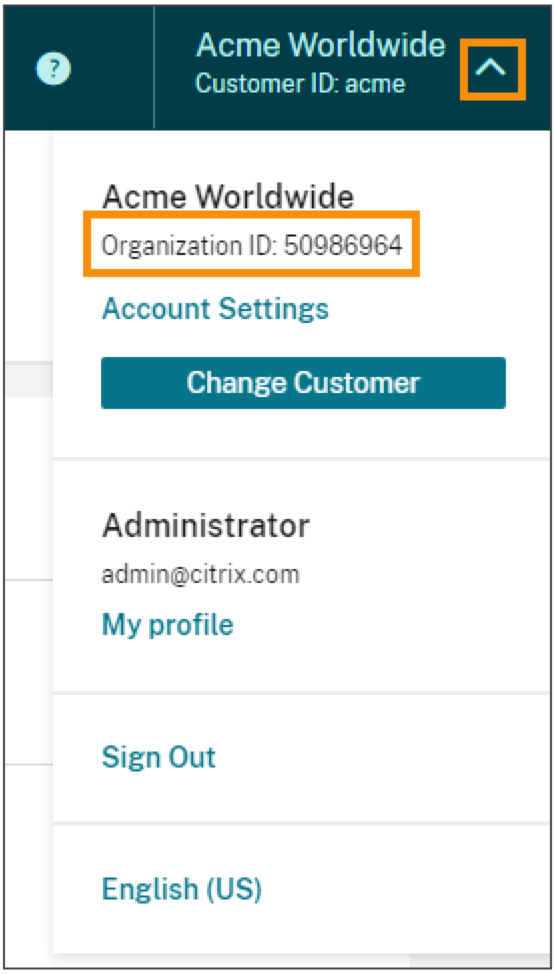
Congratulations, you set up your Citrix Cloud account! Before you start using Citrix Cloud, take a moment to verify your OrgID and invite other administrators to help you manage your Citrix Cloud account.

Verify your account OrgID

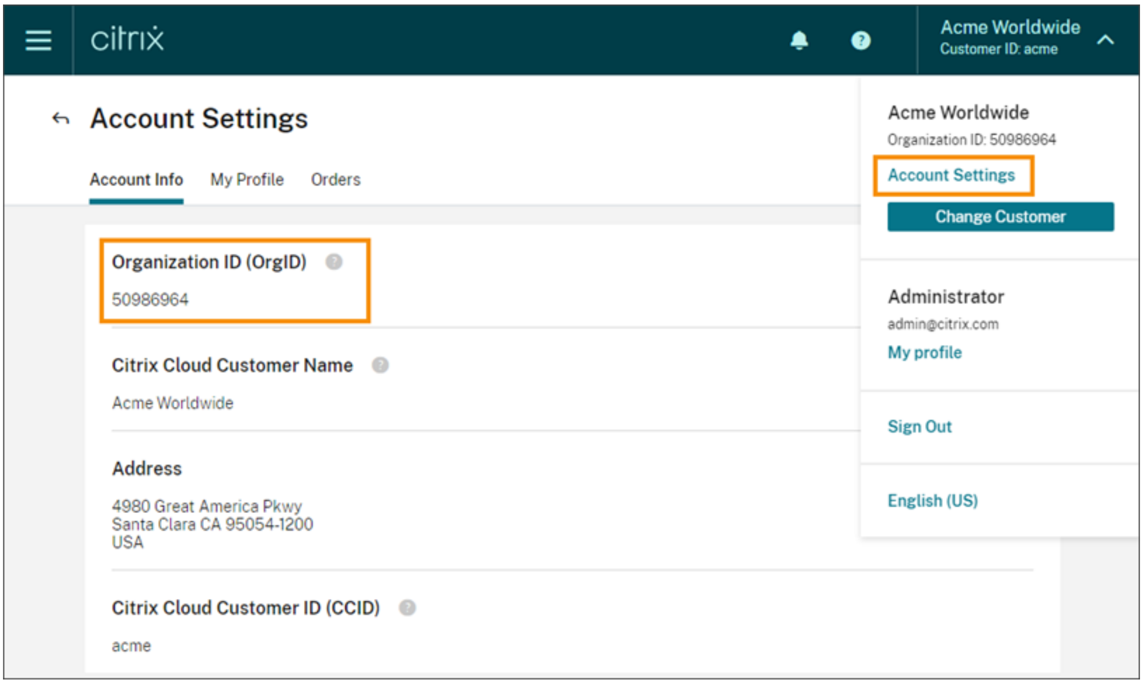
Make sure your account OrgID matches the OrgID that you use to place orders. One of the benefits of Citrix Cloud is that if you try a service (such as the Virtual Apps and Desktops service) and decide to purchase it, then all the configurations you made in the trial are retained in the purchased service, since the purchase occurs in the same account. So, making sure that the trial starts in the right OrgID saves effort when you decide to purchase.

Your OrgID appears in the following locations in the management console:

- In the menu beneath your customer name. Click on your customer name in the top-right corner to reveal the menu.



- On your **Account Settings** page. Select **Account Settings** from the customer menu.



Organization ID (OrgID)
50986964

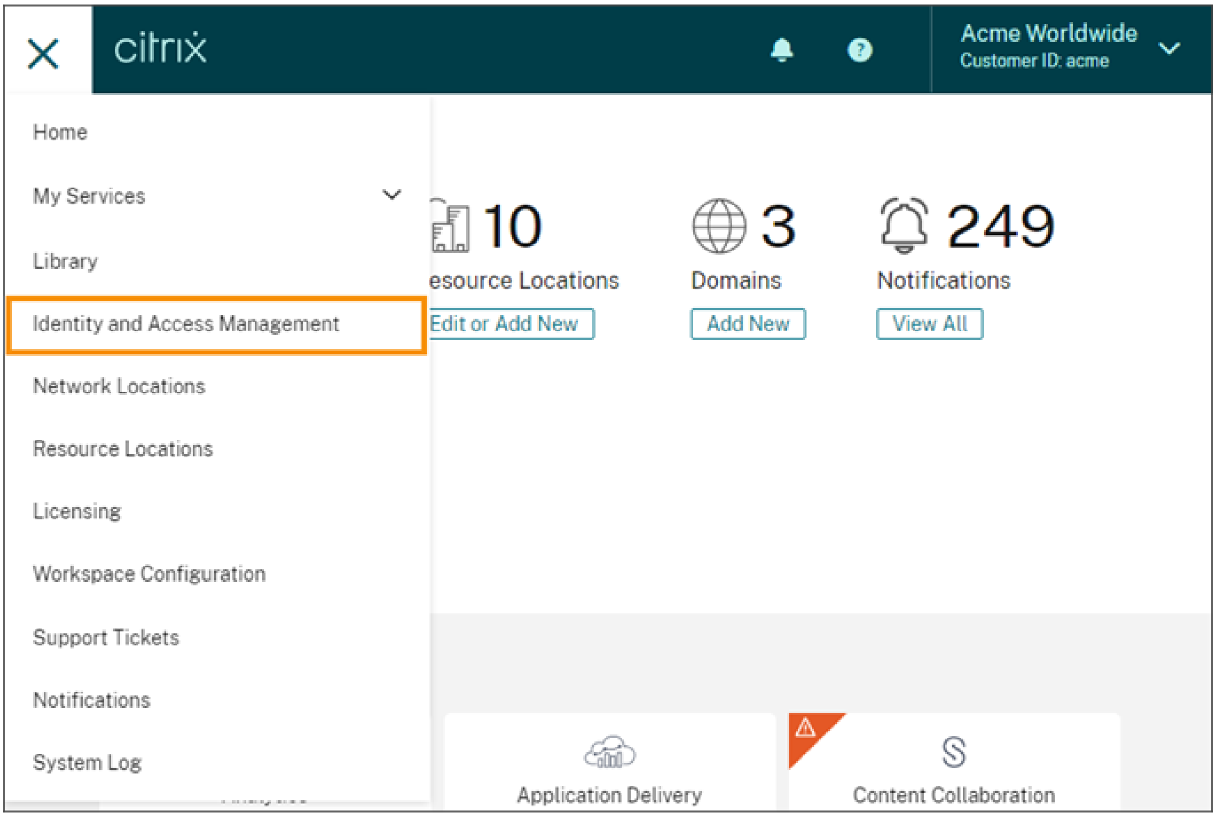
Citrix Cloud Customer Name
Acme Worldwide

Address
4980 Great America Pkwy
Santa Clara CA 95054-1200
USA

Citrix Cloud Customer ID (CCID)
acme

Invite one or more administrators

Remember, even if your other administrators have access to your Citrix account on Citrix.com, you still need to invite them to the Citrix Cloud account. To do this from the Citrix Cloud management console, click the menu button in the top left corner and select **Identity and Access Management**. For more information, see Add administrators to a Citrix Cloud account.



Step 7: Request trials for Citrix Cloud services

Trials are designed to be tested with your choice of on-premises infrastructure or public cloud, your applications, and your Microsoft Active Directory. You can set up and configure services, workspaces, and resource locations.

During your trial, if you decide that you want to purchase a subscription package, you can do so at any time. All your existing configurations are saved and available for your continued use.

To request a trial, click Request Trial for the service you would like to try. For more information, see Citrix Cloud Service Trials.

Geographical Considerations

September 22, 2021

This article discusses the commercial regions that Citrix Cloud uses and the presence of Citrix Cloud commercial services within each region.

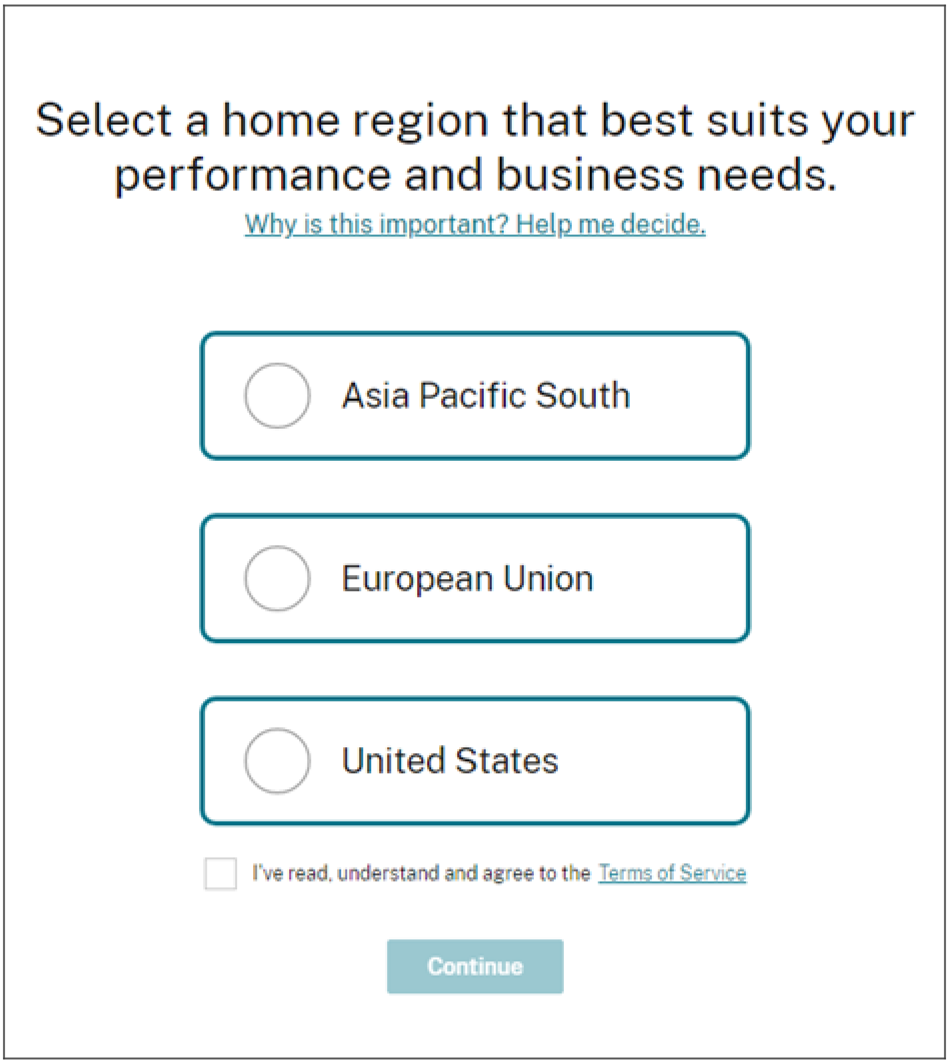
For more information about the geographical regions and service presence for Citrix's public-sector and dedicated cloud platforms, see Other cloud platforms from Citrix in this article.

Choose a region

When your organization is onboarded to Citrix Cloud and you sign in for the first time, you are asked to choose one of the following regions:

- United States
- European Union
- Asia Pacific South

Pick a region that maps to where most of your users and resources are located.



Select a home region that best suits your performance and business needs.

Why is this important? Help me decide.

○ Asia Pacific South

○ European Union

○ United States

□ I've read, understand and agree to the Terms of Service

> **Important notes:**
>
> - You can choose a region only once, when your organization is onboarded. You cannot change your region later.
> - If you are located in one region and use a service in another region, any performance impacts are minimal. Citrix Cloud services are designed to be used on a global basis. For

> example, customers in the US that have users and connectors in Australia will see minimal impact from latency.
> - If you aren't in a region that Citrix Cloud supports, you can still use Citrix Cloud. Simply pick the region that is either closest to most of your users or that provides the best controls for protecting the integrity of your data.

Types of data stored in regions

Your region is where certain metadata is stored about your environment. For example:

- Citrix Cloud administrator details, including the name, user name, and password.
- Data resulting from traffic directed through your region by any connectors you install. For example, any authentication data using your domain controllers (whether managed on your premises or through your subscription with a public cloud vendor) stays in your region.
- Data used to map users to library offerings. For example, if you add Microsoft Office to your library as an offering for your users, and then add five users to that offering as subscribers, the data linking each user to that offering (such as user name and domain name) is stored in your region.
- Data about users for any services available in your region. For example, if you use Endpoint Management in your region, data such as name, address, and telephone number is stored in your region.

Service presence in each region

All services are globally available, regardless of the region you select for your organization. Also, your data might be processed on a global basis by Citrix affiliates or subprocessors as necessary to perform the services. Certain services, like the Virtual Apps and Desktops service, have dedicated regional instances. However, some services have US-based instances only.

Where a service is not available in the region you selected for your organization, certain information (such as authentication data) might be transferred between regions as needed.

Where a service is globally replicated, all data in that service is stored in all regions.

Service	US	EU	Asia Pacific South
Citrix Cloud control plane	Yes	Yes	Yes
Citrix Analytics for Security	Yes	Yes	No (Uses US region)
Citrix Analytics for Performance	Yes	Yes	Yes

Service	US	EU	Asia Pacific South
Application Delivery Management	Yes	Yes	Yes
Citrix Content Collaboration	Yes ⋆⋆⋆	Yes ⋆⋆⋆	No - Select from US or EU ⋆⋆
Citrix Endpoint Management	Yes ⋆⋆	Yes ⋆⋆	Yes ⋆⋆
SD-WAN Orchestrator	Yes	Yes	No (Uses US region)
Secure Browser Service	Yes ⋆	Yes ⋆	Yes ⋆
Citrix Virtual Apps and Desktops service	Yes ⋆	Yes ⋆	Yes ⋆
Citrix Virtual Apps and Desktops Standard for Azure	Yes ⋆	Yes ⋆	Yes ⋆
Citrix Virtual Apps Essentials	Yes ⋆	Yes ⋆	Yes ⋆
Citrix Virtual Desktops Essentials	Yes ⋆	Yes ⋆	Yes ⋆
Web App Firewall	Yes	Yes	No (Uses US region)
Citrix Workspace	Yes ⋆	Yes ⋆	Yes ⋆
Workspace Environment Management	Yes	Yes	Yes
Networking services	Yes	No (Uses US region)	No (Uses US region)
License Usage Insights (CSPs only)	Globally replicated	Globally replicated	Globally replicated
Citrix Gateway Access Nodes/POP	Multiple WW nodes; traffic routed as needed to ensure the best experience	Multiple WW nodes; traffic routed as needed to ensure the best experience	Multiple WW nodes; traffic routed as needed to ensure the best experience

Service	US	EU	Asia Pacific South
Citrix Secure Internet Access Nodes/POP	Multiple WW nodes; traffic routed as needed to ensure the best experience	Multiple WW nodes; traffic routed as needed to ensure the best experience	Multiple WW nodes; traffic routed as needed to ensure the best experience

⋆ Service uses the Citrix Cloud region.

⋆⋆ Select from multiple locations across multiple regions. See Endpoint Management service locations in this article.

⋆⋆⋆ Storage zone can be selected from multiple locations. See Content Collaboration locations and storage zones in this article.

For more information about the data stored by individual services, refer to the Technical Security Overview for each service.

Endpoint Management service locations

You can select one of the following Endpoint Management service locations from your home region:

- US East
- US West
- EU West
- SE Asia
- Sydney

Secure Internet Access service locations

Traffic is routed to the following Secure Internet Access service locations based on availability and end-user proximity to ensure the best experience.

North America

- Sterling, VA, USA
- Toronto, Canada
- Los Angeles, CA, USA
- Irvine, CA, USA
- Seattle, WA, USA
- Denver, CO, USA
- Charlotte, NC, USA

- Dallas, TX, USA
- Allen, TX, USA
- Miami, FL, USA
- Chicago, IL, USA
- New York, NY, USA
- Boston, MA, USA
- Vancouver, Canada

South America

- Queretaro, Mexico
- Sao Paulo, Brazil
- Buenos Aires, Argentina
- Bogota, Colombia

Asia-Pacific

- Perth, Australia
- Sydney, Australia
- Tokyo, Japan
- Singapore, Singapore
- Mumbai, India
- Delhi, India

Africa

Johannesburg, South Africa

Middle East

- Dubai, United Arab Emirates
- Istanbul, Turkey

Western Europe

- London, UK
- Manchester, UK
- Frankfurt, Germany
- Düsseldorf, Germany
- Mannheim, Germany

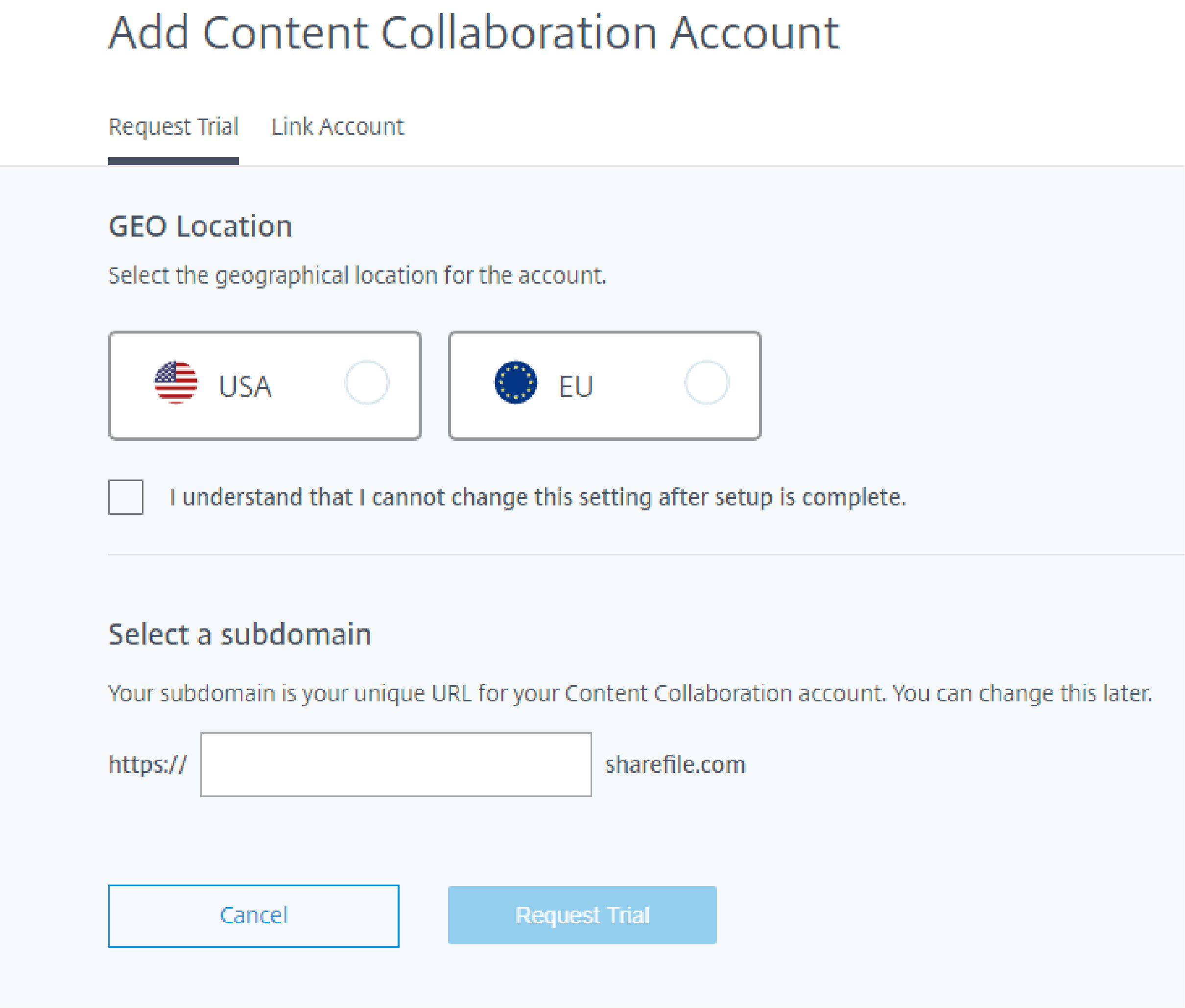
- Paris, France

Europe

- Helsinki, Finland
- Amsterdam, Netherlands
- Stockholm, Sweden
- Warsaw, Poland
- Madrid, Spain
- Sofia, Bulgaria
- Zurich, Switzerland
- Milan, Italy

Content Collaboration locations and storage zones

When setting up a Content Collaboration account in Citrix Cloud, you can select a region in the US or the EU. Your Content Collaboration region is separate from your Citrix Cloud home region. However, like the Citrix Cloud home region, you cannot change the Content Collaboration region after setting up your Content Collaboration account.



Add Content Collaboration Account

GEO Location

Select the geographical location for the account.

USA ○ EU ○

□ I understand that I cannot change this setting after setup is complete.

Select a subdomain

Your subdomain is your unique URL for your Content Collaboration account. You can change this later.

https:// sharefile.com

For Content Collaboration accounts created within Citrix Cloud, your default storage zone is initially in the US region.

For ShareFile Enterprise accounts created outside of Citrix Cloud, your storage zone is located in the region you select, either the US or EU. Linking to Citrix Cloud does not change your selection.

After your Content Collaboration account is set up, you can enable and disable storage zones around the world, as well as choose a new default zone. You can also specify a default specific to individual users or folders based on the storage zone that are turned on in the Content Collaboration management console. Choose from the following locations:

- Japan
- Singapore
- Australia
- European Union
- United States - East

- United States - West
- United States - Northwest
- Brazil

Other cloud platforms from Citrix

In addition to Citrix Cloud, Citrix offers other clouds that are isolated and separate from Citrix Cloud.

Citrix Cloud Government

Citrix Cloud Government allows US government agencies and other public-sector customers in the US to use Citrix cloud services according to regulatory and compliance requirements. Citrix Cloud Government is a geographical boundary within which Citrix operates, stores, and replicates services and data for delivery of Citrix Cloud Government services. Citrix may use multiple public or private clouds located in one or more states within the US to provide services.

Citrix Cloud Government and offered services are available only in the US region.

For more information, see the Citrix Cloud Government product documentation.

Citrix Cloud Japan

Citrix Cloud Japan allows Japanese customers to use Citrix Cloud services in a dedicated Citrix-managed environment. Citrix Cloud Japan is a geographical boundary within which Citrix operates, stores, and replicates services and data for delivery of Citrix Cloud services.

Citrix Cloud Japan and offered services are available only in Japan.

For more information, see the Citrix Cloud Japan product documentation.

Verify your email for Citrix Cloud

April 6, 2018

From time to time, Citrix might ask you to verify your Citrix Cloud account. Some reasons why you might be asked to verify your email:

- You haven’t logged in to Citrix Cloud in a while.
- You changed your email address.
- You added a new administrator to your Citrix Cloud account.

FAQ

How often will I be asked for verification? Verifying your account is a one-time event. Citrix Cloud won't ask you for verification every time you sign in or when something in your account changes. If you're asked to verify frequently, contact Citrix Technical Support.

Has something happened to my account? No, being asked to verify your account doesn't mean that anything is wrong with either your account or any of your Citrix Cloud services. It's simply a part of how Citrix keeps your information safe and secure.

I haven't received an email. What do I do? Perform the following steps:

- Search your inbox for an email from "Citrix."
- If it's not in your inbox, check your folders. If a spam filter or email rule moved the email, it might be in your spam or trash folders.
- Ensure you're checking the correct email account. Citrix sends the verification email to the email address currently on file for your account. Often, this is the email address you originally signed up with for Citrix Cloud or the one with which you were invited to join the Citrix Cloud account.

Contact Citrix Technical Support

If you are experiencing an issue that's not covered here, contact Citrix Technical Support to open a support case.

Citrix Cloud Service Trials

September 24, 2021

Trials for individual Citrix Cloud services are delivered through the Citrix Cloud 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 trial access is managed on a per-service basis. For some services, you need to request a demo before you receive trial access. See Request a service demo in this article for more information.

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

> **Tip:**
>
> The "Getting Started with Citrix Cloud" education module, included in the Fundamentals of Citrix Cloud course, provides a short video that walks you through requesting a trial. The full course

> also gives you a firm foundation for understanding Citrix Cloud, its benefits for your organization, and important use cases that Citrix Cloud services address.

Fast facts about service trials

	Citrix Cloud 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
Endpoint Management	Full feature set
Customizable	Yes

Request a service demo

For some services, you must request a demo from a Citrix sales representative before you can try out the service. Requesting a demo allows you to discuss your organization's cloud service needs with a Citrix sales representative and ensures you have all the information needed to try out the service successfully.

1. Sign in to your Citrix Cloud account.
2. From the management console, click **Request Demo** for the service you want. The service's demo request page appears.
3. Complete and submit the form. A Citrix sales representative will contact you to provide more information and walk you through using the service.

Request a service trial

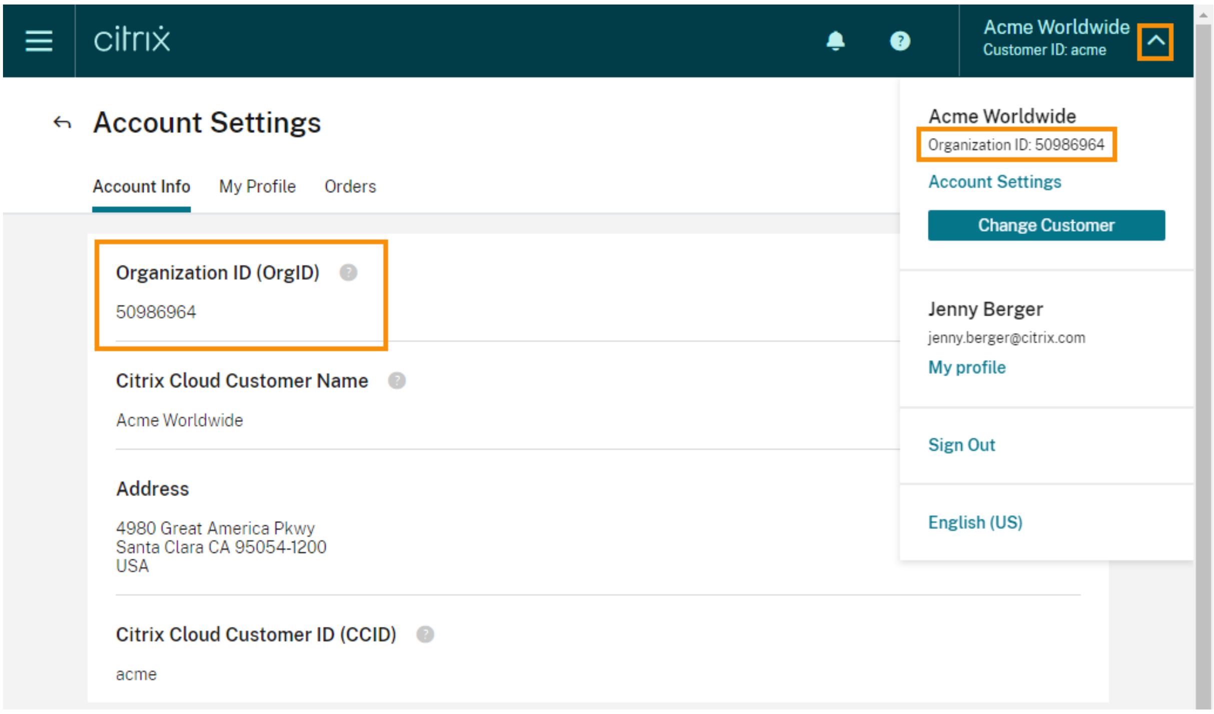
To request a trial, log on to your Citrix Cloud account. From the management console, click **Request Trial** for the service you want to try out. When your trial is approved and ready to use, you'll receive an email notification. You have 60 days to complete the trial.

> **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 Citrix Cloud services

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

To complete the purchase, you'll need your Organization ID, available in the Citrix Cloud management console. Your OrgID appears on the customer menu in the top-right corner of the console and on the **Account Settings** page.



Organization ID: 50986964

Organization ID (OrgID)
50986964

Citrix Cloud Customer Name
Acme Worldwide

Address
4980 Great America Pkwy
Santa Clara CA 95054-1200
USA

Citrix Cloud Customer ID (CCID)
acme

> **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.

Extend Citrix Cloud service subscriptions

This article describes how purchased subscriptions for Citrix Cloud services expire and how you can extend your subscription. The manner in which a service expires is different for services that are purchased as monthly subscriptions, such as Virtual Apps and Desktops Essentials, and services that are purchased as annual or multiannual subscriptions, such as Virtual Apps and Desktops service.

In this article, *monthly subscriptions* refer to services that are purchased on a month-to-month basis. *Annual subscriptions* refer to services that are purchased on a yearly basis. *Multiannual subscriptions* refer to services that are purchased on a multi-yearly basis.

> **Tip:**
>
> The "Getting Started with Citrix Cloud" education module, included in the Fundamentals of Citrix Cloud course, provides a short video that walks you through the subscription expiration process. The full course also gives you a firm foundation for understanding Citrix Cloud, its benefits for your organization, and important use cases that Citrix Cloud services address.

Before expiration

For monthly subscriptions, Citrix Cloud does not send notifications prior to expiration.

For annual and multiannual subscriptions, Citrix Cloud notifies you at certain intervals when your existing subscription approaches expiration. These notifications alert you to extend the subscription and avoid service interruption. The following notifications appear in the Citrix Cloud management console:

- 90 days before expiration: A yellow banner appears, showing the services that need to be extended and their expiration dates. This notification appears in the console every seven days or until the service is extended.
- Seven days before expiration: A red banner appears, showing the services that need to be extended and their expiration dates. This notification appears in the console until the service is extended or the 30-day expiration grace period elapses.

You can dismiss these notifications when they appear; however, they will reappear after seven days.

Citrix also sends you an email notification that includes a list of the services that need to be extended and their expiration dates. Citrix sends this notification at the following intervals:

- 90 days before expiration
- 60 days before expiration
- 30 days before expiration
- Seven days before expiration
- One day before expiration

After expiration: Service grace periods

When your service subscription expires, Citrix provides grace periods so you can extend your subscription or remove your data from the service. The grace period provided is different for monthly subscriptions and annual subscriptions.

Monthly service subscriptions

In the event you cancel your monthly service subscription, Citrix sends you an expiration notification email on the expiration date. The expiration date is the last day of the month in which you cancel the subscription. After expiration, Citrix allows administrators and users to continue accessing the service for five days. During this time, administrators are limited to enumeration and delete functions only. Citrix bills you for any charges you incur while using resources during the 5-day grace period.

If you don't extend your subscription during the grace period, Citrix blocks administrators and users from accessing the service when the grace period elapses. As a reminder, Citrix sends you email notifications at the following intervals:

- One day after expiration (five days before the service is blocked)
- Three days after expiration (two days before the service is blocked)

After the grace period elapses, all resources associated with the service are shut down and powered off. If you need to retrieve any data you added to the service after the grace period ends, you can submit a request to Citrix Technical Support within 30 days after the service expiration date.

Annual and multiannual service subscriptions

For annual and multiannual subscriptions, Citrix allows you to continue accessing the service for 30 days after your subscription expires. If you don't extend your subscription during this period, Citrix blocks administrators and users from accessing the service. As a reminder, Citrix sends you an email notification at the following intervals:

- 15 days after expiration (15 days before the service is blocked)
- 22 days after expiration (seven days before the service is blocked)
- 29 days after expiration (one day before the service is blocked)

The email notification includes a list of the expired services and their expiration dates.

If you extend your subscription during this 30-day grace period, your subscription term begins on the date of the service's original expiration. For example, if the service expires on May 31 and you extend your subscription on June 25 (before the grace period ends), your extended subscription starts on May 31.

Support during service grace periods

If the service experiences a technical issue during the grace period, you must extend the subscription before submitting a support request. Citrix does not provide support for services with expired subscriptions.

After expiration: Service block and data retention

If the service subscription is not extended during the grace period, Citrix blocks access to the service in the following manner:

- For expired monthly subscriptions, administrators and users are blocked from access after five days past the expiration date.
- For expired annual and multiannual subscriptions, administrators and users are blocked from access after 30 days past the expiration date.

Citrix retains any data that you added to the service for 30 days after the service expiration date. If you extend your subscription before the 30-day retention period ends, your administrators and users can access the service with your data intact. Your extended subscription starts as follows:

- For monthly subscriptions, the start date of your first month's subscription is the date you purchase the extension. Afterward, your subscription automatically renews on the first of each subsequent month.
- For annual and multiannual subscriptions, the start date of your extended subscription is the date you purchase the extension.

If you don't extend your subscription before the 30-day retention period ends, Citrix resets the service and deletes any data that you added. If you agreed to allow Citrix to manage your cloud deployment (for example, when using Citrix Essentials services or the Azure Quick Deploy option in the Virtual Apps and Desktops service), Citrix performs the following actions after the 30-day retention period ends:

- Removes all customer-related data from Citrix databases.
- Deletes all resources related to Citrix Cloud services, including Citrix-managed VMs, that Citrix provisioned in your cloud environment. For a description of the Citrix-managed components that are included in specific Citrix Cloud services, refer to the service's documentation.

Customer-managed Azure subscriptions

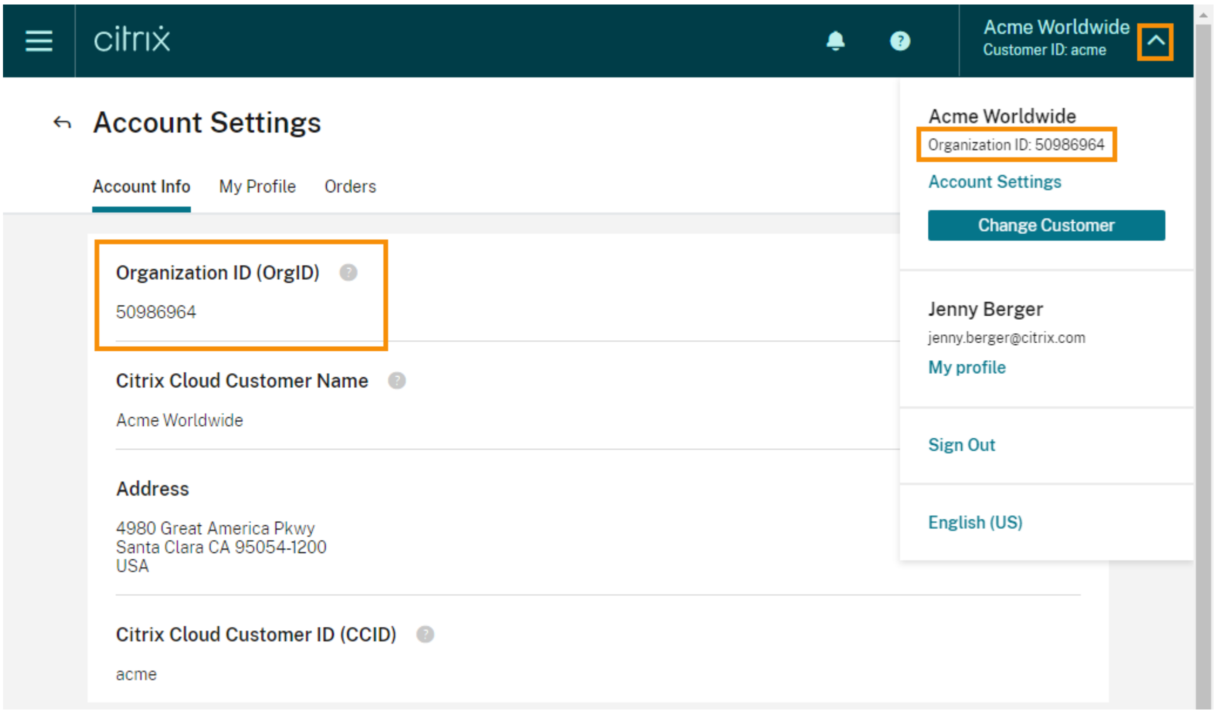
If you are using your own Azure subscription with a Citrix Cloud service, the service installs an app when you connect your Azure subscription to the service. If you don't extend your Citrix Cloud service subscription, Citrix does not remove this app from your Azure subscription after the 30-day retention period ends. You must delete this app to remove the service completely from your Azure subscription. You can delete the app using one of the following methods:

- If administrators are not yet blocked from accessing the service, delete this app from within the service.
- If administrators are blocked from accessing the service, delete this app from within the Azure portal.

Purchase service extensions

To extend your subscription to Citrix Cloud services, visit https://www.citrix.com/products/citrix-cloud/.

To complete the purchase, you need your Organization ID, available in the Citrix Cloud management console. Look in the upper-right corner of the console or under account settings.



Organization ID (OrgID)

50986964

Citrix Cloud Customer Name

Acme Worldwide

Address

4980 Great America Pkwy
Santa Clara CA 95054-1200
USA

Citrix Cloud Customer ID (CCID)

acme

System and Connectivity Requirements

September 15, 2021

Citrix Cloud provides administrative functions (through a web browser) and operational requests (from other installed components) that connect to resources within your deployment. This article describes the system requirements, required contactable Internet addresses, and considerations for establishing connectivity between your resources and Citrix Cloud.

System requirements

Citrix Cloud requires the following minimum configuration:

- An Active Directory domain
- Two physical or virtual machines, joined to your domain, for the Citrix Cloud Connector. For more information, see Citrix Cloud Connector Technical Details.
- Physical or virtual machines, joined to your domain, for hosting workloads and other components such as StoreFront. For more information about system requirements for specific services, refer to the Citrix documentation for each service.

For information about scale and size requirements, see Scale and size considerations for Cloud Connectors.

Supported web browsers

- Latest version of Google Chrome
- Latest version of Mozilla Firefox
- Latest version of Microsoft Edge
- Microsoft Internet Explorer 11
- Latest version of Apple Safari

Citrix Cloud management console

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

Console notifications

The management console uses Pendo to display critical alerts, notifications about new features, and in-product guidance for some features and services. To ensure you can view Pendo content within the management console, Citrix recommends that the address `https://citrix-cloud-content.customer.pendo.io/` is contactable.

Services that display Pendo content include:

- Analytics
- Content Collaboration
- Virtual Apps and Desktops
- Workspace

Pendo is a third-party sub-processor that Citrix uses to provide cloud and support services to Citrix customers. For a complete list of these sub-processors, see Sub-Processors for Citrix Cloud & Support Services and Citrix Affiliates.

Session timeouts

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

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

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

On-premises product registration

If you are using Citrix Cloud with Citrix License Server to register your on-premises products, ensure the following addresses are contactable:

- `https://trust.citrixnetworkapi.net` (for retrieving a code)
- `https://trust.citrixworkspacesapi.net/` (for confirming the license server is registered)
- `https://cis.citrix.com` (for data upload)
- `https://core-eastus-release-a.citrixworkspacesapi.net`
- `https://core.citrixworkspacesapi.net`
- `ocsp.digicert.com port 80`
- `crl3.digicert.com port 80`
- `crl4.digicert.com port 80`
- `ocsp.entrust.net port 80`

- `crl.entrust.net port 80`

If you are using a proxy server with Citrix License Server, ensure the proxy server is configured as described in Configure a proxy server in the Licensing product documentation.

Citrix Cloud Connector

The Citrix Cloud Connector is a software package that deploys a set of services that run on Microsoft Windows servers. The machine hosting the Cloud Connector resides within the network where the resources you use with Citrix Cloud reside. The Cloud Connector connects to Citrix Cloud, allowing it to operate and manage your resources as needed.

For requirements for installing the Cloud Connector, see System 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 service with which it is being used.

The machine hosting the Cloud Connector must have stable network connectivity with Citrix Cloud. Networking components must support HTTPS and long-lived secure web sockets. If a timeout is configured in the networking components, it must be greater than 2 minutes.

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

Cloud Connector common service 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. For more information, see Cloud Connector Proxy and Firewall Configuration.

The addresses for each service in this article must be contactable to properly operate and consume the service. The following list includes the addresses that are common to most Citrix Cloud services and their function. These addresses are provided only as domain names because Citrix Cloud services are dynamic and their IP addresses are subject to routine changes.

- `https://*.citrixworkspacesapi.net` (provides access to Citrix Cloud APIs that the services use)
- `https://*.cloud.com` (provides access to the Citrix Cloud sign-in interface)
- `https://*.blob.core.windows.net` (provides access to Azure Blob Storage, which stores updates for Citrix Cloud Connector)

  - Customers who can't enable all sub-domains can use the following addresses instead:
    - `https://cwsproduction.blob.core.windows.net`
    - `https://ccprodaps.blob.core.windows.net`
    - `https://ccprodeu.blob.core.windows.net`
- `https://*.servicebus.windows.net` (provides access to Azure Service Bus, which is used for logging, the Active Directory agent and Machine Creation Services)

As a best practice, use Group Policy to configure and manage these addresses. Also, configure only the addresses that are applicable to the services that you and your end-users are consuming.

If you are using Citrix Cloud with Citrix License Server to register your on-premises products, see On-premises product registration in this article for additional required contactable addresses.

Certificate validation

Cloud Connector binaries and endpoints that the Cloud Connector contacts are protected by X.509 certificates that are verified when the software is installed. To validate these certificates, each Cloud Connector machine must meet the following requirements:

- HTTP port 80 is open to *.digicert.com. This port is used during Cloud Connector installation and during periodic Certificate Revocation List checks.
- The following addresses must be contactable:
  - `http://*.digicert.com`
  - `https://*.digicert.com`
  - `https://dl.cacerts.digicert.com/DigiCertAssuredIDRootCA.crt`
  - `https://dl.cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA.crt`

For more information about these certificates, see Certificate validation requirements.

SSL Decryption

Enabling SSL decryption on certain proxies might prevent the Cloud Connector from connecting successfully to Citrix Cloud. For more information about resolving this issue, see CTX221535.

Citrix Connector Appliance for Cloud Services

The Connector Appliance is an appliance that you can deploy in your hypervisor. The hypervisor hosting the Connector Appliance resides within the network where the resources you use with Citrix Cloud reside. The Connector Appliance connects to Citrix Cloud, allowing it to operate and manage your resources as needed.

For requirements for installing the Connector Appliance, see System requirements.

To operate, the Connector Appliance requires outbound connectivity on port 443. 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:

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.citrixnetworkapi.net`
- `https://*.*.nssvc.net`
  - Customers who can't enable all sub-domains can use the following addresses instead
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`
- `https://*.servicebus.windows.net`
- `https://iwsprodeastusuniconacr.azurecr.io`
- `https://iwsprodeastusuniconacr.eastus.data.azurecr.io`

Citrix Analytics service connectivity

- For in-product messages including new features and critical communications: `https://citrix-cloud-content.customer.pendo.io/`
- Additional requirements: Prerequisites

For more information about onboarding data sources to the service, see Supported data sources.

Content Collaboration service connectivity

Citrix resource location / Cloud Connector:

- Cloud Connector common service connectivity requirements
- `https://*.sharefile.com`
- Additional requirements: ShareFile Firewall Configuration and IP Address (CTX208318)
- For in-product messages including new features and critical communications: `https://citrix-cloud-content.customer.pendo.io/`

Administration console:

- `https://*.citrixworkspacesapi.net`
- `https://*.cloud.com`
- Additional requirements: ShareFile Firewall Configuration and IP Address (CTX208318)

Endpoint Management service connectivity

Citrix resource location / Cloud Connector:

- Cloud Connector common service connectivity requirements
- Additional requirements: /en-us/citrix-endpoint-management/endpoint-management.html

Administration console:

- `https://*.citrix.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.cloud.com`
- `https://*.blob.core.windows.net`
- Additional requirements: /en-us/citrix-endpoint-management/endpoint-management.html

Citrix Gateway service connectivity

- Cloud Connector common service connectivity requirements
- `https://*.*.nssvc.net`
  - Customers who can't enable all subdomains can use the following addresses instead:
    - `https://*.g.nssvc.net`
    - `https://*.c.nssvc.net`

SD-WAN Orchestrator service connectivity

For complete Internet connectivity requirements, see Prerequisites for Citrix SD-WAN Orchestrator service usage.

Secure Browser service connectivity

Citrix resource location / Cloud Connector:

Cloud Connector common service connectivity requirements

Administration console:

- `https://*.cloud.com`
- `https://*.citrixworkspacesapi.net`
- `https://browser-release-a.azureedge.net`
- `https://browser-release-b.azureedge.net`

Citrix Secure Workspace Access service connectivity

- `https://*.netscalergateway.net`

- `https://*.*.nssvc.net`
  - Customers who can't enable all subdomains can use the following addresses instead:
    * `https://*.g.nssvc.net`
    * `https://*.c.nssvc.net`

Virtual Apps and Desktops service service connectivity

Citrix resource location / Cloud Connector:

- Cloud Connector common service connectivity requirements
- `https://[customerid].xendesktop.net`, where `[customerid]` is the customer ID parameter displayed on the **Secure Clients** tab (**Identity and Access Management > API Access > Secure Clients**) of the Citrix Cloud management console.
  - Customers using Citrix Virtual Apps Essentials need to use `https://*.xendesktop.net` instead.
- `https://*.*.nssvc.net`
  - Customers who can't enable all subdomains can use the following addresses instead:
    * `https://*.g.nssvc.net`
    * `https://*.c.nssvc.net`

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

Administration console:

- `https://*.citrixworkspacesapi.net`
- `https://*.citrixnetworkapi.net`
- `https://*.cloud.com`
- `https://[customerid].xendesktop.net`, where `[customerid]` is the customer ID parameter displayed on the **Secure Clients** tab (**Identity and Access Management > API Access > Secure Clients**) of the Citrix Cloud management console.
  - Customers using Citrix Virtual Apps Essentials need to use `https://*.xendesktop.net` instead.
- `https://*.*.nssvc.net` (Not required for Virtual Apps and Desktops Standard for Azure)
  - Customers who can't enable all sub-domains can use the following addresses instead:
    * `https://*.g.nssvc.net`
    * `https://*.c.nssvc.net`
- For in-product messages including new features and critical communications: `https://citrix-cloud-content.customer.pendo.io/`

Citrix Workspace service connectivity

- `https://*.cloud.com`

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

To ensure subscribers can successfully access their content in Citrix Files and Content Collaboration through Workspace, Citrix recommends allowing the domains listed in CTX208318.

Workspace single sign-on with Citrix Federated Authentication Service

The console and FAS service access the following addresses using the user's account and the Network Service account, respectively.

- FAS administration console, under the user's account
  - `*.cloud.com`
  - `*.citrixworkspacesapi.net`
  - Addresses required by a third party identity provider, if one is used in your environment
- FAS service, under the Network Service account: `*.citrixworkspacesapi.net`

If your environment includes proxy servers, configure the user proxy with the addresses for the FAS administration console. Also, ensure the address for the Network Service account is configured as appropriate for your environment.

Workspace Environment Management service connectivity

`https://*.wem.cloud.com`

Connect to Citrix Cloud

June 8, 2020

Connecting your resources to Citrix Cloud involves deploying connectors in your environment and creating *resource locations*.

Resource locations contain the resources required to deliver cloud services to your subscribers. You manage these resources from the Citrix Cloud console. Resource locations contain different resources depending on which Citrix Cloud services you are using and the services that you want to provide to your subscribers.

To create a resource location, install at least two Cloud Connectors in your domain. Cloud Connectors are required for enabling communication between Citrix Cloud and your resources. For more information about deploying the Cloud Connector, see the following articles:

Resource types

Resource locations contain different resources depending on which Citrix Cloud services you are using and the services that you want to provide to your subscribers. Different resources use different types of connector. Most services make use of the Citrix Cloud Connector, but some specific services need a Connector Appliance.

Services that use Citrix Cloud Connector

For example, if you want to provide access to applications and desktops through the Virtual Apps and Desktops service, your resource location might include:

- Active Directory user and resource domains
- A hypervisor such as Citrix Hypervisor
- Servers running the Virtual Desktop Agent (VDAs)
- An on-premises Citrix Gateway or the Citrix Gateway service for secure external access to resources
- An on-premises StoreFront server so users can access resources through a single easy-to-use app store

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

For a list of Citrix Cloud services that use the Cloud Connector, see Services that require the Cloud Connector.

Services that use Connector Appliance

For example, if you want to deliver actions and notifications from your applications right into your Workspace or other channels, your resource location might include:

- Citrix Workspace microapps service access to systems residing in your resource location
- Citrix Workspace microapps service access to external systems from within your resource location

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

Location of resources

Your resource location is wherever your resources reside, whether that's a public or private cloud, a branch office, or a data center. If you already have resources in your own cloud or data center, your resources remain where they are. There's no need to move them elsewhere to use them with Citrix Cloud.

Your choice of location might be impacted by the following factors:

- Proximity to subscribers
- Proximity to data
- Scale requirements
- Security attributes

There is no restriction on the number of resource locations you can have. The overhead of a resource location is small.

Example of a resource location deployment

- Build your first resource location in your data center for the head office based on subscribers and applications that need to be close to the data.
- Add a second resource location for your global users in a public cloud. Alternatively, build separate resource locations in branch offices to provide the applications best served close to the branch workers.
- Add another resource location on a separate network that provides restricted applications. This provides restricted visibility to other resources and subscribers without the need to adjust the other resource locations.

Naming restrictions

Names that you assign to resource locations must conform to the following restrictions:

- Maximum length: 64 characters
- Disallowed characters:
  - ##, $, %, ^, &, ?, +
  - Braces: [], { }
  - Pipes (|)
  - Less-than symbol (<) and greater-than symbol (>)
  - Forward and backward slashes (/, \)
- Must not match any other resource location name (case-insensitive) in the Citrix Cloud account

Primary resource locations

A primary resource location is a resource location that you designate as "most preferred" for certain communications between your domain and Citrix Cloud. The Cloud Connectors in a primary resource location are used for user logons and provisioning operations. 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.

For more information, see Select a primary resource location.

Citrix Cloud Connector

July 21, 2021

The Citrix Cloud Connector is a Citrix component that serves as a channel for communication between Citrix Cloud and your resource locations, enabling cloud management without requiring any complex networking or infrastructure configuration. This removes all the hassle of managing delivery infrastructure. It enables you to manage and focus on the resources that provide value to your users.

Services that require the Cloud Connector

The Virtual Apps and Desktops service requires the Cloud Connector. For an overview of how the Cloud Connector communicates with the service, refer to the Virtual Apps and Desktops diagram in Citrix Tech Zone.

Citrix Endpoint Management requires the Cloud Connector for enterprise connectivity to the Endpoint Management service. The Secure Browser service requires the Cloud Connector for authenticated external web apps.

Cloud Connector functions

- **Active Directory (AD)**: 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.
- **Virtual Apps and Desktops publishing**: Enables publishing from resources in your resource locations.
- **Endpoint Management**: Enables a mobile device management (MDM) and mobile application management (MAM) environment for managing device and app policies and delivering apps to users.
- **Machine catalog provisioning**: Enables provisioning of machines directly into your resource locations.

> **Note:**
>
> Although operational, functionality might be reduced for the period of time that the connection to Citrix Cloud is unavailable. You can monitor the health of the Cloud Connector from the Citrix Cloud console.

Cloud Connector communication

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

Cloud Connector availability and load management

For continuous availability and to manage load, install multiple Cloud Connectors in each of your resource locations. Citrix recommends at least two Cloud Connectors in each resource location. If one Cloud Connector is unavailable for any period of time, the other Cloud Connectors can maintain the connection. Since each Cloud Connector is stateless, the load can be distributed across all available Cloud Connectors. There is no need to configure this load balancing function. It is completely automated.

As long as there is one Cloud Connector available, there will be no loss in communication with Citrix Cloud. The end user's connection to the resources in the resource location does not rely on a connection to Citrix Cloud, wherever possible. This enables the resource location to provide users access to their resources regardless of a connection being available to Citrix Cloud.

Where to obtain the Cloud Connector

You can download the Cloud Connector software from within Citrix Cloud.

1. Sign in to Citrix Cloud.
2. From the menu in the top-left of the screen, select **Resource Locations**.
3. If you have no existing resource locations, click **Download** on the Resource Locations page. When prompted, save the **cwcconnector.exe** file.
4. If you have a resource location but no Cloud Connectors installed in it, click the Cloud Connectors bar and then click **Download**. When prompted, save the **cwcconnector.exe** file.

Where to install the Cloud Connector

Review the system requirements for supported platforms, operating systems, and versions.

Install the Cloud Connector on a dedicated machine running Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019. This machine must be joined to your domain and able to communicate with the resources that you want to manage from Citrix Cloud.

> **Important:**
>
> - Do not install the Cloud Connector, or any other Citrix components, on an Active Directory domain controller.
> - Do not install the Cloud Connector on machines that are part of other Citrix deployments (for example, Delivery Controllers in a Virtual Apps and Desktops deployment).

For more deployment information, see the following articles:

- Deployment scenarios for Cloud Connectors in Active Directory
- Cloud Connector Installation

Citrix Cloud Connector Technical Details

October 15, 2021

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

System requirements

The machines hosting the Cloud Connector must meet the following requirements. Citrix strongly recommends installing at least two Cloud Connectors in each resource location to ensure high availability.

Hardware requirements

Each Cloud Connector requires of minimum of:

- 2 vCPU
- 4 GB memory
- 20 GB disk space

More vCPU memory enables a Cloud Connector to scale up for larger sites. For recommended configurations, see Scale and size considerations for Cloud Connectors.

Operating systems

The following operating systems are supported:

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

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

.NET requirements

Microsoft .NET Framework 4.7.2 or later is required. Download the latest version from the Microsoft website.

> **Note:**
>
> Do not use Microsoft .NET Core with the Cloud Connector. If you use .NET Core instead of .NET Framework, installing the Cloud Connector might fail. Use only .NET Framework with the Cloud Connector.

Server requirements

If you're using Cloud Connectors with the Virtual Apps and Desktops service, refer to Scale and size considerations for Cloud Connectors for machine configuration guidance.

The following requirements apply to all machines where the Cloud Connector is installed:

- Use dedicated machines for hosting the Cloud Connector. Do not install any other components on these machines.
- The machines are **not** configured as Active Directory domain controllers. Installing the Cloud Connector on a domain controller is not supported.
- Server clock is set to the correct UTC time.
- Internet Explorer Enhanced Security Configuration (IE ESC) is turned off. If this setting is turned on, the Cloud Connector might not be able to establish connectivity with Citrix Cloud.
- Citrix strongly recommends enabling Windows Update on all machines hosting the Cloud Connector. When configuring Windows Update, configure Windows to automatically download and install updates outside of business hours, but do not allow automatic restarts for at least 4 hours. The Citrix Cloud platform handles machine restarts when it identifies that an update is waiting for a restart, allowing a restart for only one Cloud Connector at a time. You can configure a fallback restart using Group Policy or a system management tool for when the machine must be restarted after an update. For more information, see https://docs.microsoft.com/en-us/windows/deployment/update/waas-restart.

Certificate validation requirements

Cloud Connector binaries and endpoints that the Cloud Connector contacts are protected by X.509 certificates issued by widely respected enterprise certificate authorities (CAs). Certificate verification in Public Key Infrastructure (PKI) includes the Certificate Revocation List (CRL). When a client receives a certificate, the client checks whether it trusts the CA that issued the certificates and whether the certificate is on a CRL. If the certificate is on a CRL, the certificate is revoked and should not be trusted, even though it appears valid.

The CRL servers use HTTP on port 80 instead of HTTPS on port 443. Cloud Connector components, themselves, do not communicate over external port 80. The need for external port 80 is a byproduct of the certificate verification process that the operating system performs.

The X.509 certificates are verified during the Cloud Connector installation. So, all Cloud Connector machines must be configured to trust these certificates to ensure 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 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://crl3.digicert.com`
  - `http://crl4.digicert.com`
  - `http://ocsp.digicert.com`
  - `http://www.d-trust.net`
  - `http://root-c3-ca2-2009.ocsp.d-trust.net`
  - `http://crl.microsoft.com`
  - `http://oneocsp.microsoft.com`
  - `http://ocsp.msocsp.com`
- Communication with the following addresses is enabled:
  - `https://*.digicert.com`
- The following certificates are installed:
  - `https://dl.cacerts.digicert.com/DigiCertAssuredIDRootCA.crt`
  - `https://dl.cacerts.digicert.com/DigiCertSHA2AssuredIDCodeSigningCA.crt`
  - `https://cacerts.digicert.com/DigiCertGlobalRootG2.crt`
  - `https://cacerts.digicert.com/DigiCertGlobalRootCA.crt`
  - `https://cacerts.digicert.com/BaltimoreCyberTrustRoot.crt`
  - `https://www.d-trust.net/cgi-bin/D-TRUST_Root_Class_3_CA_2_2009.crt`
  - `https://www.microsoft.com/pkiops/certs/Microsoft%20RSA%20Root%20Certificate%20Authority%202017.crt`
  - `https://www.microsoft.com/pkiops/certs/Microsoft%20EV%20ECC%20Root%20Certificate%20Authority%202017.crt`

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

Active Directory requirements

- Joined to an Active Directory domain that contains the resources and users that you will use to create offerings for your users. For multi-domain environments, see Deployment scenarios for Cloud Connectors in Active Directory in this article.
- Each Active Directory forest you plan to use with Citrix Cloud should be reachable by two Cloud Connectors at all times.
- The Cloud Connector 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 will use in your resource location. For more information, see Cloud Connector Proxy and Firewall Configuration.
- Connected to the Internet. For more information, see System and Connectivity Requirements.

Supported Active Directory functional levels

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

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

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

Federal Information Processing Standard (FIPS) support

The Cloud Connector currently supports the FIPS-validated cryptographic algorithms that are used on FIPS-enabled machines. Only the latest version of the Cloud Connector software available in Citrix Cloud includes this support. If you have existing Cloud Connector machines in your environment (installed before November 2018) and you want to enable FIPS mode on these machines, perform the following actions:

1. Uninstall the Cloud Connector software on each machine in your resource location.
2. Enable FIPS mode on each machine.
3. Install the latest version of the Cloud Connector on each FIPS-enabled machine.

> **Important:**
>
> - Do not attempt to upgrade existing Cloud Connector installations to the latest version. Always uninstall the old Cloud Connector first and then install the newer one.
> - Do not enable FIPS mode on a machine hosting an older Cloud Connector version. Cloud Connectors older than Version 5.102 do not support FIPS mode. Enabling FIPS mode on a machine with an older Cloud Connector installed prevents Citrix Cloud from performing regular maintenance updates for the Cloud Connector.

For instructions to download the latest version of the Cloud Connector, see Where to obtain the Cloud Connector.

Cloud Connector installed services

This section describes the services that are installed with the Cloud Connector and their system privileges.

During installation, the Citrix Cloud Connector executable installs and sets the necessary service configuration to the default settings required to function. If the default configuration is manually altered, the Cloud Connector might not perform as expected. In this case, the configuration resets to the default state when the next Cloud Connector update occurs, assuming the services that handle the update process can still function.

Citrix Cloud Agent System facilitates all elevated calls necessary for the other Cloud Connector services to function and does not communicate on the network directly. When a service on the Cloud Connector needs to perform an action requiring Local System permissions, it does so through a predefined set of operations that the Citrix Cloud Agent System can perform.

Service Name	Description	Runs As
Citrix Cloud Agent System	Handles the system calls necessary for the on-premises agents. Includes installation, reboots, and registry access. Can only be called by Citrix Cloud Services Agent WatchDog.	Local System
Citrix Cloud Services Agent WatchDog	Monitors and upgrades the on-premises agents (evergreen).	Network Service
Citrix Cloud Services Agent Logger	Provides a support logging framework for the Citrix Cloud Connector services.	Network Service
Citrix Cloud Services AD Provider	Enables Citrix Cloud to facilitate management of resources associated with the Active Directory domain accounts in which it is installed.	Network Service

Service Name	Description	Runs As
Citrix Cloud Services Agent Discovery	Enables Citrix Cloud to facilitate management of XenApp and XenDesktop legacy on-premises Citrix products.	Network Service
Citrix Cloud Services Credential Provider	Handles storage and retrieval of encrypted data.	Network Service
Citrix Cloud Services WebRelay Provider	Enables HTTP Requests received from WebRelay Cloud service to be forwarded to On-Premises Web Servers.	Network Service
Citrix CDF Capture Service	Captures CDF traces from all configured products and components.	Network Service
Citrix Config Synchronizer Service	Copies brokering configuration locally for high availability mode.	Network Service
Citrix Connection Lease Exchange Service	Enables Connection Lease files to be exchanged between Workspace app and Cloud Connector for Service Continuity for Workspace	Network Service
Citrix High Availability Service	Provides continuity of service during outage of central site.	Network Service
Citrix ITSM Adapter Provider	Automates provisioning and management of virtual apps and desktops.	Network Service
Citrix NetScaler CloudGateway	Provides Internet connectivity to on-premises desktops and applications without the need to open in-bound firewall rules or deploying components in the DMZ.	Network Service

Service Name	Description	Runs As
Citrix Remote Broker Provider	Enables communication to a remote Broker Service from local VDAs and StoreFront servers.	Network Service
Citrix Remote HCL Server	Proxies communications between the Delivery Controller and the Hypervisor(s).	Network Service
Citrix WEM Cloud Authentication Service	Provides authentication service for Citrix WEM agents to connect to cloud infrastructure servers.	Network Service
Citrix WEM Cloud Messaging Service	Provides service for Citrix WEM cloud service to receive messages from cloud infrastructure servers.	Network Service

Deployment scenarios for Cloud Connectors in Active Directory

Install Cloud Connector within your secure, internal network.

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. If you have multiple domains in your environment, you must consider where to install the Cloud Connectors so your users can access the resources you make available.

> **Note:**
>
> The below resource locations form a blueprint that may need to be repeated in other physical locations depending on where your resources are hosted.

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

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

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

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

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

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

> **Note:**
>
> You might need to restart the Cloud Connectors to ensure Citrix Cloud 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 console. This carries the following limitations:

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

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

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

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

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

View the health of the Cloud Connector

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

Event messages

The Cloud Connector generates certain event messages that you can view through 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 download 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.

Event logs

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

Troubleshooting

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

Cloud Connector connectivity

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

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

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

Installation

If the Cloud Connector is in an "error" state, there might be a problem hosting the Cloud Connector. Install the Cloud Connector on a new machine. If the issue persists, contact Citrix Support. To troubleshoot common issues with installing or using the Cloud Connector, see CTX221535.

Deploying Cloud Connectors as Secure Ticket Authority servers

If using multiple Cloud Connectors as Secure Ticket Authority (STA) servers with Citrix ADC, the ID for each STA server might be displayed as **CWSSTA** in both the ADC management console and the ICA file for application and desktop launches. As a result, STA tickets are not routed correctly and launching sessions fails. This issue can occur if the Cloud Connectors are deployed under separate Citrix Cloud accounts with different customer IDs. In this scenario, a ticketing mismatch occurs between the separate accounts that prevents sessions from being created.

To resolve this issue, ensure the Cloud Connectors that you bind as STA servers belong to the same Citrix Cloud account with the same customer ID. If you need to support multiple customer accounts from the same ADC deployment, create a new Gateway virtual server for each account. For more information, refer to the following articles:

- Creating Gateway virtual servers: Create virtual servers
- Configuring the Secure Ticket Authority on Citrix Gateway
- Deployment Guide: Migrating Citrix Virtual Apps and Desktops from on-premises to Citrix Cloud
- CTX232640: How do I configure Citrix Gateway to use a Cloud Connector as a STA

Cloud Connector Proxy and Firewall Configuration

August 10, 2021

The Cloud Connector supports connection to the Internet through an unauthenticated web proxy server. Both the installer and the services it installs need connections to Citrix Cloud. Internet access needs to be available at both of these points.

Connectivity requirements

Use port 443 for HTTP traffic, egress only. For a list of required contactable addresses, see System and Connectivity Requirements. For a list of the addresses common to most Citrix Cloud services and their function, see Cloud Connector common service connectivity requirements.

The required contactable addresses for Citrix Cloud are specified as domain names, not IP addresses. Because IP addresses might change, allowing domain names ensures that the connection to Citrix Cloud remains stable. Also, as Citrix continually improves and augments the Citrix Cloud platform, allowing these domains as wildcards (for example, *.citrixworkspacesapi.net), instead of using more specific addresses (for example, trust.citrixworkspacesapi.net), allows customers to benefit from these improvements without affecting their connectivity to Citrix Cloud. Some critical functions of the platform, such as traffic failover based on geographical region, rely on being able to route calls under multiple subdomains. Specifying allowed subdomains instead of allowed wildcard domains increases the risk of outage as these functions might use subdomains the customer hasn't explicitly allowed. Specifying the wildcard domain allows these functions to work without placing an undue burden on the customer to allow a large number of subdomains for every Citrix Cloud service.

> **Important:**
>
> Enabling SSL decryption on certain proxies might prevent the Cloud Connector from connecting successfully to Citrix Cloud. For more information about resolving this issue, see CTX221535.

Check Cloud Connector connectivity

The Cloud Connector Connectivity Check Utility helps you verify connectivity between the Cloud Connector and Citrix Cloud using a series of connectivity checks. If you use a proxy server in your environment, the utility can help you configure proxy settings on the Cloud Connector and test connectivity through the proxy server. When a proxy server is configured, the connectivity tests are tunneled through the proxy server.

For more information about downloading and using the Cloud Connector Connectivity Check utility, see CTX260337.

> **Note:**
>
> Cloud Connector Connectivity Check utility is for use with commercial Citrix Cloud accounts only. Do not use it with Citrix Cloud Government or Citrix Cloud Japan.

Installer

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

Services at Runtime

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

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

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

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

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

> **Note:**
>
> There is no support for auto-detect or PAC scripts or authenticated proxies.

Connections to internal resources

Due to Windows proxy configuration, the Cloud Connector may attempt to access internal resources through the web proxy. These resources may not be able to connect to the Cloud Connector and Virtual Apps and Desktops service, even if the required connectivity URLs are allowed. Also, the web proxy may block connections between the Cloud Connector and Azure Service bus because an IP address is used as a URL in the HTTP Connect command. As a result, some resource functions might fail. For example, Citrix Provisioning can't create machine catalogs successfully.

To ensure that these internal resources can connect as expected, add the FQDN or IP address of each resource to the proxy bypass list on the Cloud Connector machine. For more information about this issue, see CTX241222 in the Citrix Support Knowledge Center.

Connections between Citrix Federated Authentication Service and Citrix Cloud

The console and FAS service access the following addresses using the user's account and the Network Service account, respectively.

- FAS administration console, under the user's account

  - `*.cloud.com`
  - `*.citrixworkspacesapi.net`
  - Addresses required by a third party identity provider, if one is used in your environment
- FAS service, under the Network Service account: `*.citrixworkspacesapi.net`

If your environment includes proxy servers, configure the user proxy with the addresses for the FAS administration console. Also, ensure that the address for the Network Service account is configured using netsh or a similar tool.

Cloud Connector Installation

September 10, 2021

You can install the Cloud Connector software interactively or using the command line.

The installation occurs with the privileges of the user who begins the install. The Cloud Connector requires access to the cloud to:

- Authenticate the user that performs the installation
- Validate the installer's permissions
- Download and configure the Cloud Connector services

Information to review before installation

- System requirements: To prepare the machines for hosting the Cloud Connector.
- Antivirus Exclusions section of the Endpoint Security and Antivirus Best Practices Tech Zone article: Provides guidelines to help you determine the appropriate balance between security and performance for the Cloud Connectors in your environment. Citrix strongly recommends reviewing these guidelines with your organization's antivirus and security teams, and performing rigorous lab-based testing before applying them to a production environment.
- System and Connectivity Requirements: To ensure all machines hosting the Cloud Connector can communicate with Citrix Cloud.
- Cloud Connector Proxy and Firewall Configuration: If you're installing the Cloud Connector in an environment that has a web proxy or strict firewall rules.
- Scale and size considerations for Cloud Connectors: Provides details of tested maximum capacities and best practice recommendations for configuring machines to host the Cloud Connector.

Installation considerations and guidance

- Don't 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 performs machine operations that cause an outage to these additional resources.

- Don't download or install other Citrix products on the machines hosting the Cloud Connector.
- Don't download or install the Cloud Connector on machines that belong to other Citrix product deployments (for example, Delivery Controllers in a Citrix Virtual Apps and Desktops deployment).
- Don't upgrade a previously installed Cloud Connector with a newer version. Instead, uninstall the old Cloud Connector and then install the new one.
- The Cloud Connector installer is downloaded from Citrix Cloud. So, your browser must allow downloading executable files.
- After installation, do not move the machine hosting the Cloud Connector into a different domain. If you need to join the machine to a different domain, uninstall the Cloud Connector and then reinstall it after the machine is joined to the different domain.
- After installation, keep all Cloud Connectors powered on continuously to ensure an always-on connection to Citrix Cloud.

Considerations for cloned machines

Each machine hosting the Cloud Connector must have a unique SID and connector ID so that Citrix Cloud can communicate reliably with the machines in your resource location. 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.

Installing the Cloud Connector on a machine template (before cloning) isn't supported. If you clone a machine with the Cloud Connector installed, the Cloud Connector services won't run and the machine can't connect to Citrix Cloud.

Default resource locations

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

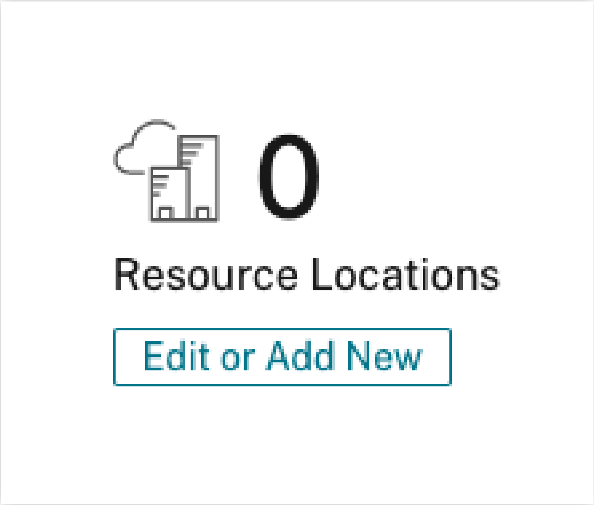
Alternatively, you can first create the resource locations you need in the console, before you install Cloud Connectors in your domains. The Cloud Connector installer prompts you to select the resource location you want during installation.

Interactive installation

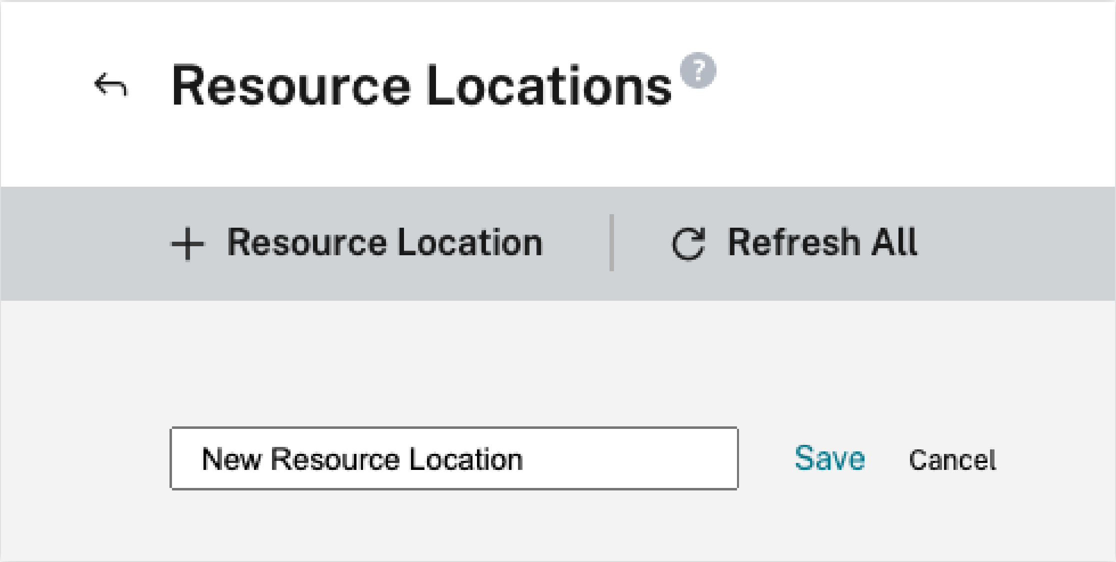
You can download and install Cloud Connectors using the graphical installer interface. Before you do this, you must create one or more resource locations in the Citrix Cloud management console to deploy Cloud Connectors on. For more information on resource locations, see Location of resources.

To create a resource location

1. Sign in as a Windows administrator to the machine you intend to install Citrix Cloud Connectors on.
2. Visit https://citrix.cloud.com and sign in to your administrator account.
3. In the Citrix Cloud console, navigate to **Resource Locations** from the main menu, or select **Edit or Add New** under **Resource Locations** at the top of the page.



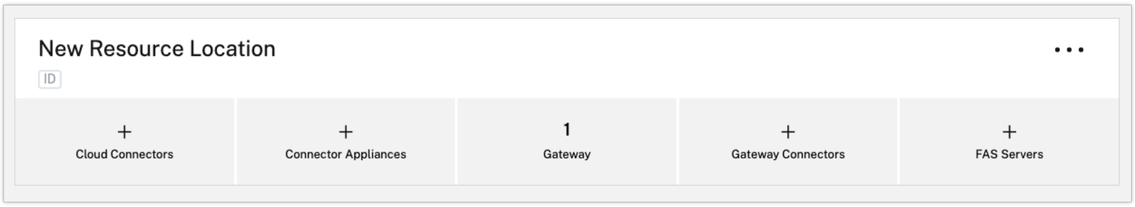
4. In Resource Locations, select **+ Resource Location** at the top of the page and save a new, meaningful name for it.



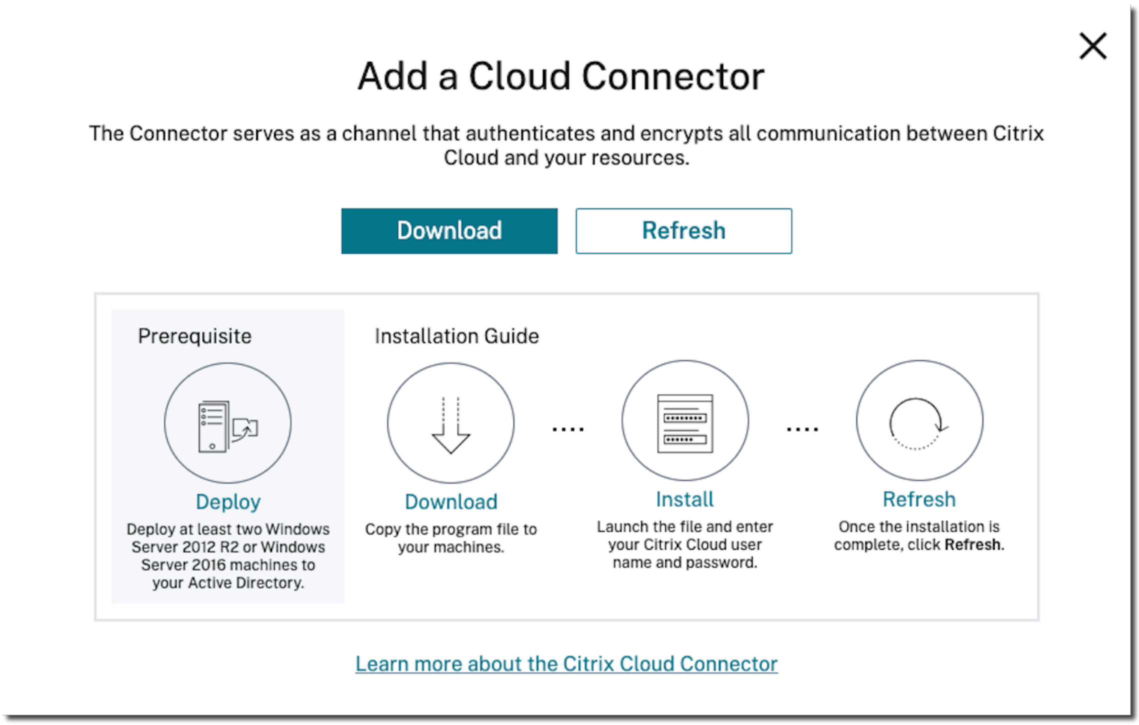
5. Repeat these steps on each machine you want to use for Cloud Connectors.

Download the Citrix Cloud Connector software

1. Locate the resource location you want to manage and select **+ Cloud Connectors**.



2. Select **Download** in the window that opens. Save the **cwcconnector.exe** file to a local file location on your connector machine.



Add a Cloud Connector

The Connector serves as a channel that authenticates and encrypts all communication between Citrix Cloud and your resources.

Deploy
Deploy at least two Windows Server 2012 R2 or Windows Server 2016 machines to your Active Directory.

Download
Copy the program file to your machines.

Install
Launch the file and enter your Citrix Cloud user name and password.

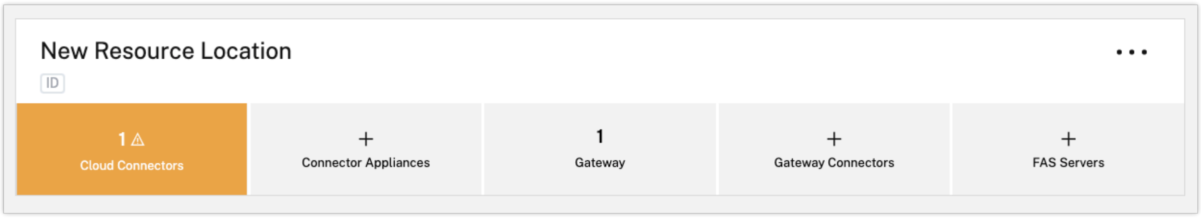
Refresh
Once the installation is complete, click **Refresh**.

Learn more about the Citrix Cloud Connector

Install the Citrix Cloud Connector software

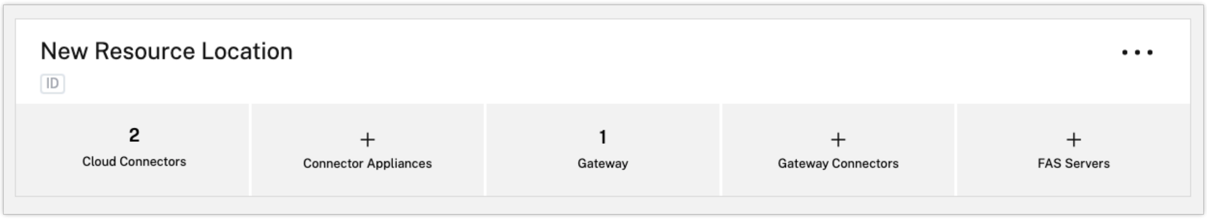
1. Right-click the **cwcconnector.exe** installer file and select **Run as administrator**. The installer performs an initial connectivity check to ensure you can connect to Citrix Cloud.
2. When prompted, sign in to Citrix Cloud.
3. To install and configure the Cloud Connector, follow the wizard instructions. When the installation finishes, the installer performs a final connectivity check to verify communication between the Cloud Connector and Citrix Cloud.
4. Repeat these steps on other machines you want to use as Citrix Cloud Connectors. For high availability, Citrix recommends that you install at least two Cloud Connectors for every resource location.

Citrix Cloud displays the newly installed Cloud Connector on the **Connectors** page for your resource location.



New Resource Location

1 ⚠	+	1	+	+
Cloud Connectors	Connector Appliances	Gateway	Gateway Connectors	FAS Servers



After installation, Citrix Cloud also registers your domain in **Identity and Access Management > Domains**. For more information, see Identity and access management.

Create additional resource locations

1. From the Citrix Cloud management console, click the menu button and select **Resource Locations**.
2. Click **+ Resource Location** and enter a meaningful name.
3. Click **Save**. Citrix Cloud 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 prompts you to select the resource location you want to associate with the Cloud Connector.

Installation with multiple customers and existing resource locations

If you're an administrator for multiple customer accounts, Citrix Cloud prompts you to select the customer account you want to associate with the Cloud Connector.

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

Command-line installation

Silent or automated installation is supported. However, using the same installer for repeated installations isn't recommended. Download a new Cloud Connector from the Resource Locations page in the Citrix Cloud console.

Requirements

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

- The customer ID of the Citrix Cloud account for which you are installing the Cloud Connector. This ID appears at the top of the **API Access** tab in **Identity and Access Management**.

- The client ID and secret of the secure API client you want to use to install the Cloud Connector. To acquire these values, you must first create a secure client. The client ID and secret ensures that your access to the Citrix Cloud API is secured appropriately. When you create a secure client, the client operates with the same level of administrator permissions that you have. To install a Cloud Connector, you must use a secure client which was created by a Full Access administrator, which means the secure client that also has full access permissions.
- The resource location ID for the resource location that you want to associate with the Cloud Connector. To retrieve this value, select the **ID** button located beneath the resource location name on the **Resource Locations** page. If you don't supply this value, Citrix Cloud uses the ID of the default resource location.

Create a secure client

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

1. From the Citrix Cloud menu, select **Identity and Access Management** and then select **API Access**.
2. From the **Secure Clients** tab, enter a name for your client and select **Create Client**. Citrix Cloud generates and displays a client ID and secret for the secure client.
3. Select **Download** to download the client ID and secret as a CSV file and store it in a secure location. Alternatively, select **Copy** to manually acquire each value. When finished, select **Close** to return to the console.

Supported parameters

To ensure the security of the secure client details, a JSON configuration file must be provided to the installer. This file must be deleted after the installation has completed. Supported values for the configuration file are:

- **customerName** Required. The customer ID shown on the API Access page in the Citrix Cloud 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** 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”
 }

<!--NeedCopy-->
```

A sample command line that installs using the parameter file:

```
CWCConnector.exe /q /ParametersFilePath:c:\cwcconnector_install_params.json
<!--NeedCopy-->
```

Use **Start /Wait CWCConnector.exe /ParametersFilePath:value** to examine a potential error code in the case of a failure. You can use the standard mechanism of running **echo %ErrorLevel%** after the installation completes.

> **Note:**
>
> Using parameters to pass the Client ID and Client Secret is no longer supported, the configuration file must be used for automated installations.

Next steps

1. Set up the Citrix Cloud Connector update schedule. For information on Citrix Cloud Connector updates and managing update schedules, visit Connector updates
2. Set up an identity provider to authenticate your workspace subscribers. You can change the default Citrix identity provider to your Active Directory or other identity providers in the **Identity and Access Management** console. For more information, visit To connect your Active Directory to Citrix Cloud.

Troubleshooting installation issues

This section details some ways of diagnosing and fixing problems you might encounter during installation. For more guidance about troubleshooting installation issues, see the Citrix Cloud Connector

Troubleshooting Guide.

Installation logs

You can troubleshoot issues encountered with installation by first consulting the available log files.

Events that occurred during installation are available in the **Windows Event Viewer**. You can also review Cloud Connector installation logs, which are located at **%LOCALAPPDATA%\Temp\CitrixLogs\CloudServices** Logs are also added to **%ProgramData%\Citrix\WorkspaceCloud\InstallLogs** after installation.

Exit codes

The following exit codes might be returned depending on the success or failure of the installation process:

- 1603 - An unexpected error occurred
- 2 - A prerequisite check failed
- 0 - Installation completed successfully

Installation error

If you install the Citrix Cloud Connector software by double-clicking the installer, you might receive the following error message:

```
Can't reach this page.
```

This error can occur even if you are logged in to the machine as an administrator to install the Citrix Cloud Connector. To avoid this error, run the Citrix Cloud Connector software as an administrator by right-clicking the installer and selecting Run as administrator.

Connectivity failures

To ensure that the Cloud Connector can communicate with Citrix Cloud, confirm that the following Citrix services are in a **Started** state:

- Citrix Cloud AD Provider
- Citrix Cloud Agent Logger
- Citrix Cloud Agent System
- Citrix Cloud Agent Watchdog
- Citrix Cloud Credential Provider
- Citrix Config Synchronizer Service
- Citrix High Availability Service
- Citrix NetScaler CloudGateway

- Citrix Remote Broker Provider
- Citrix Remote HCL Server
- Citrix Session Manager Proxy

For more information about these services, see Installed Services.

If you continue to experience connectivity failures, use the Cloud Connector Connectivity Check Utility available from the Citrix Support Knowledge Center. For more information, see CTX260337 on the Knowledge Center website.

The tool can be used to perform the following tasks:

- Test whether Citrix Cloud and its related services are reachable.
- Check for commonly misconfigured settings.
- Configure proxy settings on the Citrix Cloud Connector.

For more information on how to resolve a failed connectivity check, see CTX224133: Cloud Connector Connectivity Check Failed.

Log Collection for Citrix Cloud Connector

June 4, 2020

CDF logs are used for troubleshooting purposes within Citrix products. Citrix Support uses CDF traces to identify issues with application and desktop brokering, user authentication, Virtual Delivery Agent (VDA) registration. This article discusses how to capture Cloud Connector data that can be used to troubleshoot and resolve issues you might experience in your environment.

> **Important notes:**
>
> - Enable logging on all Cloud Connector machines in your resource locations.
> - To ensure that you're capturing the full spectrum of data, Citrix recommends using the CDFControl capturing tool that resides on the VDA. For more information, see CTX111961 in the Citrix Support Knowledge Center. For more information about log collection for Citrix Workspace app, CTX141751.
> - To submit CDF traces to Citrix, you must have an open Citrix Support case. Citrix Support technicians can't review CDF traces that are not attached to an existing support case.

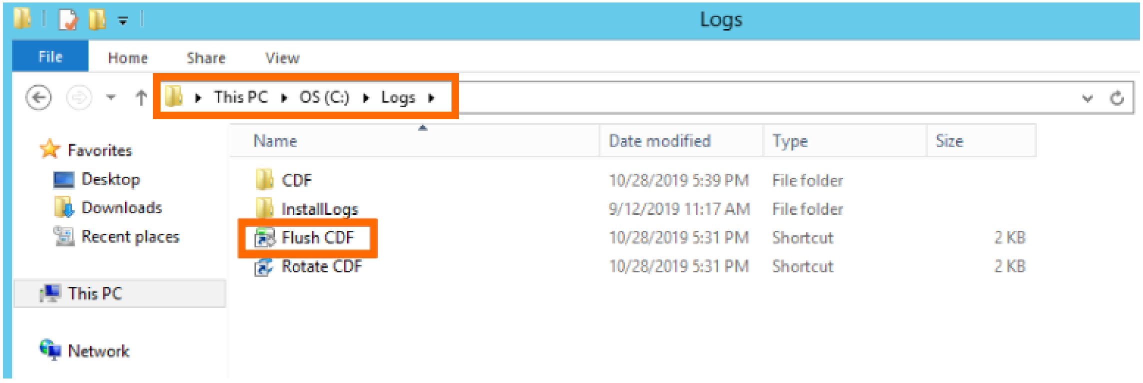
Step 1: Recreate the issue

In this step, recreate the issue you're experiencing in your environment. If the issue is related to app launches or brokering, recreate the launch failure. If the issue is related to VDA registration, recreate the VDA registration attempt by manually restarting the Citrix Desktop Service on the VDA machine.

Step 2: Collect CDF traces

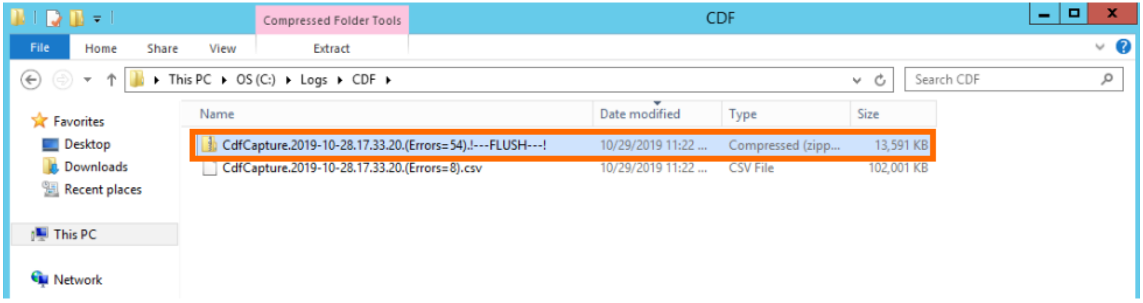
In this step, you collect CDF flush traces from each Cloud Connector in your resource location.

1. Access the Cloud Connector machine by initiating an RDP connection using a Domain Admin or Local Administrator account.
2. On the Cloud Connector machine, open the File Explorer and navigate to `C:\logs`.



Name	Date modified	Type	Size
CDF	10/28/2019 5:39 PM	File folder	
InstallLogs	9/12/2019 11:17 AM	File folder	
Flush CDF	10/28/2019 5:31 PM	Shortcut	2 KB
Rotate CDF	10/28/2019 5:31 PM	Shortcut	2 KB

3. Run **Flush CDF**. An icon appears briefly on the Taskbar of the Cloud Connector machine and then disappears.
4. From the File Explorer, navigate to C:\logs\CDF and identify the most recent folder ending in **!–FLUSH–!**.



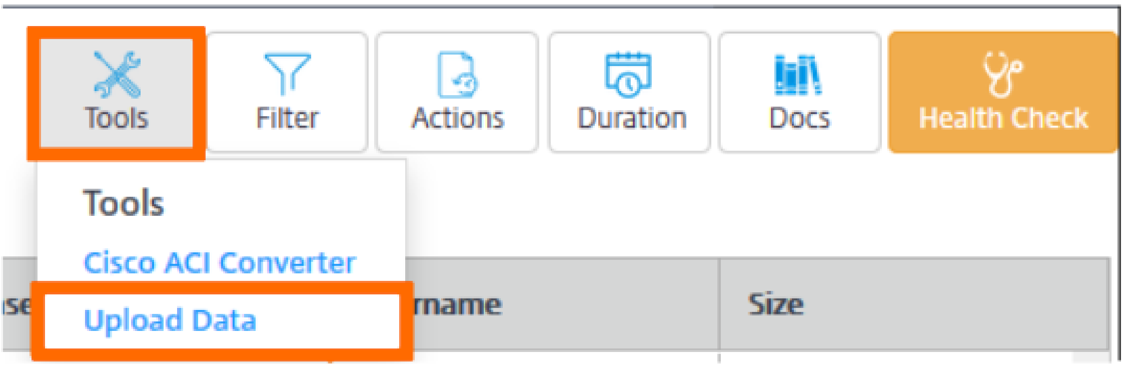
Name	Date modified	Type	Size
CdfCapture.2019-10-28.17.33.20.(Errors=54).!---FLUSH---!	10/29/2019 11:22 ...	Compressed (zipp...	13,591 KB
CdfCapture.2019-10-28.17.33.20.(Errors=8).csv	10/29/2019 11:22 ...	CSV File	102,001 KB

5. Perform Steps 1-5 on every Cloud Connector machine in your resource location and combine all Cloud Connector flush traces into a single ZIP archive. If you don't create a ZIP archive of the flush traces from all your Cloud Connector machines, you will need to submit them one at a time to Citrix.

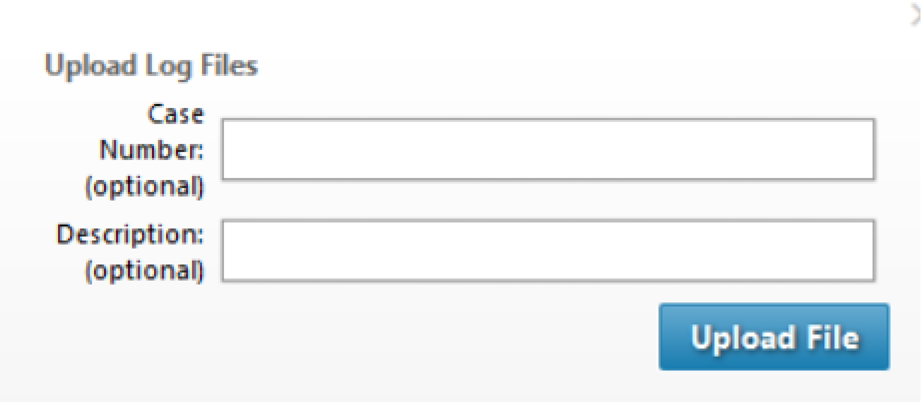
Step 3: Submit data to Citrix

In this step, you attach your traces to your Citrix support case and submit them for review.

1. Visit https://cis.citrix.com/ and sign in using your Citrix.com credentials.
2. Select **Diagnostics**.
3. Select **Tools** and then select **Upload Data**.



4. In **Case Number**, enter the Citrix Support case number of the existing support case. Citrix Support technicians can't review CDF traces appropriately without a case number attached to the data upload.



5. In **Description** (optional), you can enter a brief description or leave this field blank.
6. Select **Upload File** and select the ZIP archive you created earlier. If you didn't create a ZIP archive of flush traces from all your Cloud Connector machines, repeat Steps 3-6 to attach each flush trace you want to submit.

After you submit your flush traces, Citrix Insight Services processes them and attaches them to the support case you specified. This process can take up to 24 hours, depending on the size of the files.

Connector Appliance for Cloud Services

September 29, 2021

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.

The Connector Appliance provides the following function:

- **Citrix Workspace Microapps service** delivers actions and notifications from your applications right into your Workspace or other channels.

  Build integrations from your application data sources to the Microapps service that pull actions from your applications into Workspace. Microapps then deliver actionable forms and notifications that write back to the source system to complete the application workflow. For more information, see Microapps.

  Citrix Workspace Microapps service uses the Connector Appliance to deliver content from the following locations:

  - Your on-premises applications
  - External systems that connect through your resource location

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

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 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.

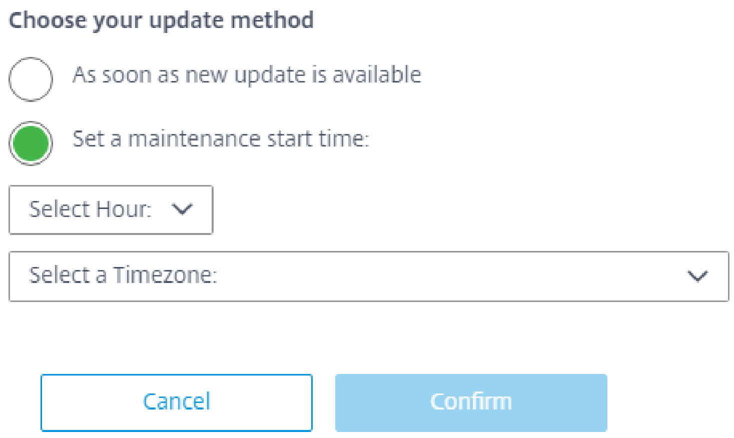
If you have only one connector configured for a resource location, Citrix Cloud shows a warning on both the **Resource Locations** and the **Connectors** page.

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. To configure the maintenance window:

1. On your resource location, go to the ellipsis (…) menu and select **Manage Resource Location**.
2. In the **Choose your update method** section, select **Set a maintenance start time**.
3. Choose the start time and timezone from the lists.
4. Click **Confirm**.



Choose your update method

○ As soon as new update is available

● Set a maintenance start time:

As part of the update the Connector Appliance becomes temporarily unavailable. Automatic update only updates one Connector Appliance in a resource location at a time. For this reason, it is important to 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 accepted.

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.com`
- `https://*.citrixworkspacesapi.net`
- `https://*.citrixnetworkapi.net`
- `https://*.nssvc.net`
- `https://*.servicebus.windows.net`
- `https://iwsprodeastusuniconacr.azurecr.io`
- `https://iwsprodeastusuniconacr.eastus.data.azurecr.io`

System requirements

The Connector Appliance is supported on the following hypervisors:

- Citrix XenServer 7.1 CU2 LTSR
- Citrix Hypervisor 8.2 LTSR
- VMware ESXi version 6.5
- Hyper-V on Windows Server 2016 or Windows Server 2019
- Microsoft Azure
- AWS
- Google Cloud Platform

Your hypervisor must provide the following minimum capabilities:

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

Ensure that your environment has the following configuration:

- The network allows the Connector Appliance to use DHCP to get DNS servers, an IP address, a host name, and a domain name.
- 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.
- The hypervisor clock is set to Coordinated Universal Time (UTC) and is synchronized with a time server.
- If you use a proxy with Connector Appliance, the proxy must be unauthenticated or use basic authentication.

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.

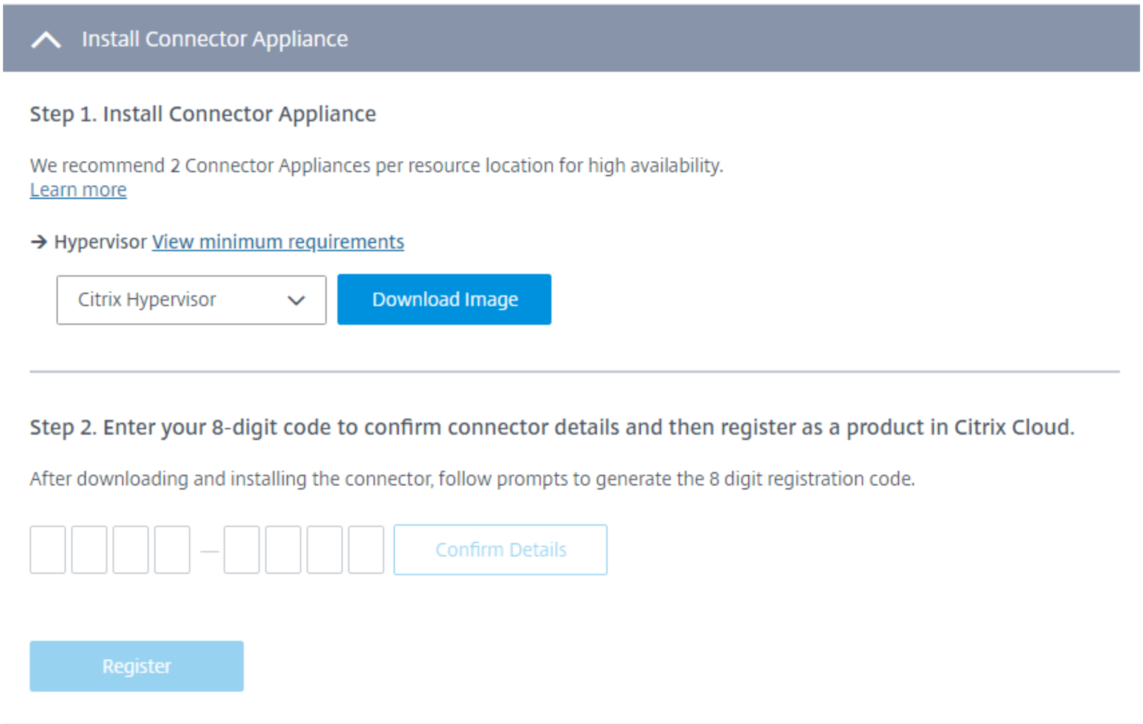
> **Note:**
>
> Cloning, suspending, and taking snapshots of the Connector Appliance VM are not supported.

Obtain the Connector Appliance

Download the Connector Appliance software from within Citrix Cloud.

1. Sign in to Citrix Cloud.
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 **Install Connector Appliance** task opens.

   Install Connector Appliance

   Step 1. Install Connector Appliance

   We recommend 2 Connector Appliances per resource location for high availability.
   Learn more

   → Hypervisor View minimum requirements

   Citrix Hypervisor

   Step 2. Enter your 8-digit code to confirm connector details and then register as a product in Citrix Cloud.

   After downloading and installing the connector, follow prompts to generate the 8 digit registration code.

5. From the **Hypervisor** list in **Step 1**, choose the type of hypervisor that you use to host your Connector Appliance. Click **Download Image**.
6. Review the Citrix End User Service Agreement and, if you agree, select **Agree and Continue**.
7. When prompted, save the provided Connector Appliance file.

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

8. 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

The XVA, OVA, or ZIP file you downloaded from Citrix Cloud contains a self-contained Connector Appliance that you can host on your hypervisor.

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

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 and continue the installation 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.

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**.
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 and continue the installation 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: 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 use to identify your Connector Appliance in the **Name** field. Click **Next**.
8. On the **Specify Generation** panel, select Generation 1. Click **Next**.
9. On the **Assign Memory** panel:

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

   Click *Next*.
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, go to **Hardware > Processors**. Change the value for **Number of virtual processors** to 2. Click **Apply**, then **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 and continue the installation 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.
3. Extract the contents of the ZIP file: A PowerShell script and a VHDX file.
4. In a PowerShell console, change the 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 press 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 press Enter to accept the default value of `connector-appliance.vhdx`.
8. When prompted, select the switch to use. Press Enter.
9. Review the summary of the VM import information. If the information is correct, press 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 continue the installation 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 VM by using the included PowerShell script.

The `connector-appliance.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 directory to where the ZIP file contents are located and run the following command:

   ```
   .\connector-appliance-upload.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 and continue the installation process.

Next step: Register your Connector Appliance with Citrix Cloud.

AWS

This section describes how to deploy Connector Appliance in AWS. You can deploy the VM 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 target, select the **NAT Gateway** you created from the list.
    f) Click **Save change**.
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.
    1 In the display page, go to the **Subnet Associations** tab.
    1 Click **Edit subnet associations**.
    c) Select the subnetor subnets to attach to the route table.
    d) Click **Save Associations**.

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/vmie_prereqs.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 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 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.

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 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 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 and continue the installation 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.

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/vmie_prereqs.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 directory to the folder where the extracted files are located and run the following command:

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

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 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 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.

Google Cloud Platform

This section describes how to deploy Connector Appliance on the Google Cloud Platform.

The file `connector-appliance-gcp.zip` contains the file `connector-appliance.tar.gz`, which is the disk image of the Connector Appliance, and a PowerShell script that can be used to automatically deploy the Connector Appliance.

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**.
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 just 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 continue the installation 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 continue the installation process. For more information, see https://cloud.google.com/compute/docs/instances/connecting-advanced#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 Google Cloud SDK installed on your system.

1. On your local system, extract the contents of `connector-appliance-gcp.zip` to a folder.
2. In PowerShell, change 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.

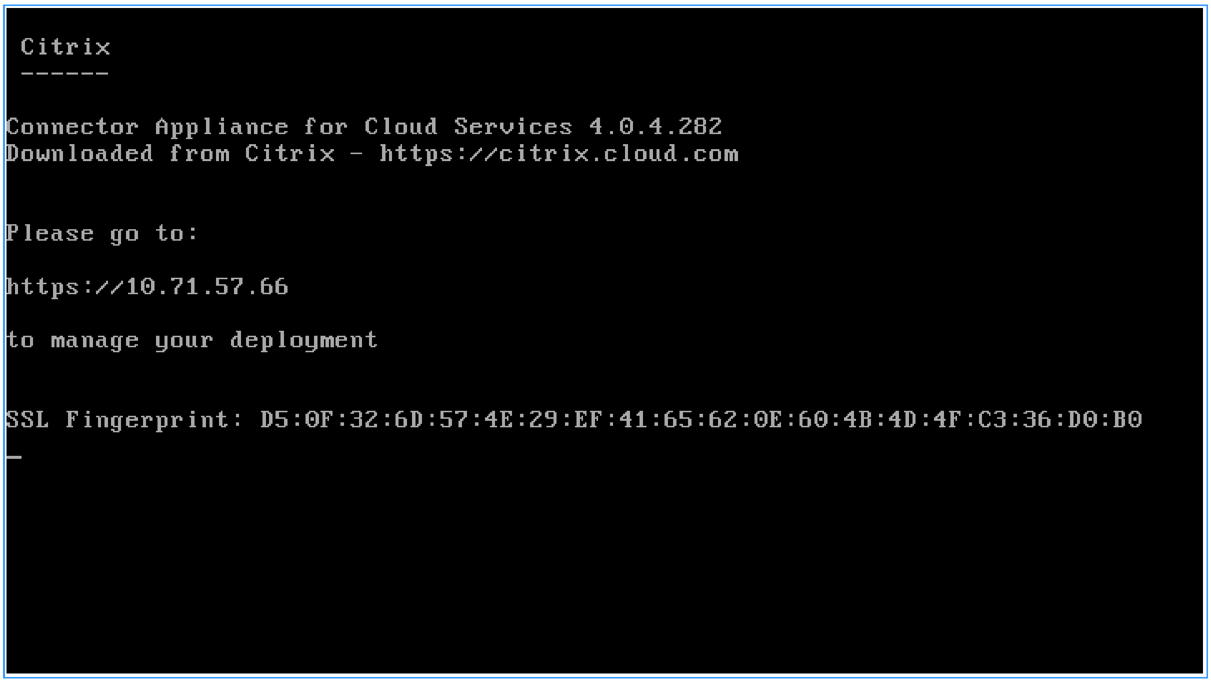
Use a bastion host to go to the Connector Appliance administration page at the internal IP address from your browser and continue the installation process. For more information, see https://cloud.google.com/compute/docs/instances/connecting-advanced#bastion_host.

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.

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.



```
 Citrix
 ------

Connector Appliance for Cloud Services 4.0.4.282
Downloaded from Citrix - https://citrix.cloud.com


Please go to:

https://10.71.57.66

to manage your deployment


SSL Fingerprint: D5:0F:32:6D:57:4E:29:EF:41:65:62:0E:60:4B:4D:4F:C3:36:D0:B0
_
```

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

   The Connector Appliance UI uses a self-signed certificate. 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.

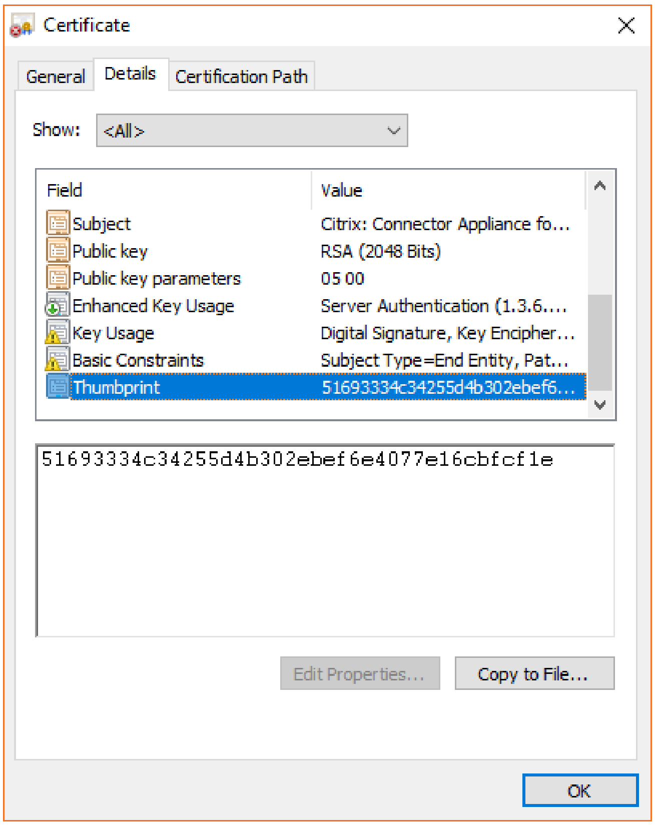
   For example, in the Google Chrome browser, complete the following steps:

   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.



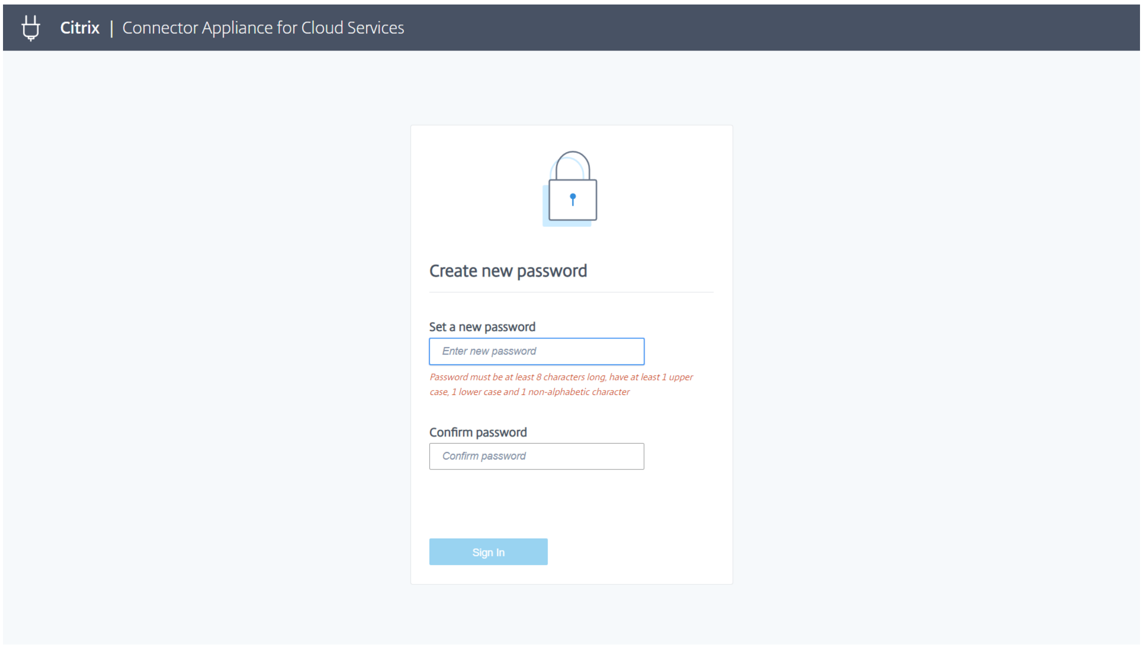
Field	Value
Subject	Citrix: Connector Appliance fo…
Public key	RSA (2048 Bits)
Public key parameters	05 00
Enhanced Key Usage	Server Authentication (1.3.6.…
Key Usage	Digital Signature, Key Encipher…
Basic Constraints	Subject Type=End Entity, Pat…
Thumbprint	51693334c34255d4b302ebef6…

```
51693334c34255d4b302ebef6e4077e16cbfcf1e
```

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**.



Password must be at least 8 characters long, have at least 1 upper case, 1 lower case and 1 non-alphabetic character

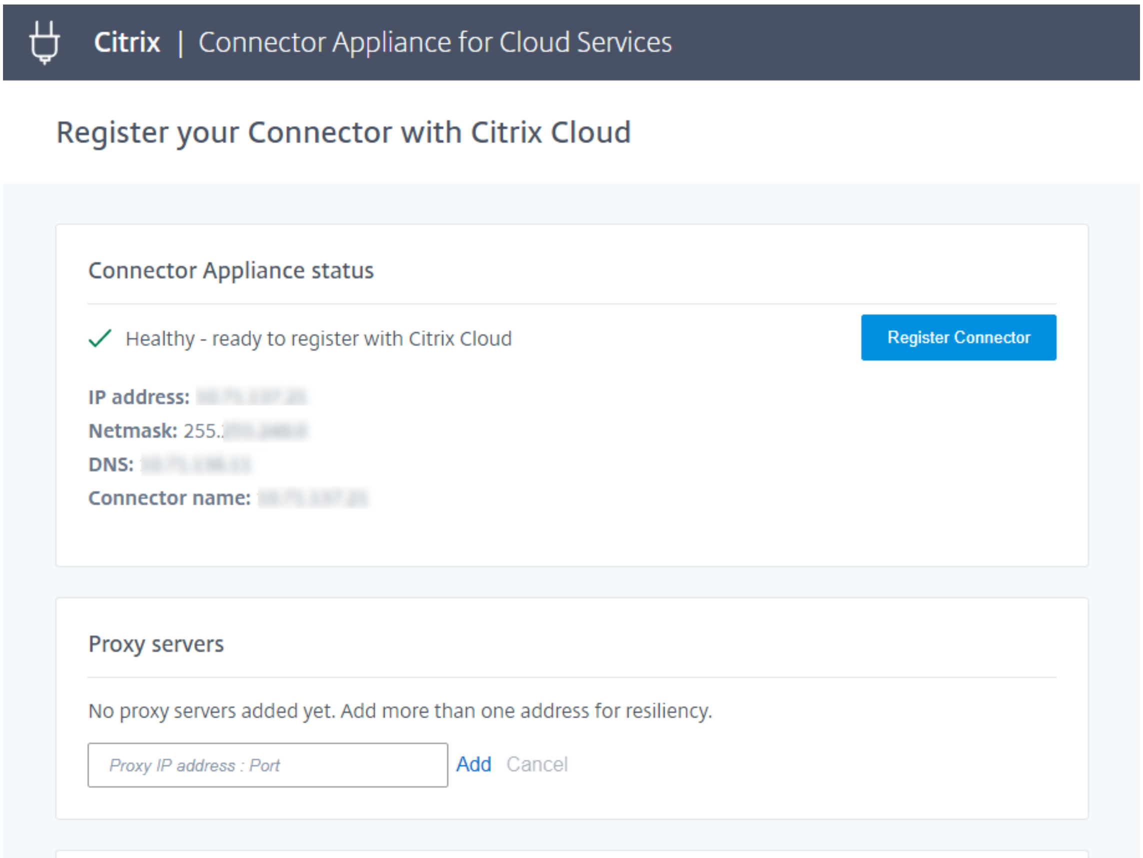
The password you set must meet the following requirements:

- 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 just set.

   The **Connector Appliance administration page** opens.



Citrix | Connector Appliance for Cloud Services

Register your Connector with Citrix Cloud

Connector Appliance status

✓ Healthy - ready to register with Citrix Cloud

IP address: [redacted]
Netmask: 255.[redacted]
DNS: [redacted]
Connector name: [redacted]

Proxy servers

No proxy servers added yet. Add more than one address for resiliency.

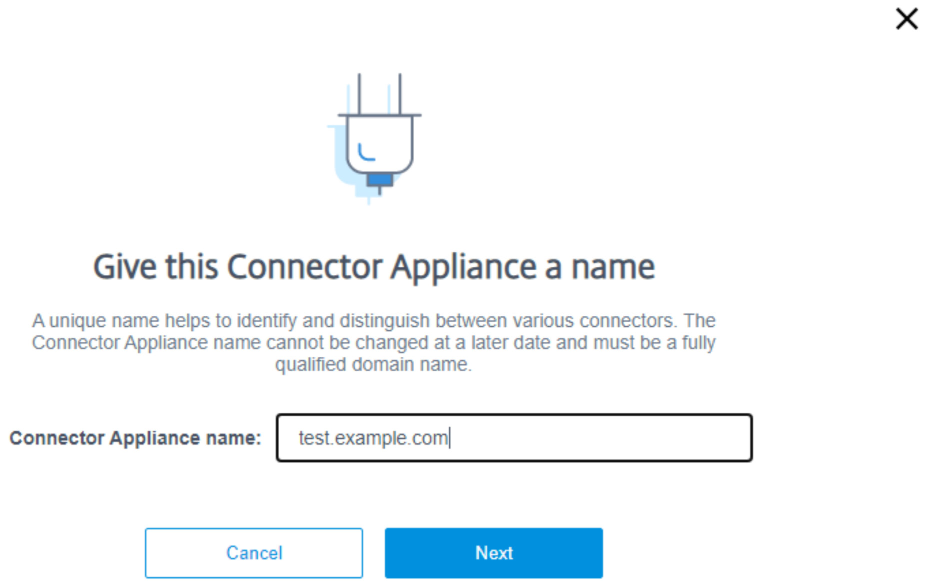
5. (Optional) If you use one or more web proxies, you can add the proxy addresses here. Both unauthenticated and authenticated proxies are supported. To add an unauthenticated proxy, provide a valid **Proxy IP Address and Port**. To add an authenticated proxy, provide a valid **Username** and **Password**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

   > **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. Click **Register Connector** to open the registration task.
7. 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**.

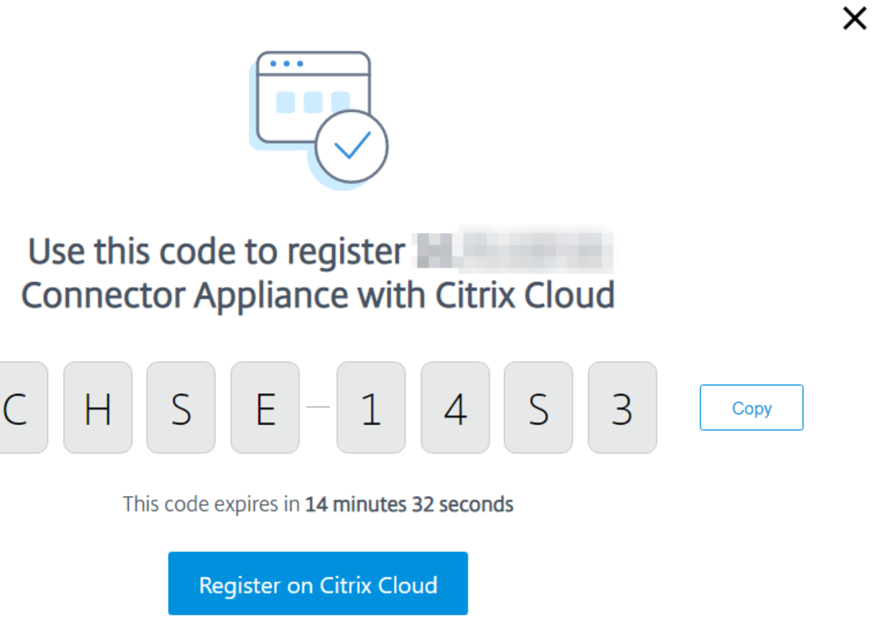
   

   Give this Connector Appliance a name

   A unique name helps to identify and distinguish between various connectors. The Connector Appliance name cannot be changed at a later date and must be a fully qualified domain name.

   Connector Appliance name: test.example.com

   The webpage provides a code to use to register with Citrix Cloud. This code expires in 15 minutes.

   Use this code to register [redacted] Connector Appliance with Citrix Cloud

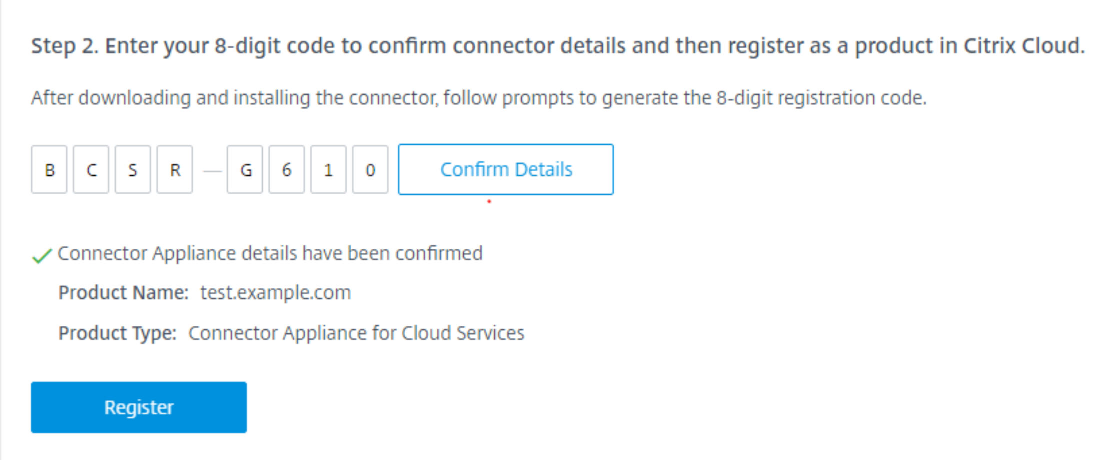
   C H S E – 1 4 S 3

   This code expires in **14 minutes 32 seconds**

8. Use the **Copy** button to copy the code to the clipboard.

9. Return to the **Resource Locations** webpage.
10. 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.

    Step 2. Enter your 8-digit code to confirm connector details and then register as a product in Citrix Cloud.

    After downloading and installing the connector, follow prompts to generate the 8-digit registration code.

    B C S R — G 6 1 0

    ✓ Connector Appliance details have been confirmed

    Product Name: test.example.com

    Product Type: Connector Appliance for Cloud Services

11. Click **Register**.

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

12. 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.

After registering your Connector Appliance

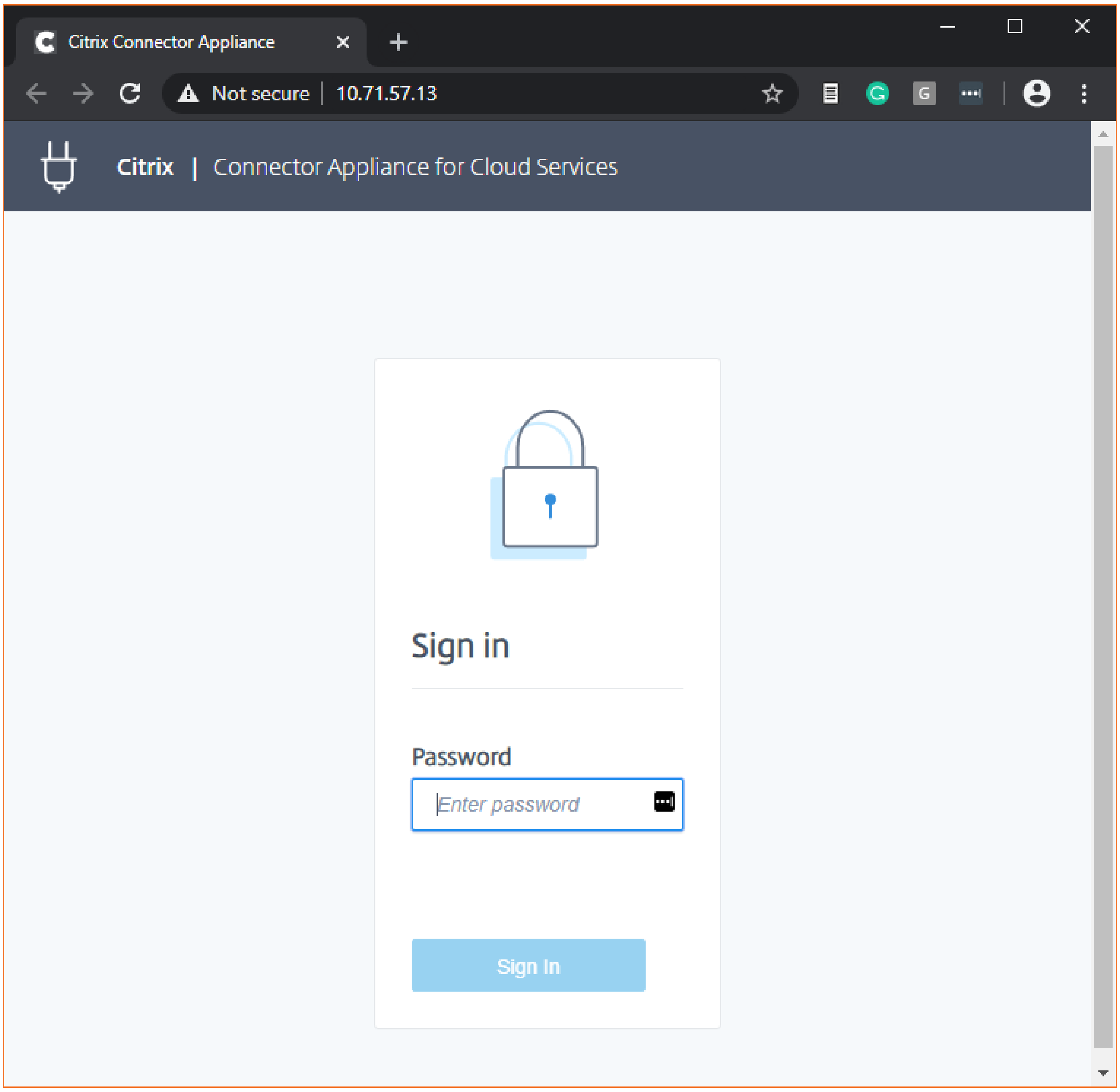
For each resource location, we advise that you install and register two or more Connector Appliances. This configuration ensures continuous availability and enables the connectors to balance the load.

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.

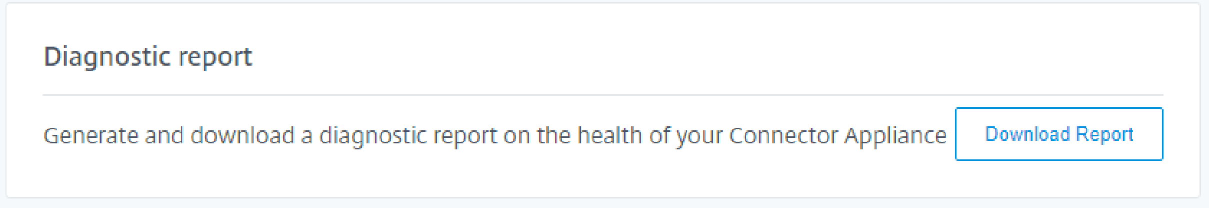
Do not clone, suspend, or take a snapshot of your Connector Appliance VMs. These actions are not supported.

You are only presented with the **Create new password** page the first time you connect to the Connector Appliance UI. On subsequent connections to the UI, you are asked to input the password you set when registering the Connector Appliance.


Citrix Connector Appliance
Not secure
10.71.57.13
Citrix | Connector Appliance for Cloud Services
Sign in
Password
Enter password
Sign In

Generating a diagnostic report

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



Diagnostic report

Generate and download a diagnostic report on the health of your Connector Appliance

1. From the Connector Appliance console in your hypervisor, copy the IP address to your browser address bar.

2. Enter the password 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.

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 on your account name in the header bar and select **Network Diagnostics**.
2. (Optional) In the **TCP Capture** section, enter the enter the target IP address, hostname, 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 just capture the headers for diagnosis. This best-effort approach captures the first 94 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.

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.

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:

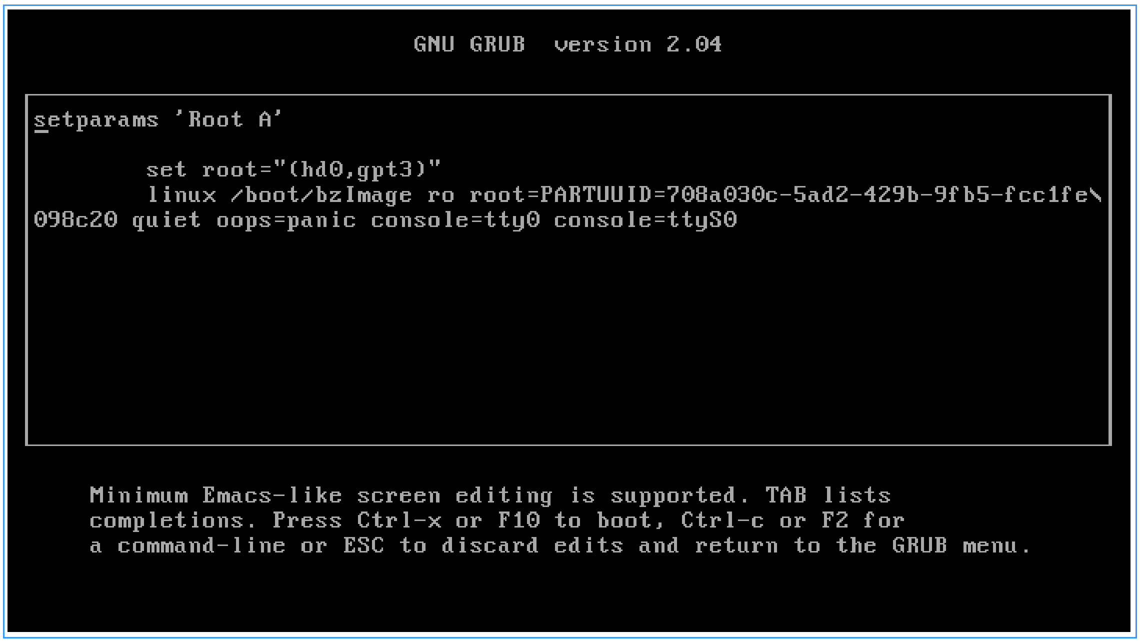
1. In your hypervisor, restart the Connector Appliance.

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:



```
                          GNU GRUB  version 2.04

setparams 'Root A'

        set root="(hd0,gpt3)"
        linux /boot/bzImage ro root=PARTUUID=708a030c-5ad2-429b-9fb5-fcc1fe\
098c20 quiet oops=panic console=tty0 console=ttyS0




     Minimum Emacs-like screen editing is supported. TAB lists
     completions. Press Ctrl-x or F10 to boot, Ctrl-c or F2 for
     a command-line or ESC to discard edits and return to the GRUB menu.
```

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>
    <!--NeedCopy-->
    ```

    Replace the placeholder values with the values for your configuration.

6. Press **Ctrl+X** to start the Connector Appliance with the new configuration.

Connector updates

July 30, 2021

Periodically, Citrix releases updates to increase the performance, security, and reliability of the Cloud Connector or Connector Appliance. By default, Citrix Cloud installs updates on each connector, one at a time, as soon as these updates become available. To ensure updates are installed timely without unduly affecting your users' Citrix Cloud experience, you can schedule these updates for a preferred time of day and a preferred day of the week. You can also verify your connectors are up-to-date by comparing the current connector version in your resource location with the target version in Citrix Cloud.

Preferred time of day

When you specify a preferred time of day, Citrix Cloud installs updates 24 hours after they become available, at your preferred time. For example, if your preferred time of day is 2:00 AM US Pacific time and an update becomes available on Tuesday, Citrix Cloud waits for 24 hours and then installs the update at 2:00 AM the next day.

Preferred day of the week

When you specify a preferred day of the week, Citrix Cloud waits for seven days before installing updates on your preferred day. This seven-day waiting period gives you enough time to choose whether to install the update on demand or wait for Citrix Cloud to install it on your preferred day. Depending on the day of the week you select and the day on which updates become available, Citrix Cloud might wait to install updates for up to 13 days.

Example of an 8-day waiting period

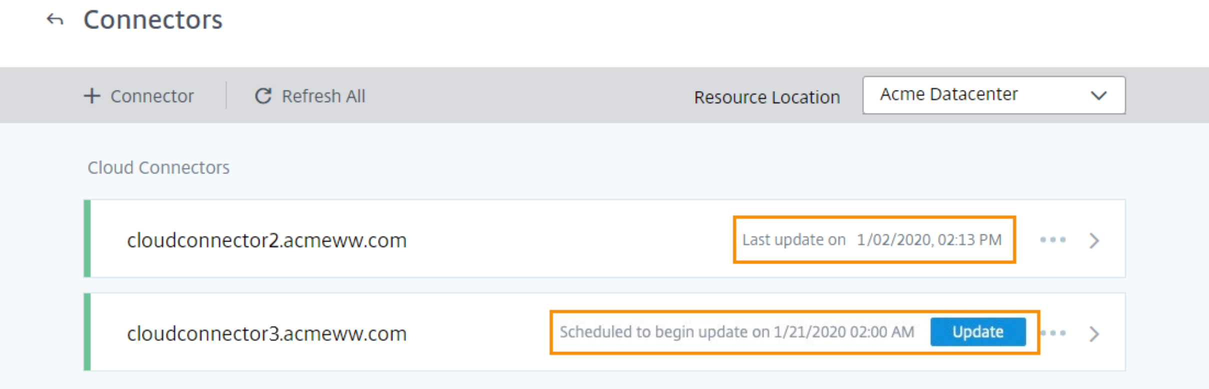
On Monday, you configure Tuesdays at 6:00 PM as your preferred day for updates. Later that day, Citrix Cloud notifies you that there's an update available and displays the **Update** button. If you don't initiate the update, Citrix Cloud waits for seven days and then installs the update the next day, on Tuesday at 6:00 PM.

Example of a 13-day waiting period

You configured Mondays at 6:00 PM as your preferred time of day for updates. On Tuesday, Citrix Cloud notifies you that there's an update available and displays the **Update** button. If you don't initiate the update, Citrix Cloud waits for seven days and then installs the update six days later, on Monday at 6:00 PM.

Update notifications and on-demand updates

When updates are available, Citrix Cloud informs you with an alert in your Notifications. Also, each connector displays the date and time when the update will be installed.

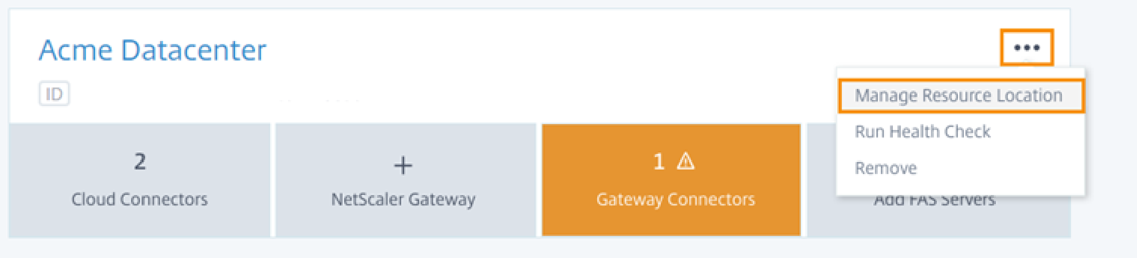

Connectors
+ Connector
Refresh All
Resource Location
Acme Datacenter
Cloud Connectors
cloudconnector2.acmeww.com
Last update on 1/02/2020, 02:13 PM
cloudconnector3.acmeww.com
Scheduled to begin update on 1/21/2020 02:00 AM
Update

After Citrix Cloud notifies you of an available update, each connector displays an **Update** button so you can install the update sooner than your preferred time or day. After you select **Update** for each connector, Citrix Cloud queues the updates and installs them one at a time. You can't cancel updates after you initiate them.

After the update finishes, Citrix Cloud displays the date of the last update. If some updates cannot be completed, a notification is sent informing you.

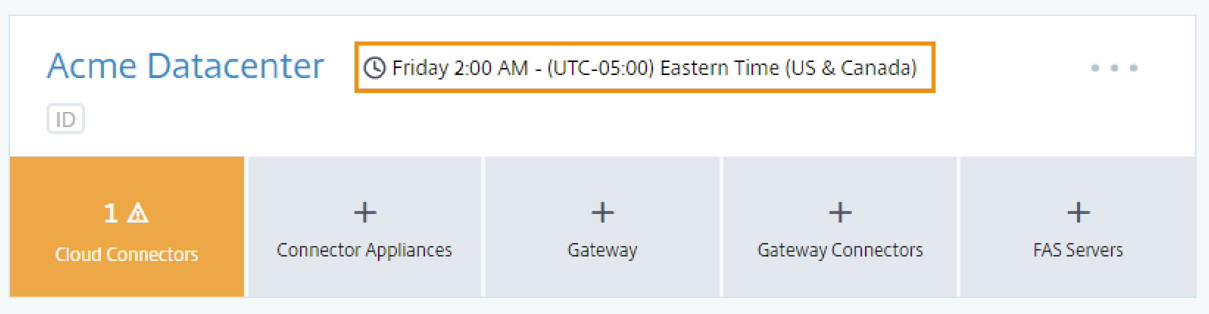
Choose an update schedule

1. From the Citrix Cloud menu, select **Resource Locations**.
2. Locate the resource location you want to modify and, from the ellipsis menu, select **Manage Resource Location**.

3. Under **Choose your update method**, select **Set a maintenance start time** and choose the preferred day, time, and timezone for installing updates.
   - To specify only a preferred time of day, select the hour and timezone that you want updates to be installed. Citrix Cloud installs updates 24 hours after they become available, at your preferred time.
   - To specify a preferred day of the week, select the hour, day, and timezone. Citrix Cloud waits for seven days after updates become available before installing them on your preferred day.

After you configure your update schedule, Citrix Cloud displays it next to the resource location name.



The start time you select is applied to all connectors regardless of the timezone in which they are located. If you have connectors in different timezones, Citrix Cloud installs updates at your selected time and timezone. For example, if you schedule updates for 2:00 AM in the US Pacific timezone, and you have connectors in London, Citrix Cloud starts to install the update on those connectors at 2:00 AM US Pacific time.

> **Note:**
>
> If the connector experiences an issue during update installation, the installation pauses until the issue is resolved. Because updates are installed on each connector, one at a time, a paused update on one connector can prevent updates on all remaining Cloud Connectors in your Citrix Cloud account.

Unscheduled updates

Even if you choose a preferred time or day for installing updates, Citrix Cloud might still install an update as soon as possible after it becomes available. Unscheduled updates occur when:

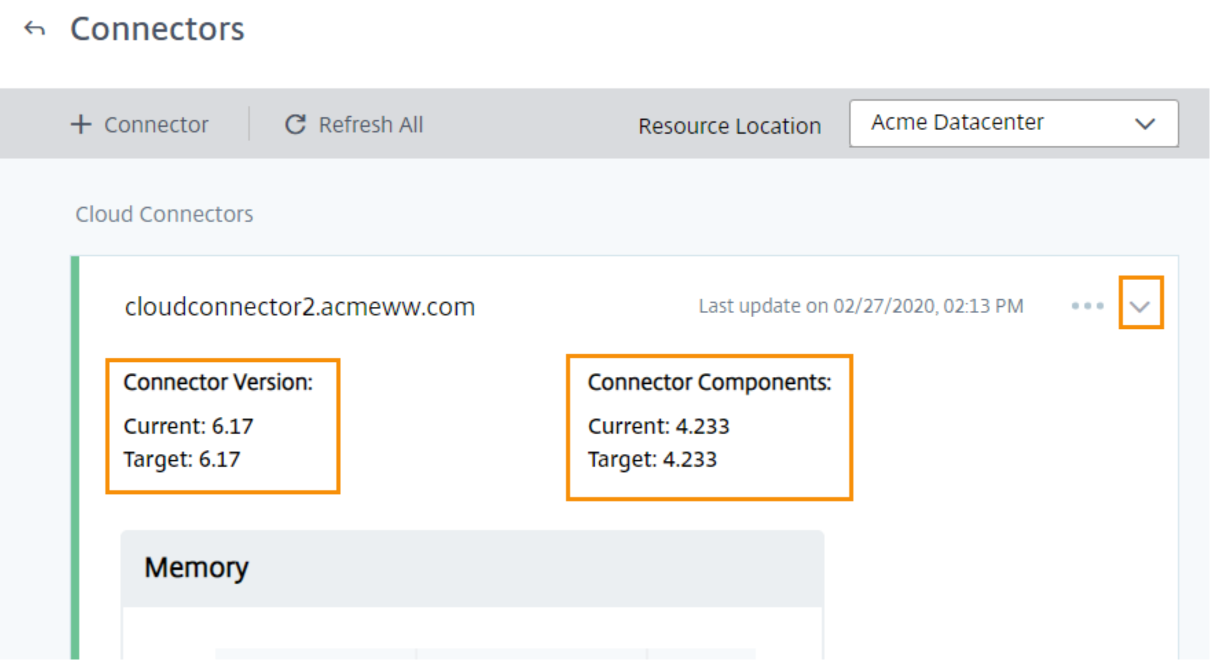
- The update can't be installed at the preferred time within 48 hours of its availability. For example, if your preferred time is 2:00 AM and the connector is offline for three days following the update release, Citrix Cloud installs the update immediately when the connector is back online.
- The update contains a fix for a critical security or feature issue.

Compare Cloud Connector versions

You can check to see which version of the Cloud Connector is running in your resource location and whether it's the latest version. This information helps you verify that the Cloud Connector is updating successfully.

> **Note:**
>
> This information is not available for Connector Appliances.

From the **Resource Locations** page, select the **Cloud Connectors** tile for the resource location you want to manage. Then, expand the tile for the Cloud Connector.



Connector Version:

Current: 6.17
Target: 6.17

Connector Components:

Current: 4.233
Target: 4.233

The **Current** version number is the version of the Cloud Connector software currently running on the Cloud Connector machine. The **Target** version number is the latest version of the Cloud Connector software that Citrix released. If the machine was updated successfully, the Current and Target version numbers match.

Troubleshooting update failures

Conflicting software installed on your Cloud Connector machine or unexpected errors during maintenance can result in the Cloud Connector failing to update and service outages. For information on dealing with a failed update following Cloud Connector maintenance, visit Resolve a Failed Cloud Connector Maintenance.

If the Cloud Connector isn't updating successfully, you can start troubleshooting issues by verifying the following conditions:

- The Cloud Connector is powered on and connected to Citrix Cloud using the Cloud Connector Connectivity Check utility.
- Proxy and firewalls are configured correctly.
- Required Windows services are in the Started state.
- Advanced logging is enabled on the Cloud Connector.

For instructions for troubleshooting Cloud Connector update failures, see CTX270718 in the Citrix Support Knowledge Center.

For troubleshooting assistance, you can send Citrix Cloud Connector logs to Citrix. For information, see Log Collection for Citrix Cloud Connector.

Identity and access management

September 24, 2021

Identity and Access Management defines the identity providers and accounts used for Citrix Cloud administrators and workspace subscribers.

Identity providers

Identity providers supported for Citrix Cloud can be used to authenticate Citrix Cloud administrators, workspace subscribers, or both.

Identity provider	Administrators	Subscribers
Citrix identity provider	Yes	No
On-premises Active Directory	No	Yes
Active Directory plus token	No	Yes
Azure Active Directory	Yes	Yes
Citrix Gateway	No	Yes
Okta	No	Yes
SAML 2.0	No	Yes

By default, Citrix Cloud uses the Citrix identity provider to manage your Citrix Cloud account. Citrix identity provider authenticates Citrix Cloud administrators only.

You can add the following identity providers to your Citrix Cloud account:

- On-premises Active Directory. For authenticating workspace subscribers only.
- Active Directory plus token. For authenticating workspace subscribers only.
- Azure Active Directory. For authenticating Citrix Cloud administrators and workspace subscribers.
- Citrix Gateway. For authenticating workspace subscribers only.
- Okta. For authenticating workspace subscribers only.
- SAML 2.0. For authenticating workspace subscribers only.

Citrix Cloud also supports using the Citrix Federated Authentication Service to provide single sign-on access for workspace subscribers. For more information, see Enable single sign-on for workspaces with Citrix Federated Authentication Service.

> **Tip:**
>
> Learn more about supported identity providers with the Introduction to Citrix Identity and Authentication education course. Each module provides short videos that walk you through connecting each identity provider to Citrix Cloud and enabling authentication for Citrix Workspace.

Administrators

Administrators use their identity to access Citrix Cloud, 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.

Add new administrators

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

To invite other administrators and define their access to Citrix Cloud, see Manage Citrix Cloud administrators.

Reset your password

If you forget or want to reset your password, click **Forgot your username or password?** on the Citrix Cloud sign in page. After you enter your email address or username to find your account, Citrix sends you an email with a link to reset your password.

Citrix requires you to reset your password under certain conditions to help you keep your account password safe and secure. For more information about these conditions, see Changing your password.

> **Note:**
>
> Add **customerservice@citrix.com** to your list of allowed email addresses to ensure that Citrix Cloud emails don't land in your spam or trash folders.

Remove administrators

You can remove administrators from your Citrix Cloud account on the **Administrators** tab. When you remove an administrator, they can no longer sign-in to Citrix Cloud.

If an administrator is logged in when you remove the account, the administrator stays active for a maximum of one minute. Afterward, access to Citrix Cloud is denied.

> **Note:**
>
> - If there's only one administrator in the account, you can't remove that administrator. Citrix Cloud requires at least one administrator for each customer account.
> - Citrix Cloud Connectors are not linked to administrator accounts. So, Cloud Connectors continue operating even if you remove the administrator who installed them.

Subscribers

A subscriber's identity defines the services to which they have access in Citrix Cloud. 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 Citrix Cloud Connectors in each forest. Citrix recommends at least two Citrix Cloud Connectors to maintain a high availability environment. For more information about deploying Cloud Connectors in Active Directory, see Deployment scenarios for Cloud Connectors in Active Directory.

> **Note:**
>
> - Disabling domains prevents new identities only from being selected. It does not prevent subscribers from using identities that are already allocated.
> - Each Citrix 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 after you assign the group to an offering.

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

Primary resource locations

A primary resource location is a resource location that you designate as "most preferred" for communications between your domain and Citrix Cloud. For your primary resource locations, select the resource location that has Citrix Cloud Connectors that have the best performance and connectivity to your domain. Making this resource location your primary resource location enables your users to log on quickly to Citrix Cloud.

For more information, see Select a primary resource location.

Connect Active Directory to Citrix Cloud

September 25, 2021

Citrix Cloud supports using your on-premises Active Directory (AD) to authenticate workspace subscribers. Also, some workspace authentication methods require a connection between your AD and Citrix Cloud. For more information, see Change authentication to workspaces.

Citrix Cloud also supports using tokens as a second factor of authentication for subscribers signing in to their workspaces through Active Directory. Workspace subscribers can generate tokens using any app that follows the Time-Based One-Time Password standard, such as Citrix SSO.

For more information about authenticating workspace subscribers with Active Directory plus tokens, see Active Directory plus token.

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

Active Directory authentication

Connecting your Active Directory to Citrix Cloud involves installing Cloud Connectors in your domain. Citrix recommends installing at least two Cloud Connectors for high availability. For more information, see the following articles:

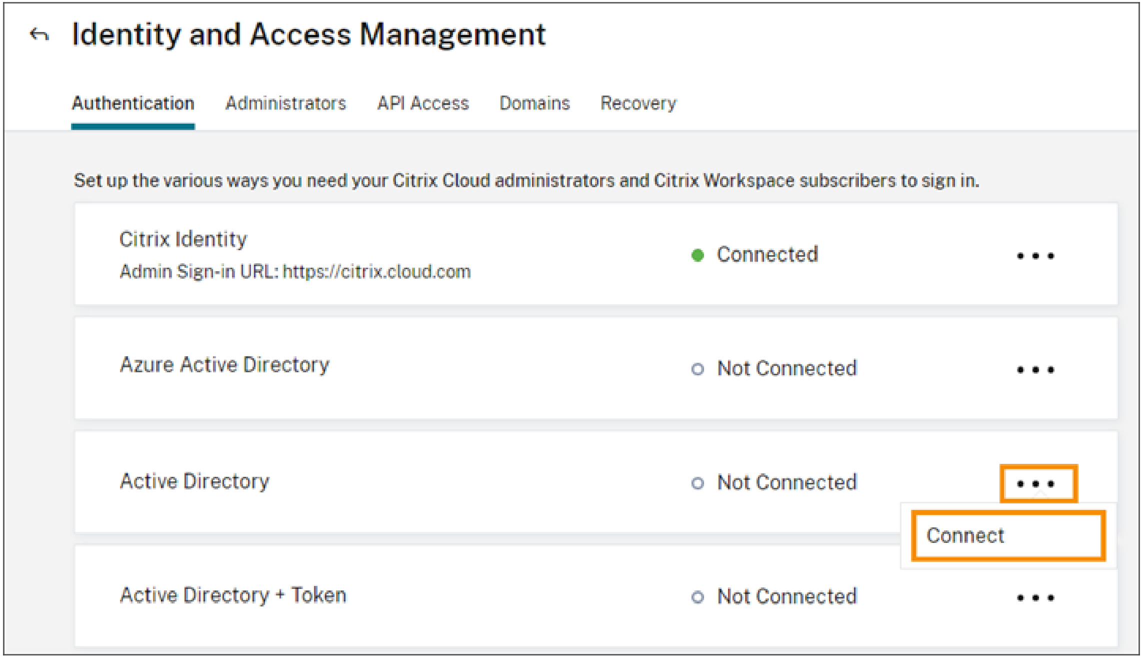
- Cloud Connector Technical Details: For system requirements and deployment recommendations.
- Cloud Connector Installation: For installation instructions using either the graphical interface or the command line.

Connecting your Active Directory to Citrix Cloud involves the following tasks:

1. Install Cloud Connectors in your domain. Citrix recommends installing two Cloud Connectors for high availability.
2. If applicable, enable tokens for user devices. Subscribers can enroll only one device at a time.

To connect your Active Directory to Citrix Cloud

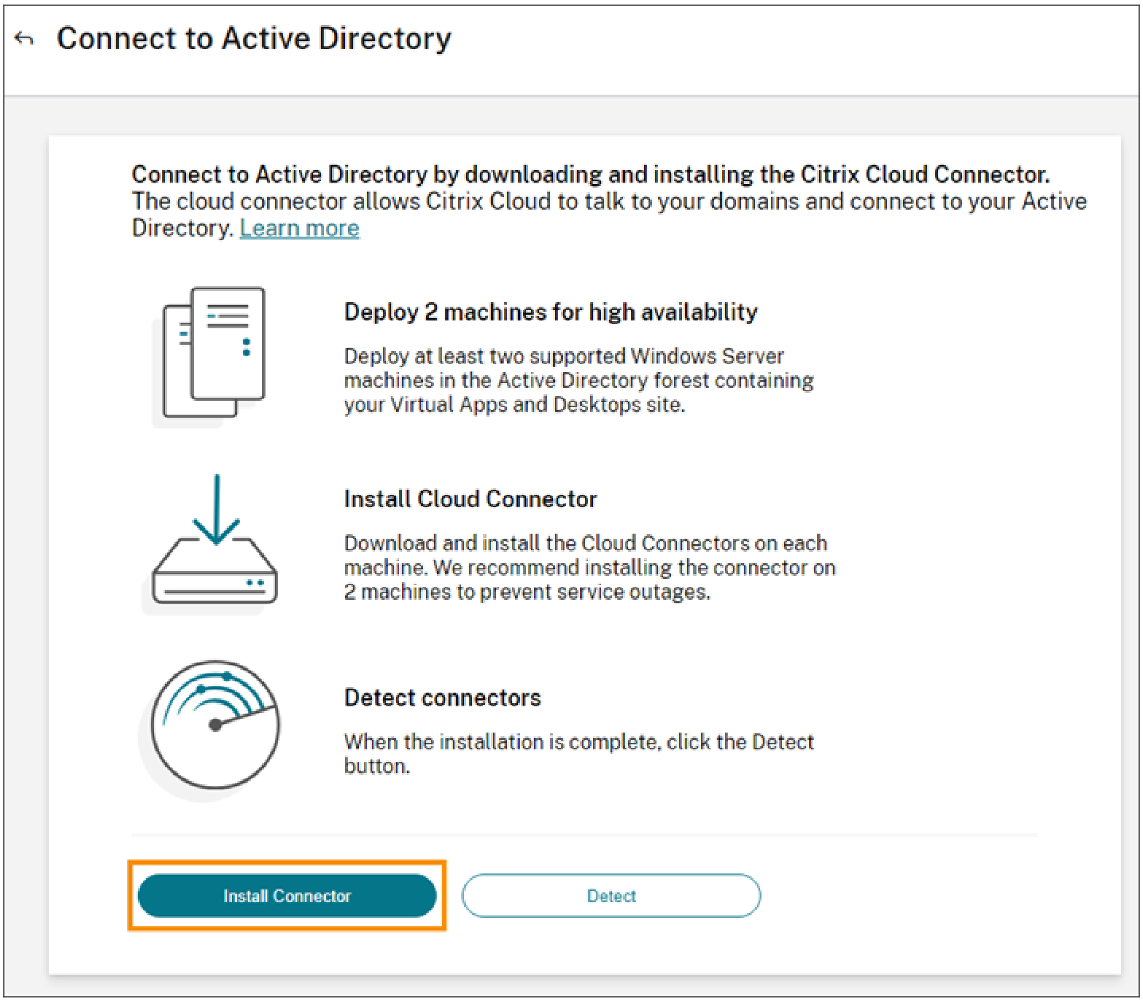
1. From the Citrix Cloud menu, select **Identity and Access Management**.
2. From the **Authentication** tab, in **Active Directory**, click the ellipsis menu and select **Connect**.



Set up the various ways you need your Citrix Cloud administrators and Citrix Workspace subscribers to sign in.

Citrix Identity Admin Sign-in URL: https://citrix.cloud.com	● Connected	•••
Azure Active Directory	○ Not Connected	•••
Active Directory	○ Not Connected	•••
Active Directory + Token	○ Not Connected	•••

3. Click **Install Connector** to download the Cloud Connector software.



Connect to Active Directory

Connect to Active Directory by downloading and installing the Citrix Cloud Connector. The cloud connector allows Citrix Cloud to talk to your domains and connect to your Active Directory. Learn more

Deploy 2 machines for high availability

Deploy at least two supported Windows Server machines in the Active Directory forest containing your Virtual Apps and Desktops site.

Install Cloud Connector

Download and install the Cloud Connectors on each machine. We recommend installing the connector on 2 machines to prevent service outages.

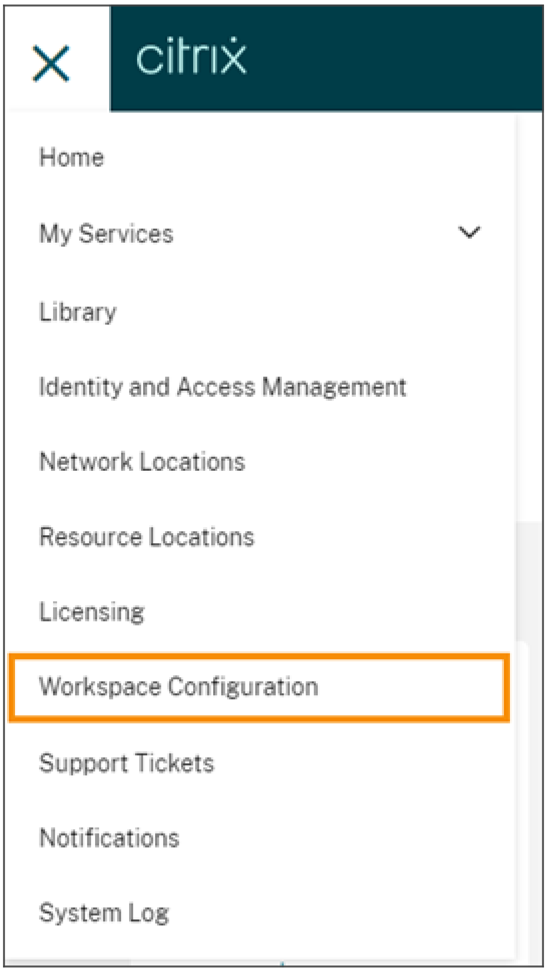
Detect connectors

When the installation is complete, click the Detect button.

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.

To enable Active Directory plus token authentication

1. Perform Steps 1–5 as described in To connect your Active Directory to Citrix Cloud.
2. After Citrix Cloud verifies the connection with your Active Directory, click **Next**. The **Configure Token** page appears and the **Single device** option is selected by default.
3. Click **Save and Finish** to complete the configuration. On the **Authentication** tab, the **Active Directory + Token** entry is marked as **Enabled**.
4. Enable token authentication for workspaces:
   a) From the Citrix Cloud menu, select **Workspace Configuration**.



b) From the **Authentication** tab, select **Active Directory + Token**.

After enabling Active Directory plus token authentication, Workspace subscribers can register their device and use an authenticator app to generate tokens. Subscribers can register only one device at a time. For instructions to register subscribers' devices, see Register devices for two-factor authentication.

For options to re-enroll subscribers' devices, see To re-enroll devices.

Connect Azure Active Directory to Citrix Cloud

September 15, 2021

Citrix Cloud supports using Azure Active Directory (AD) to authenticate Citrix Cloud administrators and workspace subscribers.

By using Azure AD with Citrix Cloud, you can:

- Leverage 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're signing in at the right place.
- Use federation to an identity provider of your choice including ADFS, Okta, and Ping, among others.

Azure AD app and permissions

Citrix Cloud includes an Azure AD app that allows Citrix Cloud to connect with Azure AD without the need for you to be logged in to an active Azure AD session. As of August 2018, this app was upgraded to improve performance and allow you to be ready for future releases. If you previously connected your Azure AD to Citrix Cloud (before August 2018), you might need to update your Azure AD connection in Citrix Cloud. For more information, see Reconnect to Azure AD for the upgraded app in this article.

For more information about the Azure AD applications and permissions that Citrix Cloud uses to connect with your Azure AD, see Azure Active Directory permissions for Citrix Cloud.

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

Prepare your Active Directory and Azure AD

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

- You have a Microsoft Azure account. Every Azure account comes with Azure AD free of charge. If you don't have an Azure account, sign up at https://azure.microsoft.com/en-us/free/?v=17.36.
- You have the Global Admin role in Azure AD. This role is required to give Citrix Cloud your consent to connect with Azure AD.
- Administrator accounts have their "mail" property configured in Azure AD. To do this, you can sync accounts from your on-premises Active Directory into Azure AD using Microsoft's Azure AD Connect tool. Alternatively, you can configure non-synced Azure AD accounts with Office 365 email.

Sync accounts with Azure AD Connect

1. Ensure that the Active Directory accounts have the Email user property configured:

   a) Open Active Directory Users and Computers.
   b) In the **Users** folder, locate the account you want to check, right-click and select **Properties**. On the **General** tab, verify the **Email** field has a valid entry. Citrix Cloud requires that administrators added from Azure AD have different email addresses than administrators who sign in using a Citrix-hosted identity.
2. Install and configure Azure AD Connect. For complete instructions, see Getting started with Azure AD Connect using express settings on the Microsoft Azure website.

Connect Citrix Cloud to Azure AD

When connecting your Citrix Cloud account to your Azure AD, Citrix Cloud needs permission to access your user profile (or the profile of the signed-in user) in addition to 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. For more information about the application permissions that Citrix Cloud requests, see Azure Active Directory permissions for Citrix Cloud.

> **Important:**
>
> You must be a Global Admin in Azure AD to complete this task.

1. Sign in to Citrix Cloud at https://citrix.cloud.com.
2. Click the menu button in the top-left corner of the page and select **Identity and Access Management**.
3. Locate Azure Active Directory and select **Connect** from the ellipsis menu.
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.
5. When prompted, sign in to the Azure account with which you want to connect. Azure shows you the permissions that Citrix Cloud needs to access the account and acquire the information required for connection. Most of these permissions are read-only and allow Citrix Cloud to gather basic information from your Microsoft Graph such as groups and user profiles. If you integrated Citrix Endpoint Management or XenMobile Server with Microsoft Intune, you must grant Microsoft Intune-related read-write permissions. For more information, see Azure Active Directory Permissions for Citrix Cloud.
6. Click **Accept** to accept the permissions request.

Add administrators to Citrix Cloud from Azure AD

1. In Citrix Cloud, 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 Manage Citrix Cloud administrators. Citrix Cloud 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.

Sign in to Citrix Cloud using Azure AD

After the Azure AD user accounts are connected, users can sign in to Citrix Cloud 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.com/go/mycompany`
- From the Citrix Cloud sign-in page, click **Sign in with my company credentials**., type the identifier you created when you initially connected Azure AD (for example, "mycompany"), and click **Continue**.

Enable Azure AD authentication for workspaces

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

> **Important:**
>
> Before enabling Azure AD workspace authentication, review the Azure Active Directory section for considerations for using Azure AD with workspaces.

1. In Citrix Cloud, click the menu button in the top-left corner and select **Workspace Configuration**.
2. From the **Authentication** tab, select **Azure Active Directory**.
3. Click **Confirm** to accept the workspace experience changes that will occur when Azure AD authentication is enabled.

Enable advanced Azure AD capabilities

Azure AD provides advanced multifactor 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 to leverage those capabilities automatically.

To compare Azure AD service level capabilities and pricing, see https://azure.microsoft.com/en-us/pricing/details/active-directory/.

Reconnect to Azure AD for the upgraded app

If you've previously connected your Azure AD to Citrix Cloud (before May 2019), Citrix Cloud might not be using the most current app to connect with Azure AD. As a result, Citrix Cloud might prompt you to reconnect your Azure AD and grant additional permissions. To add Azure AD groups to your library offerings, improve logon performance, and realize other benefits, you must grant Citrix Cloud additional permissions through the Global Admin role in Azure AD. To do this, you must be a Global Admin in Azure AD. By reconnecting to Azure AD, you grant application-level permissions to Citrix Cloud and allow Citrix Cloud to reconnect to Azure AD on your behalf.

For more information about the type of Azure AD permissions that Citrix Cloud requests, see Azure Active Directory Permissions for Citrix Cloud.

> **Important:**
>
> Reconnecting your Azure AD to Citrix Cloud requires you to sign in to Citrix Cloud using a Citrix Cloud administrator account under the Citrix identity provider. If you are signed in to Citrix Cloud with your Azure AD credentials, the reconnection fails. If you are using an Azure AD administrator account with Citrix Cloud and you don't have any administrators using the Citrix identity provider in your account, you can add one temporarily to perform this reconnection and delete it afterward.

To perform the reconnection, sign in to Citrix Cloud with your Citrix Cloud administrator credentials. When prompted to reconnect, you can sign in to Azure with your Global Admin credentials.

Azure Active Directory Permissions for Citrix Cloud

July 12, 2021

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

Enterprise applications

Name	Application ID	Usage
Citrix Cloud	e95c4605-aeab-48d9-9c36-1a262ef8048e	Workspace subscriber login

Name	Application ID	Usage
Citrix Cloud	f9c0e999-22e7-409f-bb5e-956986abdf02	Default connection between Azure AD and Citrix Cloud
Citrix Cloud	1b32f261-b20c-4399-8368-c8f0092b4470	Administrator invitations; administrator logins
Citrix Cloud	5c913119-2257-4316-9994-5e8f3832265b	Default connection between Azure AD and Citrix Cloud with Citrix Endpoint Management
Citrix Cloud	e067934c-b52d-4e92-b1ca-70700bd1124e	Legacy connection between Azure AD and Citrix Cloud with Citrix Endpoint Management

Workspace subscriber login

The Citrix Cloud application (ID: e95c4605-aeab-48d9-9c36-1a262ef8048e) uses the same permissions for both the Microsoft Graph and the Windows Azure Active Directory resource applications.

API Name	Claim Value	Permission Name	Type
Microsoft Graph	User.Read	Sign in and read user profile	Delegated
Windows Azure Active Directory	User.Read	Sign in and read user profile	Delegated

Default connection between Azure AD and Citrix Cloud

The Citrix Cloud application (ID: f9c0e999-22e7-409f-bb5e-956986abdf02) uses the following permissions:

API Name	Claim Value	Permission	Type
Microsoft Graph	Group.Read.All	Read all groups	Delegated
Microsoft Graph	User.ReadBasic.All	Read all users' basic profiles	Delegated
Microsoft Graph	User.Read.All	Read all users' full profiles	Delegated

API Name	Claim Value	Permission	Type
Microsoft Graph	User.Read	Sign in and read user profile	Delegated
Microsoft Graph	Group.Read.All	Read all groups	Application
Microsoft Graph	Directory.Read.All	Read directory data	Application
Microsoft Graph	User.Read.All	Read all users' full profile	Application
Microsoft Graph	User.Read	Sign in and read user profile	Application
Windows Azure Active Directory	User.Read	Sign in and read user profile	Delegated
Windows Azure Active Directory	User.ReadBasic.All	Read all users' basic profile	Delegated
Windows Azure Active Directory	Group.Read.All	Read all groups	Delegated
Windows Azure Active Directory	Directory.Read.All	Read directory data	Application

Administrator invitations and logins

The Citrix Cloud application (ID: 1b32f261-b20c-4399-8368-c8f0092b4470) uses the following permissions:

API Name	Claim Value	Permission Name	Type
Microsoft Graph	User.Read	Sign in and read user profile	Delegated
Microsoft Graph	User.ReadBasic.All	Read all users' basic profiles	Delegated
Windows Azure Active Directory	User.Read	Sign in and read user profile	Delegated
Windows Azure Active Directory	User.ReadBasic.All	Read all users' basic profile	Delegated

Default connection between Azure AD and Citrix Cloud with Endpoint Management

The Citrix Cloud application (ID: 5c913119-2257-4316-9994-5e8f3832265b) uses the following permissions:

API Name	Claim Value	Permission Name	Type
Microsoft Graph	Group.Read.All	Read all groups	Delegated
Microsoft Graph	User.ReadBasic.All	Read all users' basic profiles	Delegated
Microsoft Graph	User.Read	Sign in and read user profile	Delegated
Microsoft Graph	Directory.Read.All	Read directory data	Application
Microsoft Graph	Directory.Read.All	Read directory data	Delegated
Microsoft Graph	DeviceManagementApps.ReadWrite.All	Read and write Microsoft Intune apps	Delegated
Microsoft Graph	Directory.AccessAsUser	Access directory as the signed-in user	Delegated

Legacy connection between Azure AD and Citrix Cloud with Endpoint Management

The Citrix Cloud application (ID: e067934c-b52d-4e92-b1ca-70700bd1124e) uses the following permissions:

API Name	Claim Value	Permission Name	Type
Microsoft Graph	Group.Read.All	Read all groups	Delegated
Microsoft Graph	User.ReadBasic.All	Read all users' basic profiles	Delegated
Microsoft Graph	User.Read	Sign in and read user profile	Delegated
Microsoft Graph	DeviceManagementApps.ReadWrite.All	Read and write Microsoft Intune apps	Delegated
Microsoft Graph	Directory.AccessAsUser	Access directory as the signed-in user	Delegated

Permissions

API Name

There are two resource applications from which Citrix Cloud requests permissions: Microsoft Graph and Windows Azure Active Directory, listed under **API Name**. Citrix Cloud requests the same permissions from both resource applications.

Type

There are two levels of access that Citrix Cloud can request for a permission: Delegated and Application, listed under **Type**.

- **Delegated permissions** are used to act on behalf of a signed-in user, such as when querying the profile of the user.
- **Application permissions** are used when the application performs an action without the user's presence, such as querying users within a particular group. This permission type requires consent of a Global Administrator in Azure AD.

Claim Value

Azure AD assigns string values to permissions, listed under **Claim Value**. You can find descriptions of specific claim values in the following table:

Name	Description
User.Read	Allows Citrix Cloud administrators to add users from the connected Azure AD as administrators on the Citrix Cloud account.
User.ReadBasic.All	Gathers basic info from the user's profile. It's a subset from User.Read.All but the permission itself remains for backwards compatibility.

Name	Description
User.Read.All	Citrix Cloud calls https://docs.microsoft.com/en-us/graph/api/user-list?view=graph-rest-1.0&tabs=http to enable browsing and selection of users from the customer's connected Azure AD. For example, users from Azure AD can be given access to a Virtual Apps and Desktops resource with the workspace. Citrix Cloud can't use User.ReadBasic.All as Citrix Cloud needs to access properties outside of the basic profile such as onPremisesSecurityIdentifier.
Group.Read.All	Citrix Cloud calls https://docs.microsoft.com/en-us/graph/api/group-list?view=graph-rest-1.0&tabs=http to allow browsing and selection of groups from the customer's connected Azure AD. For example, groups from Azure AD can also be granted access to Virtual Apps and Desktops applications.
Directory.Read.All	Citrix Cloud calls https://docs.microsoft.com/en-us/graph/api/user-list-memberof?view=graph-rest-1.0&tabs=http to get the user's group membership as Groups.Read.All is not sufficient.
DeviceManagementApps.ReadWrite.All	Allows Citrix Cloud to read and write the properties, group assignments, status of apps, app configurations, and app protection policies managed by Microsoft Intune.
Directory.AccessAsUser.All	Allows Citrix Cloud to have the same access to information in the directory as the signed-in user.

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

August 24, 2021

Citrix Cloud 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 Virtual Apps and Desktops deployment through Citrix Workspace.
- Use the Citrix Gateway authentication, authorization, and auditing (AAA) functions with Citrix Workspace.
- Use features such as pass-through authentication, smart cards, secure tokens, conditional access policies, federation, and many others while providing your users access to the resources they need through Citrix Workspace.

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

Supported versions

Citrix Gateway authentication is supported for use with the following on-premises product versions:

- Citrix Gateway 12.1 54.13 Advanced edition or later
- Citrix Gateway 13.0 41.20 Advanced edition or later

Prerequisites

Cloud Connectors

You need at least two (2) servers on which to install the Citrix Cloud Connector software. These servers must meet the following requirements:

- Meets the system requirements described in Cloud Connector Technical Details.
- Does not have any other Citrix components installed, is not an Active Directory domain controller, and is not a machine critical to your resource location infrastructure.
- Joined to the domain where your Site resides. If users access your Site's applications in multiple domains, you must install at least two Cloud Connectors in each domain.

- Connected to a network that can contact your Site.
- Connected to the Internet. For more information, see System and Connectivity Requirements.
- Citrix recommends two servers for Cloud Connector high availability. After installation, the Cloud Connectors allow Citrix Cloud to locate and communicate with your Site.

For more information about installing the Cloud Connector, see Cloud Connector Installation.

Active Directory

Before enabling Citrix Gateway authentication, perform the following tasks:

- Verify that your workspace subscribers have user accounts in Active Directory (AD). Subscribers without AD accounts can't sign in to their workspaces successfully.
- Ensure that the user properties in your subscribers' AD accounts are populated. Citrix Cloud requires these properties to establish the user context when subscribers sign in. If these properties aren't populated, subscribers can't sign in to their workspace. These properties include:
  - Email address
  - Display name
  - Common name
  - SAM account name
  - User Principal Name
  - OID
  - SID
- Connect your Active Directory (AD) to your Citrix Cloud 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 to communicate with your on-premises environment. For instructions, see Connect Active Directory to Citrix Cloud.
- If you are performing federation with Citrix Gateway authentication, synchronize your AD users to the federation provider. Citrix Cloud requires the AD user attributes for your workspace subscribers so they can sign in successfully.

Requirements

Citrix Gateway advanced policies

Citrix Gateway authentication requires the use of advanced policies on the on-premises Gateway due to deprecation of classic policies. Advanced policies support multifactor authentication for Citrix Cloud, 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. 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 and Gateway conform to the OIDC protocol, which involves digitally signing tokens. Therefore, you must configure a certificate for signing these tokens. This certificate must be issued from a public Certificate Authority (CA). Using a certificate issued by a private CA is not supported as there is no way to provide Citrix Cloud with the private root CA certificate. So, the certificate chain of trust cannot be established. If you configure multiple certificates for signature, these keys are rotated for each message.

Keys must be bound to **vpn global**. Without these keys, subscribers can't access their workspace successfully after signing in.

Clock synchronization

Because digitally signed messages in OIDC carry a timestamp, the Gateway must be synchronized to NTP time. If the clock isn't synchronized, Citrix Cloud assumes that tokens are stale when checking their validity.

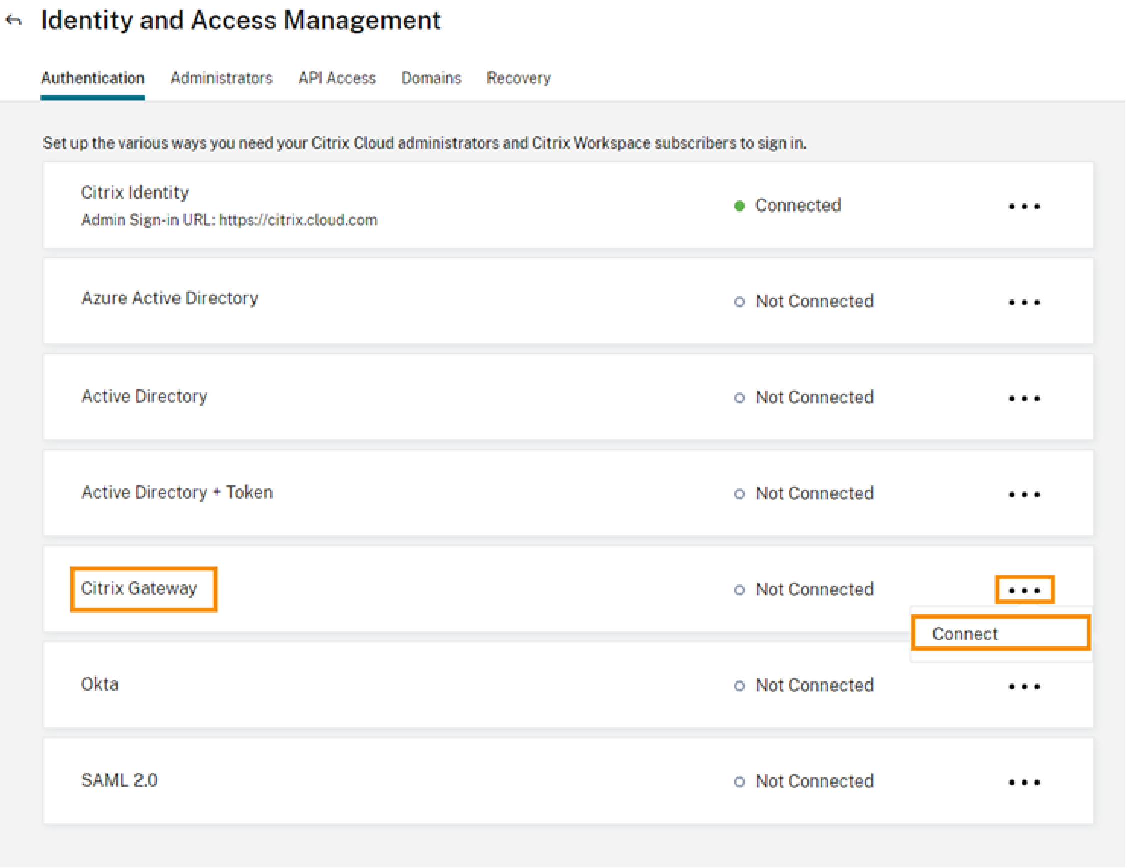
Task overview

To set up Citrix Gateway authentication, you perform the following tasks:

1. In **Identity and Access Management**, start configuring the connection to your Gateway. In this step, you generate the client ID, secret, and redirect URL for the Gateway.
2. On the Gateway, create an OAuth IdP advanced policy using the generated information from Citrix Cloud. This enables Citrix Cloud 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

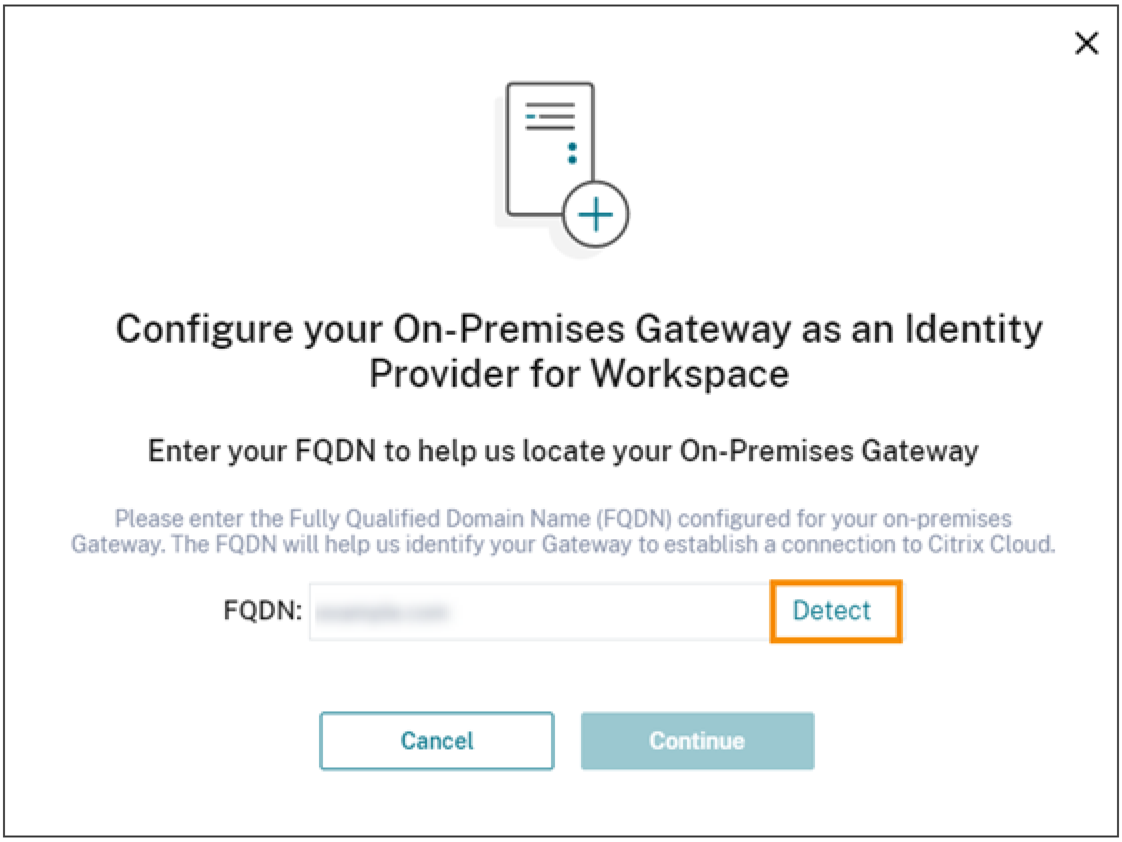
1. From the Citrix Cloud menu, select **Identity and Access Management**.
2. From the **Authentication** tab, in **Citrix Gateway**, click the ellipsis menu and select **Connect**.



Set up the various ways you need your Citrix Cloud administrators and Citrix Workspace subscribers to sign in.

Citrix Identity Admin Sign-in URL: https://citrix.cloud.com	● Connected
Azure Active Directory	○ Not Connected
Active Directory	○ Not Connected
Active Directory + Token	○ Not Connected
Citrix Gateway	○ Not Connected
Okta	○ Not Connected
SAML 2.0	○ Not Connected

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



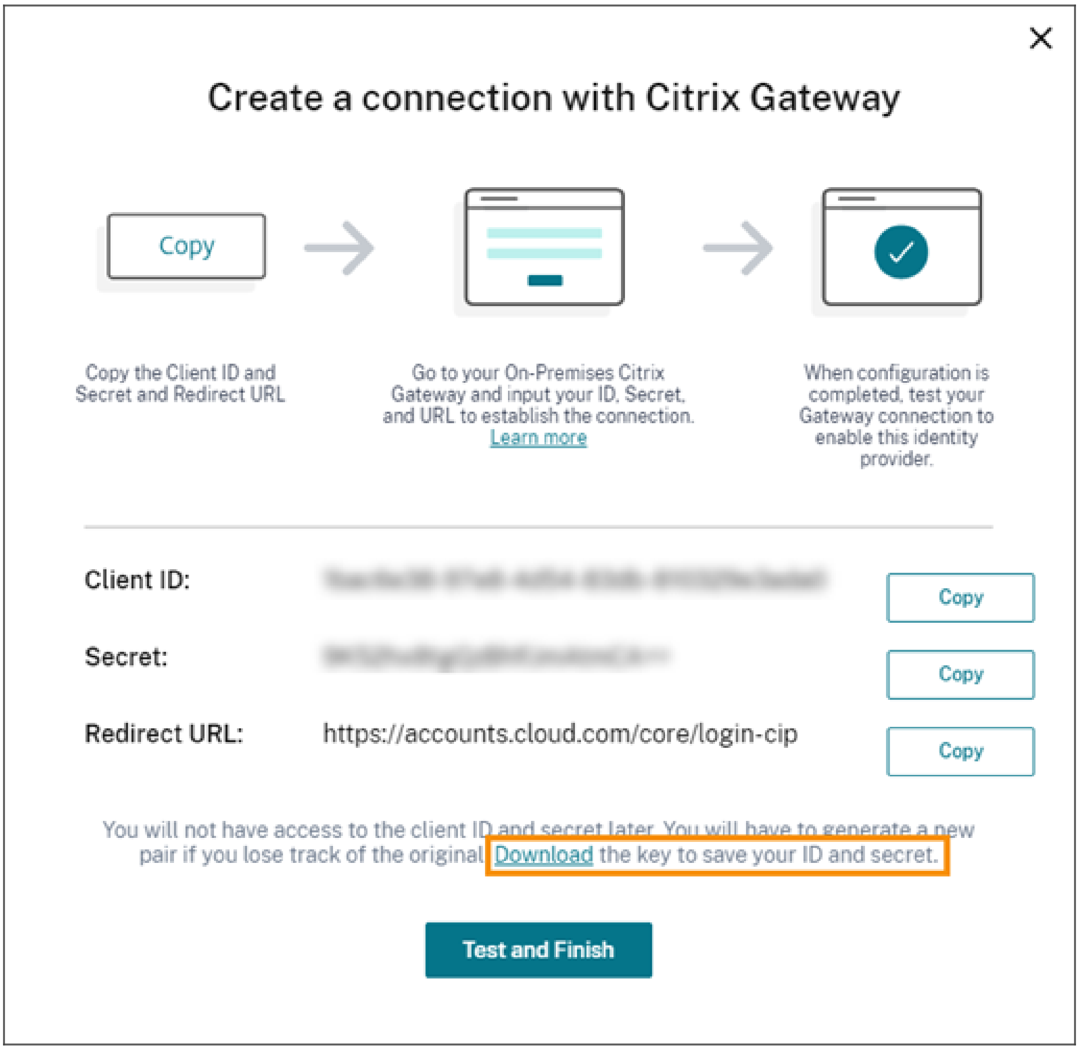
Configure your On-Premises Gateway as an Identity Provider for Workspace

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

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

After Citrix Cloud 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 displays.



Create a connection with Citrix Gateway

Copy the Client ID and Secret and Redirect URL

Go to your On-Premises Citrix Gateway and input your ID, Secret, and URL to establish the connection. Learn more

When configuration is completed, test your Gateway connection to enable this identity provider.

Client ID:	[redacted]	Copy
Secret:	[redacted]	Copy
Redirect URL:	https://accounts.cloud.com/core/login-cip	Copy

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

Also, download a copy of this information and save it securely offline for your reference. This information is not available in Citrix Cloud 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. 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 verifies that your Gateway is reachable and configured correctly.

5. Enable Citrix Gateway authentication for workspaces:
   a) From the Citrix Cloud menu, select **Workspace Configuration**.
   b) From the **Authentication** tab, select **Citrix Gateway**.
   c) Select **I understand the impact on subscriber experience** and then click **Save**.

Troubleshooting

As a first step, review the Prerequisites and Requirements sections in this article. Verify you have all the required components in your on-premises environment and that you have made all required configurations. If any of these items are missing or misconfigured, workspace authentication with Citrix Gateway does not work.

If you experience an issue establishing a connection between Citrix Cloud and your on-premises Gateway, verify the following items:

- The Gateway FQDN is reachable from the Internet.
- You have entered the Gateway FQDN correctly in Citrix Cloud.
- 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 are entered correctly in the Client ID, Client Secret, Redirect URL, and Audience fields of the OAuth IdP policy. Verify that the correct client ID has been entered in the Audience field of the policy.
- The OAuth IdP authentication policy is configured correctly. For instructions, see the following articles:
  - Citrix Gateway 12.1: Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud
  - Citrix Gateway 13.0: Use an on-premises Citrix Gateway as the identity provider for Citrix Cloud
- Verify the policy is bound correctly to the AAA authentication server as described in Binding Authentication Policies.

Global catalog servers

In addition to retrieving user account details, Gateway retrieves users' domain name, AD NETBIOS name, and the root AD domain name. To retrieve the AD NETBIOS name, Gateway searches the AD where the user accounts reside. NETBIOS names are not replicated on global catalog servers.

If you use global catalog servers in your AD environment, LDAP actions configured on these servers do not work with Citrix Cloud. Instead, you must configure the individual ADs in the LDAP action. If you have multiple domains or forests, you can configure multiple LDAP policies.

AD search for single sign-on with Kerberos or IdP chaining

If you use Kerberos or an external identity provider that uses SAML or OIDC protocols for subscriber sign-in, verify that AD lookup is configured. Gateway requires AD lookups to retrieve subscribers' AD user properties and AD configuration properties.

Ensure that you have LDAP policies configured, even if authentication is handled by third party servers. To configure these policies, you add a second authentication factor to your existing login schema profile by performing the following tasks:

1. Create an LDAP authentication server that performs only attribute and group extraction from Active Directory.
2. Create an LDAP advanced authentication policy.
3. Create an Authentication Policy Label.
4. Define the Authentication Policy Label as the next factor, after the primary identity provider.

To add LDAP as a second authentication factor

1. Create the LDAP authentication server:
   a) Select **System > Authentication > Basic Policies > LDAP > Servers > Add**.
   b) On the **Create Authentication LDAP Server** page, enter the following information:
      - In **Choose Server Type**, select **LDAP**.
      - In **Name**, enter a friendly name for the server.
      - Select **Server IP** and then enter LDAP server's IP address.
      - In **Security Type**, select your required LDAP security type.
      - In **Server Type**, select **AD**.
      - In **Authentication**, do not select the check box. This check box must be cleared because this authentication server is only for extracting user attributes and groups from Active Directory, not authentication.
   c) Under **Other Settings**, enter the following information:
      - In **Server Logon Name Attribute**, enter **UserPrincipalName**.
      - In **Group Attribute**, select **memberOf**.
      - In **Sub Attribute Name**, select **cn**.
2. Create the LDAP advanced authentication policy:
   a) Select **Security > AAA - Application Traffic > Policies > Authentication > Advanced Policies > Policy > Add**.
   b) On the **Create Authentication Policy** page, enter the following information:
      - In **Name**, enter a friendly name for the policy.
      - In **Action Type**, select **LDAP**.
      - In **Action**, select the LDAP authentication server you created earlier.
      - In **Expression**, enter **TRUE**.
   c) Click **Create** to save the configuration.
3. Create the Authentication Policy Label:
   a) Select **Security > AAA – Application Traffic > Policies > Authentication > Advanced Policies > Policy Label > Add**.
   b) In **Name**, enter a friendly name for the authentication policy label.
   c) In Login Schema, select **LSCHEMA_INT**.

    d) Under **Policy Binding**, in **Select Policy**, select the LDAP advanced authentication policy you created earlier.
    e) In **GoTo Expression**, select **END**.
    f) Click **Bind** to finish the configuration.
4. Define the LDAP Authentication Policy Label as the next factor, after the primary identity provider:
    a) Select **System > Security > AAA - Application Traffic > Virtual Servers**.
    b) Select the virtual server that contains the binding for your primary identity provider and select **Edit**.
    c) Under **Advanced Authentication Policies**, select the existing **Authentication Policy** bindings.
    d) Select the binding for your primary identity provider and then select **Edit Binding**.
    e) On the **Policy Binding** page, in **Select Next Factor**, select the LDAP Authentication Policy Label you created earlier.
    f) Click **Bind** to save the configuration.

Default password for multifactor authentication

If you use multifactor authentication for workspace subscribers, Gateway uses the last factor's password as the default password for single sign-on. This password is sent to Citrix Cloud 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. Enable **SSOCredentials** on the login schema corresponding to the LDAP factor.

Connect Okta as an identity provider to Citrix Cloud

September 15, 2021

Citrix Cloud supports using Okta as an identity provider to authenticate subscribers signing in to their workspaces. By connecting your Okta organization to Citrix Cloud, you can provide a common sign-in experience for your subscribers to access resources in Citrix Workspace.

After enabling Okta authentication in Workspace Configuration, subscribers have a different sign-in experience. Selecting Okta authentication provides federated sign-in, not single sign-on. Subscribers sign in to workspaces from an Okta sign-in page, but they may have to authenticate a second time when opening an app or desktop from the Citrix Virtual Apps and Desktops service. To enable single sign-on and prevent a second logon prompt, you need to use the Citrix Federated Authentication Service with Citrix Cloud. For more information, see Connect Citrix Federated Authentication Service to Citrix Cloud.

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

Prerequisites

Cloud Connectors

You need at least two (2) servers in your Active Directory domain on which to install the Citrix Cloud Connector software. Cloud Connectors are required for enabling communication between Citrix Cloud 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, is not an Active Directory domain controller, and is not a machine critical to your resource location infrastructure.
- Joined to your Active Directory (AD) domain. If your workspace resources and users reside in multiple domains, you must install at least two Cloud Connectors in each domain. For more information, see Deployment scenarios for Cloud Connectors in Active Directory.
- Connected to a network that can contact the resources that users access through Citrix Workspace.
- Connected to the Internet. For more information, see System and Connectivity Requirements.

For more information about installing Cloud Connectors, see Cloud Connector Installation.

Okta domain

When connecting Okta to Citrix Cloud, 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. Review the important considerations for using custom domains in Customize the Okta URL domain on the Okta web site.

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

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. After you create and configure the application, note the Client ID and Client Secret. You supply these values to Citrix Cloud when you connect your Okta organization.

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

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

Workspace URL

When creating the Okta application, you must supply your Workspace URL from Citrix Cloud. To locate the Workspace URL, select **Workspace Configuration** from the Citrix Cloud 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 requires an API token for your Okta organization. Create this token using a Read-Only Administrator account in your Okta organization. This token must be able to read the users and groups in your Okta organization.

To create the API token, see Create an Okta API token in this article. For more information about API tokens, see Create an API Token on the Okta website.

> **Important:**
>
> When you create the API token, make a note of the token value (for example, copy the value temporarily to a plain text document). Okta displays this value only once, so you might create the token just before you perform the steps in Connect Citrix Cloud 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 web site. Afterward, you import your AD users and groups to Okta. When importing, include the SID, UPN, and OID values associated with your AD accounts.

> Note:
>
> If you are using Citrix Gateway service with Workspace, you don't need to synchronize your AD accounts with your Okta organization.

To synchronize your AD users and groups with your Okta organization:

1. Install and configure the Okta AD agent. For complete instructions, refer to the following articles on the Okta website:
   - Install the Okta Active Directory agent
   - Configure Active Directory import and account settings
   - Configure Active Directory provisioning settings
2. Add your AD users and groups to Okta by performing a manual import or an automated import. For more information about Okta import methods and instructions, refer to Manage Active Directory users and groups on the Okta website.

Create an Okta OIDC web app integration

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

After you save the app integration, the console displays **Client ID** and **Client Secret** values in the **Client Credentials** sections. You use these values When you connect Citrix Cloud 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. Citrix Cloud requires these settings to authenticate your subscribers through Okta when they sign in to their workspaces.

1. (Optional) Update client permissions for the implicit grant type. You might choose to perform this step if you prefer to allow the least amount of privilege for this grant type.

  a) From the Okta application configuration page, under **General Settings**, select **Edit**.
  b) In the **Application** section, under **Client acting on behalf of itself**, clear the **Allow Access Token with implicit grant type**.
  c) Select **Save**.

2. Add application attributes. These attributes are case-sensitive.
   a) From the Okta console menu, select **Directory > Profile Editor**.
   b) Locate the Okta **user** profile and select **Profile**. Under **Attributes**, select **Add attribute**.
   c) Enter the following information:
      - Display Name: cip_sid
      - Variable Name: cip_sid
      - Description: AD User Security Identifier
      - Attribute Length: Greater than 1
      - Attribute Required: Yes
   d) Select **Save and Add Another**.
   e) Enter the following information:
      - Display Name: cip_upn
      - Variable Name: cip_upn
      - Description: AD User Principal Name
      - Attribute Length: Greater than 1
      - Attribute Required: Yes
   f) Select **Save and Add Another**.
   g) Enter the following information:
      - Display Name: cip_oid
      - Variable Name: cip_oid
      - Description: AD User GUID
      - Attribute Length: Greater than 1
      - Attribute Required: Yes
   h) Select **Save**.
3. Edit attribute mappings for the application:
   a) From the Okta console, select **Directory > Directory Integrations**.
   b) Select the AD you previously integrated. For more information, see Sync accounts with the Okta AD agent
   c) Select the **Provisioning** tab and then select **Settings > To Okta**.
   d) Under **Okta Attribute Mappings**, map the following attributes. Select **Save** after modifying each attribute.
      - Select `appuser.objectSid` and map to the `cip_sid` attribute.
      - Select `appuser.userName` and map to the `cip_upn` attribute.
      - Select `appuser.externalId` and map to the `cip_oid` attribute.
   e) Select **Force Sync**.

Create an Okta API token

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

Connect Citrix Cloud to your Okta organization

1. Sign in to Citrix Cloud at https://citrix.cloud.com.
2. From the Citrix Cloud 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 verifies your Okta details and tests the connection.

Enable Okta authentication for workspaces

1. From the Citrix Cloud menu, select **Workspace Configuration > Authentication**.
2. Select **Okta**. When prompted, select **I understand the impact on the subscriber experience**.
3. Click **Accept** to accept the permissions request.

Connect SAML as an identity provider to Citrix Cloud

September 14, 2021

Citrix Cloud supports using SAML (Security Assertion Markup Language) as an identity provider to authenticate subscribers signing in to their workspaces. You can use the SAML 2.0 provider of your choice with your on-premises Active Directory (AD).

For most SAML providers, use the information in this article to set up SAML authentication for your workspace subscribers. If you want to use SAML authentication with your Azure AD, you have the option to use the Citrix Cloud SAML SSO app from the Azure AD app gallery. For more information about using the Citrix Cloud SAML SSO app to set up SAML authentication in Citrix Cloud, see Tutorial: Azure Active Directory single sign-on (SSO) integration with Citrix Cloud SAML SSO on the Azure AD app documentation website.

Prerequisites

Using SAML authentication with Citrix Cloud has the following requirements:

- SAML provider that supports SAML 2.0
- On-premises Active Directory 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 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 two servers for Cloud Connector high availability. 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, is not an Active Directory domain controller, and is not a machine critical to your resource location infrastructure.
- Joined to the domain where your resources reside. If users access resources in multiple domains, you need to install at least two Cloud Connectors in each domain.
- Connected to a network that can contact the resources that subscribers access through Citrix Workspace.
- Connected to the Internet. For more information, see System and Connectivity Requirements.

For more information about installing the Cloud Connector, see Cloud Connector Installation.

Active Directory

Before configuring SAML authentication, perform the following tasks:

- Verify that your workspace subscribers have user accounts in Active Directory (AD). Subscribers without AD accounts can't sign in to their workspaces successfully when SAML authentication is configured.
- Ensure that the user properties in your subscribers' AD accounts are populated. Citrix Cloud requires these properties to establish the user context when subscribers sign in to Citrix Workspace. If these properties aren't populated, subscribers can't sign in. These properties include:

    - Email address
    - Display name (optional)
    - Common name
    - SAM account name
    - User Principal Name
    - Object GUID
    - SID
- Connect your Active Directory (AD) to your Citrix Cloud account by deploying Cloud Connectors in your on-premises AD.
- Synchronize your AD users to the SAML provider. Citrix Cloud 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 above, create the custom attributes and map them to AD. For reference, the general steps for this task are described in Create and map custom SAML attributes in this article.
3. Synchronize your AD users to your SAML provider.

> **Note:**
>
> If you have already created custom attributes that map to the required AD user attributes listed earlier in this section, you don't need to create and map more custom attributes. Instead, use your existing custom attributes when you configure the metadata from your SAML provider in Citrix Cloud.

For more information about integrating your AD with your SAML provider, consult your SAML provider's product documentation.

Task overview

To set up SAML authentication for workspace subscribers, you perform the following tasks:

1. In **Identity and Access Management**, connect your on-premises AD to Citrix Cloud as described in Connect Active Directory to Citrix Cloud.
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. This task involves configuring your SAML provider with the SAML metadata from Citrix Cloud and then configuring Citrix Cloud with the metadata from your SAML provider to create the SAML connection.
4. In **Workspace Configuration**, select the SAML authentication method.

Create and map custom SAML attributes

If you already have custom attributes for the SID, UPN, OID, and email attributes configured in your SAML provider, you don't have to perform this task. Proceed to Create a SAML connector application and use your existing custom SAML attributes in Step 8.

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

1. Sign in to the administration console of your SAML provider and select the option for creating custom user attributes. For example, depending on your SAML provider's console, you might select **Users > Custom User Fields > New User Field**.
2. Add the following attributes:
   - cip_sid
   - cip_upn
   - cip_oid
   - cip_email
3. Select the AD that you connected with Citrix Cloud. For example, depending on your SAML provider's console, you might select **Users > Directories**.
4. Select the option for adding directory attributes. For example, depending on your SAML provider's console, you might select **Directory Attributes**.
5. Select the option for adding attributes and map the following AD attributes to the custom user attributes you created in Step 2:
   - Select `objectSid` and map to the `cip_sid` attribute.

- Select `userPrincipalName` and map to the `cip_upn` attribute.
- Select `ObjectGUID` and map to the `cip_oid` attribute.
- Select `mail` and map to the `cip_email` attribute.

Configure the SAML provider metadata

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

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

Create a SAML connector application

1. Sign in to Citrix Cloud at https://citrix.cloud.com.
2. From the Citrix Cloud menu, select **Identity and Access Management**.
3. Locate **SAML 2.0** and select **Connect** from the ellipsis menu. The **Configure SAML** screen appears.
4. From your SAML provider's administration console, add an application for an identity provider with attributes and sign response. For example, depending on your provider's console, you might select **Applications > Applications > Add App** and then select **SAML Test Connector (IdP w/ attr w/ sign response)**.
5. If applicable, enter a display name and save the app.
6. From the **Configure SAML** screen in Citrix Cloud, 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.com`.
   - In the **Recipient** field, enter `https://saml.cloud.com/saml/acs`.
   - In the field for ACS URL validator, enter `https://saml.cloud.com/saml/acs`.
   - In the field for ACS URL, enter `https://saml.cloud.com/saml/acs`.
   - In the field for a single logout URL, enter `https://saml.cloud.com/saml/logout/callback`.

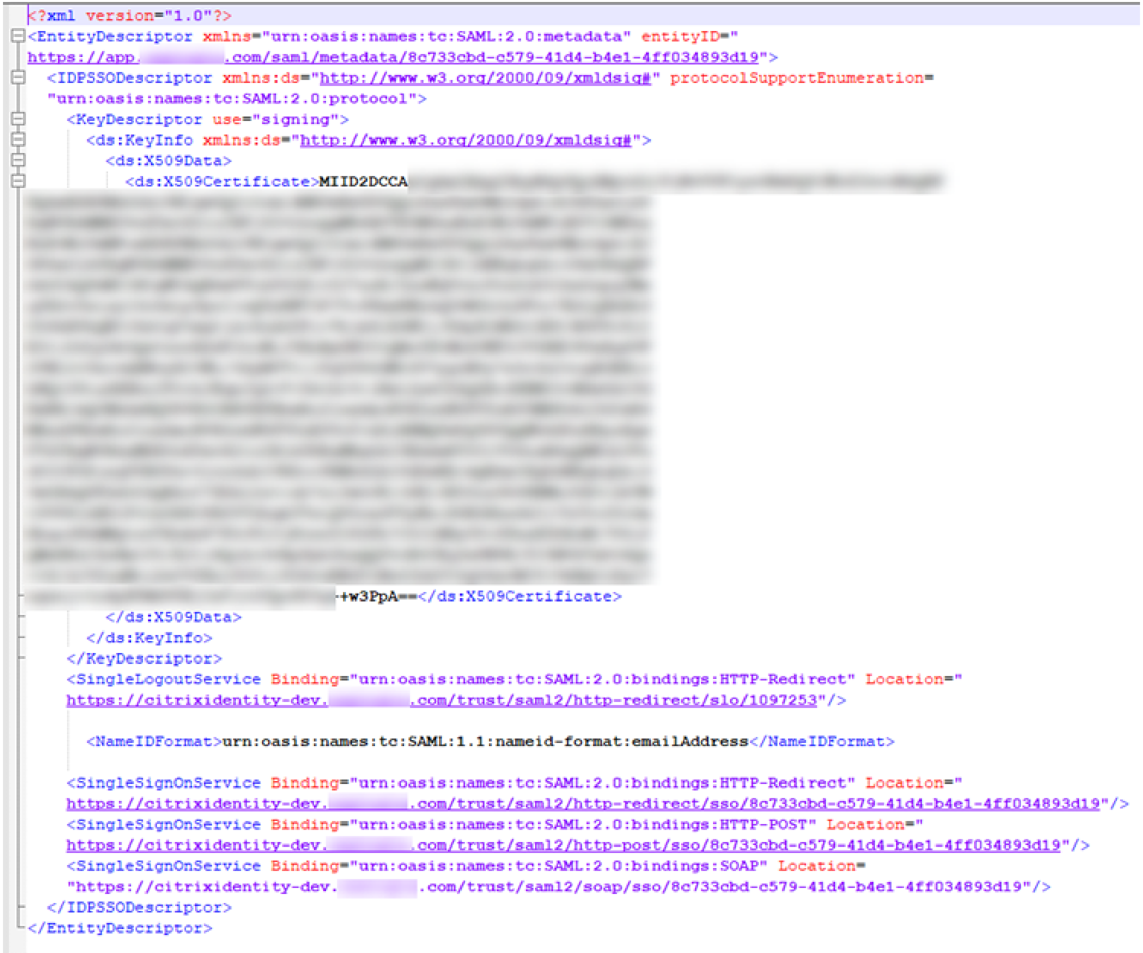
8. Add your custom SAML attributes as parameter values in the application:

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

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



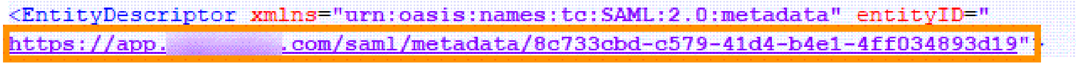
```
<?xml version="1.0"?>
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="
https://app.[redacted].com/saml/metadata/8c733cbd-c579-41d4-b4e1-4ff034893d19">
  <IDPSSODescriptor xmlns:ds="http://www.w3.org/2000/09/xmldsig#" protocolSupportEnumeration=
  "urn:oasis:names:tc:SAML:2.0:protocol">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

      <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>

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

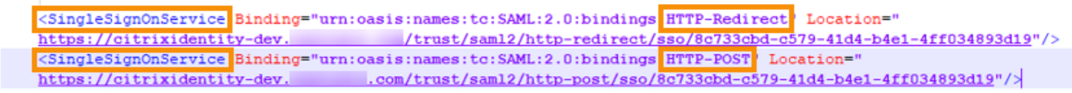
2. In the **Configure SAML** screen in Citrix Cloud, enter the following values from your SAML provider's metadata file:

- In **Entity ID**, enter the **entityID** value from the **EntityDescriptor** element in the metadata.

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

- In **Sign Authentication Request**, select **Yes** to allow Citrix Cloud to sign authentication requests, certifying they came from Citrix Cloud and not a malicious actor. Select **No** if you prefer to add the Citrix ACS URL to an allow list that your SAML provider uses for posting SAML responses safely.
- In **SSO Service URL**, enter the URL for the binding mechanism you want to use. You can use either HTTP-POST or HTTP-Redirect binding. In the metadata file, locate the **SingleSignOnService** elements with Binding values of either **HTTP-POST** or **HTTP-Redirect**.

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

- In **Binding Mechanism**, select the mechanism that matches the binding for the SSO Service URL you chose from the metadata file.
- In **SAML Response**, select the signing method your SAML provider uses for the SAML Response and SAML Assertion. By default, Citrix Cloud 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, 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 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.

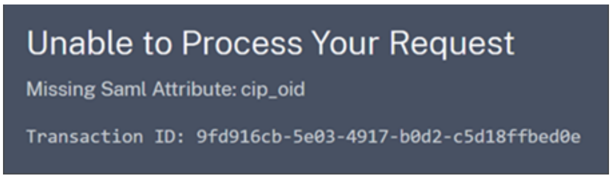
Enable SAML authentication for workspaces

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 are not encoded correctly. When an attribute error occurs, Citrix Cloud displays an error message that includes the faulty attribute.


Unable to Process Your Request

Missing Saml Attribute: cip_oid

Transaction ID: 9fd916cb-5e03-4917-b0d2-c5d18ffbed0e

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

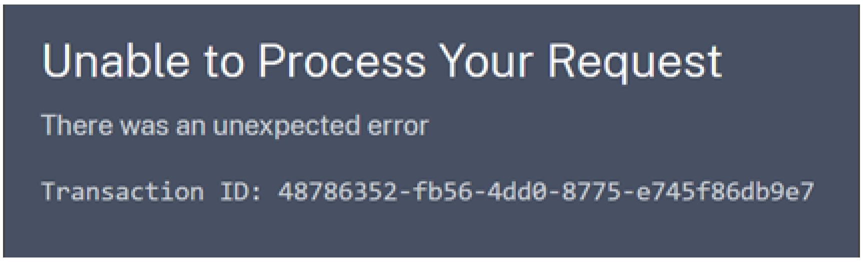
Attribute	Encoding
cip_email	Must be in String format (`user@domain`)
cip_oid	Must be in Base64 or String format
cip_sid	Must be in Base64 or String format
cip_upn	Must be String format (`user@domain`)

Unexpected errors

Citrix Cloud might experience an unexpected error when:

- A user initiates a SAML request using an IDP-initiated flow. For example, the request is made by selecting a tile through the identity provider's app portal instead of navigating directly to the workspace URL (`customer.cloud.com`).
- The SAML certificate is invalid or has expired.
- The authentication context is invalid.
- SAML assertion and response signature is mismatched.

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



Unable to Process Your Request

There was an unexpected error

Transaction ID: 48786352-fb56-4dd0-8775-e745f86db9e7

If this error results from navigating to Citrix Cloud 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.com`).
2. Assign users to both the SAML app and the bookmark app.
3. Change the visibility settings of the SAML app and the bookmark app so that the bookmark app is visible and the SAML app is hidden in the app portal.
4. Disable the Prompt=Login parameter to remove additional password prompts.

Select a primary resource location

August 5, 2019

If you have multiple resource locations in your domain, you can choose one to be the "primary" or "most preferred" location for Citrix Cloud. The primary resource location provides the best performance and connectivity between Citrix Cloud and your domain, enabling users to sign in quickly.

When you select a primary resource location, the Cloud Connectors in that resource location are used for user logons and provisioning operations. If the Cloud Connectors in the primary resource location are unavailable, these operations are performed using another Cloud Connector in the domain.

> **Note:**
>
> To ensure that Cloud Connectors are always available in any resource location, Citrix recommends installing at least two Cloud Connectors.

To decide which resource location you want to use for your primary resource location, consider the following:

- Does the resource location have the best connectivity to your domain?
- Is the resource location the closest to the geographical region in which you use the Citrix Cloud management console? For example, if your Citrix Cloud console is at https://us.cloud.com, the resource location you choose would be the closest one to the US region.

To select a primary resource location

1. From the Citrix Cloud management console, click the menu button and select **Identity and Access Management**.
2. Click **Domains** and then expand the domain containing the resource location you want to use.
3. Click **Set Primary Resource Location** and then select the resource location you want to designate as primary.
4. Click **Save**. Citrix Cloud displays "Primary" next to the resource location you selected.

> **Note:**
>
> Be sure to save your selections in one domain before expanding a different domain. When you expand a domain and then expand another domain, the previously expanded domain collapses and discards any unsaved selections.

Select a different primary resource location

1. From the Citrix Cloud management console, click the menu button and select **Identity and Access Management**.
2. Click **Domains** and then expand the domain that contains the primary resource location you want to change.
3. Click **Change Primary Resource Location** and then select the resource location you want to use.
4. Click **Save**.

Reset a primary resource location

Resetting the primary resource location allows you to remove the "Primary" designation from a resource location without selecting a different one. When you remove the "Primary" designation, any of the Cloud Connectors in the domain can handle user logon operations. As a result, some users might experience slower logons.

1. From the Citrix Cloud management console, click the menu button and choose **Identity and Access Management**.
2. Choose **Domains** and then expand the domain that contains the primary resource location you want to change.
3. Choose **Change Primary Resource Location** and then choose **Reset**. A notification appears, warning you that logon performance might be affected.
4. Select **I understand the potential impact to subscribers** and then click **Confirm Reset**.

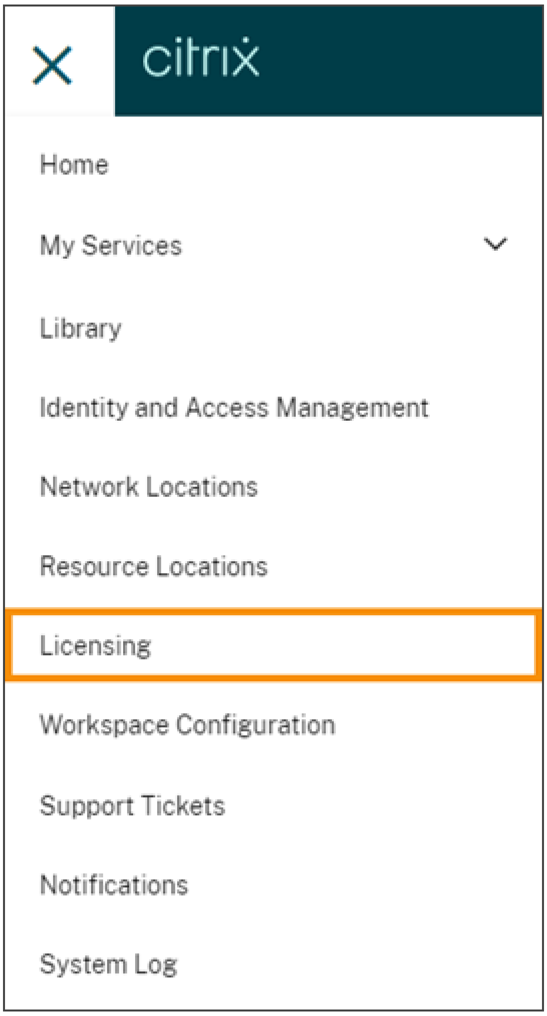
Licensing for Citrix Cloud

August 27, 2021

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

Licensing for enterprise customers

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



For more information about enterprise license and usage monitoring for cloud services, see Monitor licenses and active usage for cloud services.

Licensing for on-premises deployments

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

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

For more information about license and usage monitoring for on-premises Virtual Apps and Desktops deployments, see Monitor licenses and usage for on-premises deployments.

Licensing for Citrix Service Providers (CSP)

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

- License Usage Insights is a free service in Citrix Cloud that collects and aggregates product usage information across single-tenant and multitenant customers. For more information, see Licensing for Citrix Service Providers.
- The Licensing feature in Citrix Cloud enables customers of CSPs to monitor their licenses and usage for supported Virtual Apps and Desktops products. CSPs can sign in under their customer's Citrix Cloud account to view and export this information as well. For more information, see the following articles:
  - Customer license and usage monitoring for Citrix Virtual Apps and Desktops service
  - Customer license and usage monitoring for Citrix Virtual Apps and Desktops Standard for Azure

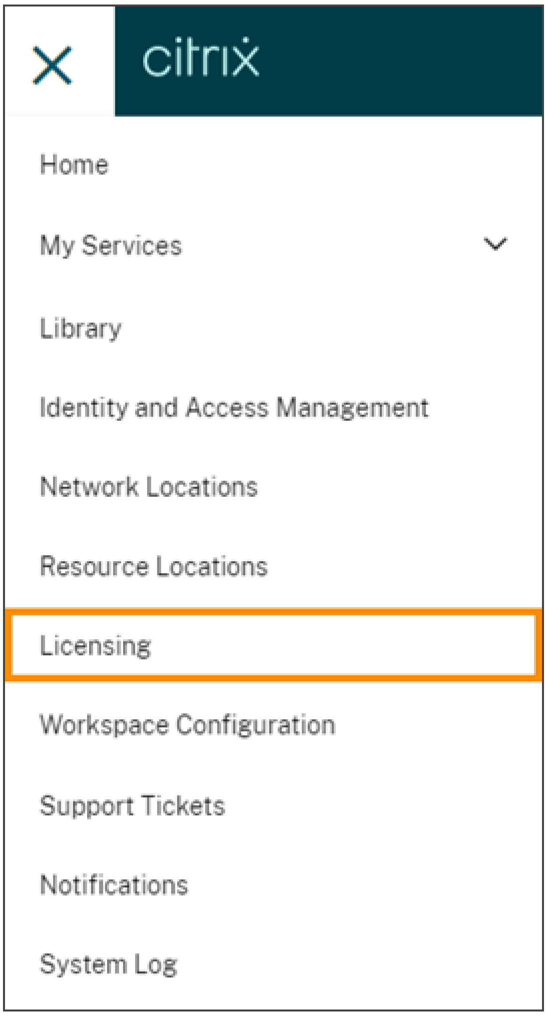
Monitor licenses and active usage for cloud services

August 15, 2021

Licensing in Citrix Cloud enables you to stay on top of license consumption for the cloud services you have purchased. Using the summary and detail reports, you can:

- View license availability and assignments at a glance
- View daily and monthly active usage trends for applicable cloud services
- Drill down to see individual license assignment details and usage trends
- Export license usage data to CSV

To view licensing data for your cloud services, select **Licensing** from the console menu.



> **Note:**
>
> This article covers Licensing features that are common to all supported Citrix Cloud services. Some aspects of Licensing might be different, depending on the service (for example, license assignment). For more information about licenses and usage for each service, see the following articles:
>
> - Monitor licenses and active usage for Virtual Apps and Desktops service (User/Device)
> - Monitor licenses and peak usage for Virtual Apps and Desktops service (Concurrent)
> - Monitor licenses and active usage for Virtual Apps and Desktops Standard for Azure
> - Monitor licenses and active usage for Endpoint Management service

Supported regions and cloud services

Licensing is available for supported services in the US, EU, and Asia Pacific South regions only.

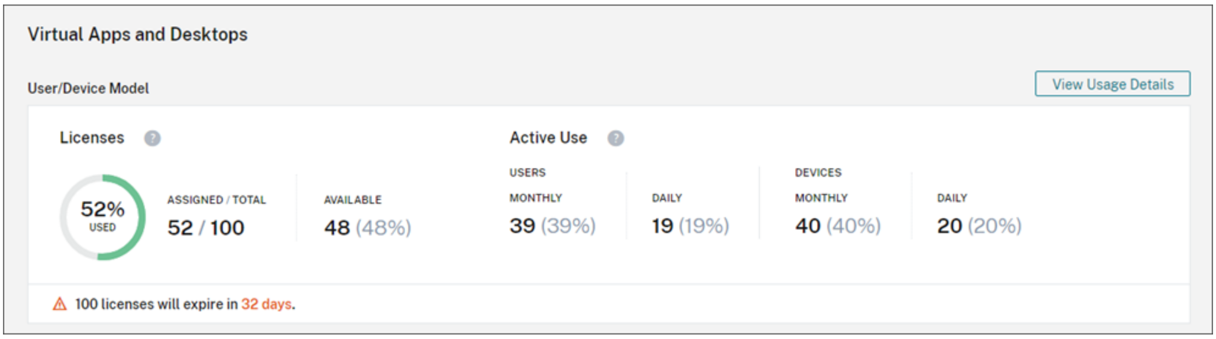
Licensing is supported for the following cloud services:

- Virtual Apps and Desktops (User/Device and Concurrent licensing models)
- Virtual Apps and Desktops Standard for Azure (User/Device licensing model)
- Endpoint Management
- Gateway

License assignment

In general, users are assigned a license upon first use of the cloud service. Some services might assign licenses differently based on the licensing model they use. For more information about how licenses are assigned for each service, see the Licensing articles referenced at the top of this article.

Licensing summary and details



Virtual Apps and Desktops

User/Device Model

Licenses

52% USED

ASSIGNED / TOTAL 52 / 100

AVAILABLE 48 (48%)

Active Use

USERS MONTHLY 39 (39%)

DAILY 19 (19%)

DEVICES MONTHLY 40 (40%)

DAILY 20 (20%)

⚠ 100 licenses will expire in 32 days.

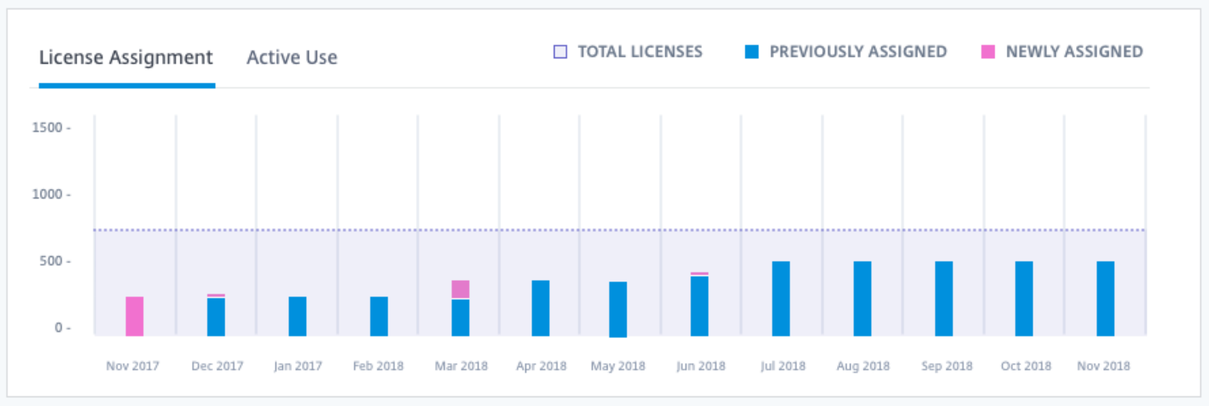
The Licensing summary provides an at-a-glance view of the following information for each supported service:

- Percentage of total purchased licenses assigned. As the percentage approaches 100%, the percentage goes from green to yellow. If the percentage exceeds 100%, the percentage turns red.
- The ratio of assigned licenses to purchased licenses and the number of available licenses remaining.
- The time remaining before the cloud service subscription expires. If the subscription expires within the next 90 days, a warning message appears.

For some services, this summary might include additional information such as active use. For more information about service-specific details, see the Licensing articles referenced at the top of this article.

Usage trends and license activity

For a detailed view of your cloud service licenses, click **View Usage Details**. You can then see a breakdown of usage trends and consumers of cloud service licenses.



This breakdown includes varying information, depending on the cloud service. For more information about service-specific usage trends and license activity, see the Licensing articles referenced at the top of this article.

Release assigned licenses

In general, an assigned license is eligible for release if the consumer hasn't used the cloud service for 30 consecutive days. When a license is released, the number of remaining licenses increases and the number of assigned licenses decreases accordingly.

For some services, releasing licenses might be different, depending on the licensing model used. For more information about releasing licenses for a specific service, see the Licensing articles referenced at the top of this article.

FAQ

- **Does Citrix prevent cloud service usage if assigned licenses exceed purchased licenses?** No, Citrix does not prevent any service launches if you overuse your cloud license amount. License Usage provides information for understanding your cloud license usage, so Citrix expects that you will monitor your license assignments and stay within your purchased license amount. If, at any point, you believe that you are going to overuse your service, Citrix encourages you to contact your sales representative to discuss your licensing requirements.
- **What licensing information is being captured?** Currently, only license information associated with user logins is captured.
- **Is multi-type licensing supported with Virtual Apps and Desktops service (for example, using both User/Device and Concurrent User models)?** If both licensing models are introduced into a single Citrix Cloud account, the Virtual Apps and Desktops tile no longer appears on the Licensing console page in Citrix Cloud. Because of this loss of visibility into licensing for Virtual Apps and Desktops service, Citrix does not recommend using multi-type licensing.

- **Is multi-edition licensing supported for Virtual Apps and Desktops service? For example, can I use both Premium and Advanced editions on the same Citrix Cloud account?** No, this use case is not supported. A Virtual Apps and Desktops site can be licensed for only one edition. If you want to use multiple Virtual Apps and Desktops services on the same Citrix Cloud account (for example, Virtual Apps and Virtual Apps and Desktops), they must be the same edition.
- **What is the difference between Monitor reporting (in Director) vs Concurrent licensing insights?** The Monitor report and explanation of concurrent sessions provides a different interpretation and metric than a measure of concurrent licenses in use. In most cases, using the number of concurrent sessions within Director as a representation or forecast of peak concurrent licenses in use greatly overstates the number of concurrent licenses needed. Do not use the Monitor report in Director as a substitute for a report on concurrent license usage. The two main differences between the reporting tools are:
  - **Sampling Time Length:** Licensing has a five-minute sampling period. Every five minutes, Citrix Cloud counts the unique devices currently connected to the service. All the five-minute sampling periods are aggregated to determine peak usage in a 24-hour, monthly, and contract length period. The Monitor report in Director can show intervals of up to two hours depending on how the report is run.
  - **Uniqueness:** Licensing looks for uniqueness amongst devices when sessions are launched. The Monitor report does not account for unique devices.
- **After migrating users to a new instance of a cloud service (for example, I changed the domain name for my organization), why are my licenses in-use counted twice for the same users?** Citrix Cloud uses the User Principle Name (UPN) to count unique users. If a user accessed the cloud service before and after the migration occurred, Citrix Cloud captures two unique UPNs for the user, each with a different domain name. Therefore, Citrix Cloud counts the same user twice. You can release the older license assignment after 30 days, assuming the user doesn't access the service under the old domain name. Citrix does not prevent any service launches if you overuse your cloud license amount.

Monitor licenses and active usage for Endpoint Management

May 14, 2020

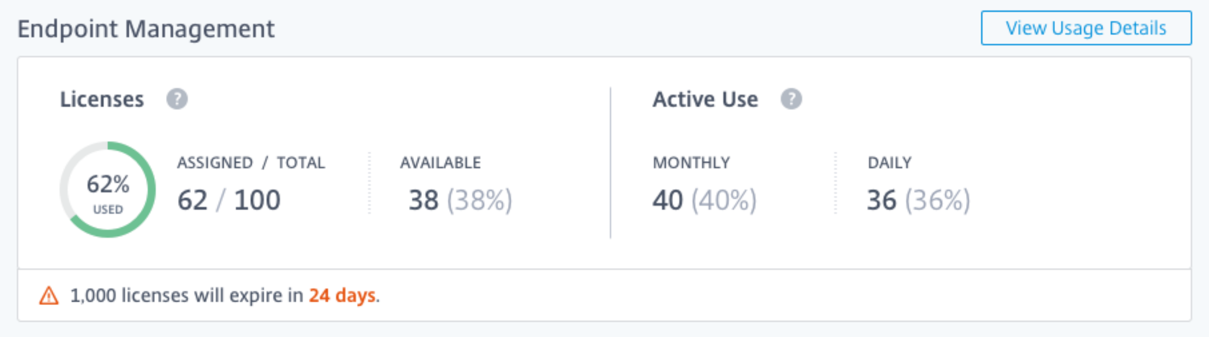
License assignment

In general, users are assigned a license upon first use of the cloud service. For Endpoint Management, a license is assigned when a user enrolls a device. After a device is enrolled, the device periodically checks in with Citrix Cloud. Citrix Cloud then uses this "check-in pulse" to calculate monthly usage and helps administrators to remain aware of users' most recent service usage.

First-time use occurs the first time a user enrolls a device or the first time a "check-in pulse" occurs for the device.

Licenses are assigned on a per-user basis. So, if two users enroll and use the same device, two licenses are assigned.

Licensing summary and details



Endpoint Management

Licenses

62% USED

ASSIGNED / TOTAL: 62 / 100

AVAILABLE: 38 (38%)

Active Use

MONTHLY: 40 (40%)

DAILY: 36 (36%)

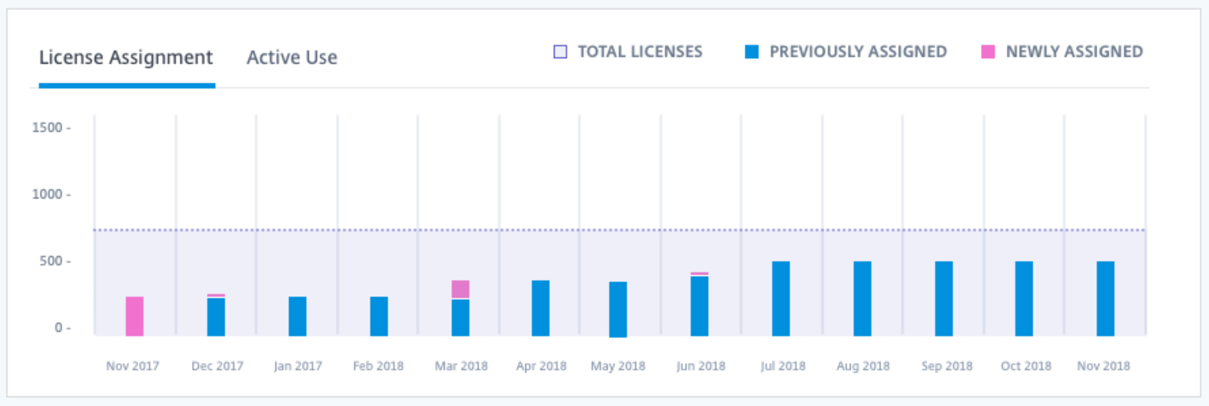
⚠ 1,000 licenses will expire in 24 days.

The Licensing summary provides an at-a-glance view of the following information for each supported service:

- Percentage of total purchased licenses assigned. As the percentage approaches 100%, the percentage goes from green to yellow. If the percentage exceeds 100%, the percentage turns red.
- The ratio of assigned licenses to purchased licenses and the number of available licenses remaining.
- Active usage statistics on a monthly and daily basis:
  - Monthly active use refers to the number of unique users that have used the service in the last 30 days.
  - Daily active use refers to the number of unique users that have used the service in the last 24 hours.
- The time remaining before the cloud service subscription expires. If the subscription expires within the next 90 days, a warning message appears.

Usage trends and license activity

For a detailed view of your licenses, click **View Usage Details**. You can then see a breakdown of usage trends and individual users and devices that are consuming cloud service licenses.

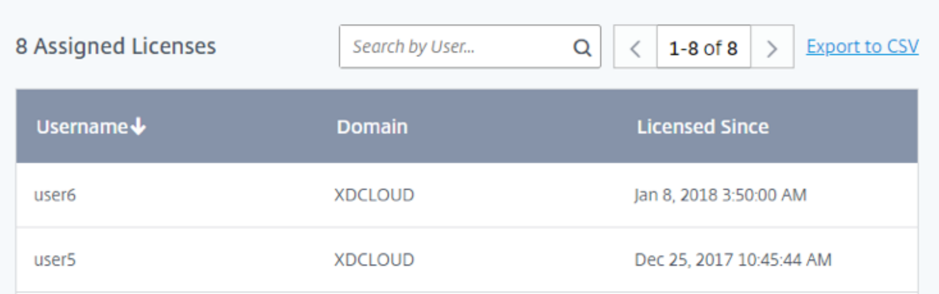


This breakdown shows you the following information:

- **Total Licenses:** Your total purchased licenses for the cloud service across all entitlements.
- **Previously Assigned:** The cloud service licenses that were already assigned at the beginning of each month. For example, if a user is assigned a license in July, that assignment is counted in the Previously Assigned number for August.
- **Newly Assigned:** The number of cloud service licenses that were assigned during each month. For example, a user who accesses the cloud service for the first time in July is assigned a license. This license is counted in the Newly Assigned number for July.
- **Active Use:** Daily and monthly active usage trends over the previous calendar month and calendar year, respectively.

The **License Activity** section also displays the following information:

- A list of the individual consumers who have assigned licenses
- The date when licenses were assigned
- The number of enrolled devices and the date of the last check-in for each user



Username↓	Domain	Licensed Since
user6	XDCLOUD	Jan 8, 2018 3:50:00 AM
user5	XDCLOUD	Dec 25, 2017 10:45:44 AM

To view the number of enrolled devices for a specific user, you can click the ellipsis button and select **View Devices**. Citrix Cloud displays a list of the enrolled devices for the user and the date of the last check-in for each device.

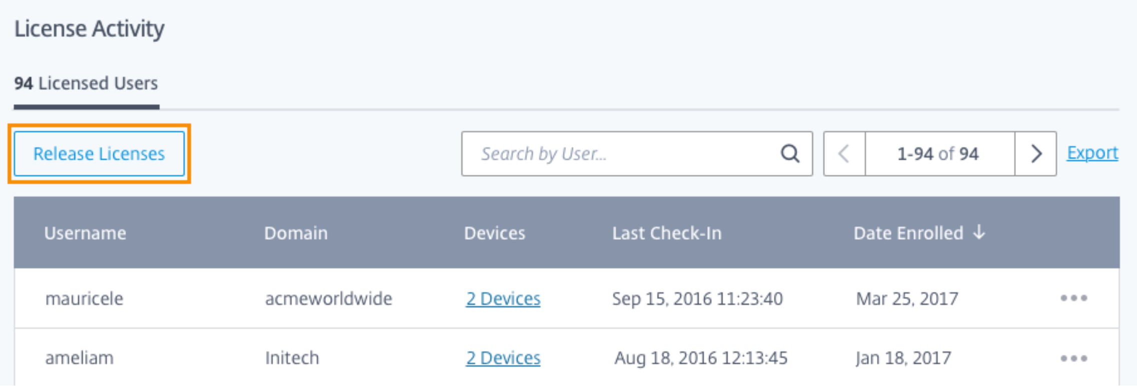
Release assigned licenses

You can release licenses for users that haven't enrolled a new device and an existing device hasn't checked in with Citrix Cloud in the last 30 days. You can release multiple licenses in bulk or individually.

When a license is released, the number of remaining licenses increases and the number of assigned licenses decreases accordingly. After a user's license is released, the user can acquire another license by enrolling a device.

To release multiple assigned licenses

1. Under **License Activity**, select **Release Licenses**.

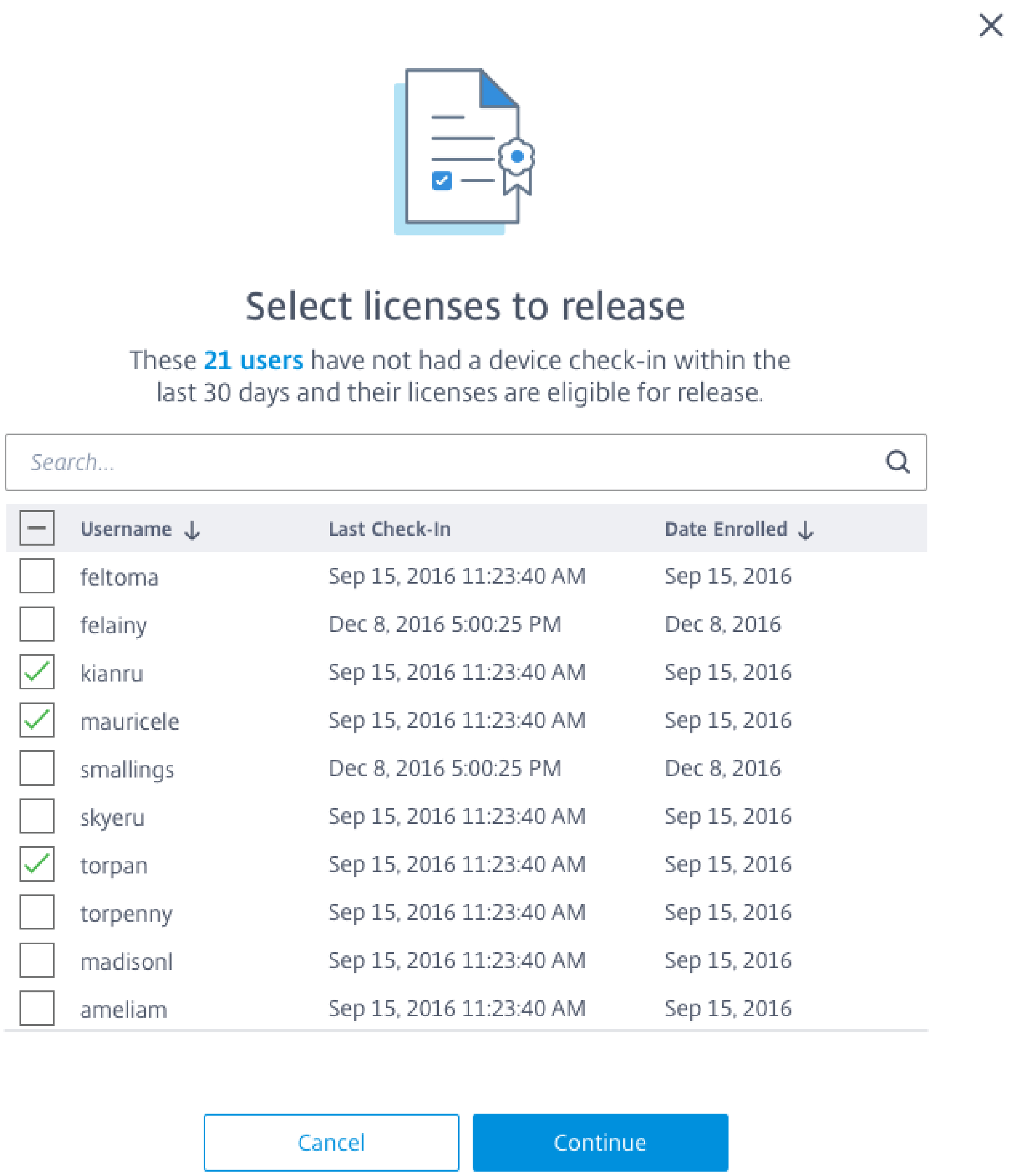


License Activity

94 Licensed Users

Username	Domain	Devices	Last Check-In	Date Enrolled ↓	
mauricele	acmeworldwide	2 Devices	Sep 15, 2016 11:23:40	Mar 25, 2017	•••
ameliam	Initech	2 Devices	Aug 18, 2016 12:13:45	Jan 18, 2017	•••

2. From the list, select the users you want to manage and select **Continue**.



Select licenses to release

These **21 users** have not had a device check-in within the last 30 days and their licenses are eligible for release.

☐	Username ↓	Last Check-In	Date Enrolled ↓
☐	feltoma	Sep 15, 2016 11:23:40 AM	Sep 15, 2016
☐	felainy	Dec 8, 2016 5:00:25 PM	Dec 8, 2016
☑	kianru	Sep 15, 2016 11:23:40 AM	Sep 15, 2016
☑	mauricele	Sep 15, 2016 11:23:40 AM	Sep 15, 2016
☐	smallings	Dec 8, 2016 5:00:25 PM	Dec 8, 2016
☐	skyeru	Sep 15, 2016 11:23:40 AM	Sep 15, 2016
☑	torpan	Sep 15, 2016 11:23:40 AM	Sep 15, 2016
☐	torpenny	Sep 15, 2016 11:23:40 AM	Sep 15, 2016
☐	madisonl	Sep 15, 2016 11:23:40 AM	Sep 15, 2016
☐	ameliam	Sep 15, 2016 11:23:40 AM	Sep 15, 2016

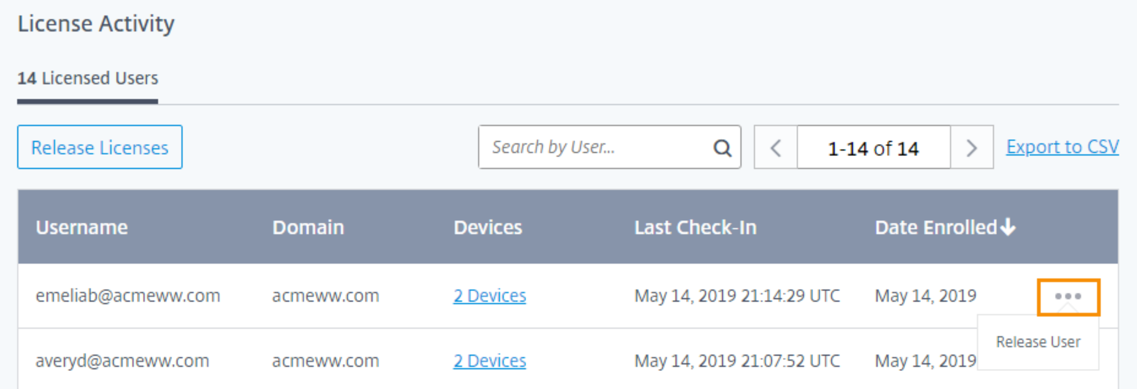
3. When prompted to confirm the release, click **Release**.

To release a single assigned license

You can release individual licenses from the **Licensed Users** list. This list displays clickable ellipsis buttons only for users with licenses that are eligible for release. The ellipsis button is inactive for users who have enrolled a new device and an existing device has checked in with Citrix Cloud in the last 30 days.

1. Under **License Activity**, select the **Licensed Users** tab.
2. Locate the user you want to manage.

3. Click the ellipsis button and select **Release User**.



License Activity

14 Licensed Users

Username	Domain	Devices	Last Check-In	Date Enrolled
emeliab@acmeww.com	acmeww.com	2 Devices	May 14, 2019 21:14:29 UTC	May 14, 2019
averyd@acmeww.com	acmeww.com	2 Devices	May 14, 2019 21:07:52 UTC	May 14, 2019

4. Review the user you selected and select **Continue**.
5. When prompted to confirm the release, click **Release**.

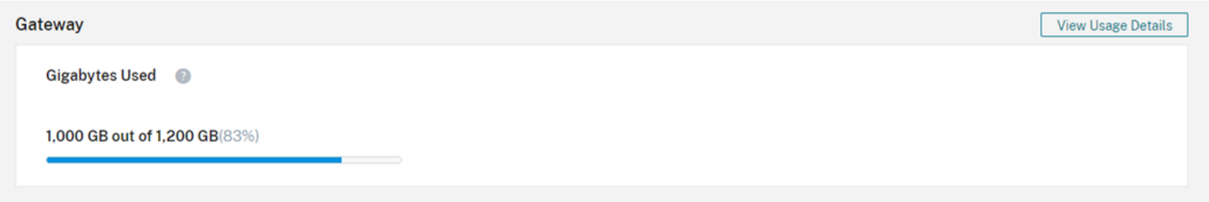
Monitor bandwidth usage for Gateway service

October 14, 2021

> **Note:**
>
> This feature is intended to help you better understand your actual bandwidth usage in Gateway service. Citrix does not enforce bandwidth usage allotments in customer environments or interfere with production workloads. Gateway service is not impacted in the event you overuse your bandwidth allotment. If Citrix changes how customer entitlements and usage policies are enforced, Citrix notifies you well before these changes become effective.

This article pertains to Gateway service when used with Citrix Virtual Apps and Desktops service and Citrix Workspace. Bandwidth consumption for the Gateway service included with Virtual Apps Essentials service is not displayed on the **Licensing** page of the Citrix Cloud management console.

Licensing summary



Gateway

Gigabytes Used

1,000 GB out of 1,200 GB(83%)

The licensing summary for the Gateway service provides an at-a-glance view of the following information:

- The amount of bandwidth consumed out of the total amount of bandwidth for all subscriptions.

- The time remaining before the cloud service subscription expires. If the subscription expires within the next 90 days, a warning message appears.

Licenses and bandwidth used

For Gateway service subscriptions, each user has access to 1 GB of bandwidth per month (12 GB per user, per year). This bandwidth is pooled across the number of licenses and for the subscription period. For example, if you buy 100 licenses for 3 years, you have 3600 GB of total bandwidth (1200 GB per year). This bandwidth is spread across all licensed users for the 3-year period. If you buy more subscriptions, Citrix Cloud displays the total number of licenses and bandwidth across all your subscriptions.

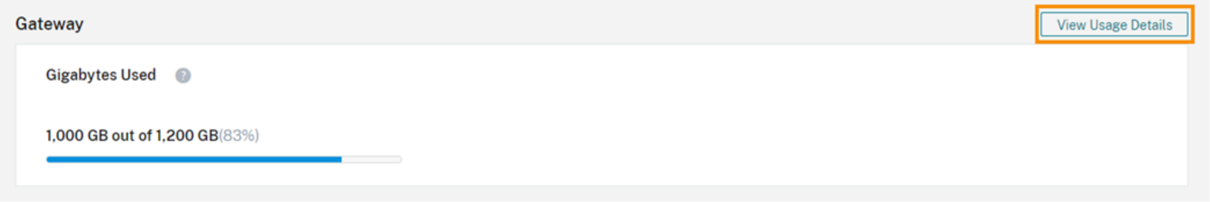
For Gateway service trials, 50 GB of bandwidth is pooled across 25 users for the 60-day trial period.

If you don't use the full amount of bandwidth during the subscription period, Citrix Cloud doesn't carry over any unused bandwidth when you renew.

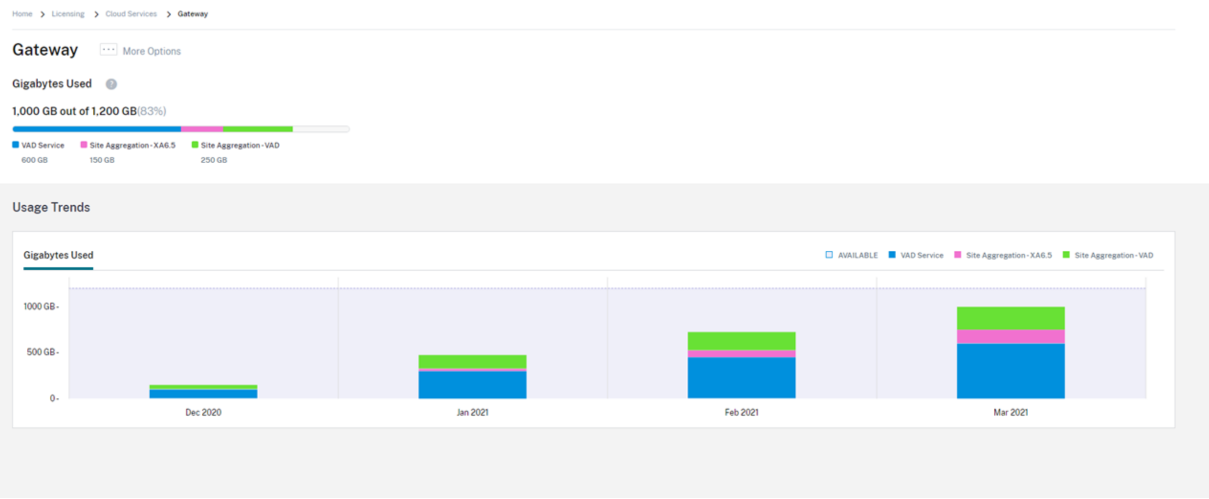
For multiple subscriptions with overlapping terms, Citrix Cloud displays the bandwidth associated with unexpired subscriptions only. For example, if you purchased two subscriptions, Citrix Cloud displays the total licenses and total bandwidth across both subscriptions. When the first subscription expires, Citrix Cloud displays only the bandwidth associated with the unexpired subscription. When the last subscription expires, Citrix Cloud displays the currently consumed bandwidth and zero total bandwidth. This display persists during the service grace period and data retention period described in Extend Citrix Cloud service subscriptions.

Usage trends

For a detailed view of your licenses, click **View Usage Details**.



You can then see a breakdown of usage trends and individual users that are consuming cloud service licenses and bandwidth.



Home > Licensing > Cloud Services > Gateway

Gateway ··· More Options

Gigabytes Used

1,000 GB out of 1,200 GB(83%)

VAD Service	Site Aggregation - XA6.5	Site Aggregation - VAD
600 GB	150 GB	250 GB

Usage Trends

Gigabytes Used

In the **Usage Trends** section, the **Gigabytes Used** tab shows you the amount of bandwidth consumed out of the total bandwidth available. The amount of bandwidth consumed is broken down based on access through the following methods:

- VAD service: The amount of bandwidth used for external connectivity by Virtual Apps and Desktops users.
- Site aggregation: The amount of bandwidth used for launching on-premises apps and desktops through Workspace with Site aggregation.

> **Note:**
>
> Usage trends are cumulative for the length of the current subscription term.

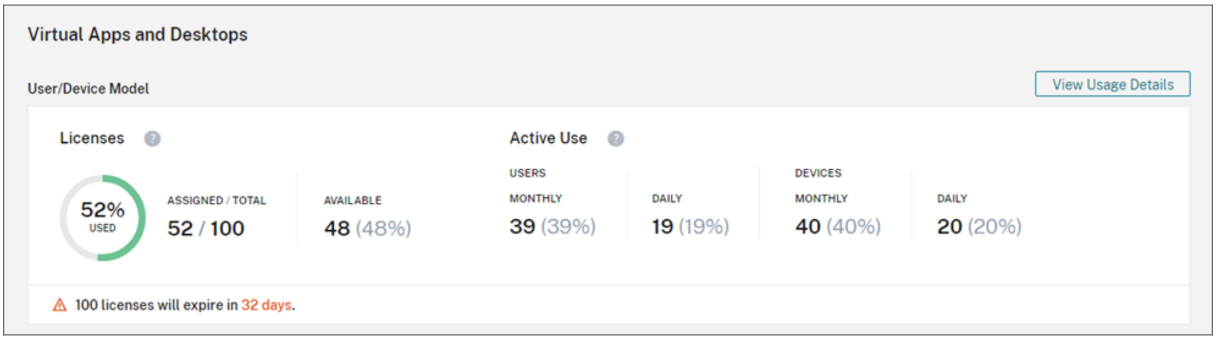
Monitor licenses and active usage for Citrix Virtual Apps and Desktops service (User/Device)

August 27, 2021

License assignment

Citrix Cloud assigns a license when a unique user or unique device launches an app or desktop for the first time.

Licensing summary



Virtual Apps and Desktops

User/Device Model

Licenses

52% USED

ASSIGNED / TOTAL 52 / 100

AVAILABLE 48 (48%)

Active Use

USERS

MONTHLY 39 (39%)

DAILY 19 (19%)

DEVICES

MONTHLY 40 (40%)

DAILY 20 (20%)

⚠ 100 licenses will expire in 32 days.

The Licensing summary provides an at-a-glance view of the following information:

- Percentage of total purchased licenses that have been assigned. As the percentage approaches 100%, the percentage goes from green to yellow. If the percentage exceeds 100%, the percentage turns red.

  The quantity of total purchased licenses is the sum of licenses that have been purchased for Virtual Apps, Virtual Desktops, and Virtual Apps and Desktops services that use the User/Device licensing model.

- The ratio of assigned licenses to purchased licenses and the number of available licenses remaining.
- Active usage statistics on a monthly and daily basis:
  - Monthly active use refers to the number of unique users or devices that have used the service in the last 30 days.
  - Daily active use refers to the number of unique users or devices that have used the service in the last 24 hours.
- The time remaining before the cloud service subscription expires. If the subscription expires within the next 90 days, a warning message appears.

Calculating assigned licenses and active use

To accurately reflect the User/Device licensing model for the Virtual Apps and Desktops service, Citrix Cloud counts the number of unique users and unique devices that have used the service. To measure assigned licenses, Citrix Cloud uses the lesser of these counts. To measure active use, Citrix Cloud uses each count as the quantity of active users and active devices in a given period.

Example of calculating assigned licenses

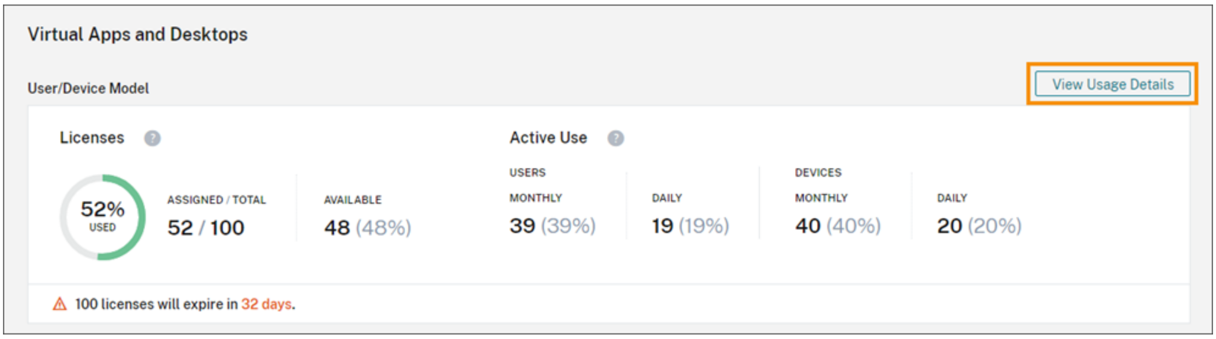
If 100 unique users and 50 unique devices have used the service, Citrix Cloud uses the lesser number (50) to determine the number of assigned licenses. The percentage of licenses used and the number of available licenses are based on these 50 assigned licenses.

Example of calculating active use

If 10 unique users and 20 unique devices used the service in the last 30 days, Citrix Cloud determines that monthly active use consists of 10 active users and 20 active devices. Likewise, if 30 unique users and 15 unique devices were counted in the last 24 hours, Citrix Cloud determines that daily active use consists of 30 active users and 15 active devices.

Usage trends and license activity

For a detailed view of your licenses, click **View Usage Details** at the far right of summary. You can then see a breakdown of usage trends and individual users and devices that are consuming cloud service licenses.



Virtual Apps and Desktops

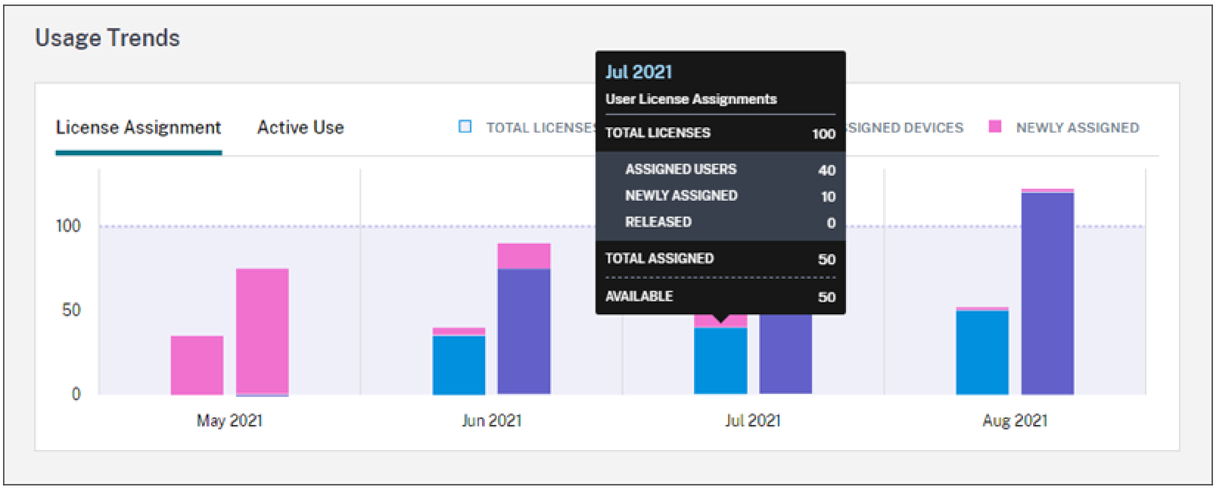
User/Device Model

View Usage Details

Licenses			Active Use			
			USERS		DEVICES	
52% USED	ASSIGNED / TOTAL	AVAILABLE	MONTHLY	DAILY	MONTHLY	DAILY
	52 / 100	48 (48%)	39 (39%)	19 (19%)	40 (40%)	20 (20%)

⚠ 100 licenses will expire in 32 days.

The **Usage Trends** section displays this breakdown as a graph.



Jul 2021
User License Assignments

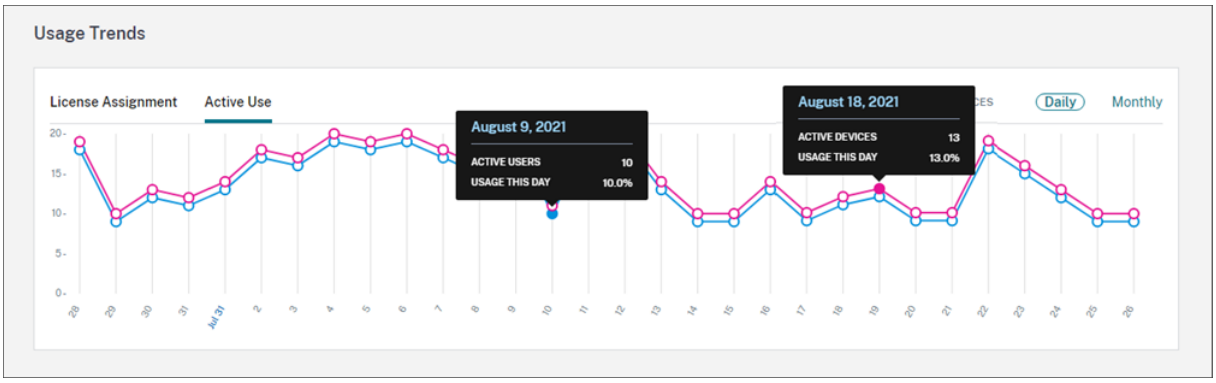
TOTAL LICENSES	100
ASSIGNED USERS	40
NEWLY ASSIGNED	10
RELEASED	0
TOTAL ASSIGNED	50
AVAILABLE	50

On the **License Assignment** graph, pointing to a bar for a specific month or day shows you the following information:

- **Total Licenses:** Your total purchased licenses for the cloud service across all entitlements.
- **Assigned Users:** The cumulative number of licenses assigned to users up to the current month.

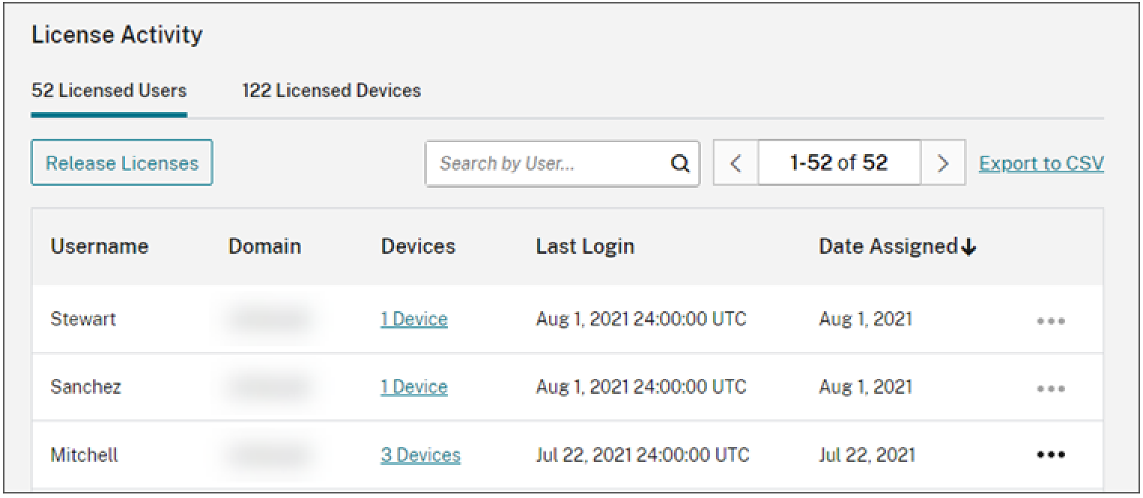
- **Assigned Devices:** The cumulative number of licenses assigned to devices up to the current month. If this number seems particularly high for a given month, this could be the result of app or desktop launches occurring through a web browser. To lower this number, Citrix recommends using a locally-installed Workspace app.
- **Newly Assigned:** The number of new licenses that were assigned for each month. For example, a user accesses the cloud service for the first time in July and is assigned a license. This license is counted as "Newly Assigned" for the month of July.
- **Released:** The number of eligible licenses that were released during each month. For example, if 20 licenses were eligible for release and you released 10 of them in July, the number of released licenses shown for July is 10.

Select **Active Use** to view a graph of active users and devices over the previous calendar month and calendar year, respectively. Pointing to a specific point on the graph reveals the number of active users or devices and the usage percentage.



The **License Activity** section also displays the following information:

- A list of the individual users who have assigned licenses, including associated devices.



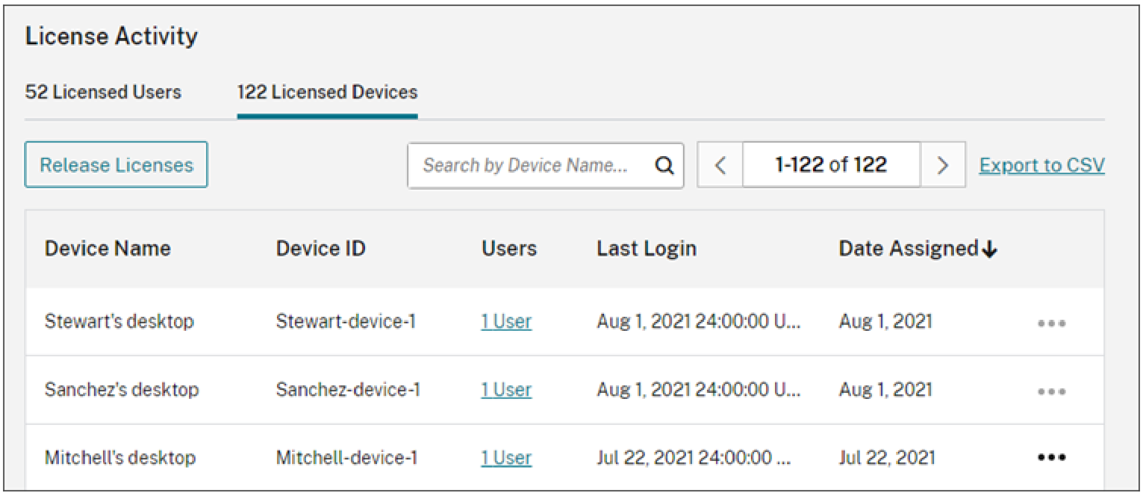
License Activity

52 Licensed Users | 122 Licensed Devices

Release Licenses | Search by User... | 1-52 of 52 | Export to CSV

Username	Domain	Devices	Last Login	Date Assigned↓
Stewart		1 Device	Aug 1, 2021 24:00:00 UTC	Aug 1, 2021
Sanchez		1 Device	Aug 1, 2021 24:00:00 UTC	Aug 1, 2021
Mitchell		3 Devices	Jul 22, 2021 24:00:00 UTC	Jul 22, 2021

- A list of the devices that have assigned licenses, including associated users.



License Activity

Device Name	Device ID	Users	Last Login	Date Assigned↓	
Stewart's desktop	Stewart-device-1	1 User	Aug 1, 2021 24:00:00 U...	Aug 1, 2021	•••
Sanchez's desktop	Sanchez-device-1	1 User	Aug 1, 2021 24:00:00 U...	Aug 1, 2021	•••
Mitchell's desktop	Mitchell-device-1	1 User	Jul 22, 2021 24:00:00 ...	Jul 22, 2021	•••

- The date when a license was assigned to the user or device.

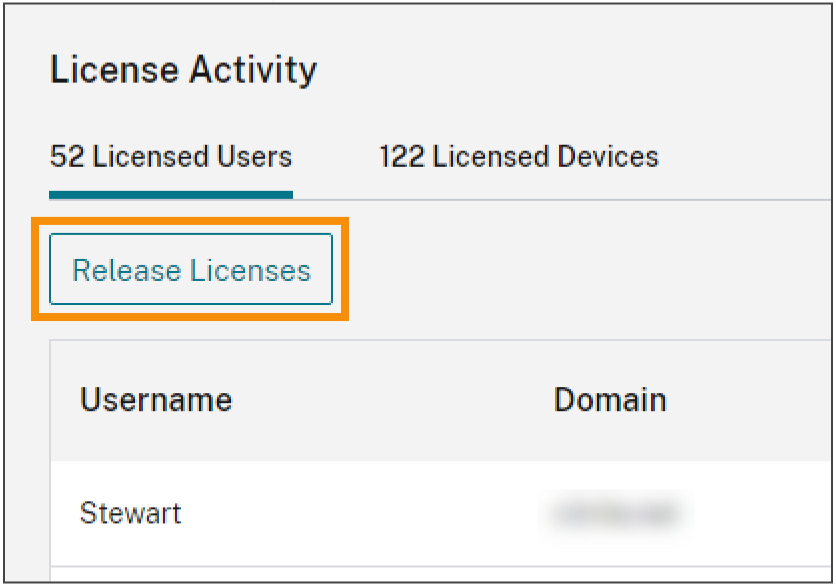
Release assigned licenses

You can release licenses for users that haven't launched an app or a desktop in the last 30 days. You can release licenses for devices if no apps or desktops have been launched from the device in the last 30 days. You can release multiple licenses in bulk or individually. (This differs from on-premises Citrix Virtual Apps and Desktops deployments, where inactive licenses are released automatically after 90 days.)

When a license is released, the number of remaining licenses increases and the number of assigned licenses decreases accordingly. After a license is released, the user can acquire another license by logging in and using the cloud service.

To release multiple assigned licenses

1. Under **License Activity**, select **Release Licenses**.



License Activity

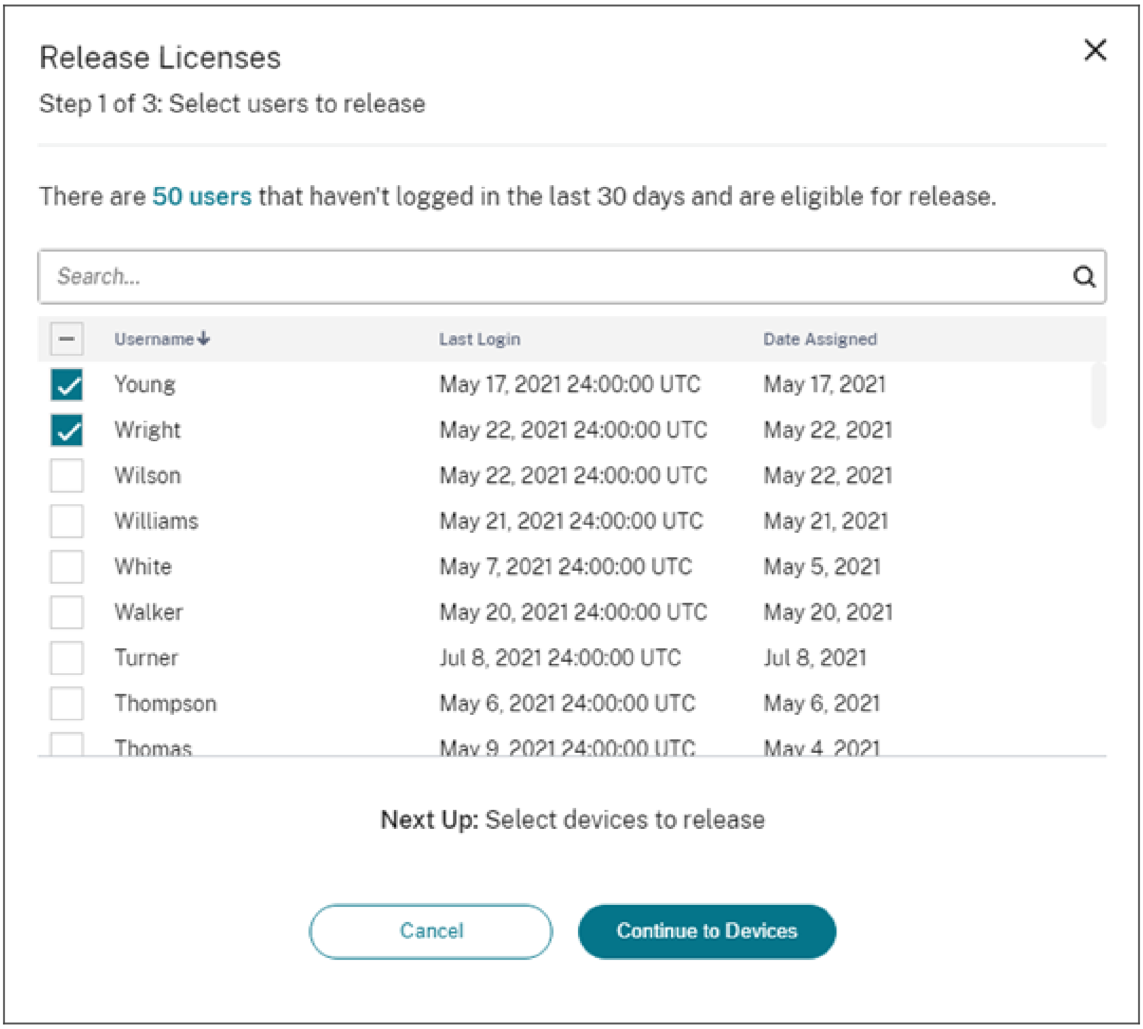
52 Licensed Users

122 Licensed Devices

Release Licenses

Username	Domain
Stewart	[illegible]

2. From the list, select the users you want to manage and select **Continue to Devices**.



Release Licenses

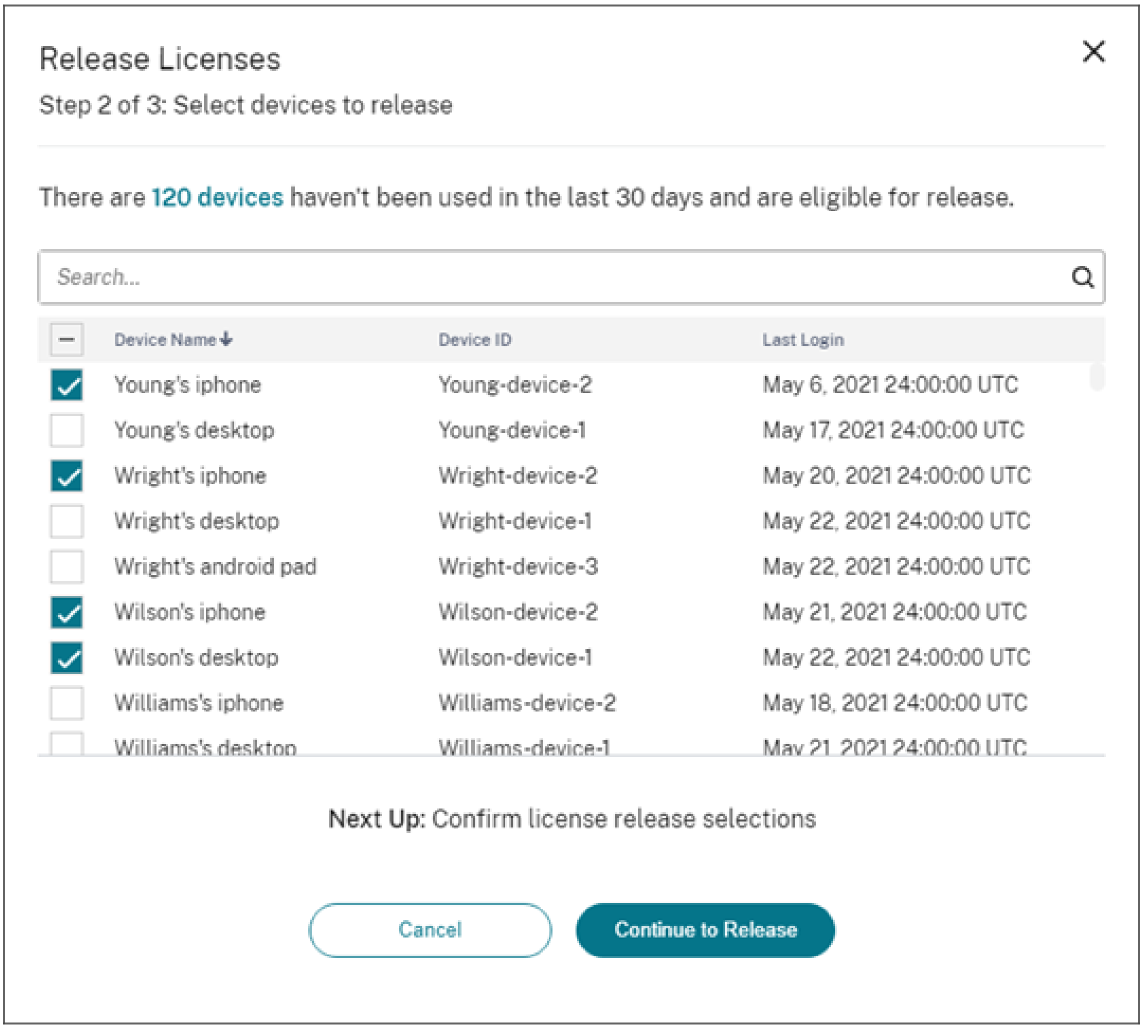
Step 1 of 3: Select users to release

There are 50 users that haven't logged in the last 30 days and are eligible for release.

▬	Username ↓	Last Login	Date Assigned
☑	Young	May 17, 2021 24:00:00 UTC	May 17, 2021
☑	Wright	May 22, 2021 24:00:00 UTC	May 22, 2021
□	Wilson	May 22, 2021 24:00:00 UTC	May 22, 2021
□	Williams	May 21, 2021 24:00:00 UTC	May 21, 2021
□	White	May 7, 2021 24:00:00 UTC	May 5, 2021
□	Walker	May 20, 2021 24:00:00 UTC	May 20, 2021
□	Turner	Jul 8, 2021 24:00:00 UTC	Jul 8, 2021
□	Thompson	May 6, 2021 24:00:00 UTC	May 6, 2021
□	Thomas	May 9, 2021 24:00:00 UTC	May 4, 2021

Next Up: Select devices to release

3. Select the devices you want to manage and select **Continue to Release**.



Release Licenses

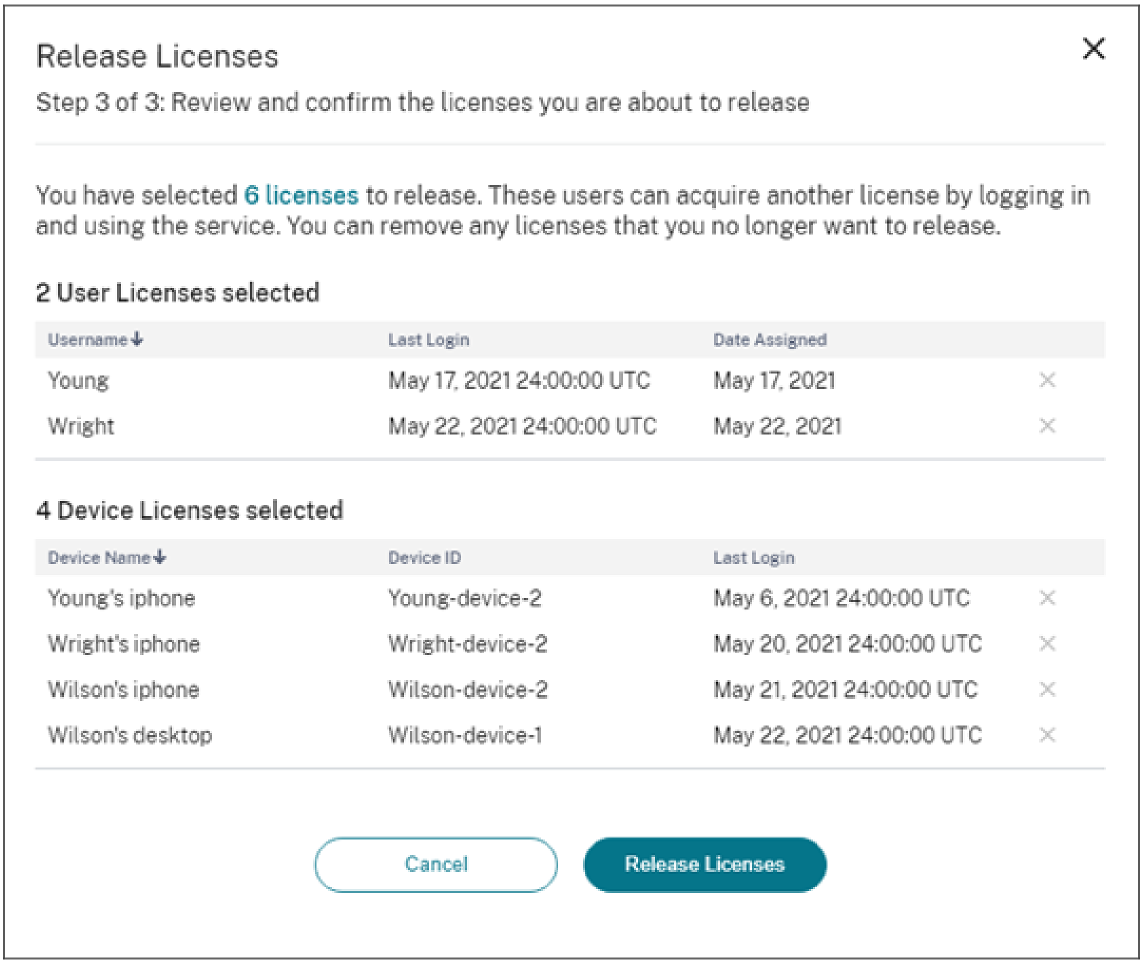
Step 2 of 3: Select devices to release

There are 120 devices haven't been used in the last 30 days and are eligible for release.

	Device Name	Device ID	Last Login
☑	Young's iphone	Young-device-2	May 6, 2021 24:00:00 UTC
□	Young's desktop	Young-device-1	May 17, 2021 24:00:00 UTC
☑	Wright's iphone	Wright-device-2	May 20, 2021 24:00:00 UTC
□	Wright's desktop	Wright-device-1	May 22, 2021 24:00:00 UTC
□	Wright's android pad	Wright-device-3	May 22, 2021 24:00:00 UTC
☑	Wilson's iphone	Wilson-device-2	May 21, 2021 24:00:00 UTC
☑	Wilson's desktop	Wilson-device-1	May 22, 2021 24:00:00 UTC
□	Williams's iphone	Williams-device-2	May 18, 2021 24:00:00 UTC
□	Williams's desktop	Williams-device-1	May 21, 2021 24:00:00 UTC

Next Up: Confirm license release selections

4. Review the licenses you've selected and select **Release Licenses**.



Release Licenses

Step 3 of 3: Review and confirm the licenses you are about to release

You have selected 6 licenses to release. These users can acquire another license by logging in and using the service. You can remove any licenses that you no longer want to release.

2 User Licenses selected

Username ↓	Last Login	Date Assigned	
Young	May 17, 2021 24:00:00 UTC	May 17, 2021	×
Wright	May 22, 2021 24:00:00 UTC	May 22, 2021	×

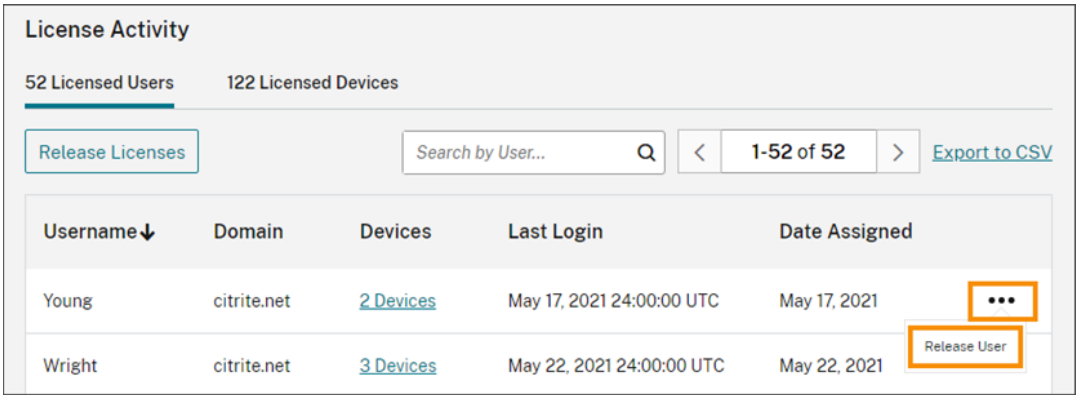
4 Device Licenses selected

Device Name ↓	Device ID	Last Login	
Young's iphone	Young-device-2	May 6, 2021 24:00:00 UTC	×
Wright's iphone	Wright-device-2	May 20, 2021 24:00:00 UTC	×
Wilson's iphone	Wilson-device-2	May 21, 2021 24:00:00 UTC	×
Wilson's desktop	Wilson-device-1	May 22, 2021 24:00:00 UTC	×

To release a single assigned license

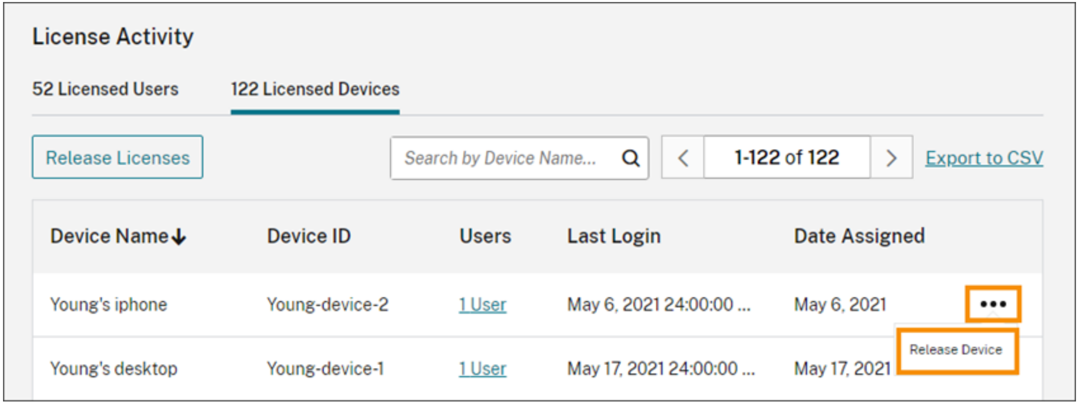
You can release individual licenses from the **Licensed Users** or **Licensed Devices** list. These lists display clickable ellipsis buttons only for users or devices with licenses that are eligible for release. The ellipsis button is inactive for individual users and individual devices that have launched any apps or desktops in the last 30 days.

1. Under **License Activity**, select the **Licensed Users** or **Licensed Devices** tab.
2. Locate the user or device you want to manage and release the license:
   a) To release a single user's license, click the ellipsis button and select **Release User**.



Username↓	Domain	Devices	Last Login	Date Assigned
Young	citrite.net	2 Devices	May 17, 2021 24:00:00 UTC	May 17, 2021
Wright	citrite.net	3 Devices	May 22, 2021 24:00:00 UTC	May 22, 2021

b) To release a single device, click the ellipsis button and select **Release Device**.



Device Name↓	Device ID	Users	Last Login	Date Assigned
Young's iphone	Young-device-2	1 User	May 6, 2021 24:00:00 ...	May 6, 2021
Young's desktop	Young-device-1	1 User	May 17, 2021 24:00:00 ...	May 17, 2021

3. Review your selection and then select **Continue**.
4. When prompted to confirm the release, select **Release**.

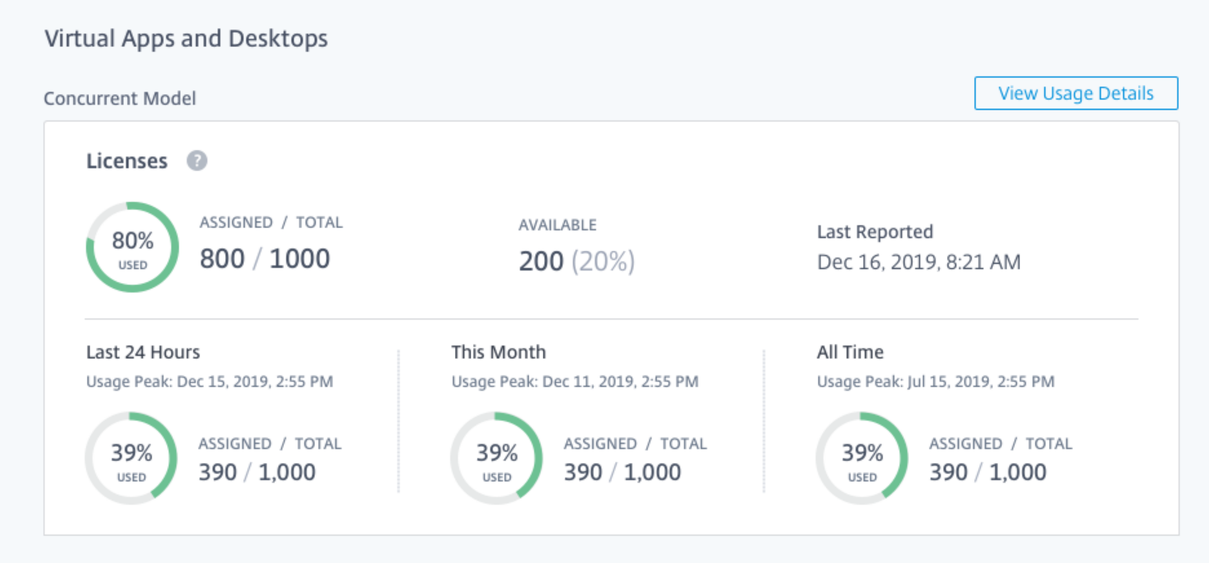
Monitor licenses and peak usage for Citrix Virtual Apps and Desktops service (Concurrent)

August 11, 2021

License assignment

Citrix Cloud assigns a license when a user launches an app or desktop on their device. When the user logs off or disconnects from the session, the license is no longer assigned. Because license assignment can change depending on the number of devices accessing apps or desktops at any given time, Citrix Cloud evaluates the number of licenses in use every five minutes. For more information about the Concurrent licensing model, see Concurrent licenses.

Licensing summary



Virtual Apps and Desktops

Concurrent Model

Licenses

80% USED

ASSIGNED / TOTAL 800 / 1000

AVAILABLE 200 (20%)

Last Reported Dec 16, 2019, 8:21 AM

Last 24 Hours
Usage Peak: Dec 15, 2019, 2:55 PM
39% USED
ASSIGNED / TOTAL 390 / 1,000

This Month
Usage Peak: Dec 11, 2019, 2:55 PM
39% USED
ASSIGNED / TOTAL 390 / 1,000

All Time
Usage Peak: Jul 15, 2019, 2:55 PM
39% USED
ASSIGNED / TOTAL 390 / 1,000

The Licensing summary provides an at-a-glance view of the following information:

- Percentage of total purchased licenses currently in use when Citrix Cloud last evaluated the licenses in use. Citrix Cloud calculates this percentage every five minutes based on unique devices with active connections to the service.

  The quantity of total purchased licenses is the sum of licenses that have been purchased for Virtual Apps, Virtual Desktops, and Virtual Apps and Desktops services that use the Concurrent licensing model.

- The ratio of currently assigned licenses to total purchased licenses and the number of available licenses remaining. The **Total** figure shown in this ratio represents the total number of licenses that are currently owned (as of the "Last Reported" date and time).

- Peak usage statistics. In calculating peak licenses in use, Citrix Cloud retrieves the the maximum number of licenses used in the following time periods:

  - **Last 24 hours:** The maximum number of licenses used at one time during the last 24-period period.
  - **This Month:** The maximum number of licenses used at one time from the start of the current calendar month.
  - **All Time:** The maximum number of licenses used at one time from the start of the subscription.

  The **Total** figure shown for these peak usage periods represents the total number of licenses that were owned at that point in time. If the total number of owned licenses increases or decreases, and there's corresponding increase in assigned licenses, the **Total** figure changes to reflect the new number of owned licenses for that point in time. However, if there is no corresponding usage peak, the **Total** figure does not change.

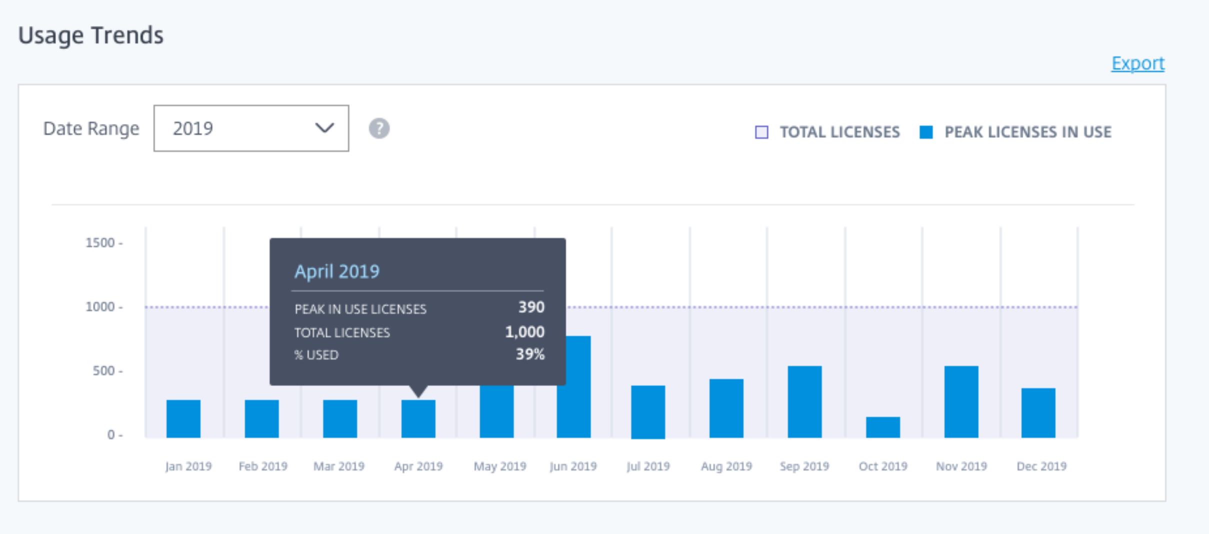
Calculating peak licenses in use

To accurately reflect the Concurrent licensing model for the Virtual Apps and Desktops service, Citrix Cloud counts the number of unique devices accessing the service simultaneously every five minutes. If the count is greater than the current peak usage displayed, Citrix Cloud displays the new peak usage with the date and time that it was reached. If the count is less than the current peak usage, the current peak usage doesn't change.

> **Important:**
>
> If you use Monitor in Director for information about concurrent sessions, be aware that the Monitor report provides a different interpretation of concurrent sessions and does not accurately reflect the number of concurrent licenses in use. For more information about the differences between Monitor reports and Licensing reports, see the FAQ.

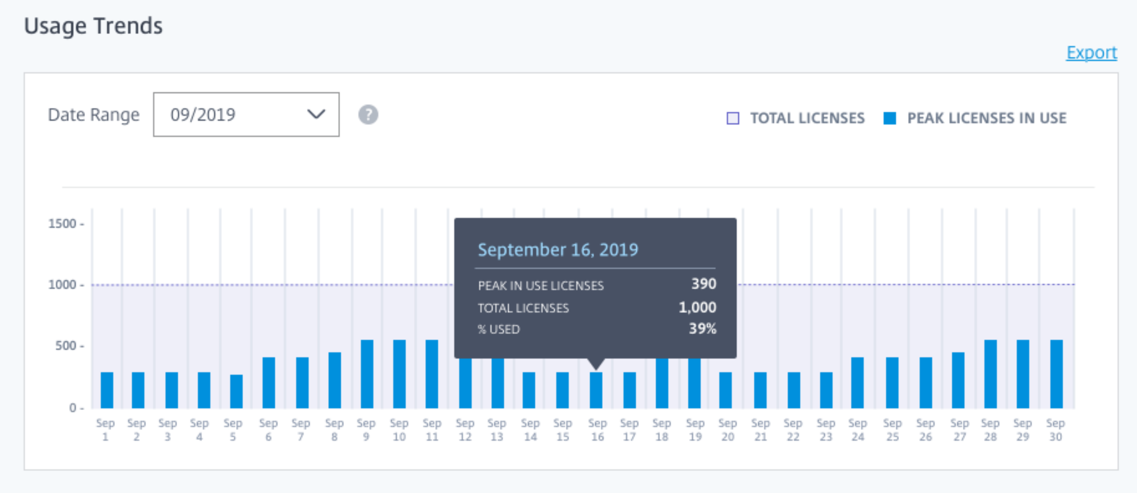
Usage trends and license activity

For a historical view of your licenses, click **View Usage Details**.



The **Usage Trends** breakdown shows you the following information:

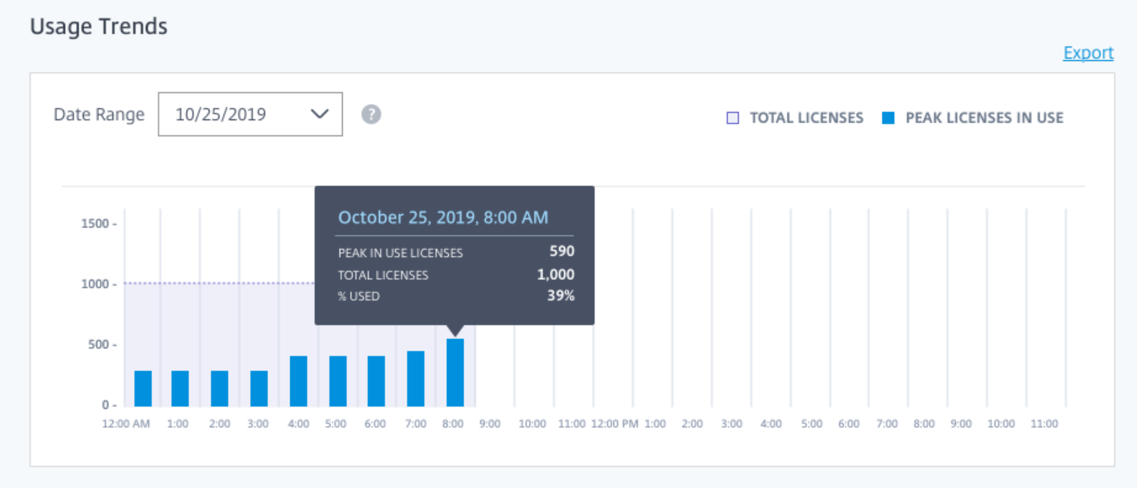
- **Total Licenses:** Your total purchased Concurrent licenses.
- **Peak Licenses In Use:** The maximum number of licenses assigned for the date range that you select. By default, Citrix Cloud displays peak usage for each month in the current calendar year. To drill down to monthly or hourly peak usage, select the calendar month or day you want to view from the **Date Range** menu.



September 16, 2019

PEAK IN USE LICENSES 390
TOTAL LICENSES 1,000
% USED 39%

If the date range you select isn't yet finished, Citrix Cloud displays the current peak usage for the latest interval of time. For example, if you drill down to view a calendar day that's still in progress, the maximum number of licenses is displayed for each hour up to the current moment in time. If the maximum number of licenses increases at the next five-minute counting interval, Citrix Cloud updates the peak usage for the current hour.



October 25, 2019, 8:00 AM

PEAK IN USE LICENSES 590
TOTAL LICENSES 1,000
% USED 39%

Monitor licenses and active usage for Citrix Virtual Apps and Desktops Standard for Azure service

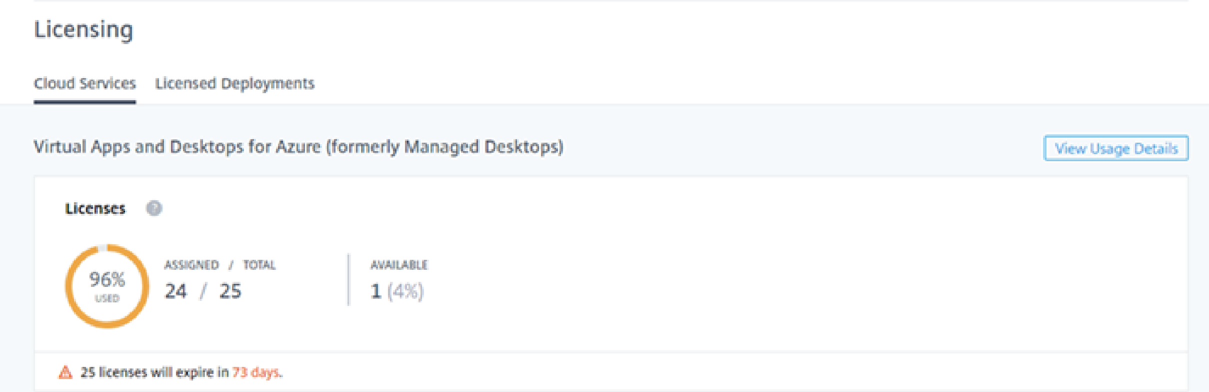
November 24, 2020

This article describes the cloud licensing reporting experience for the **User/Device** licensing model only.

License assignment

Citrix Cloud assigns a license when a unique user or unique device launches a desktop for the first time.

Licensing summary



25 licenses will expire in 73 days.

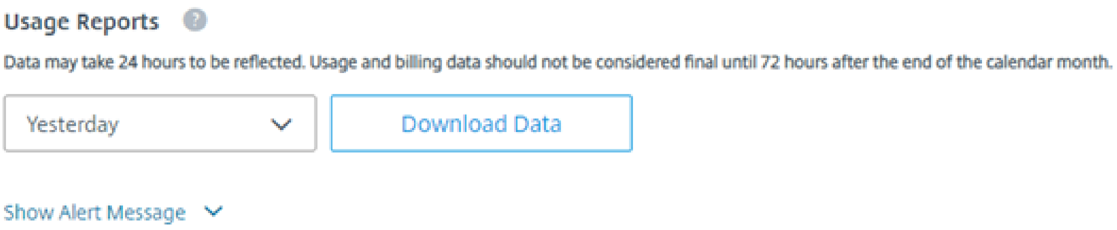
The licensing summary provides an at-a-glance view of the following information:

- Percentage of total purchased licenses assigned (used). As the percentage approaches 100%, the percentage goes from green to yellow. If the percentage exceeds 100%, the percentage turns red.
- The ratio of assigned licenses to purchased licenses and the number of available licenses remaining.

Click **View Usage Details** to see a breakdown of usage reports and trends, plus a list of users who are consuming Citrix Virtual Apps and Desktops Standard for Azure licenses.

> **Note:**
>
> Citrix Virtual Apps and Desktops Standard for Azure was formerly Citrix Managed Desktops. Some displays might contain the former name.

Usage reports



Data may take 24 hours to be reflected. Usage and billing data should not be considered final until 72 hours after the end of the calendar month.

You can download usage information for a standard or specified interval.

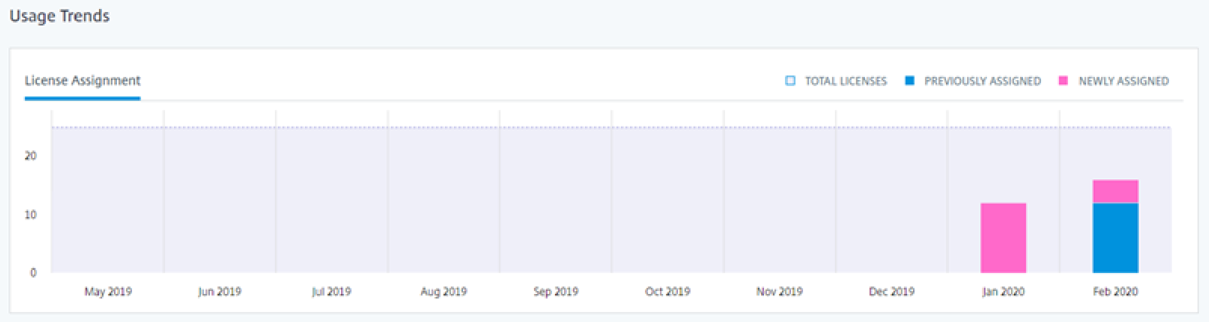
The information includes meter usage for:

- Azure VMs
- Network connections, such as VNet peering
- Azure storage items, such as managed disks, block blobs, and page blobs

Data can take up to 72 hours after the end of a day/month to reflect all usage.

Click **Download Data** to generate and download a CSV file to your local machine.

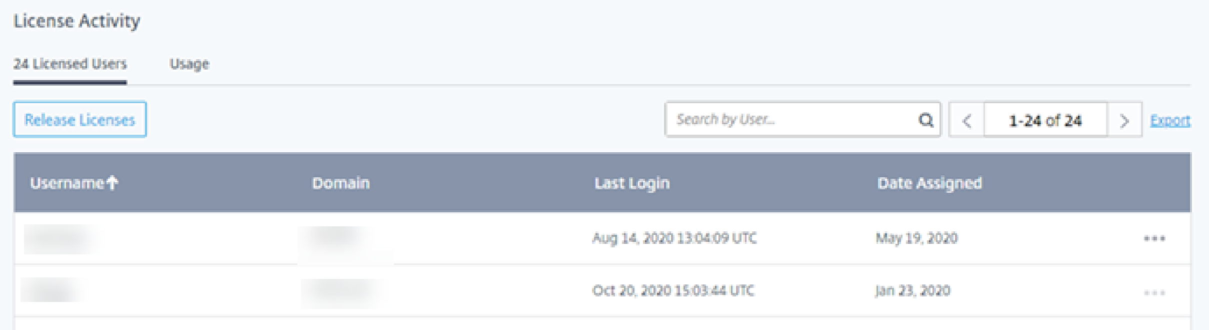
Usage trends and license activity



The **Usage Trends** breakdown shows the following information:

- **Total Licenses:** Your total purchased licenses for the cloud service across all entitlements.
- **Previously Assigned:** The number of licenses that were assigned in the previous month. For example, a user accesses the cloud service for the first time in July and is assigned a license. This license is counted as "Newly Assigned" for the month of July. For the month of August, this license is counted as "Previously Assigned."
- **Newly Assigned:** The number of new licenses that were assigned for each month. For example, a user accesses the cloud service for the first time in July and is assigned a license. This license is counted as "Newly Assigned" for the month of July.

The **License Activity** section displays a list of individual users who have assigned licenses, and the date when a license was assigned to the user.



Username↑	Domain	Last Login	Date Assigned	
[redacted]	[redacted]	Aug 14, 2020 13:04:09 UTC	May 19, 2020	•••
[redacted]	[redacted]	Oct 20, 2020 15:03:44 UTC	Jan 23, 2020	•••

Release assigned licenses

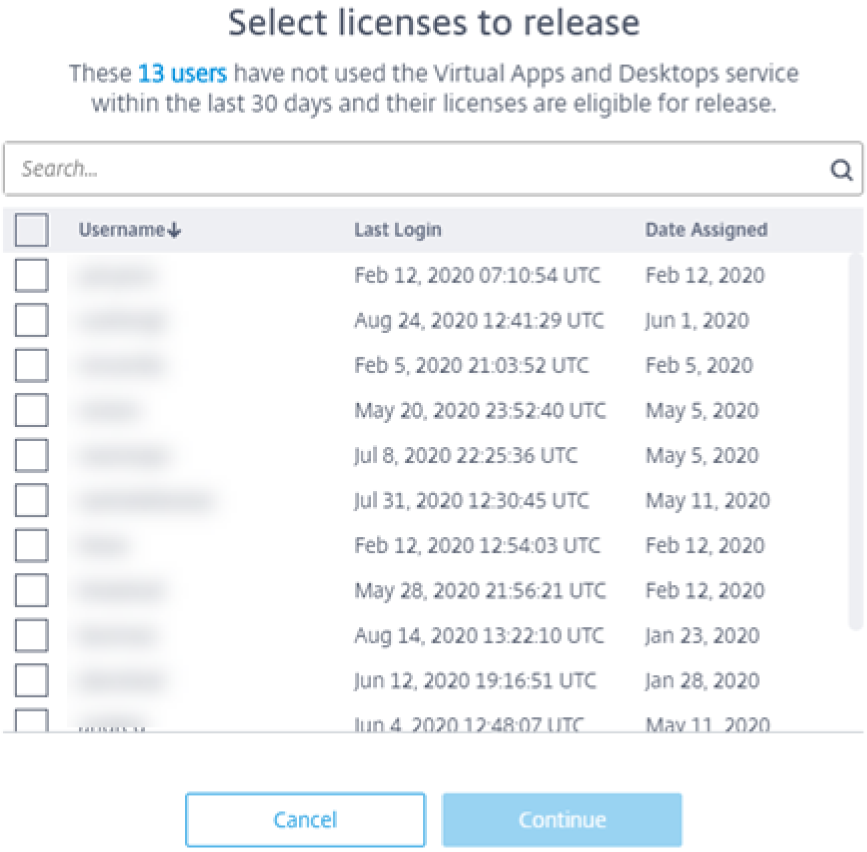
Yearly service subscriptions: If you have a yearly subscription, you can release licenses for users that haven't launched an app or a desktop in the last 30 days. You can release multiple licenses in bulk or individually.

Monthly service subscriptions: If you have a monthly subscription, you can release licenses on the first day of each month, regardless of the inactivity period.

When a license is released, the number of remaining licenses increases and the number of assigned licenses decreases accordingly. After a license is released, the user can acquire another license by logging in and using the cloud service.

To release multiple assigned licenses

1. Under **License Activity**, select **Release Licenses**.
2. From the list, select the users you want to manage and select **Continue**.



Select licenses to release

These 13 users have not used the Virtual Apps and Desktops service within the last 30 days and their licenses are eligible for release.

□	Username↓	Last Login	Date Assigned
□	[redacted]	Feb 12, 2020 07:10:54 UTC	Feb 12, 2020
□	[redacted]	Aug 24, 2020 12:41:29 UTC	Jun 1, 2020
□	[redacted]	Feb 5, 2020 21:03:52 UTC	Feb 5, 2020
□	[redacted]	May 20, 2020 23:52:40 UTC	May 5, 2020
□	[redacted]	Jul 8, 2020 22:25:36 UTC	May 5, 2020
□	[redacted]	Jul 31, 2020 12:30:45 UTC	May 11, 2020
□	[redacted]	Feb 12, 2020 12:54:03 UTC	Feb 12, 2020
□	[redacted]	May 28, 2020 21:56:21 UTC	Feb 12, 2020
□	[redacted]	Aug 14, 2020 13:22:10 UTC	Jan 23, 2020
□	[redacted]	Jun 12, 2020 19:16:51 UTC	Jan 28, 2020
□	[redacted]	Jun 4, 2020 12:48:07 UTC	May 11, 2020

3. Review the licenses you've selected and select **Release Licenses**.

To release a single assigned license

You can release individual licenses from the **License Activity** list. The list displays clickable ellipsis buttons only for users with licenses that are eligible for release.

1. Under **License Activity**, locate the user you want to manage. From the ellipsis menu for that user, select **Release User**.
2. Review your selection and then select **Continue**.
3. When prompted to confirm the release, select **Release**.

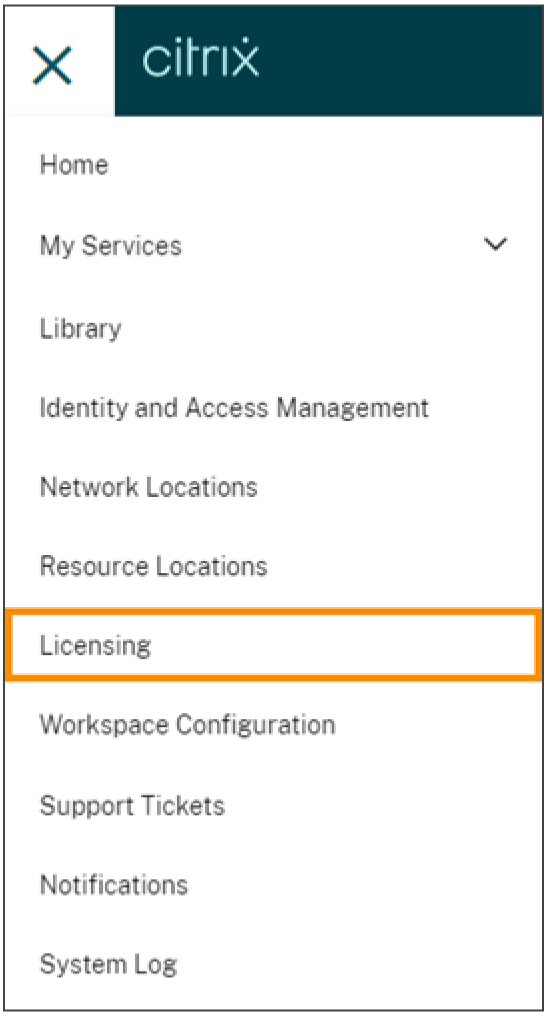
Monitor licenses and usage for on-premises deployments

January 9, 2020

The licensed deployments experience in Citrix Cloud consists of the following functions:

- Product registration: Register your existing Citrix License Servers with Citrix Cloud to get additional usage insights and reporting about your deployments. For more information about registering your License Servers, see Register on-premises products with Citrix Cloud.
- License Server status: View the status of your Citrix License Servers to understand which ones are successfully reporting usage and when they last reported usage to Citrix Cloud.
- Usage insights: View how many licenses are installed and in use across your Citrix License Servers and gain insight into historic license usage trends.

To view Citrix License Server usage insights, select **Licensing** from the console menu and then select **Licensed Deployments**.



Prerequisites

To use Citrix License Server usage insights, ensure you have the following items:

- A Citrix License Server version 11.15.0.0 or later
- A Citrix Cloud account
- Network access from the Citrix License Server to Citrix Cloud

Supported products

Citrix License Server usage insights are available for all Virtual Apps and Desktops editions under the Concurrent and User/Device licensing models.

View on-premises product license usage

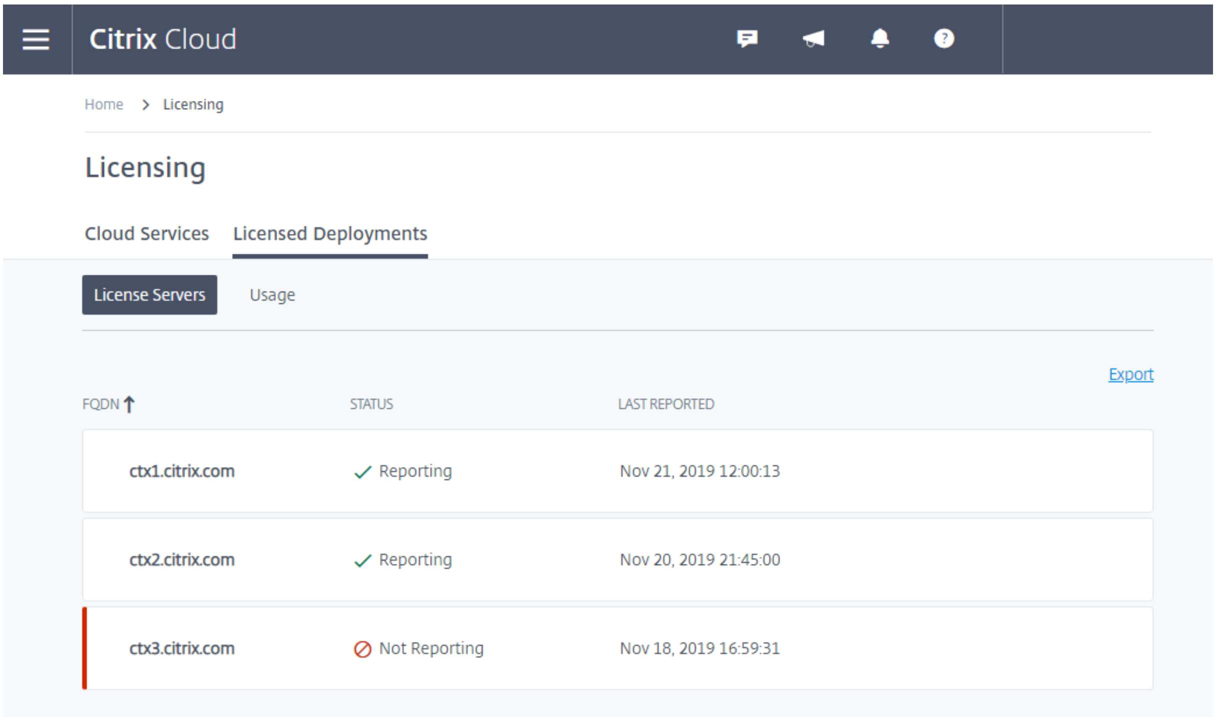
Citrix License Server usage insights provides visibility into license usage across your entire Citrix estate. After you enable usage insights for your license servers and register them with Citrix Cloud, you can access usage reporting that helps you:

- Understand how many license servers are deployed and registered, and if they are reporting usage information to Citrix Cloud.
- Get visibility into Concurrent and User/Device license usage for Virtual Apps and Desktops.
- Gain insight into aggregate Concurrent and User/Device license usage across multiple deployments.
- Understand historic license usage and monthly license usage trends.
- View the last login time for specific users.
- Compare the number of licenses installed relative to licenses in use across Citrix License Servers.
- Monitor license overdraft.
- View breakdowns of Concurrent and User/Device license usage.

For more information about registering your license servers, see Register on-premises products with Citrix Cloud.

View license server status

The license server status view shows each of the license servers reporting usage to Citrix Cloud.



FQDN ↑	STATUS	LAST REPORTED
ctx1.citrix.com	✓ Reporting	Nov 21, 2019 12:00:13
ctx2.citrix.com	✓ Reporting	Nov 20, 2019 21:45:00
ctx3.citrix.com	⊘ Not Reporting	Nov 18, 2019 16:59:31

License servers display the "Reporting" status if they have successfully uploaded usage to Citrix Cloud in the last three days. License servers display the "Not Reporting" status if they previously reported usage in the last 30 days but not reported in the last three days. License servers that haven't reported usage in the last 30 days are removed from the list.

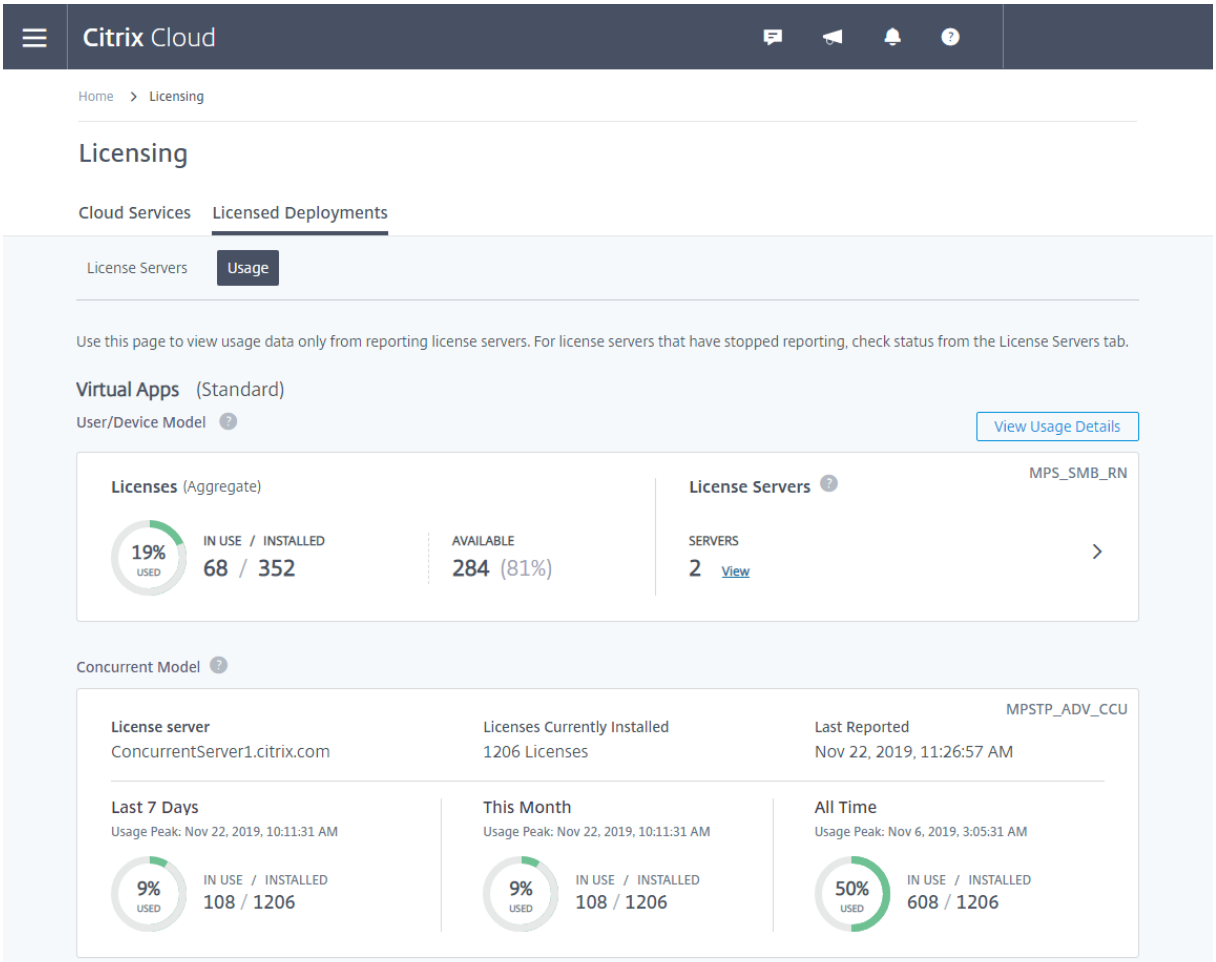
Impact of license server status on license usage views

The reporting status and Last Reported date of a license server dictates whether or not the usage from a particular license server is included in the usage insights views and reports.

- Current licenses installed and in-use are based exclusively on data from reporting license servers. If a license server is listed as "Not Reporting," installed and in-use licenses from that license server are not reflected in the usage insights experience.
- The Last Reported date for each license server determines how up-to-date the license usage information is in the usage insights experience. The license usage reports shown are only as current as the Last Reported time for each license server.
- Citrix License Servers configured for usage insights and registered with Citrix Cloud update usage once per day. If needed, you can force an update from the Citrix License Manager management console on the license server.

License Usage

The Usage tab provides a consolidated view of license usage across your Citrix deployments. Licensing information from each reporting license server is combined into a single view. This view makes it easy to see your complete licensing picture across many different deployments and license servers.



Use this page to view usage data only from reporting license servers. For license servers that have stopped reporting, check status from the License Servers tab.

Virtual Apps (Standard)

User/Device Model

Licenses (Aggregate)

19% USED

IN USE / INSTALLED 68 / 352

AVAILABLE 284 (81%)

License Servers

MPS_SMB_RN

SERVERS 2 View

Concurrent Model

MPSTP_ADV_CCU

License server	Licenses Currently Installed	Last Reported
ConcurrentServer1.citrix.com	1206 Licenses	Nov 22, 2019, 11:26:57 AM

Last 7 Days	This Month	All Time
Usage Peak: Nov 22, 2019, 10:11:31 AM	Usage Peak: Nov 22, 2019, 10:11:31 AM	Usage Peak: Nov 6, 2019, 3:05:31 AM
9% USED	9% USED	50% USED
IN USE / INSTALLED 108 / 1206	IN USE / INSTALLED 108 / 1206	IN USE / INSTALLED 608 / 1206

License usage is organized and aggregated across multiple license servers based on product edition and licensing model. A license usage summary card is displayed for each unique license edition found across all reporting license servers. A summary card is displayed for each product edition detected.

Peak license usage for the Concurrent licensing model

The reporting experience for Concurrent licenses is organized around the following data points:

- Installed licenses: The number of licenses installed on each license server.
- Peak licenses in-use: The maximum number of licenses that were used in a specific time frame.

In calculating peak licenses in-use, Citrix Cloud retrieves the the maximum number of licenses used in the following time periods:

- Last 7 days: The maximum number of licenses used at one time during the last seven days.
- This Month: The maximum number of licenses used at one time in the current calendar month.
- All Time: The maximum number of licenses used at one time since the license server was registered with Citrix Cloud.

> **Important:**
>
> The data for these time periods might not match the number of licenses in use on the license server. The license server reports only the number of licenses in use at any given time. Citrix Cloud receives these individual data points and calculates the peak for these time periods.

Considerations for interpreting license usage

Citrix licensing supports many usage scenarios and includes detailed information. Keep the following considerations in mind when monitoring usage:

- Usage information is based on licenses installed on each of the reporting license servers. If a license server is running out of available licenses, you can allocate and place additional licenses on the license server to increase the number of available licenses.
- The information available in the Citrix License Server usage insights view includes only the information collected and reported by registered and actively reporting Citrix License Servers. The licensed deployments experience does not represent and may not match the total number of licenses you actually own or purchased.
- The percentage of licenses available is computed based on the number of licenses in use relative to the licenses installed on reporting license servers.

Register on-premises products with Citrix Cloud

September 1, 2021

You can easily register your on-premises Citrix product using short-code activation through Citrix Cloud. Depending on your product, this 8-digit code might be generated during the product installation process or when you run the product's management console. When the product prompts you to register, the product requests the code from Citrix Cloud and displays it. You can then copy and paste this code or enter it manually in Citrix Cloud.

Register an on-premises License Server

Product registration is supported for Citrix License Server. To use this feature, you must perform the following tasks:

- Enable Call Home.
- Register your License Server with Citrix Cloud from the Citrix Licensing Manager console.

To register your on-premises License Server with Citrix Cloud, see Register and remove registration of your Citrix License Server.

Connectivity requirements

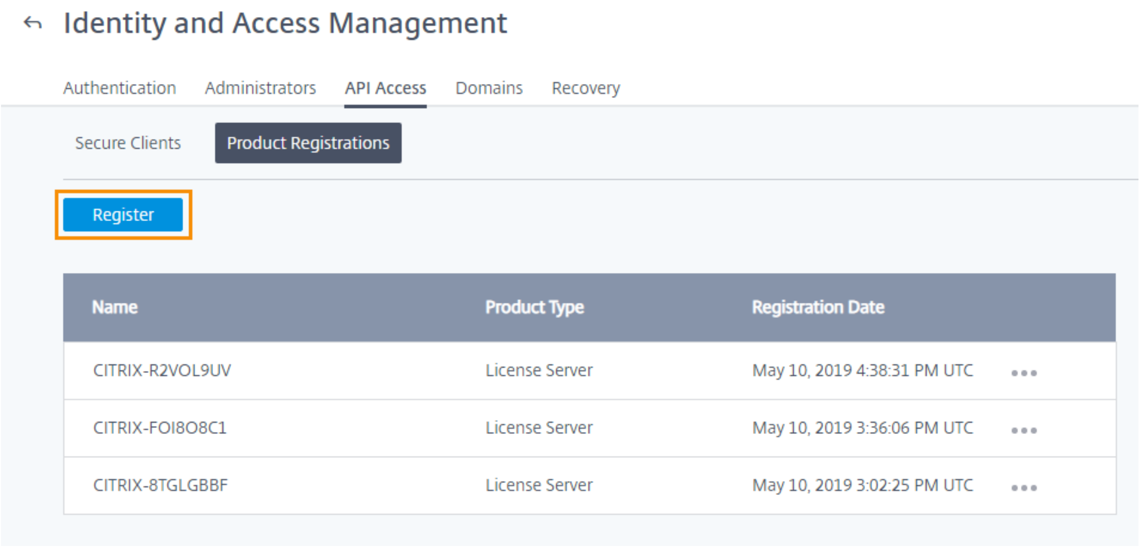
To register your on-premises products successfully, ensure that the following addresses are contactable:

- `https://trust.citrixnetworkapi.net` (for retrieving a code)
- `https://trust.citrixworkspacesapi.net/` (for confirming the license server is registered)
- `https://cis.citrix.com` (for data upload)
- `https://core-eastus-release-a.citrixworkspacesapi.net`
- `https://core.citrixworkspacesapi.net` (for confirming that the license server certificate has not been revoked)
- `ocsp.digicert.com port 80`
- `crl3.digicert.com port 80`
- `crl4.digicert.com port 80`
- `ocsp.entrust.net port 80`
- `crl.entrust.net port 80`

If you are using a proxy server with Citrix License Server, ensure that the proxy server is configured as described in Configure a proxy server in the Licensing product documentation.

Register a product

1. From the Citrix Cloud menu, select **Identity and Access Management**.
2. Select **API Access > Product Registrations** and then select **Register**.



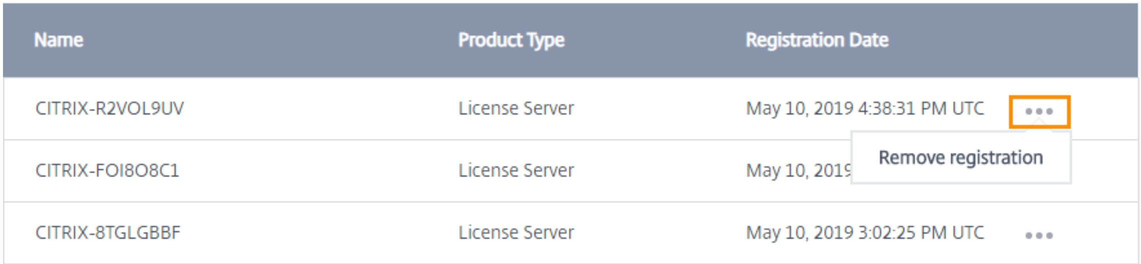
Name	Product Type	Registration Date
CITRIX-R2VOL9UV	License Server	May 10, 2019 4:38:31 PM UTC
CITRIX-FOI8O8C1	License Server	May 10, 2019 3:36:06 PM UTC
CITRIX-8TGLGBBF	License Server	May 10, 2019 3:02:25 PM UTC

3. Enter the 8-digit product registration code for your Citrix product and click **Continue**.
4. Review the registration details and then click **Register**.

Remove a product registration

If you remove servers running a registered Citrix product from your environment, the Product Registrations page still displays the servers. Use the following steps to remove the servers from Citrix Cloud. If needed, you can register the product again later to display the servers on the Product Registrations page.

1. From the Product Registrations page, locate the server you want to remove.
2. Click the ellipsis button and select **Remove registration**.



Name	Product Type	Registration Date	
CITRIX-R2VOL9UV	License Server	May 10, 2019 4:38:31 PM UTC	•••
CITRIX-FOI8O8C1	License Server	May 10, 2019	
CITRIX-8TGLGBBF	License Server	May 10, 2019 3:02:25 PM UTC	•••

3. When prompted, select **Remove**.

Licensing for Citrix Service Providers

August 26, 2021

The License Usage Insights service in Citrix Cloud is a free cloud service that helps **Citrix Service Providers (CSP)** understand and report on product licenses and usage. Only CSP partners have access to License Usage Insights.

The License Usage Insights service enables you to:

- Automatically collect and aggregate product usage information from Citrix license servers
- Automatically aggregate cloud licensing usage and consumption for single-tenant and multi-tenant customers
- Easily view which users are accessing your Virtual Apps and Desktops deployments each month
- Create customer breakdowns of licensing usage
- Optimize license costs by identifying and tracking a list of free users
- View and understand your historic business with Citrix
- Export Virtual Apps and Desktops product and cloud license usage, ADC VPX allocations data, and Virtual Apps and Desktops Standard for Azure licensing and consumption data to CSV

Additional information

For requirements and setup instructions, see Get started with License Usage Insights.

To view aggregated usage for single tenant customers and multitenant partners, see Cloud service license usage and reporting for Citrix Service Providers.

To view customers' usage of supported services using the Licensing console, see the following articles:

- Customer license and usage monitoring for Citrix Virtual Apps and Desktops service
- Customer license and usage monitoring for Citrix Virtual Apps and Desktops Standard for Azure

Get started with License Usage Insights

August 26, 2021

Supported Citrix products

The License Usage Insights service provides usage information for the following Citrix products:

- Virtual Apps and Desktops (on-premises) product usage
- Virtual Apps Premium and Virtual Apps and Desktops Premium services
- Virtual Apps and Desktops Standard for Azure
- Citrix ADC VPX allocations

Requirements

To capture license and usage information for Citrix on-premises products, Citrix License Server 11.16.3.0 or later is required. Only Windows-based and VPX-based license servers are supported.

Citrix License Server 11.16.3.0 and later contains key features that are important for Citrix Service Provider (CSP) partners:

- Optimized usage collection: License Server contains new functionality that optimizes licensing behavior and tracking to better support CSPs.
- Call home: License Server includes Call Home features that automate product usage collection for CSP partners. These features are exclusive to CSP partners and will only be activated when a CSP license is detected on the license server.

Step 1: Update Citrix License Server

If you're running license servers older than Version 11.16.3.0, you must upgrade your license servers before using License Usage Insights. Upgrading in-place is simple and fast. Complete the following tasks:

1. Download the latest license server. For more information about the latest version of Citrix License Server, refer to the Citrix Licensing documentation.
2. Upgrade your current license server.
3. Repeat the upgrade process for each of your license servers.

Step 2: Sign in to Citrix Cloud with My Citrix credentials

Before signing in, you'll need to sign up for a Citrix Cloud account. Follow the steps described in Sign up for Citrix Cloud.

When creating your account, use the same My Citrix credentials that you use to allocate and download Citrix licenses from citrix.com. Citrix Cloud sends you an email at the address associated with your My Citrix credentials to confirm the account.

When your Citrix Cloud account is ready to use, sign in at https://citrix.cloud.com using your email address and password.

Step 3: Register Citrix License Server with Citrix Cloud

To view the licensing details for different products in License Usage Insights, register your license server with Citrix Cloud. For more information about registering your license server with Citrix Cloud, see Register and remove registration of your Citrix License Server.

Step 4 (optional): Anonymize usernames through the license server

By default, usernames associated with Virtual Apps and Desktops license checkouts are securely phoned home to Citrix.

Usernames are phoned home so CSP partners can take full advantage of License Usage Insights features and the CSP licensing program which supports free users for trial, test, and administrative product use.

User information is limited to a single user@domain entry; no additional personal identifiable data is phoned home. Citrix does not share this information.

Partners sensitive to uploading username information can enable username anonymization. When active, username anonymization converts readable usernames into unique strings using a secure and irreversible algorithm prior to upload.

License Usage Insights uses these unique identifiers to track product usage instead of the actual usernames. This approach allows service providers to take advantage of month-to-month insights without visibility into the actual usernames in the cloud service user interface.

To configure username anonymization

1. On the license server, open the configuration file in a text editor. Typically, the configuration file is located at C:\Program Files\Citrix\Licensing\WebServicesForLicensing\SimpleLicenseServiceConfig.xml.
2. In the **Configurations** section, add the **UsageBasedBillingScramble** setting as follows:

```
<?xml version="1.0" encoding="utf-8"?>
<Configurations>
<EncoreConfiguration>
<SamplingPeriod>15</SamplingPeriod>
<RetentionTime>180</RetentionTime>
<Enabled>true</Enabled>
</EncoreConfiguration>
<SARenewalConfigOptions>Notify</SARenewalConfigOptions>
<UsageBasedBillingScramble>1</UsageBasedBillingScramble>
</Configurations>
<!--NeedCopy-->
```

3. Save the file.

Step 5: Use the License Usage Insights service

From the Citrix Cloud console, locate the License Usage Insights service and click **Manage**. For an overview of the service's key features, see Manage product usage, license servers, and notifications.

Additional details

When using Citrix License Server with License Usage Insights, consider the following items:

- It might take up to 24 hours for a newly updated license server to appear in the License Usage Insights management console.
- When usage data is uploaded from a license server, it's processed and stored in a secure fashion so License Usage Insights can access it at a later date. This process might take up to 24 hours to complete.
- By default, usernames associated with Virtual Apps and Desktops license checkouts are securely phoned home to Citrix.
- Usernames are phoned home so CSP partners can take full advantage of License Usage Insights features and the CSP licensing program which supports free users for trial, test, and administrative product use.
- User information is limited to a single user@domain entry; no additional personal identifiable data is phoned home. Citrix will never share this information.

Help and support

If you need assistance with License Usage Insights, open a support ticket on the My Support portal. To access My Support from Citrix Cloud:

1. Sign in to Citrix Cloud.
2. Click the **Help** icon near the top-right of the screen.
3. Select **Open a ticket**.
4. Select **Go to My Support** and sign in with your My Citrix credentials.
5. Complete and submit the form.

A member of Citrix Technical Support will follow up and assist you.

Frequently Asked Questions

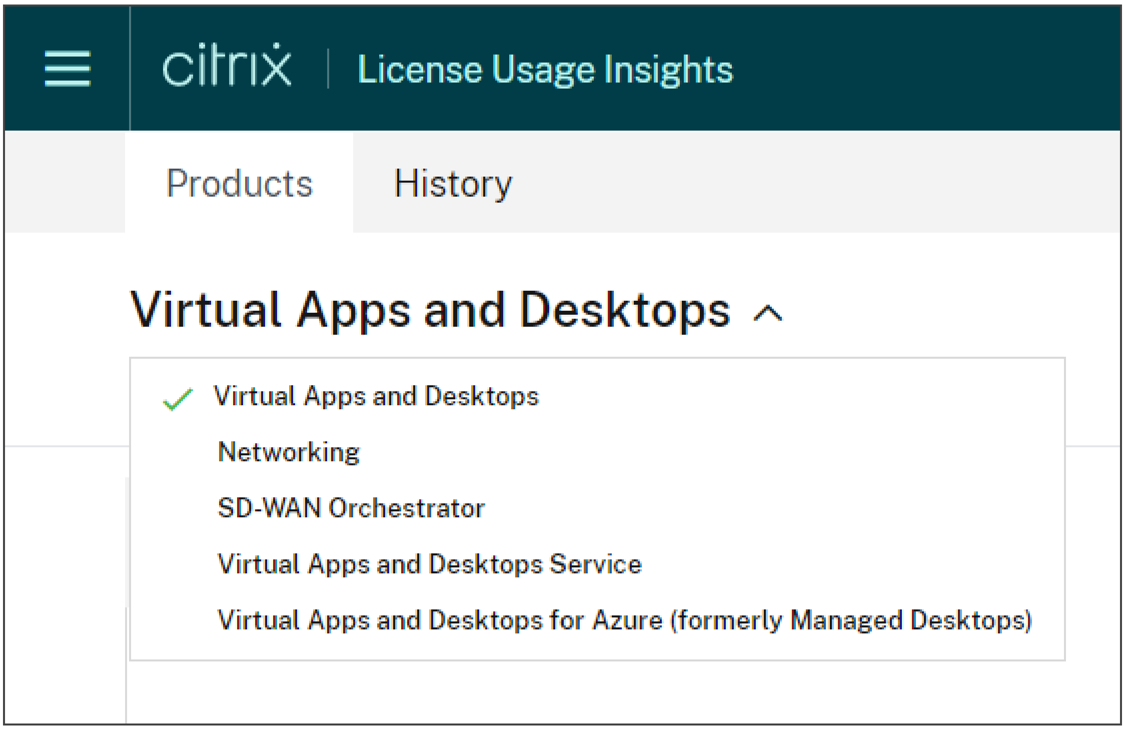
- **What information is being phoned home? Can I view the information my license servers are sending to Citrix?** Yes, you can view a copy of the information that's phoned home to Citrix. For details, see License server information included in uploads.
- **Is License Usage Insights available to Citrix customers or partners that are not Citrix Service Providers?** No. License Usage Insights is only available to Citrix Service Provider partners with an active partner agreement.
- **Can I disable Call Home on the license server?** No. Under the Citrix Service Provider license agreement, all license servers are required to phone home product usage. Partners sensitive to the phone home use case can use the username anonymization feature. For details, see Anonymize usernames through the license server.
- **Will I be billed based on the product usage shown in License Usage Insights?** No. License Usage Insights helps partners understand their product usage so they can report it quickly and accurately to their Citrix distributor. CSP partners will continue to be billed based on the product usage they report to their Citrix distributor. Citrix distributors will continue to own the billing relationship with CSP partners.

Manage product usage, license servers, and notifications

August 20, 2021

Product selection

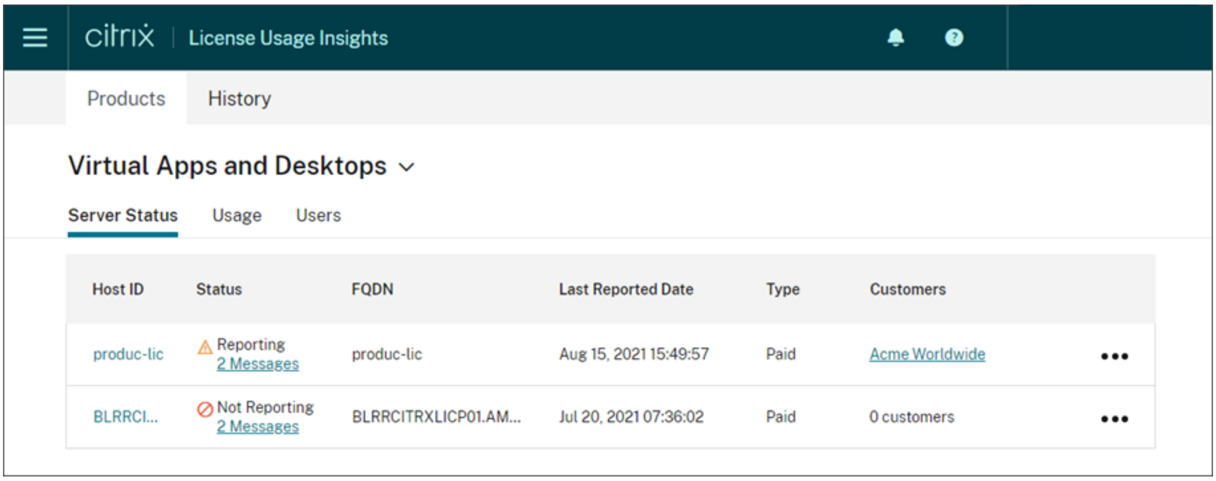
To view licensing details for a different product, click the arrow next to the product name and select the product or service you want to view.


citrix
License Usage Insights
Products
History
Virtual Apps and Desktops
✓ Virtual Apps and Desktops
Networking
SD-WAN Orchestrator
Virtual Apps and Desktops Service
Virtual Apps and Desktops for Azure (formerly Managed Desktops)

License server status

To be compliant with Citrix Service Provider license guidelines, all active license servers must be updated and reporting. The license server status shows the license servers you have and whether or not they're updated for use with License Usage Insights.

The service displays a list of active license servers using the license allocation data stored in the Citrix back office. If the license server is updated and successfully reporting, License Usage Insights displays the "Reporting" status and includes a timestamp of the most recent upload.



Host ID	Status	FQDN	Last Reported Date	Type	Customers	
produc-lic	⚠ Reporting 2 Messages	produc-lic	Aug 15, 2021 15:49:57	Paid	Acme Worldwide	•••
BLRRCI...	⊘ Not Reporting 2 Messages	BLRRCITRXLICP01.AM...	Jul 20, 2021 07:36:02	Paid	0 customers	•••

License server information included in uploads

When Call Home is activated on a license server, the following information is uploaded daily:

- License server version
- License file information:
  - License files installed on the server
  - License file expiration dates
  - Product feature and edition entitlement information
  - License quantities
- License usage:
  - Licenses used in the current calendar month
  - Usernames associated with license checkout
  - Product features and editions activated

View a license server upload

CSP partners can inspect the last uploaded payload on their license server to fully understand all of the details that the license server sends to Citrix. A copy of this payload is stored as a .zip file on the license server. By default, this location is C:\Program Files (x86)\Citrix\Licensing\LS\resource\usage\upload_1456166761.zi

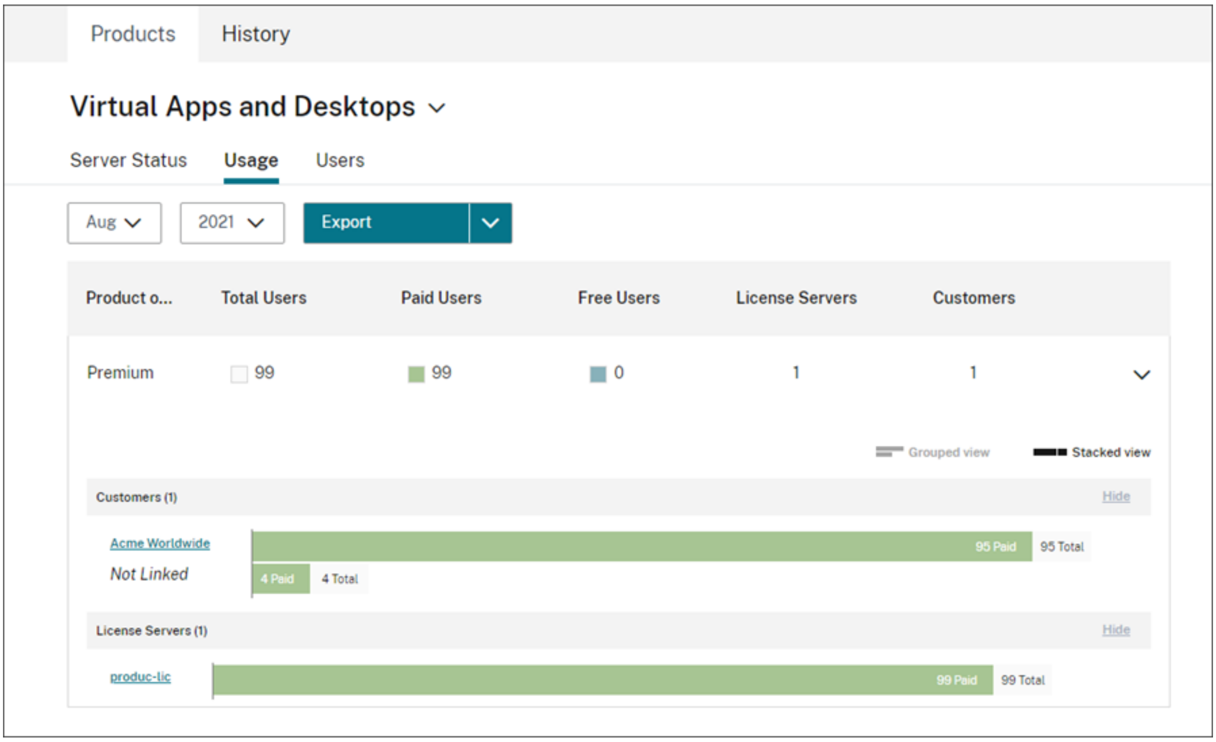
> **Note:**
>
> Successful uploads are deleted except for the last one. Unsuccessful uploads linger on the disk until a successful upload occurs. When that happens, all but the last upload are deleted.

Usage collection

Usage collection helps you understand product usage through automated data collection and aggregation. There's no need to deploy additional tools.

License Usage Insights automatically aggregates product usage across all Citrix License Servers to provide a complete view of usage across all deployments. You can also create licensing usage breakdowns by associating specific users with the customers or tenants to whom they belong.

The license servers collect and track product license usage and report it back to Citrix using a secure phone home channel. This automated approach provides you with a constant stream of updated usage data, saving time and helping partners better understand usage trends within their deployments.



Product o...	Total Users	Paid Users	Free Users	License Servers	Customers
Premium	□ 99	🟩 99	🟦 0	1	1

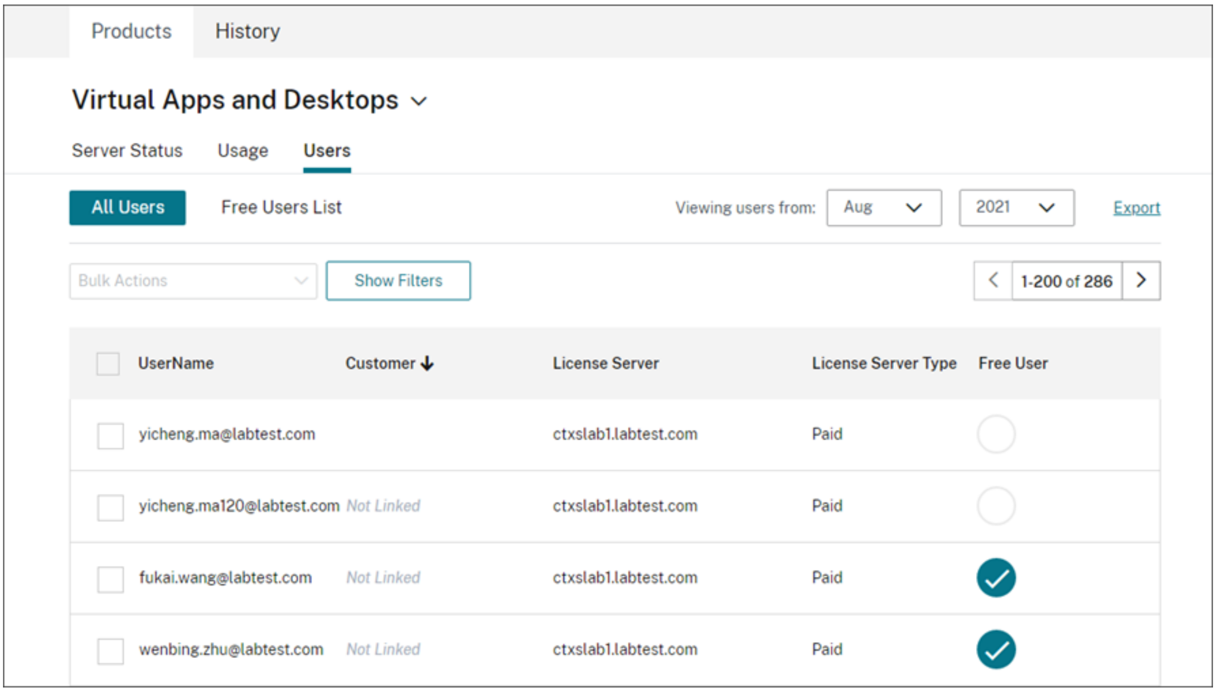
Create a customer breakdown of Virtual Apps and Desktops product usage

To break down licensing usage by customer, you must first associate users with the customers or tenants to whom they belong. If you don't have any customers defined in your Customers dashboard, you can add new ones or you can connect with existing Citrix Cloud customers.

1. If applicable, add customers to the Customers dashboard: From the Citrix Cloud management console home page, click **Customers**, click **Add or Invite**, and then follow the onscreen instructions.
2. Click the menu button and then select **My Services > License Usage Insights**.
3. With the **Virtual Apps and Desktops** product selected, click **Users**.
4. Select the users you want to associate and then click **Bulk Actions > Manage Link to Customer**.
5. From the list, select the customer with which to you want associate the users.
6. Click **Save**.
7. To view the per-customer breakdown, click the **Usage** view.

Free user management

License Usage Insights provides a comprehensive view of product usage across deployments while still allowing you to take full advantage of the Citrix Service Provider license program that supports trial, test, and administrative users.



Viewing users from: Aug 2021

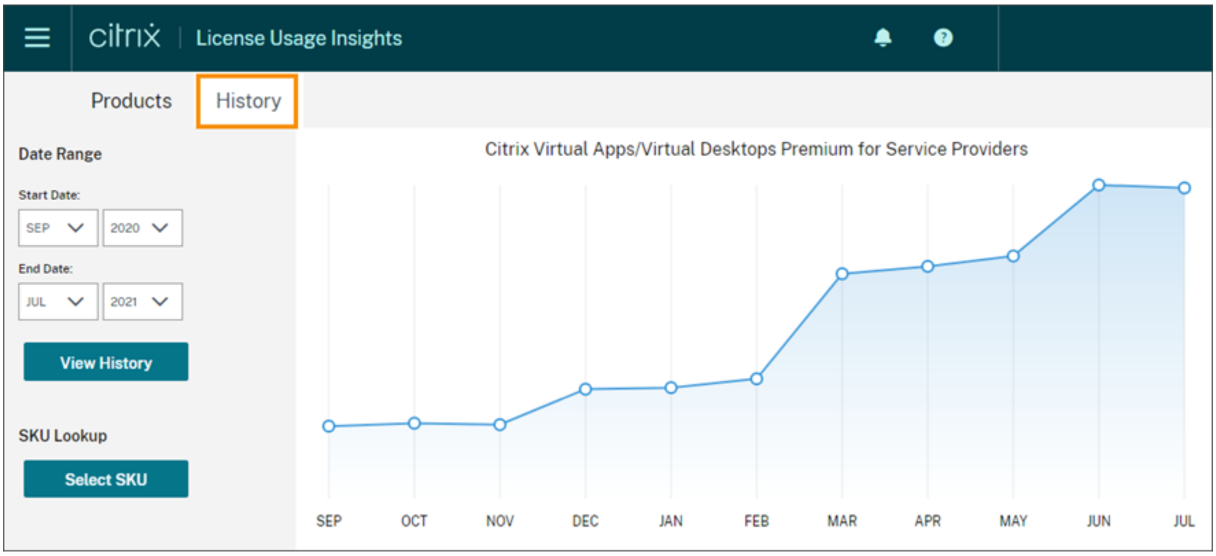
1-200 of 286

□	UserName	Customer ↓	License Server	License Server Type	Free User
□	yicheng.ma@labtest.com		ctxslab1.labtest.com	Paid	○
□	yicheng.ma120@labtest.com	*Not Linked*	ctxslab1.labtest.com	Paid	○
□	fukai.wang@labtest.com	*Not Linked*	ctxslab1.labtest.com	Paid	✓
□	wenbing.zhu@labtest.com	*Not Linked*	ctxslab1.labtest.com	Paid	✓

Historical trends

You can view a complete historical record of all of your past business with Citrix. Check the usage you reported last month, last year, or over a configurable time period.

Historical views deliver valuable business insight. As a Citrix Service Provider, you can quickly understand how your business with Citrix is trending and which products are seeing the most growth across your customers and subscribers.



Date Range

Start Date: SEP 2020

End Date: JUL 2021

Export usage and allocations data

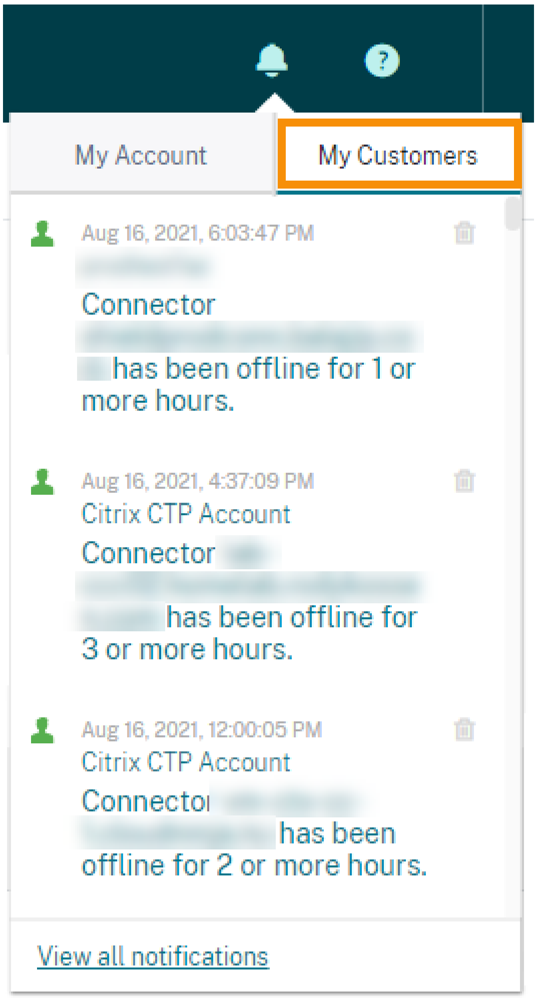
You can export the following types of data as a CSV file from License Usage Insights:

- Virtual Apps and Desktops product usage and user list for a specified month
- Current ADC VPX allocation details

1. Select **Virtual Apps and Desktops** or **Networking** from the product list.
2. If applicable, select the view you want to export. For example, to export Virtual Apps and Desktops usage details, click the **Usage** view.
3. If applicable, select the month and year you want to export.
4. On the right side of the screen, click **Export**.

View customer notifications

Citrix Cloud enables you to monitor solution health across multiple customers without having to visit each deployment individually. The Notifications area in Citrix Cloud aggregates notifications across customers on your dashboard so you can ensure alerts are addressed and services keep running.



Aug 16, 2021, 6:03:47 PM
[redacted]
Connector [redacted] has been offline for 1 or more hours.

Aug 16, 2021, 4:37:09 PM
Citrix CTP Account
Connector [redacted] has been offline for 3 or more hours.

Aug 16, 2021, 12:00:05 PM
Citrix CTP Account
Connector [redacted] has been offline for 2 or more hours.

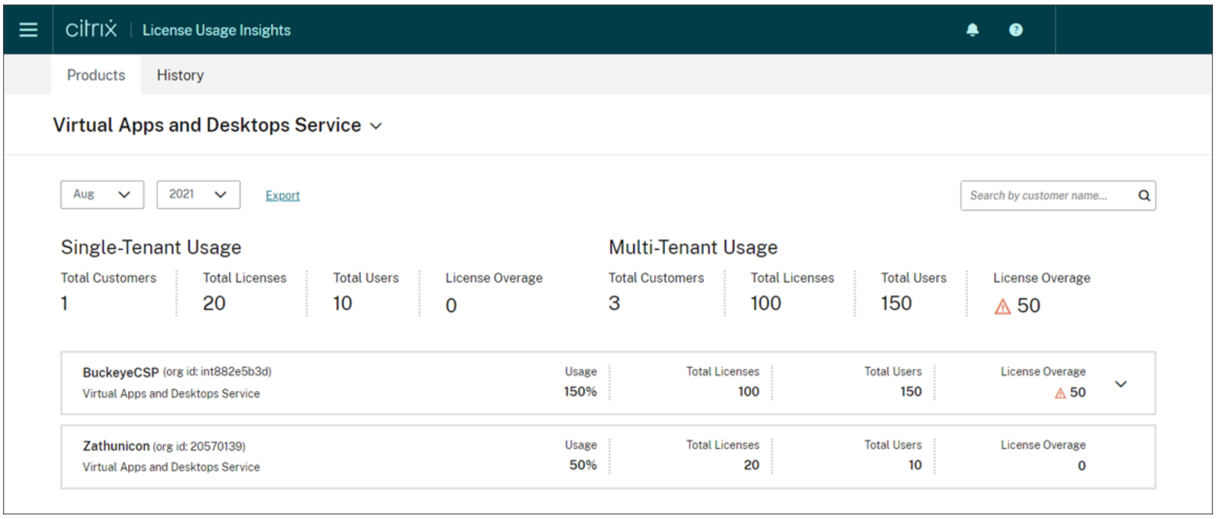
View all notifications

1. From the Citrix Cloud management console, click the **Notifications** icon and then click **My Customers**. A list of the most recent notifications appears.
2. To view a complete list of customer notifications, click **View all notifications**.

Cloud service license usage and reporting for Citrix Service Providers

August 26, 2021

License Usage Insights automatically aggregates cloud service usage to provide a complete view across all single-tenant customers and multitenant partners. You can also export these details for a given month to a CSV file for further analysis.


citrix | License Usage Insights
Products
History
Virtual Apps and Desktops Service
Aug
2021
Export
Search by customer name...

Single-Tenant Usage

Total Customers	Total Licenses	Total Users	License Overage
1	20	10	0

Multi-Tenant Usage

Total Customers	Total Licenses	Total Users	License Overage
3	100	150	⚠ 50

	Usage	Total Licenses	Total Users	License Overage
BuckeyeCSP (org id: int882e5b3d) Virtual Apps and Desktops Service	150%	100	150	⚠ 50
Zathunicon (org id: 20570139) Virtual Apps and Desktops Service	50%	20	10	0

Supported services

Single-tenant license usage is available for the following services:

- Virtual Apps Premium
- Virtual Apps and Desktops Premium

Multitenant license usage is available for the following services:

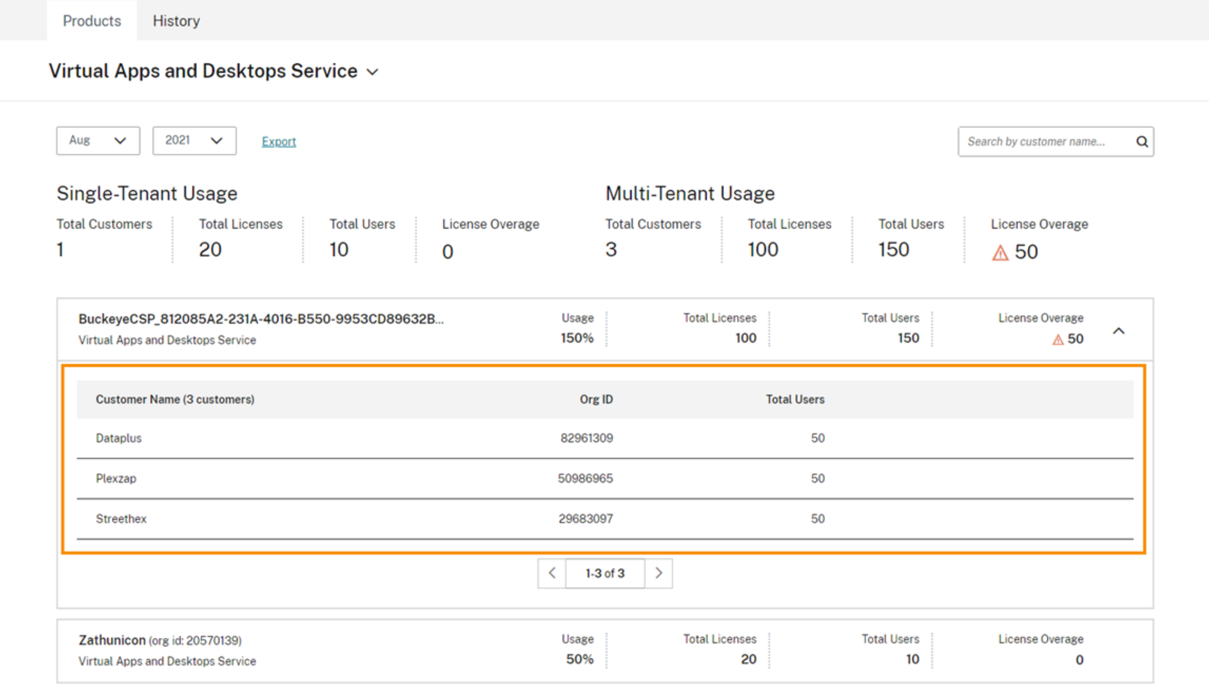
- Virtual Apps and Desktops
- Virtual Apps and Desktops Standard for Azure

Licensing summaries

License Usage Insights provides the following breakdown for single tenant and multitenant usage:

- At-a-glance summary grouped by tenant type that includes the total number of customers and the total number of purchased licenses, users, and overassigned licenses across all customers.
- Usage summary for each customer or partner that includes the percentage of total licenses in use, total purchased licenses, users, and number of overassigned licenses.

For multitenant services, you can expand the usage summary to view the customers, OrgID, and total users associated with each partner.



Single-Tenant Usage

Total Customers	Total Licenses	Total Users	License Overage
1	20	10	0

Multi-Tenant Usage

Total Customers	Total Licenses	Total Users	License Overage
3	100	150	⚠ 50

BuckeyeCSP_812085A2-231A-4016-B550-9953CD89632B...
Virtual Apps and Desktops Service

Usage	Total Licenses	Total Users	License Overage
150%	100	150	⚠ 50

Customer Name (3 customers)	Org ID	Total Users
Dataplus	82961309	50
Plexzap	50986965	50
Streethex	29683097	50

1-3 of 3

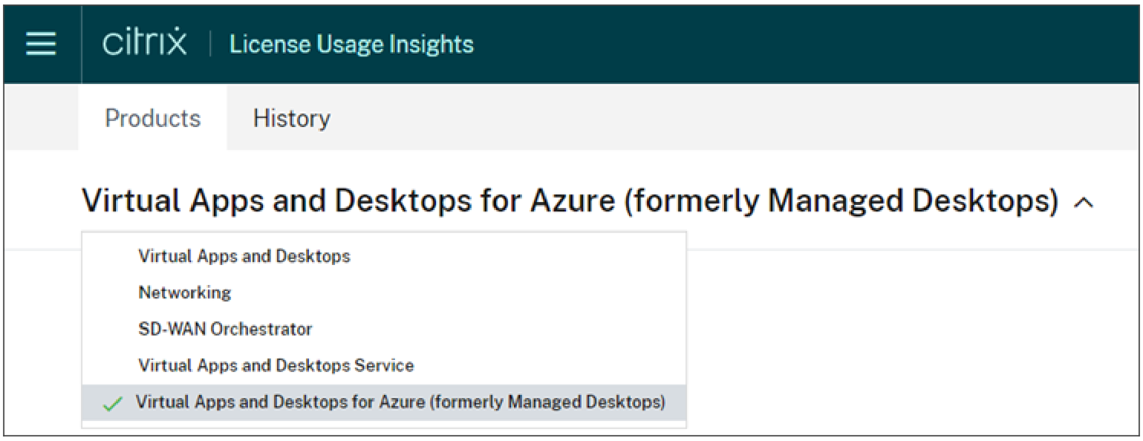
Zathunicon (org id: 20570139)
Virtual Apps and Desktops Service

Usage	Total Licenses	Total Users	License Overage
50%	20	10	0

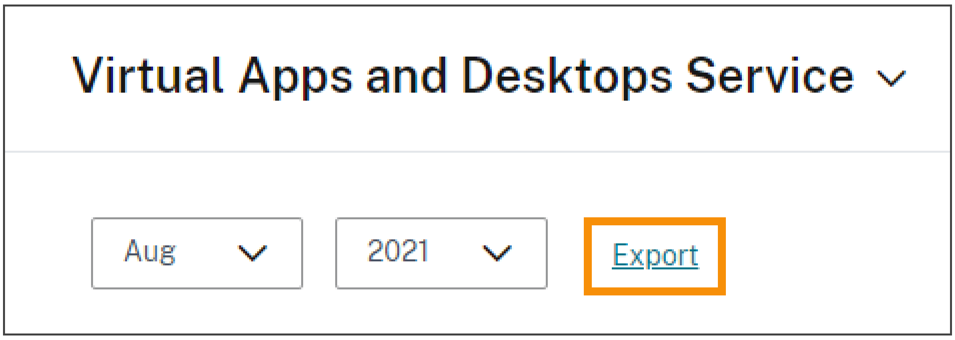
View and export monthly usage

At any time, you can view license usage from previous months for all customers and partners. You can also export this data to a CSV file for further analysis. For Virtual Apps and Desktops Standard for Azure, you can also export monthly consumption data.

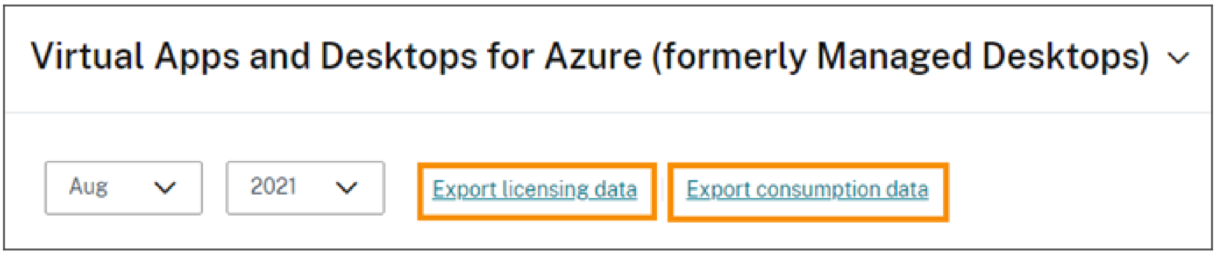
1. From the product menu, select the cloud service you want to view.


citrix | License Usage Insights
Products
History
Virtual Apps and Desktops for Azure (formerly Managed Desktops)
Virtual Apps and Desktops
Networking
SD-WAN Orchestrator
Virtual Apps and Desktops Service
✓ Virtual Apps and Desktops for Azure (formerly Managed Desktops)

For Virtual Apps and Desktops service, select the month and year you want to view and select **Export**.



For Virtual Apps and Desktops Standard for Azure, select the month and year you want to view and then select **Export licensing data** or **Export consumption data**.

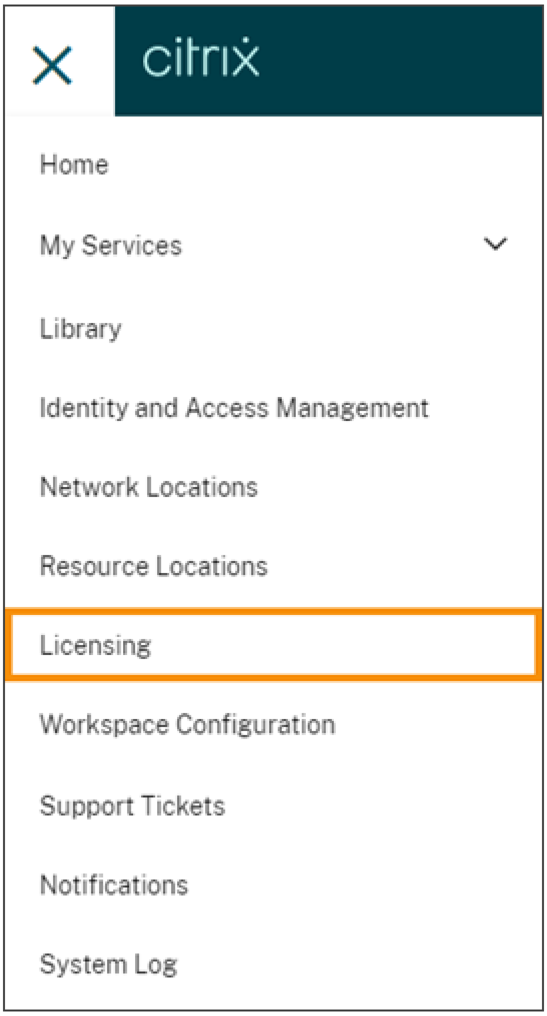

Virtual Apps and Desktops for Azure (formerly Managed Desktops)
Aug
2021
Export licensing data
Export consumption data

Customer license and usage monitoring for Citrix Virtual Apps and Desktops service

September 15, 2021

Customers of **Citrix Service Providers (CSP)** can easily monitor Virtual Apps and Desktops service licenses for their users in Citrix Cloud. As a CSP, you can access these details by signing in to your customer's account in Citrix Cloud. To view aggregated license usage information across single-tenant and multitenant customers, see Cloud service license usage and reporting for Citrix Service Providers.

Customers can view their licensing data by selecting **Licensing** from the Citrix Cloud menu.



License assignment

Citrix Cloud assigns a license when a unique customer user launches an app or desktop for the first time within the current month.

Licensing summary

The **Cloud Services** tab displays a licensing summary that provides an at-a-glance view of the following information:

- Percentage of total purchased licenses assigned. As the percentage approaches 100%, the percentage goes from green to yellow. If the percentage exceeds 100%, the percentage turns red.
- The ratio of assigned licenses to purchased licenses and the number of available licenses remaining.

- The number of over-assigned licenses, if any. If the number of assigned licenses exceeds the number of total licenses purchased, an alert message appears.

Usage trends and license activity

Select **View Usage Details** at the far right of the licensing summary for a detailed view of licenses.

The **Usage Trends** section displays a breakdown of the following information:

- **Total Licenses:** Your total purchased licenses for the cloud service across all entitlements.
- **Assigned Users:** The cumulative number of licenses assigned to customer users during each month.
- **Over-assigned Users:** The number of licenses that were assigned for each month in excess of the total licenses purchased.

The **License Activity** section displays a list of the individual customer users who have licenses assigned during the current month. This list also displays the domain to which each user belongs, the date when a license was assigned, and the last time the service was used.

Monthly release of licenses

On the first day of each month, assigned licenses from the previous month are released automatically. When this happens, the number of assigned licenses resets to zero and the list of licensed customer users is cleared. Licenses are re-assigned when users launch apps or desktops for the first time within the new month.

Review monthly license history

On the first day of each month, the list of licensed customer users from the previous month, under **License Activity**, is cleared when the number of assigned licenses resets to zero. However, you can access user details from previous months at any time and download them as a CSV file, if needed.

1. In the **License Activity** section, select **View License History** at the far right of the section.
2. Select the month you want to view. A list of the user details for the selected month appears.
3. To export the list, select **Export to CSV** at the far right of the section and then save the file.

Export license details

At any time, customers can export licensed user details to a CSV file for further analysis. The customer can then use the CSV file as needed to analyze the license details.

To export the current month's details, in the **License Activity** section, select **Export to CSV** at the far right of the section and then save the file.

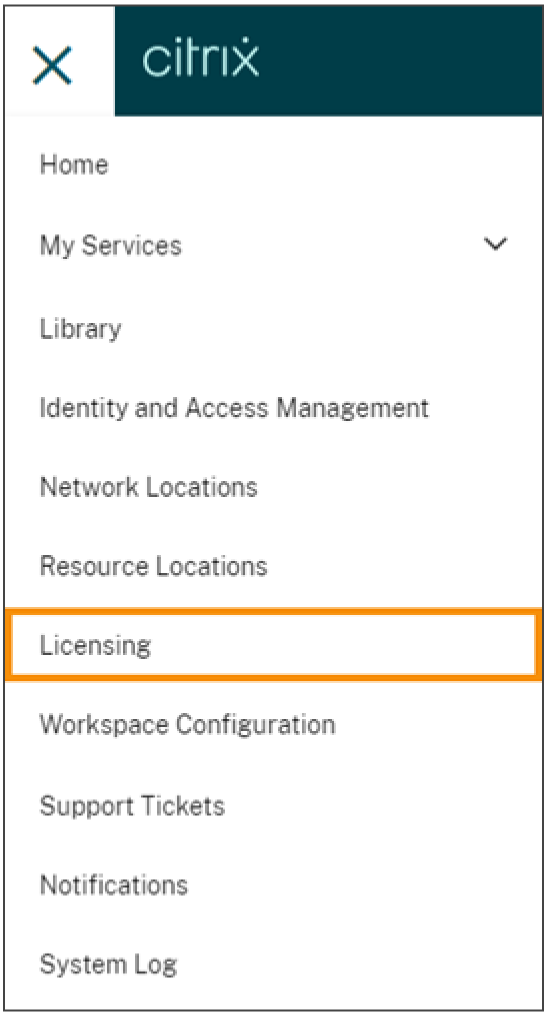
To export the details for previous months, generate a list for a selected month as described in Review monthly license history. Select **Export to CSV** and save the file.

Customer license and usage monitoring for Citrix Virtual Apps and Desktops Standard for Azure

August 26, 2021

Customers of **Citrix Service Providers (CSP)** can easily monitor Virtual Apps and Desktops Standard for Azure licenses for their users in Citrix Cloud. As a CSP, you can access these details by signing in to your customer's account in Citrix Cloud. To view aggregated license usage information across single-tenant and multitenant customers, see Cloud service license usage and reporting for Citrix Service Providers.

Customers can view their licensing data by selecting **Licensing** from the Citrix Cloud menu.



License assignment

Citrix Cloud assigns a license when a unique user launches a desktop for the first time.

Licensing summary

The **Cloud Services** tab displays a licensing summary that provides an at-a-glance view of the following information:

- Percentage of total purchased licenses assigned. As the percentage approaches 100%, the percentage goes from green to yellow. If the percentage exceeds 100%, the percentage turns red.
- The ratio of assigned licenses to purchased licenses and the number of available licenses remaining.
- The number of over-assigned licenses, if any. If the number of assigned licenses exceeds the number of total licenses purchased, an alert message appears.

Click **View Usage Details** at the far right of the summary to see a breakdown of usage reports and trends, plus a list of users who are consuming Virtual Apps and Desktops Standard for Azure licenses.

Usage reports

You can download usage information for a standard or specified interval.
The information includes meter usage for:

- Azure VMs
- Network connections, such as VNet peering
- Azure storage items, such as managed disks, block blobs, and page blobs

Data can take up to 72 hours after the end of a day/month to reflect all usage.

Under **Usage Reports**, select an interval and then select **Download Data** to generate and download a CSV file to your local machine.

Usage trends and license activity

The **Usage Trends** section of the management console shows a breakdown that includes the following information:

- **Total Licenses:** Your total purchased licenses for the cloud service across all entitlements.
- **Assigned Users:** The cumulative number of licenses assigned to customer users during each month.
- **Over-assigned Users:** The number of licenses that were assigned for each month in excess of the total licenses purchased.

Pointing to a bar on the graph for a specific month displays the total number of licenses, assigned licenses, assigned users, and any overassigned licenses.

Licensed users

The **License Activity** section displays a list of the individual customer users who have licenses assigned during the current month. This list also displays the domain to which each user belongs, the date when a license was assigned, and the last time the service was used.

Monthly release of licenses

On the first day of each month, assigned licenses from the previous month are released automatically. When this happens, the number of assigned licenses resets to zero and the list of licensed customer users is cleared. Licenses are re-assigned when users launch apps or desktops for the first time within the new month.

Review monthly license history

On the first day of each month, the list of licensed customer users from the previous month, under **License Activity**, is cleared when the number of assigned licenses resets to zero. However, you can access user details from previous months at any time and download them as a CSV file, if needed.

1. In the **License Activity** section, select **View License History** at the far right of the section.
2. Select the month you want to view. A list of the user details for the selected month appears.
3. To export the list, select **Export to CSV** at the far right of the section and then save the file.

Export license details

At any time, you can export licensed user details for a single customer to a CSV file for further analysis. You can then use the CSV file as needed to analyze the license details.

To export the current month's details, in the **License Activity** section, select **Export to CSV** at the far right of the section and then save the file.

To export the details for previous months, generate a list for a selected month as described in Review monthly license history. Select **Export to CSV** and save the file.

Manage Citrix Cloud administrators

July 8, 2021

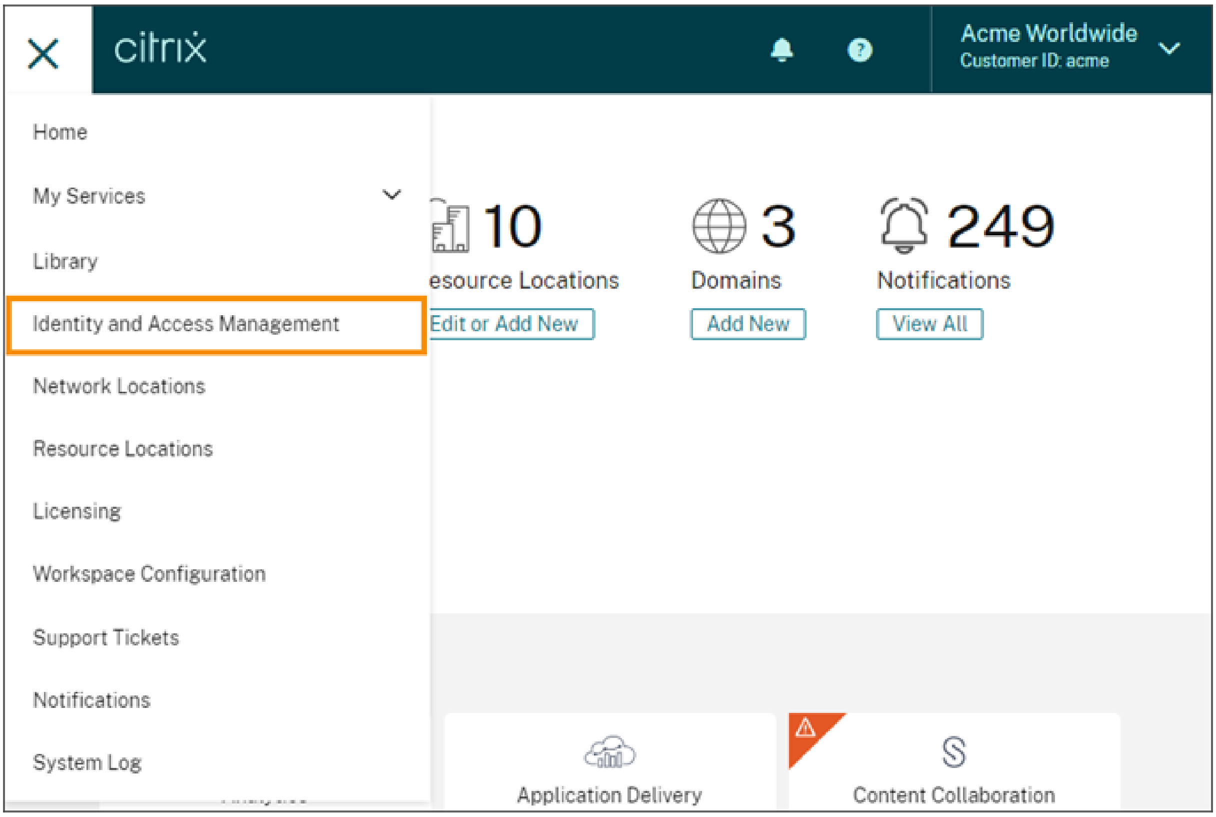
Administrators are managed from the Citrix Cloud console. If you want to be added as an administrator to an existing Citrix Cloud account, an existing administrator of the account must invite you.

Citrix Cloud also supports using tokens as a second factor of authentication for Citrix Cloud administrators. After you're added as an administrator, you can enroll your device in multifactor authentication and generate tokens using any app that follows the Time-Based One-Time Password standard, such as Citrix SSO or Google Authenticator.

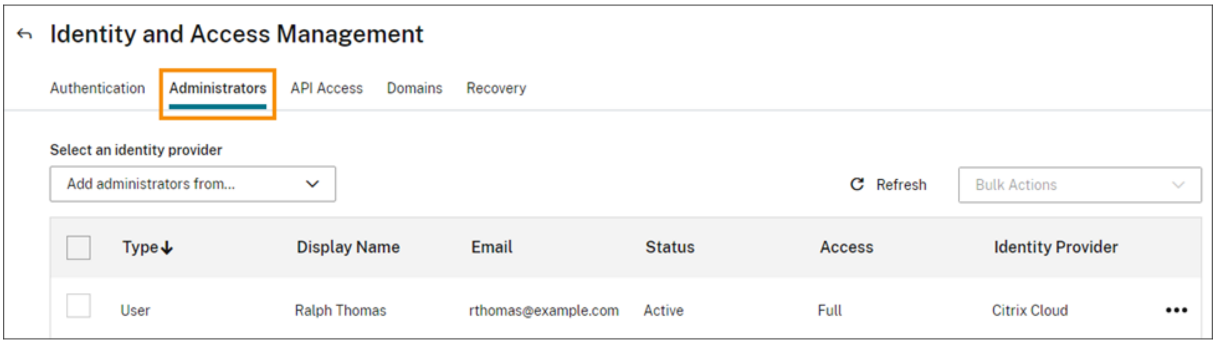
> **Tip:**
>
> The "Citrix Cloud Platform" module, included in the Fundamentals of Citrix Cloud course, provides short videos that walk you through administering Citrix Cloud and services. The full course also gives you a firm foundation for understanding Citrix Cloud, its benefits for your organization, and important use cases that Citrix Cloud services address.

Invite new administrators

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



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



Identity and Access Management

Select an identity provider: Add administrators from...

Type	Display Name	Email	Status	Access	Identity Provider
User	Ralph Thomas	rthomas@example.com	Active	Full	Citrix Cloud

To invite an administrator:

1. In **Add administrators from**, select the identity provider from which you want to select the administrator. Depending on the identity provider selected, Citrix Cloud might prompt you to sign in to the identity provider first (for example, Azure Active Directory).
2. If **Citrix Identity** is selected, enter the user's email address and then click **Invite**.
3. If Azure Active Directory is selected, type the name of the user you want to add and then click **Invite**. Inviting AAD guest users is not supported.
4. Configure the appropriate permissions for the administrator. **Full access** (selected by default) allows control of all Citrix Cloud functions and subscribed services. **Custom access** allows control of the functions and services that you select.
5. Click **Send Invite**.

Citrix Cloud sends an invitation to the user you specified and adds the administrator to the list. The email is sent from cloud@citrix.com and explains how to access the account. Citrix Cloud also displays the status of the invitation so you can see whether the user accepted it and signed in to Citrix Cloud.

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

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

Modify administrator permissions

When you add administrators to your Citrix Cloud account, you define the administrator permissions that are appropriate for their role in your organization. However, from time to time, you might need to assign a different level of access to an existing administrator.

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

To change existing administrator permissions:

1. Sign in to Citrix Cloud at https://citrix.cloud.com.

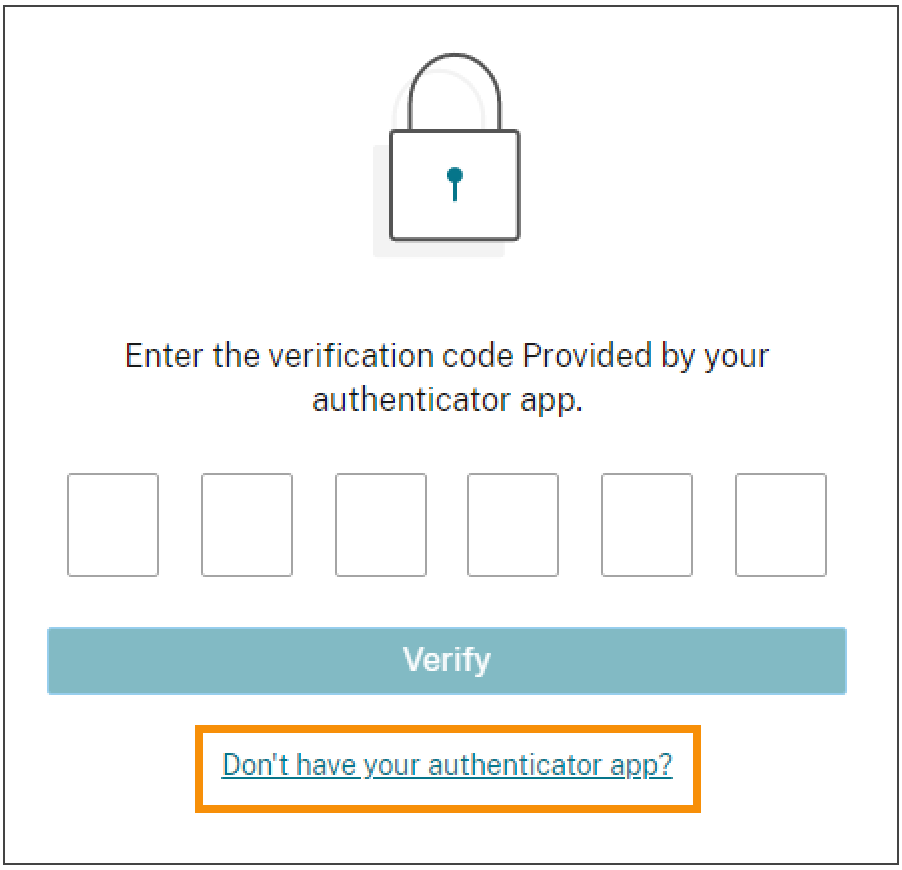
2. From the Citrix Cloud menu, select **Identity and Access Management** and then select **Administrators**.
3. Locate the administrator you want to manage, click the ellipsis button, and select **Edit access**.
4. To allow or disallow specific permissions, select **Custom access**.
5. For each permission, select or clear the check mark as needed.
6. Click **Save Changes**.

Change your device for multifactor authentication

If you lose your enrolled device, want to use a different device with Citrix Cloud, or reset your authenticator app, you can re-enroll in Citrix Cloud 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 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 entries with differing codes which can cause confusion when signing in to Citrix Cloud.
> - 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.

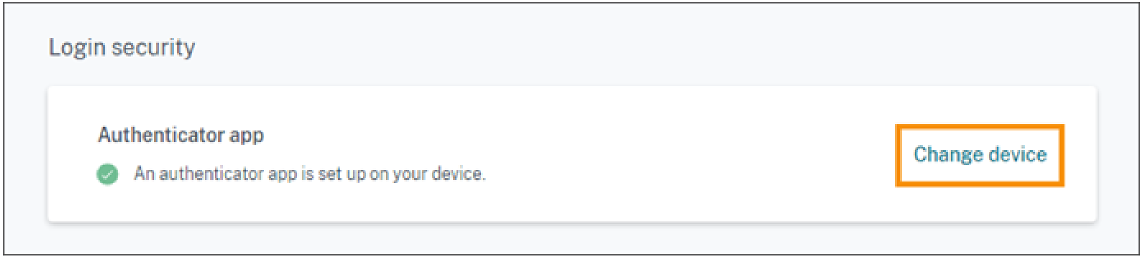
1. Sign in to Citrix Cloud and enter the code from your authenticator app.



Enter the verification code Provided by your authenticator app.

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

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



Login security

Authenticator app

✓ An authenticator app is set up on your device.

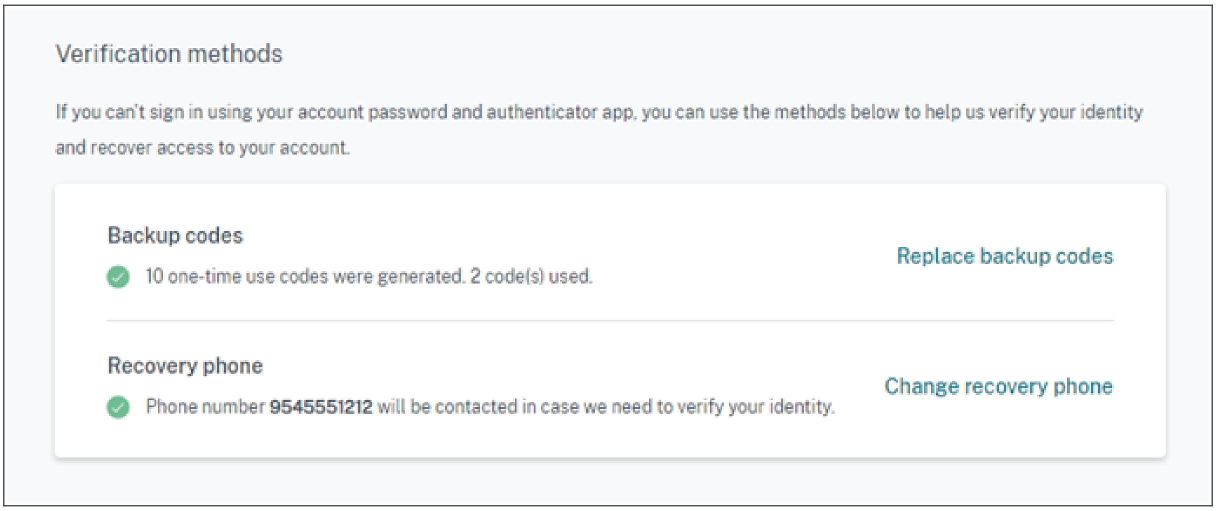
5. When prompted to confirm changing your device, select **Yes, change device**.
6. Verify your identity by entering a verification code from your authenticator app. If you don't have an authenticator app, select **Don't have your authenticator app?** and select a recovery method. Depending on the recovery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

code you receive or an unused backup code. Select **Verify**.

7. If you are using the device you originally enrolled and your original authenticator app, delete the existing Citrix Cloud entry from your authenticator app.
8. If you are enrolling a new device and don't have an authenticator app, download one from your device's app store.
9. From your authenticator app, scan the QR code with your device or enter the key manually.
10. Enter the 6-digit verification code from your authenticator app and select **Verify code**.

Manage your verification methods

> **Important:**
>
> To ensure your Citrix Cloud 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.



Verification methods

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

Backup codes

✓ 10 one-time use codes were generated. 2 code(s) used.

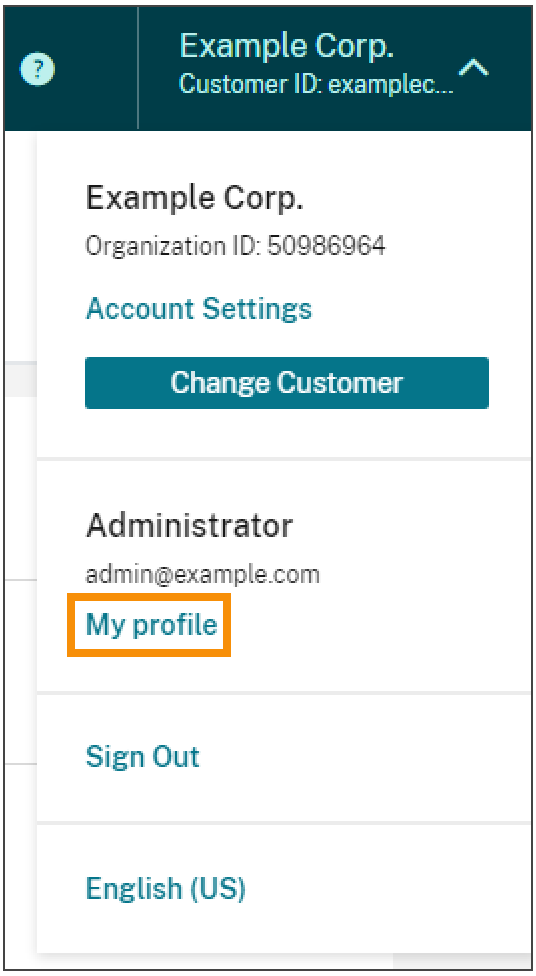
Recovery phone

✓ Phone number **9545551212** will be contacted in case we need to verify your identity.

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 and enter the code from your authenticator app.
2. If you are an administrator for multiple customer organizations, select any customer organization.
3. From the top-right menu, select **My Profile**.



4. Under **Verification methods**, in **Backup codes**, select **Replace backup codes**.
5. Verify your identity by entering a verification code from your authenticator app.
6. When prompted to replace your backup codes, select **Yes, replace**. Citrix Cloud 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**.

> **Note:**
>
> You can modify the permissions of Citrix Endpoint Management (CEM) administrators only after the administrator has accepted an administrator invitation and clicked **Manage** on the CEM tile. Like all Citrix Cloud administrators, CEM administrators have Full access by default.

Change your recovery phone number

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

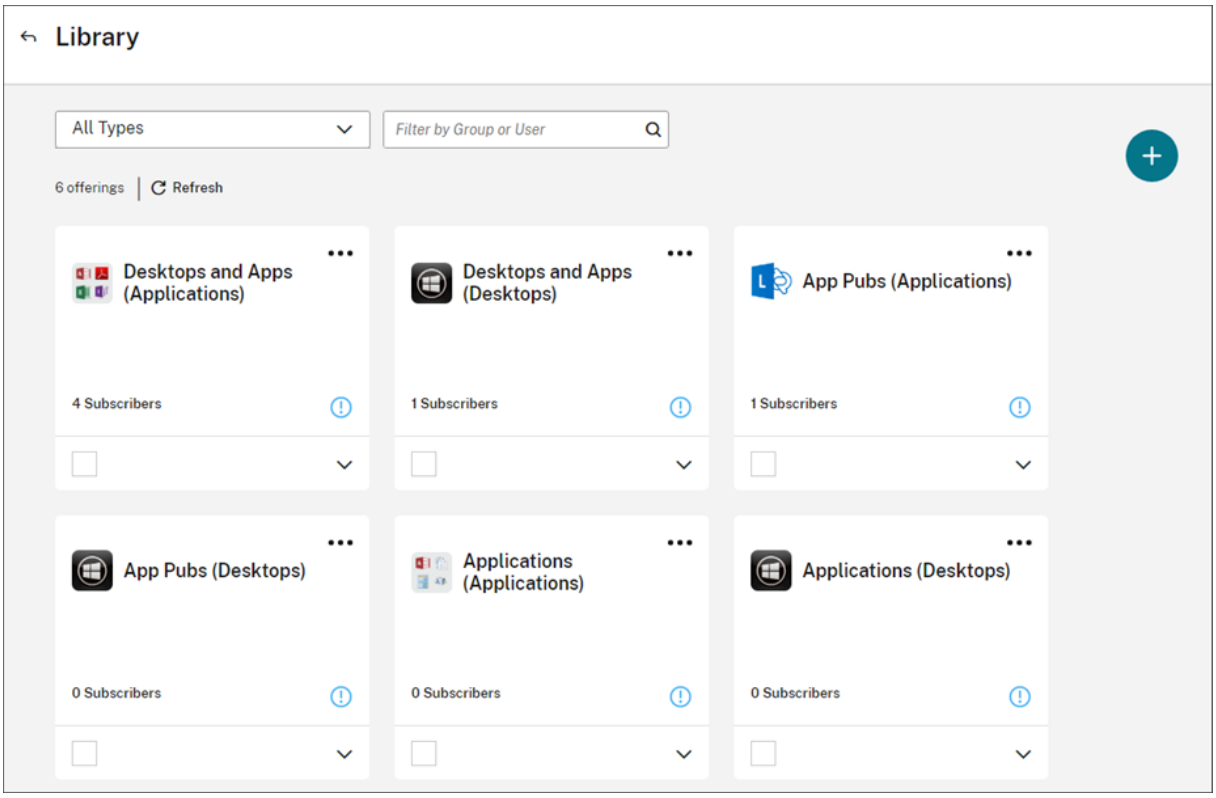
2. If you are an administrator for multiple customer organizations, select the customer organization from which you originally enrolled in multifactor authentication.
3. From the top-right menu, select **My Profile**.
4. Under **Verification methods**, in **Recovery phone**, select **Change recovery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

Assign users and groups to service offerings using Library

August 29, 2018

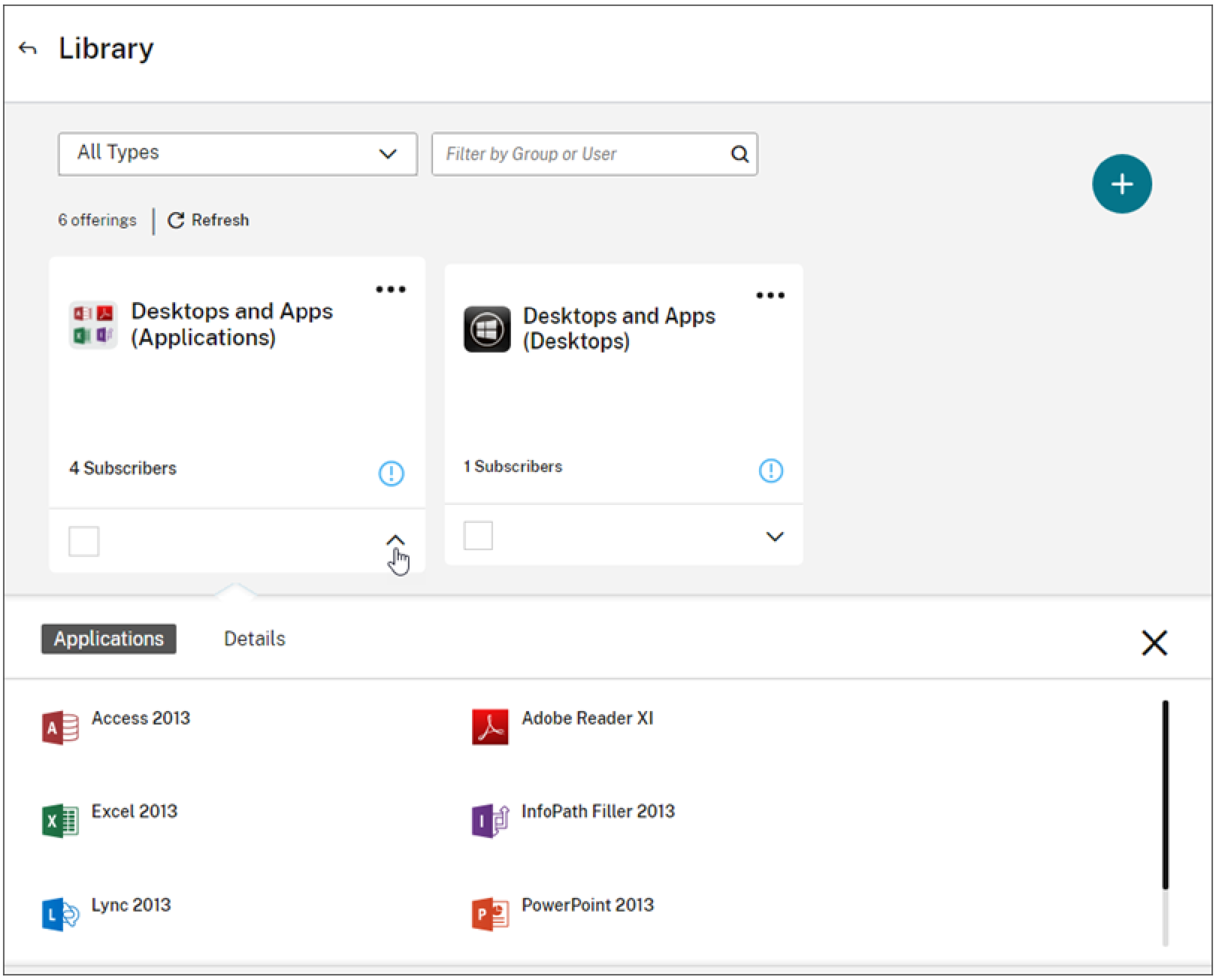
You can assign resources or other items that you configure in a service (for example, applications and desktops configured in the Virtual Apps and Desktops service) to your Active Directory users and groups using the Library.

Offerings might consist of applications, desktops, data shares, and web apps that you create through a Citrix service. The Library displays all your offerings in a single view.



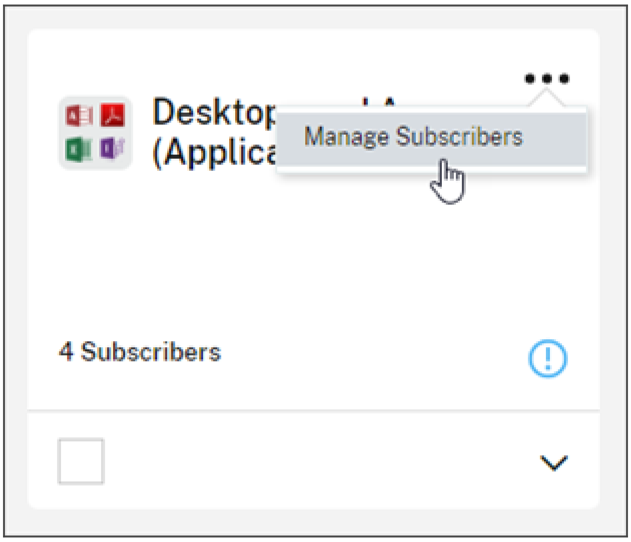
View offering details

To view applications, desktops, policies, and any other related offering information, click the arrow on the offering card.

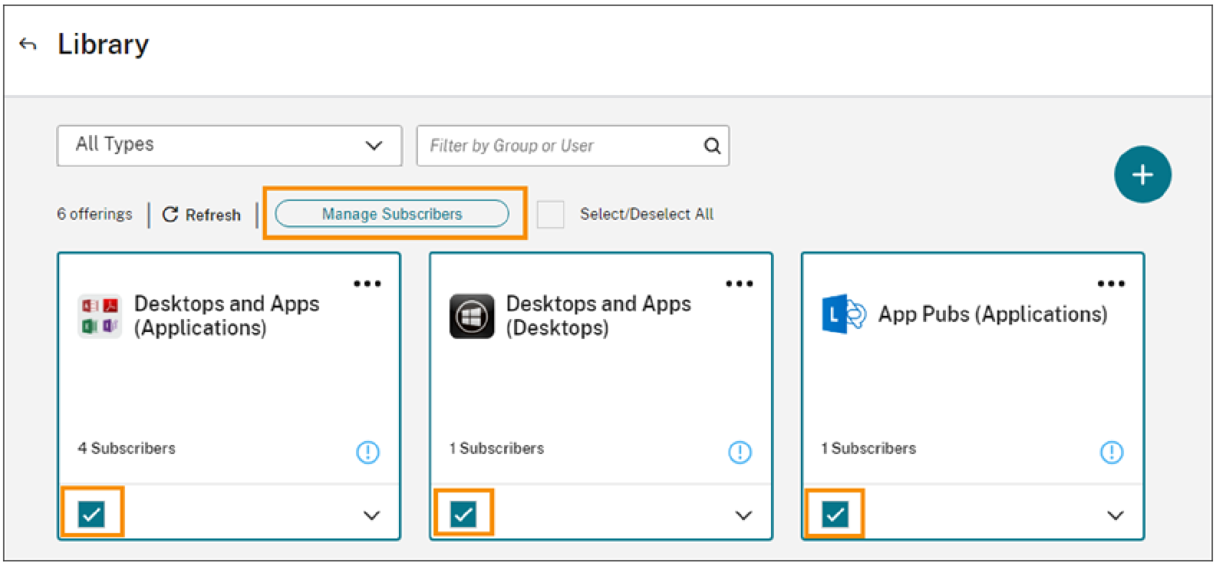


Add or remove subscribers

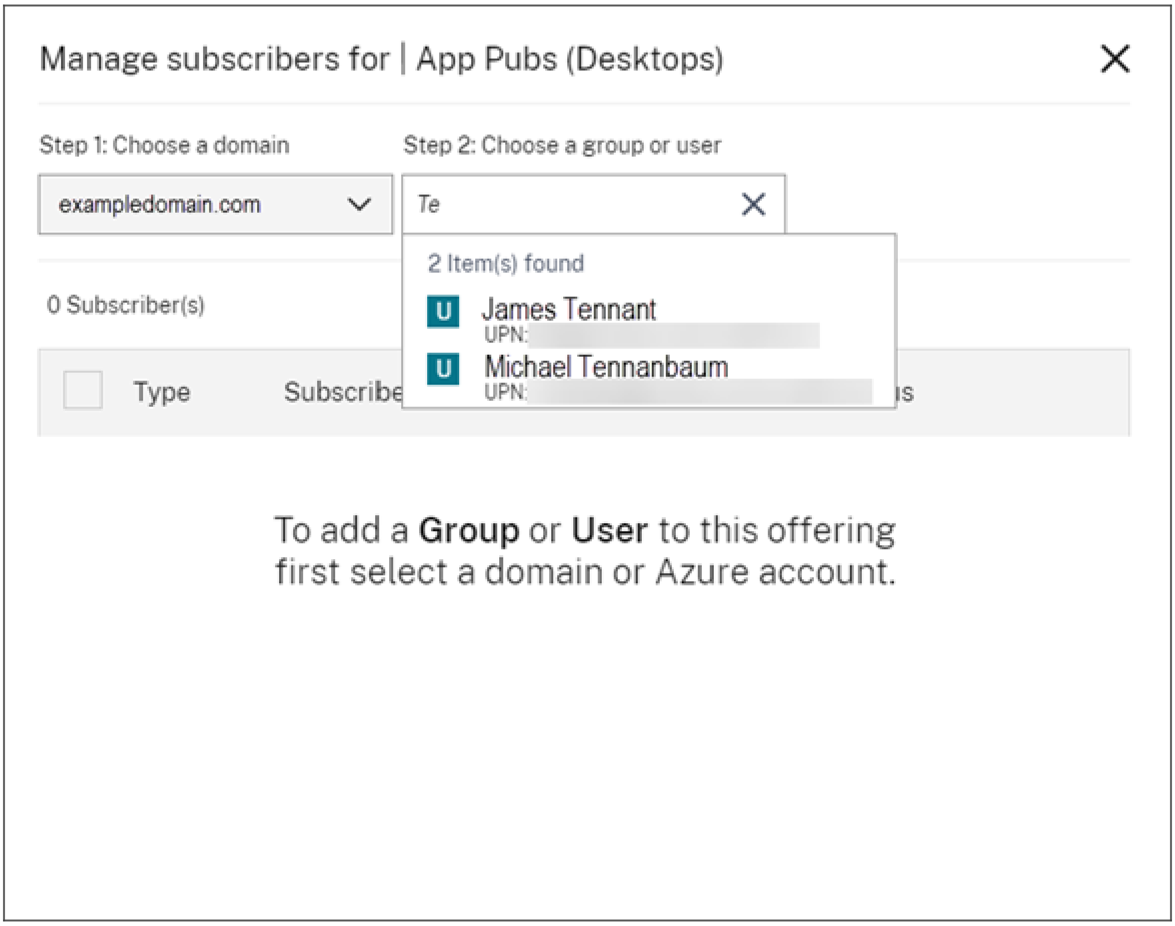
To manage users or groups for a single offering, click **Manage Subscribers** from the offering card's menu.



To manage subscribers for multiple offerings, select the check mark on each offering and then click **Manage Subscribers**.



To add subscribers to the offering, choose a domain and then select the users or groups you want to add.



Manage subscribers for | App Pubs (Desktops)

Step 1: Choose a domain

exampledomain.com

Step 2: Choose a group or user

Te

2 Item(s) found

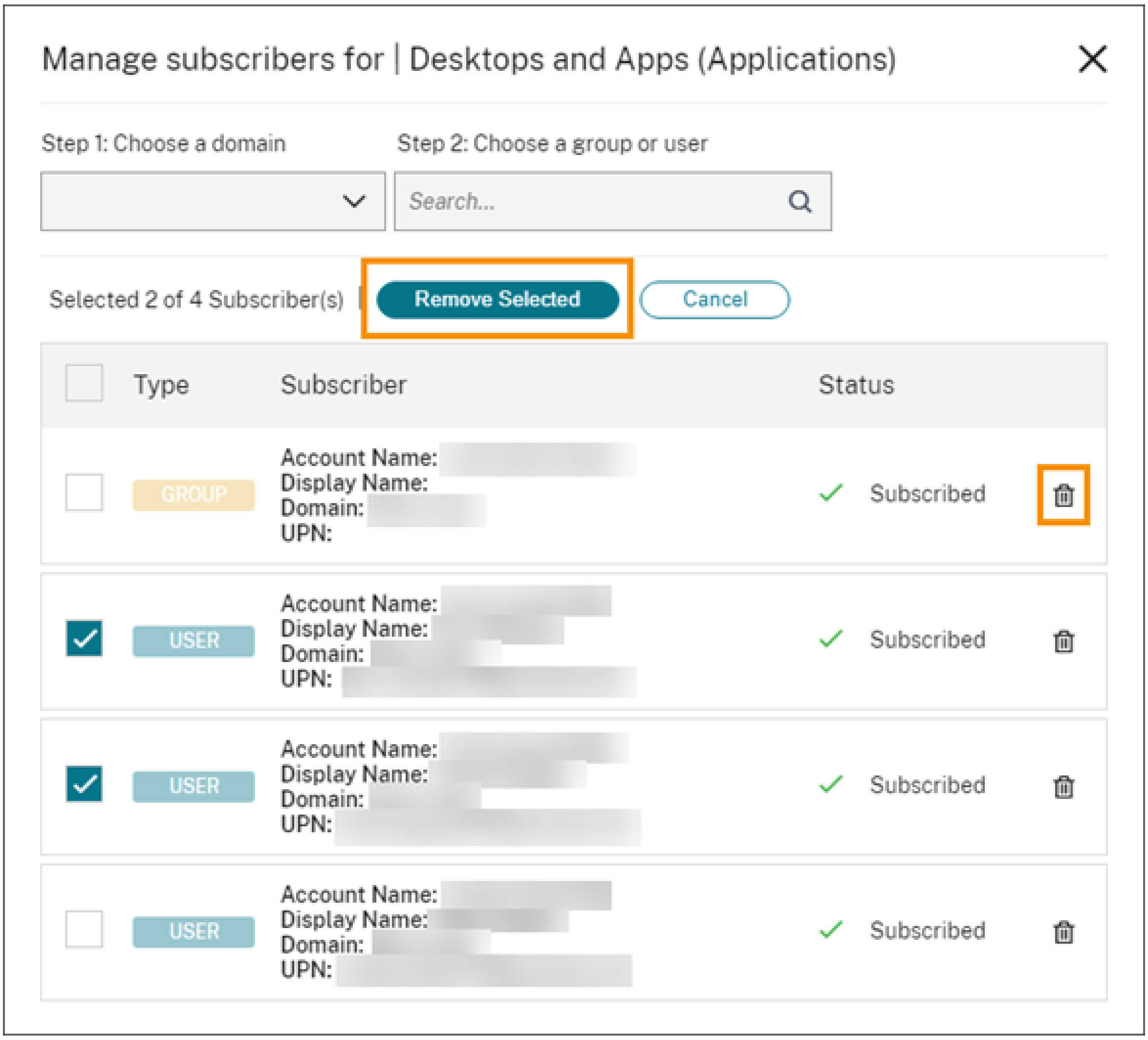
U James Tennant
UPN: [redacted]

U Michael Tennanbaum
UPN: [redacted]

0 Subscriber(s)

To add a **Group** or **User** to this offering first select a domain or Azure account.

To remove a single subscriber, click the trash icon for a user or group. To remove multiple subscribers, select the users or groups and click **Remove Selected**.


Manage subscribers for | Desktops and Apps (Applications)
Step 1: Choose a domain
Step 2: Choose a group or user
Search...
Remove Selected
Cancel

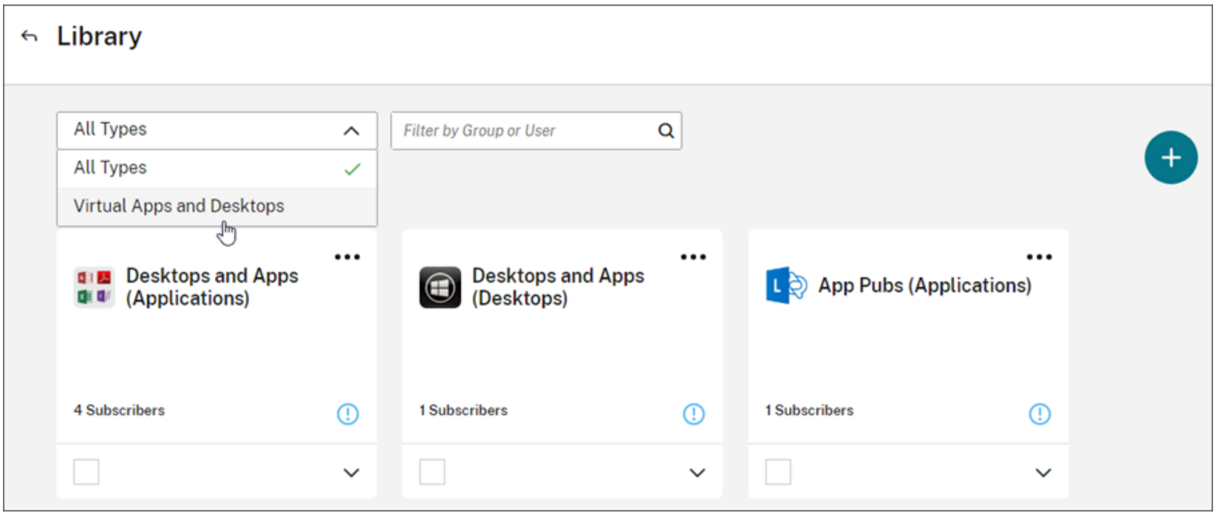
Selected 2 of 4 Subscriber(s)

□	Type	Subscriber	Status	
□	GROUP	Account Name: [redacted] Display Name: Domain: [redacted] UPN:	✓ Subscribed	🗑
☑	USER	Account Name: [redacted] Display Name: [redacted] Domain: [redacted] UPN: [redacted]	✓ Subscribed	🗑
☑	USER	Account Name: [redacted] Display Name: [redacted] Domain: [redacted] UPN: [redacted]	✓ Subscribed	🗑
□	USER	Account Name: [redacted] Display Name: [redacted] Domain: [redacted] UPN: [redacted]	✓ Subscribed	🗑

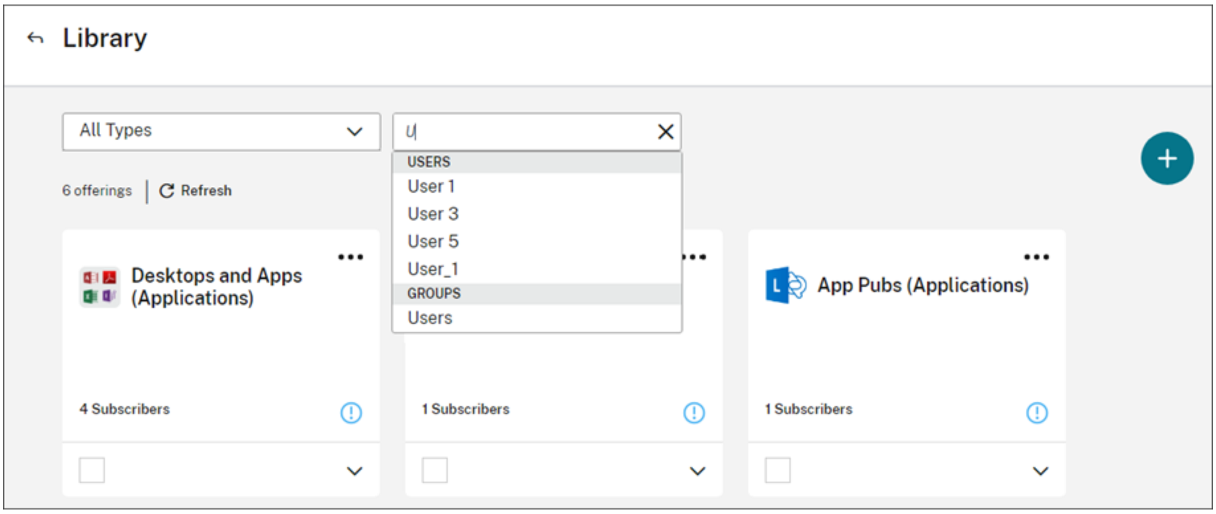
After you add or remove subscribers from an offering, the offering card displays the current number of subscribers.

Filter offerings

By default, the Library displays all offerings. To quickly view offerings for a specific service, select the filter for that service.



You can also search for any user or group that is currently subscribed to an offering in the Library. Citrix Cloud displays only the offerings that pertain to the user or group you select. To see all offerings for all users, click the X to clear the filter.



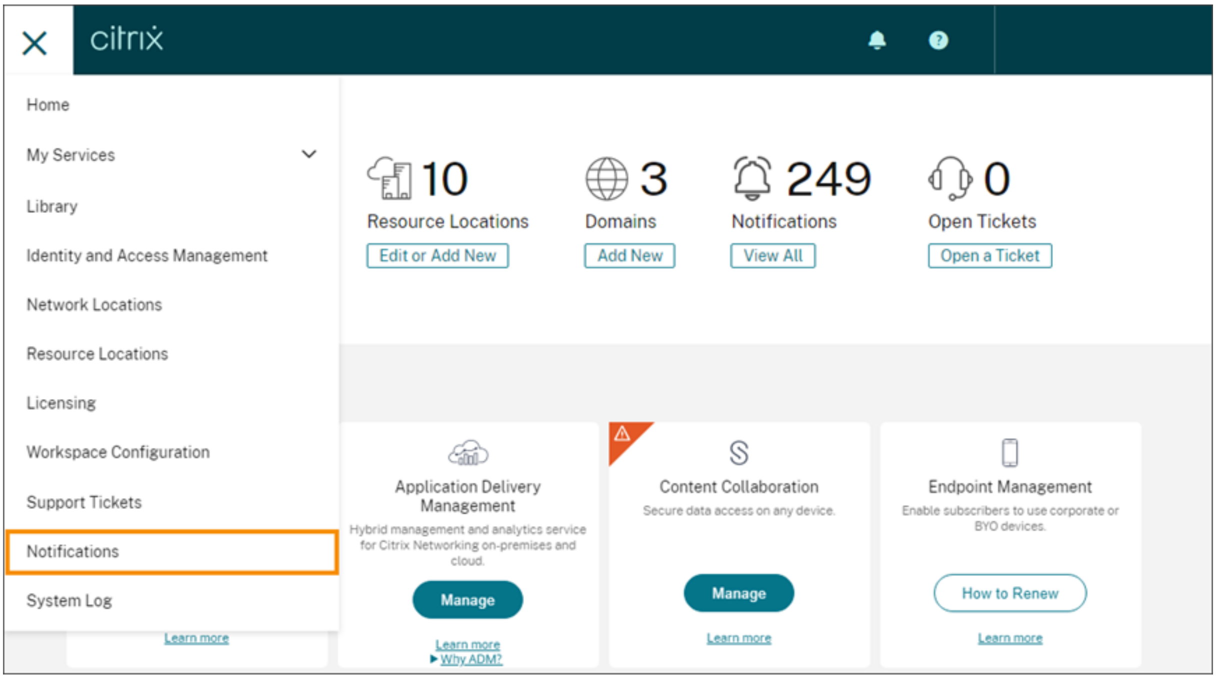
Notifications

September 24, 2021

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

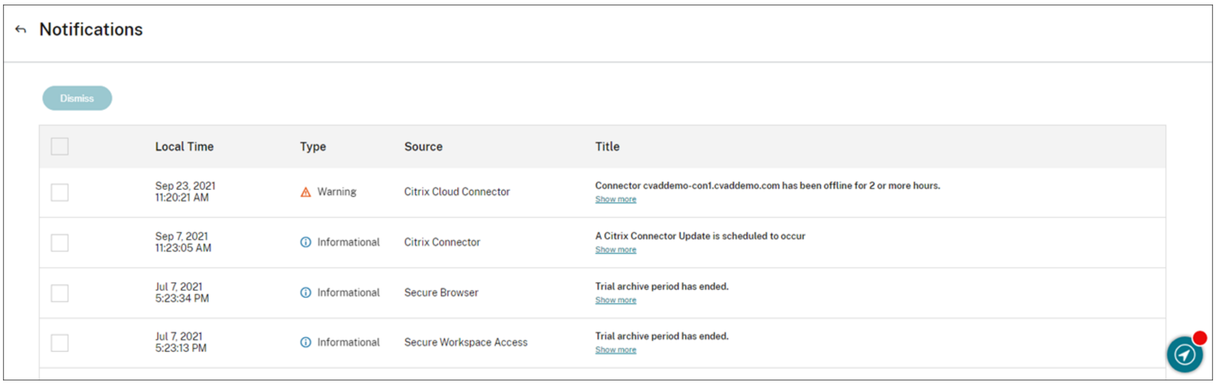
View notifications

The number of notifications appears near the top of the Citrix Cloud console page. For more details, click **View All** under **Notifications** in the console or select **Notifications** from the console menu.



Dismiss notifications

After you've read a notification and acted on it (if required), select the notification and then select **Dismiss**. Dismissing notifications removes them from your list and Citrix Cloud updates the notifications count when you return to the console home page.



Notifications

Dismiss

□	Local Time	Type	Source	Title
□	Sep 23, 2021 11:20:21 AM	⚠ Warning	Citrix Cloud Connector	Connector cvaddemo-con1.cvaddemo.com has been offline for 2 or more hours. Show more
□	Sep 7, 2021 11:23:05 AM	ⓘ Informational	Citrix Connector	A Citrix Connector Update is scheduled to occur Show more
□	Jul 7, 2021 5:23:34 PM	ⓘ Informational	Secure Browser	Trial archive period has ended. Show more
□	Jul 7, 2021 5:23:13 PM	ⓘ Informational	Secure Workspace Access	Trial archive period has ended. Show more

Administrators receive their own notifications in Citrix Cloud. So, dismissing notifications doesn't prevent other administrators from viewing their notifications.

Receive emailed notifications

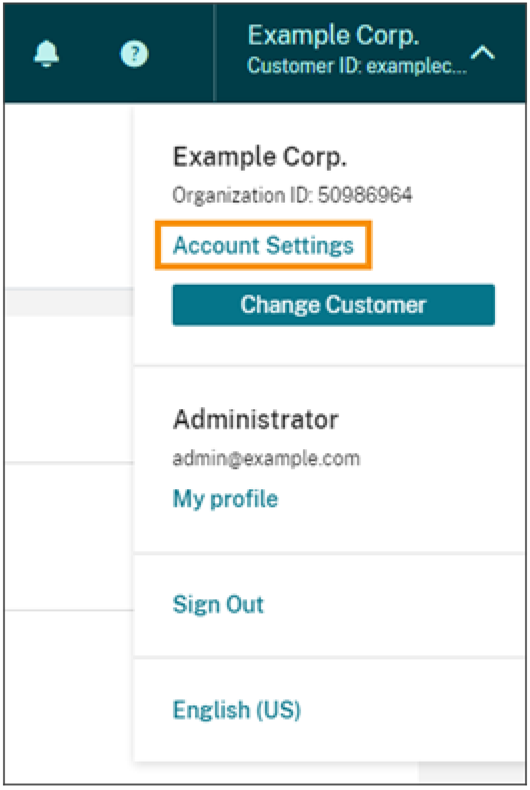
You can choose to receive notifications by email instead of signing in to view them. By default, email notifications are turned off.

When you enable emailed notifications, Citrix Cloud sends you an email for each notification. Notifications are sent as soon as possible. They are not grouped into a single email or batched for sending at a later time.

After reading an emailed notification, you can dismiss it through the **Notifications** page in Citrix Cloud.

To enable emailed notifications

1. From the Citrix Cloud management console, click **Account Settings**.



2. Select **My Profile**.
3. Click the **Email Notifications** toggle button to turn on emailed notifications.
4. Select the notifications you want to receive. By default, all notification types are selected.

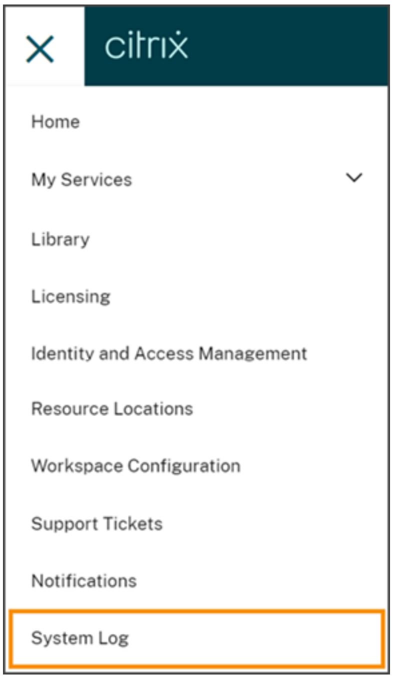
System Log (Technical Preview)

July 29, 2021

> **Note:**
>
> System Log and the SystemLog API are in Technical Preview. Citrix recommends using these features only in non-production environments.

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

To view the system log, select **System Log** from the Citrix Cloud menu.



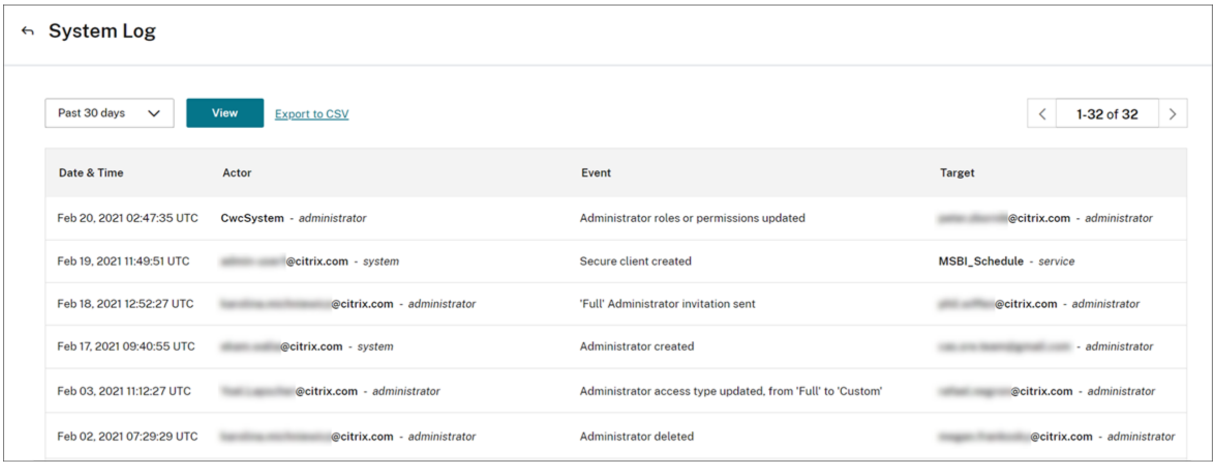
For more information about retention of data in system logs, see Data retention in this article.

Logged events

The system log captures the following events:

- Adding, modifying, and removing administrators
- Creating and deleting secure clients

By default, the system log displays events that occurred in the last 30 days. The most recent events are displayed first.

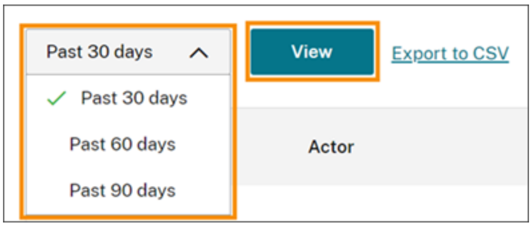


Date & Time	Actor	Event	Target
Feb 20, 2021 02:47:35 UTC	CwcSystem - *administrator*	Administrator roles or permissions updated	[redacted]@citrix.com - *administrator*
Feb 19, 2021 11:49:51 UTC	[redacted]@citrix.com - *system*	Secure client created	MSBI_Schedule - *service*
Feb 18, 2021 12:52:27 UTC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

The displayed list includes the following information:

- Date and time (UTC) when the event occurred.
- Actor that initiated the event, such as an administrator or secure client. Entries with the actor **CwcSystem** indicate that Citrix Cloud performed the operation.
- Brief description of the event, such as editing an administrator or creating a new secure client.
- Target of the event. The target is the system object that was impacted or changed as a result of the event. For example, a user who was added as an administrator.

To view events more than 30 days in the past, filter the list by selecting the time period you want to view and select **View**. You can view events that occurred up to 90 days in the past.

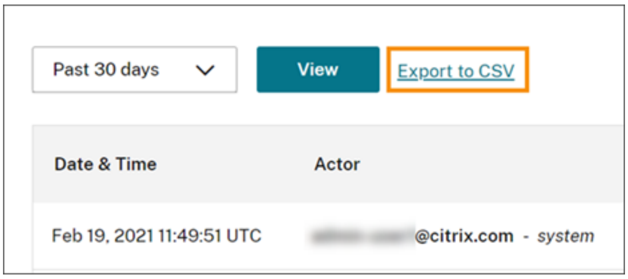


To retrieve older events that occurred during a time period that you specify, you can use the SystemLog API. For more information, see Retrieve events for a specific time period in this article.

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 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.



Date & Time	Actor
Feb 19, 2021 11:49:51 UTC	[redacted]@citrix.com - *system*

The CSV file includes the following information:

- UTC timestamp of each event
- Details of the actor who initiated the event, including the name and actor ID.
- Event details such as the type of event and the text of the event
- Details of the target of the event such as the target ID, the name of the administrator or a secure client.

Retrieve events for a specific time period

If you need to retrieve events for specific periods of time, you can use the SystemLog API. Before you use the API, you'll need to create a secure client as described in Getting Started on the Citrix Developer Docs web site.

For more information about using the SystemLog API, see Citrix Cloud - SystemLog on the Citrix Developer Docs web site.

Forward system log events

The Citrix System Log Add-on for Splunk enables you to connect your Splunk instance with Citrix Cloud. With this connection, you can forward system log data to Splunk. For more information, see the add-on documentation in the Citrix repository in GitHub.

Add-ons for other security information event management (SIEM) solutions such as Microsoft Azure Sentinel and IBM QRadar are not yet available. Please check the following resources periodically for updates on any development efforts and releases:

- Citrix Blogs
- Citrix Cloud Discussions forum
- Citrix social media: Twitter, LinkedIn, Facebook

Data retention

Citrix shares responsibility with you, the customer, for retaining the system log data that Citrix Cloud captures.

Citrix retains system log records for 90 days after events are recorded.

You are responsible for downloading the system log records that you want to retain to meet your organization’s compliance requirements and for storing these records in a long-term storage solution.

Citrix Cloud for Partners

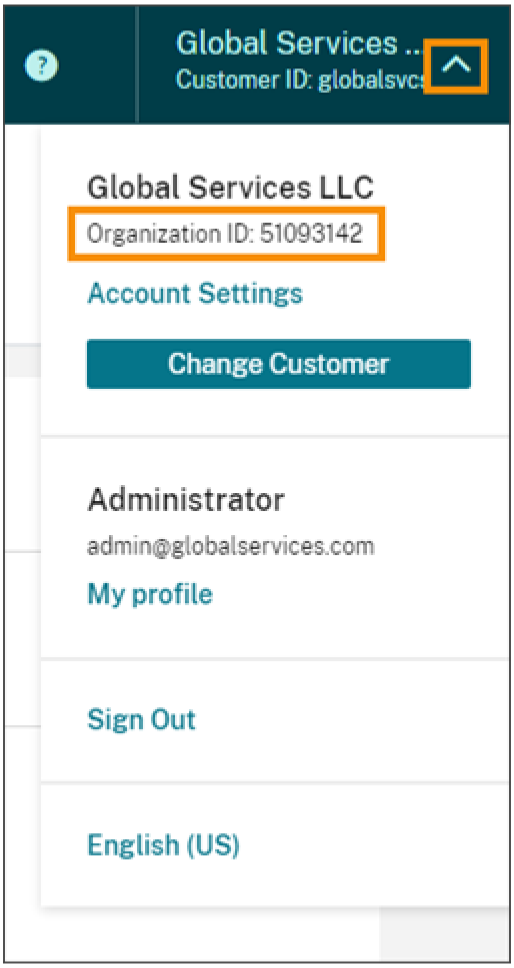
September 24, 2021

Citrix Cloud includes services, features, and experiences designed for both customers and partners. This section outlines features available to Citrix Partners that help them collaborate with customers on Citrix Cloud services and solutions.

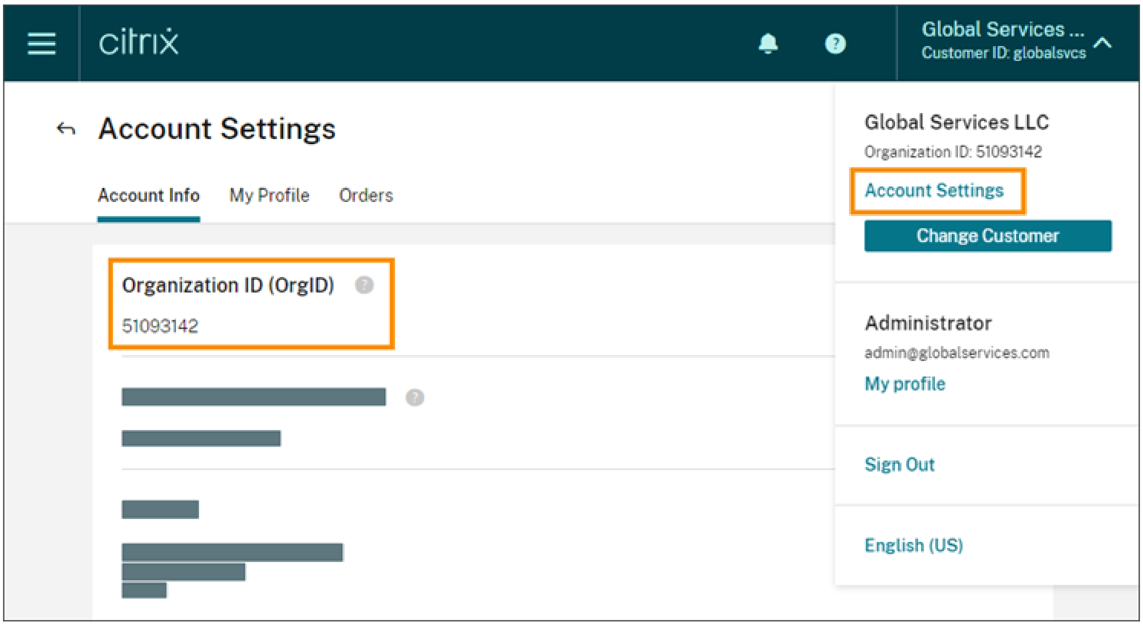
Partner identification

Partners are identified in Citrix Cloud based on their Citrix Organization ID (ORGID). Partners can view the ORGID that’s associated with their Citrix Cloud account in the following locations in the Citrix Cloud management console:

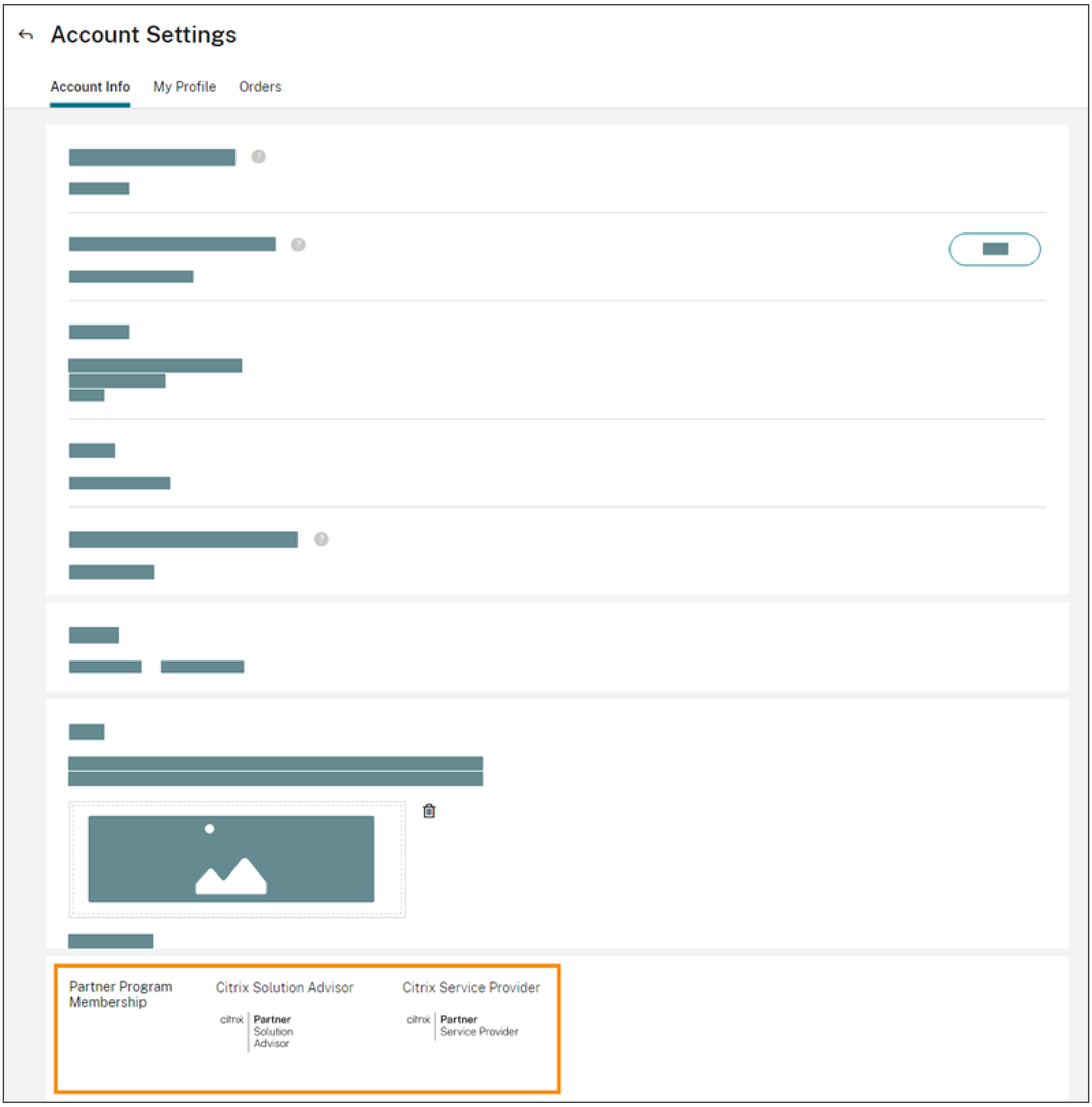
- From the customer menu. Click your customer name from the top-right corner of the console. Your ORGID appears beneath your company name in the menu.



- From the **Account Settings** page. From the customer menu in the top-right corner, select **Account Settings**.

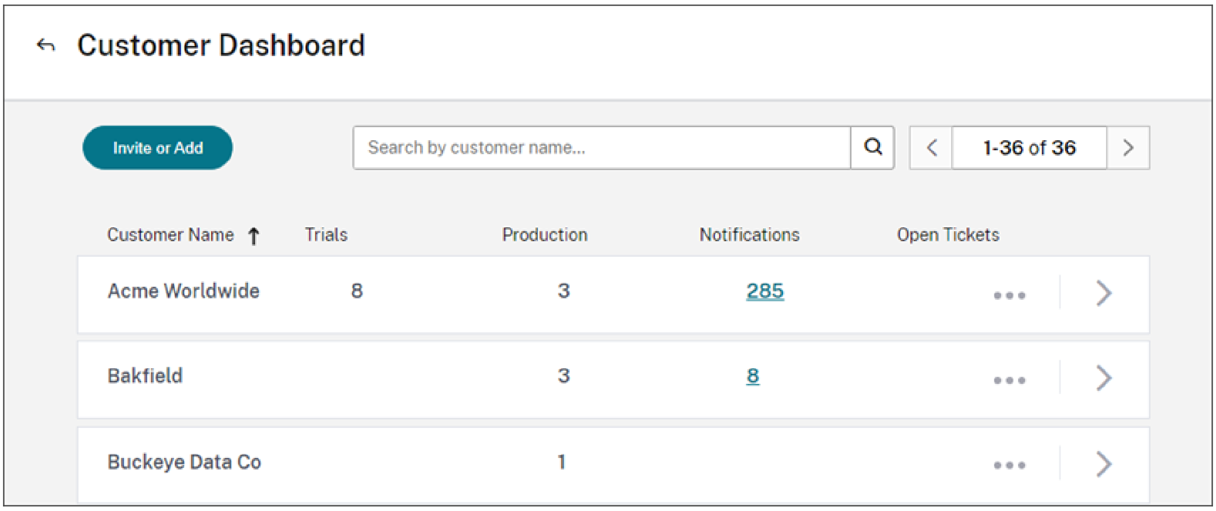


If the ORGID on the account is an active member of a Citrix partner program (such as Citrix Solution Advisor or Citrix Service Provider) the program badge indicates that a Citrix partner owns this account. Partner identification is then used to govern access to additional cloud services or features.



Customer dashboard

The customer dashboard is designed for partners to view the status of multiple Citrix Cloud customers in a consolidated view. For a customer to appear on the dashboard, a connection must be established between the partner and customer. The customer dashboard is available on partner badged Citrix Cloud accounts.



Customer Name ↑	Trials	Production	Notifications	Open Tickets
Acme Worldwide	8	3	285	
Bakfield		3	8	
Buckeye Data Co		1		

Connecting with customers

Partners collaborating with customers on Citrix Cloud solutions are able to establish a trusted link between their accounts. This account level relationship allows a customer to share specific information easily with a partner. By accepting to connect with a partner, a customer grants the partner visibility into information about their Citrix Cloud account and relationship with Citrix.

Establishing a partner connection enables the following:

- Customer appears on the partner's dashboard
- Partner appears as an active connection in the customers account settings
- Partner visibility into Citrix Cloud service entitlements
- Partner visibility into license usage and active use for Citrix Cloud entitlements

Additional information about partner connections:

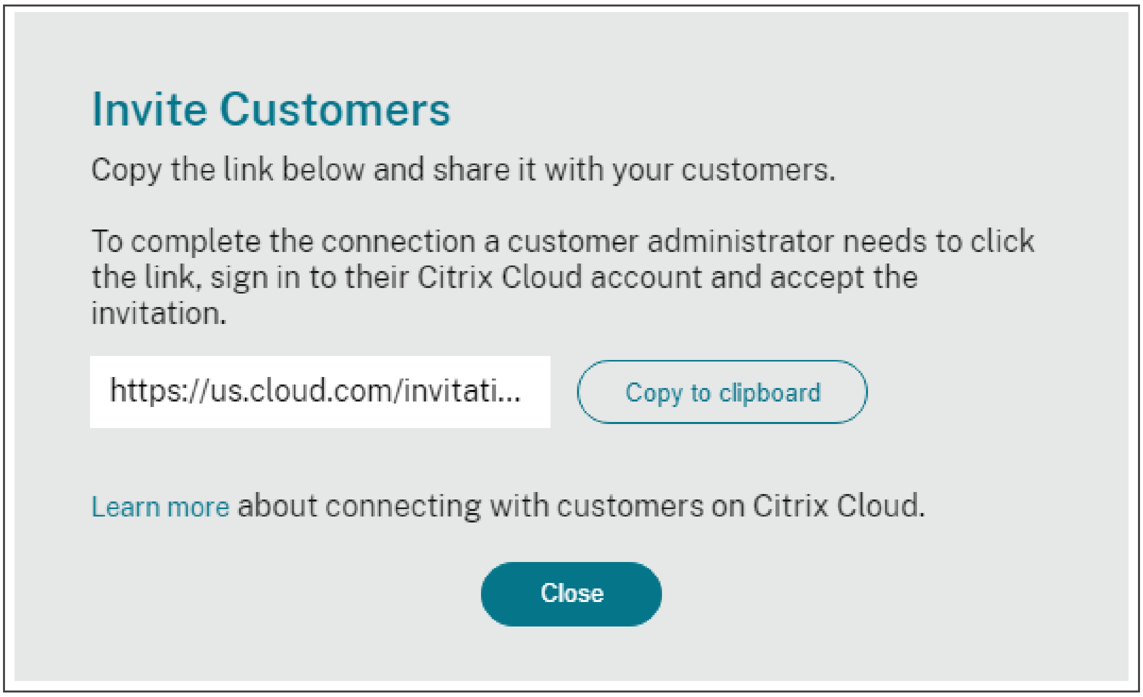
- Partners can establish connections with multiple customers
- Customers can establish connections with multiple partners
- There is no limit to the number of customer-to-partner connections
- Connections can be terminated at any time by either the customer or the partner
  - By the customer in their account details page
  - By the partner using the customer dashboard
- Citrix Cloud Notifications are sent depending on the connection workflow
  - Partner is notified when a customer connection is made
  - Partner is notified if customer terminates connection
  - Customer is notified if partner terminates connection
- Licensing visibility is limited to viewing summaries of license assignments and historical usage trends
- Partner to customer connections do not expire

Once the connection between the partner and a customer is made, partner admins can view the customer's basic account information, orders placed by the customer, and entitlement information, such as services, license counts, and expiration dates.

Inviting a customer to connect

Partners connect with customers in three simple steps:

1. Partner retrieves their invitation link from the customer dashboard. Select **Invite or Add** and choose whether the customer already has a Citrix Cloud account or needs to be onboarded. If the customer needs to be onboarded, provide their business contact details to create a Citrix Cloud for the customer. Afterward, the invitation appears.



Invite Customers

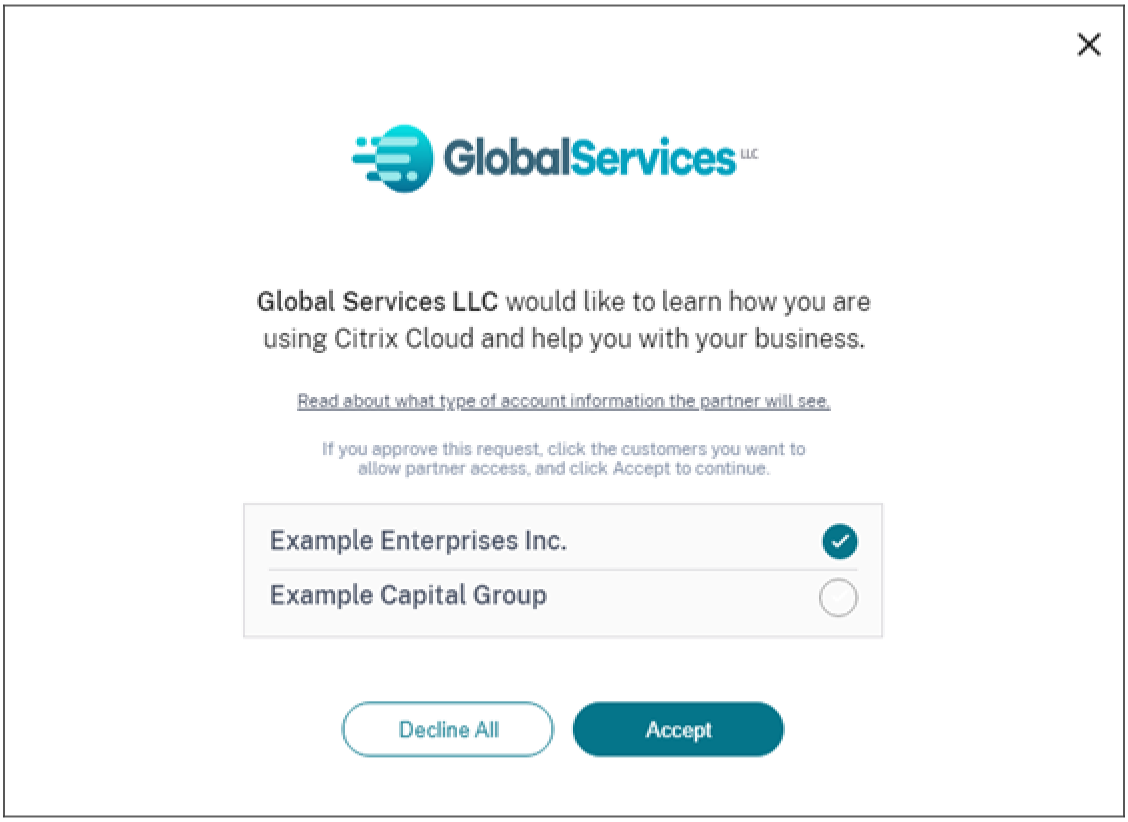
Copy the link below and share it with your customers.

To complete the connection a customer administrator needs to click the link, sign in to their Citrix Cloud account and accept the invitation.

https://us.cloud.com/invitati...

Learn more about connecting with customers on Citrix Cloud.

2. Partner copies the invitation link and provides it to the customer.
3. Customer clicks the link, signs in (or signs up) and accepts the connection request.



Global Services LLC would like to learn how you are using Citrix Cloud and help you with your business.

Read about what type of account information the partner will see.

If you approve this request, click the customers you want to allow partner access, and click Accept to continue.

- Example Enterprises Inc. ●
- Example Capital Group ○

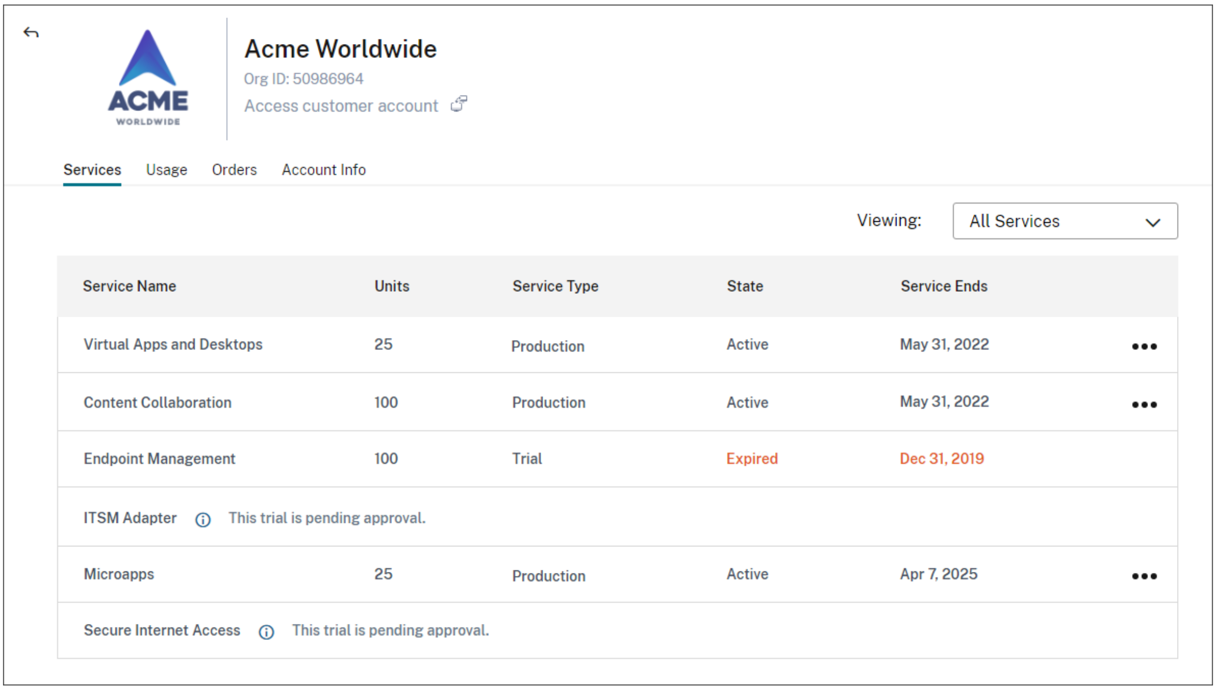
Additional information about partner invitation links:

- Partners are provided one invitation link. The link is fixed and not customizable or changeable.
- There is no limit to how many times the link can be used to establish a connection.
- The link can be reused if a connection needs to be recreated.
- The link does not expire.

Partner visibility into Citrix Cloud service entitlements

When a customer accepts a Citrix partner’s connection invitation, the partner gains basic visibility into the Citrix Cloud service entitlement status for that customer. This information includes the status of both trial and non-trial entitlements. Additional information includes:

- Active service trials
- Pending service trial requests
- Expired service trials
- Active service entitlements (services purchased or otherwise entitled or enabled for the customer)
- License count and expiration date for the entitlement



Acme Worldwide

Org ID: 50986964

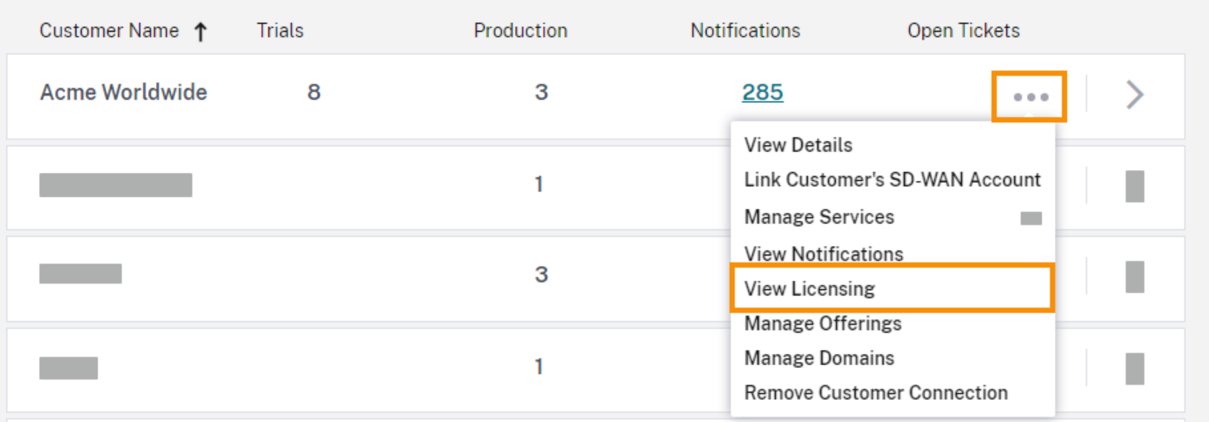
Access customer account

Viewing: All Services

Service Name	Units	Service Type	State	Service Ends
Virtual Apps and Desktops	25	Production	Active	May 31, 2022
Content Collaboration	100	Production	Active	May 31, 2022
Endpoint Management	100	Trial	Expired	Dec 31, 2019
ITSM Adapter ⓘ This trial is pending approval.				
Microapps	25	Production	Active	Apr 7, 2025
Secure Internet Access ⓘ This trial is pending approval.				

Licensing trends

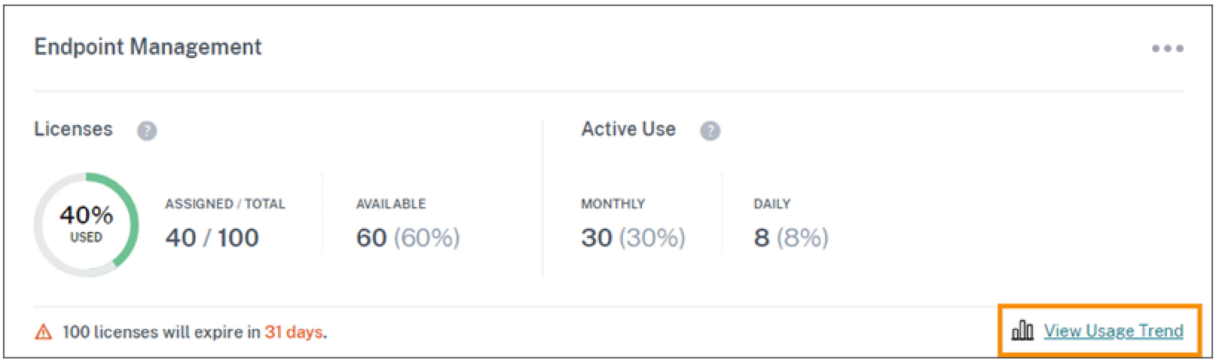
Partners can view licensing information from the customer dashboard by clicking the ellipsis button for the customer and selecting **View Licensing**.



Customer Name ↑	Trials	Production	Notifications	Open Tickets
Acme Worldwide	8	3	285	
[redacted]		1		
[redacted]		3		
[redacted]		1		

> **Note:**
>
> Citrix Partners can view only the Licensing summary view and historical active usage trends. They can't view individual users who consume licenses for a given service.

To view a summary, select **View Usage Trend** on the **Usage** tab in the customer page.



Endpoint Management

Licenses

40% USED

ASSIGNED / TOTAL 40 / 100

AVAILABLE 60 (60%)

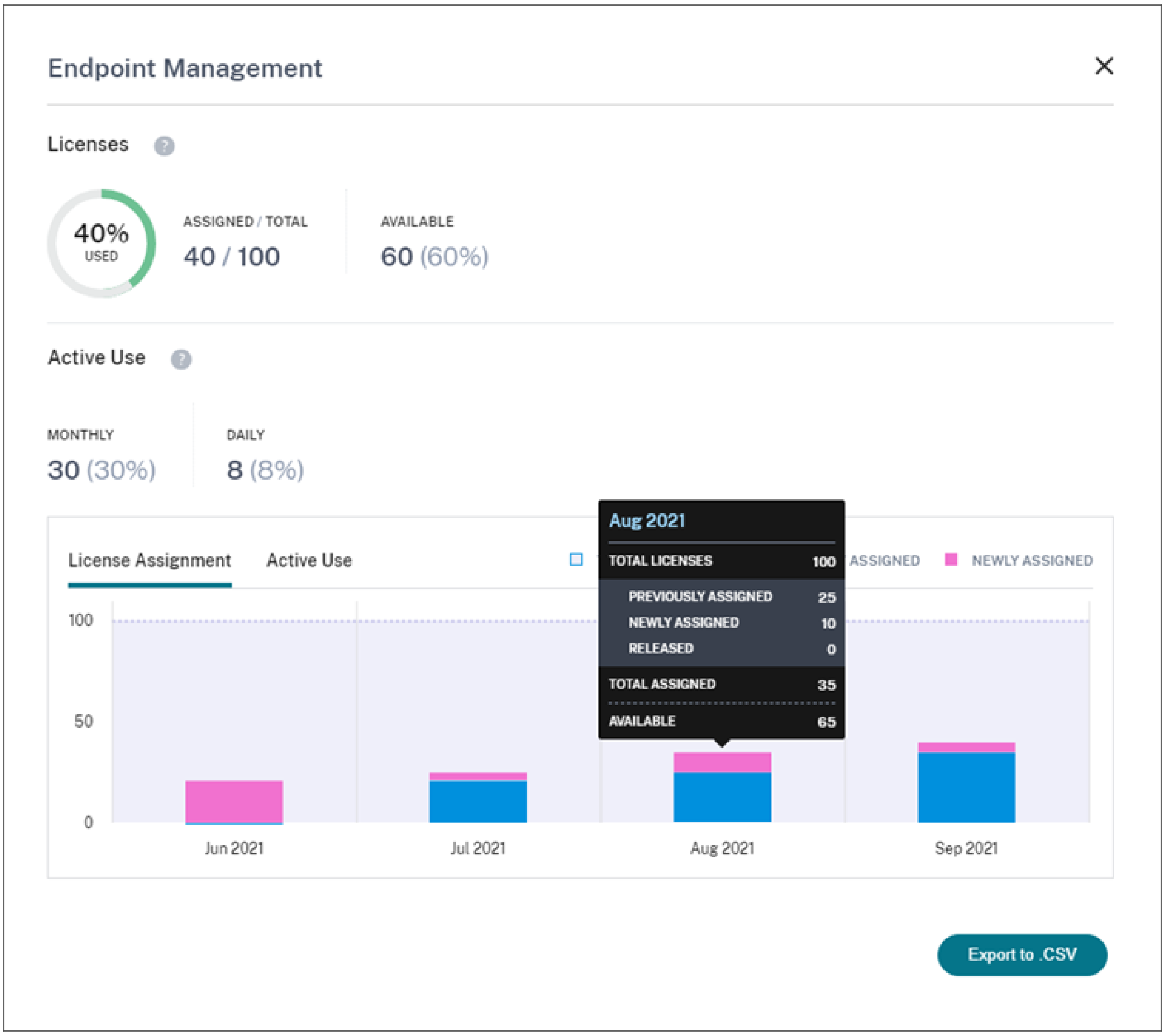
Active Use

MONTHLY 30 (30%)

DAILY 8 (8%)

⚠ 100 licenses will expire in 31 days.

The summary includes the ratio of assigned licenses to the total purchased, a breakdown of assigned licenses, and monthly and daily active users. If needed, partners can export this information as a .csv file.



Endpoint Management

Licenses

40% USED

ASSIGNED / TOTAL 40 / 100

AVAILABLE 60 (60%)

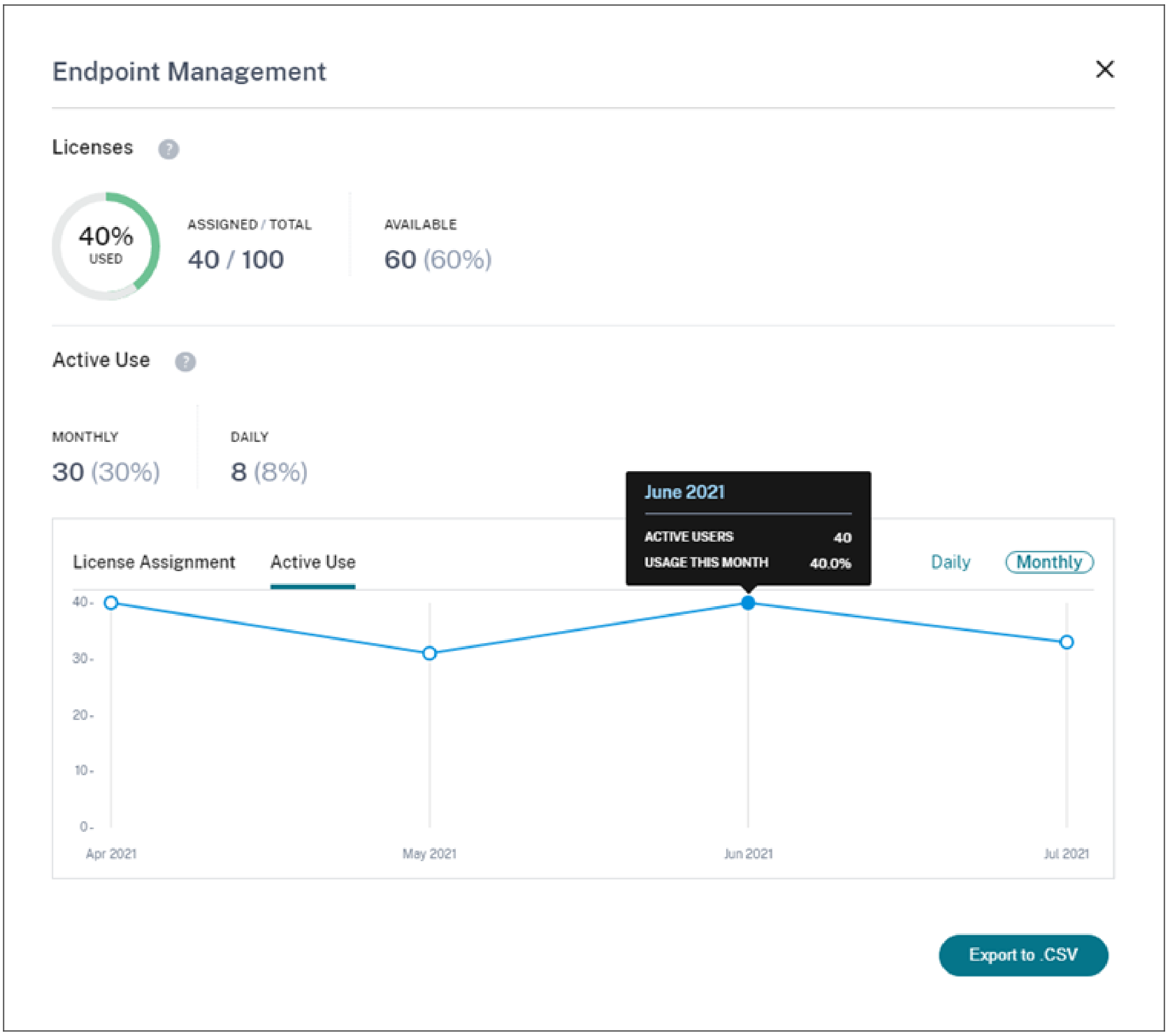
Active Use

MONTHLY 30 (30%)

DAILY 8 (8%)

Aug 2021

TOTAL LICENSES	100
PREVIOUSLY ASSIGNED	25
NEWLY ASSIGNED	10
RELEASED	0
TOTAL ASSIGNED	35
AVAILABLE	65



Endpoint Management

Licenses

40% USED

ASSIGNED / TOTAL 40 / 100

AVAILABLE 60 (60%)

Active Use

MONTHLY 30 (30%)

DAILY 8 (8%)

June 2021

ACTIVE USERS 40

USAGE THIS MONTH 40.0%

Customer licensing and usage for Citrix Service Providers

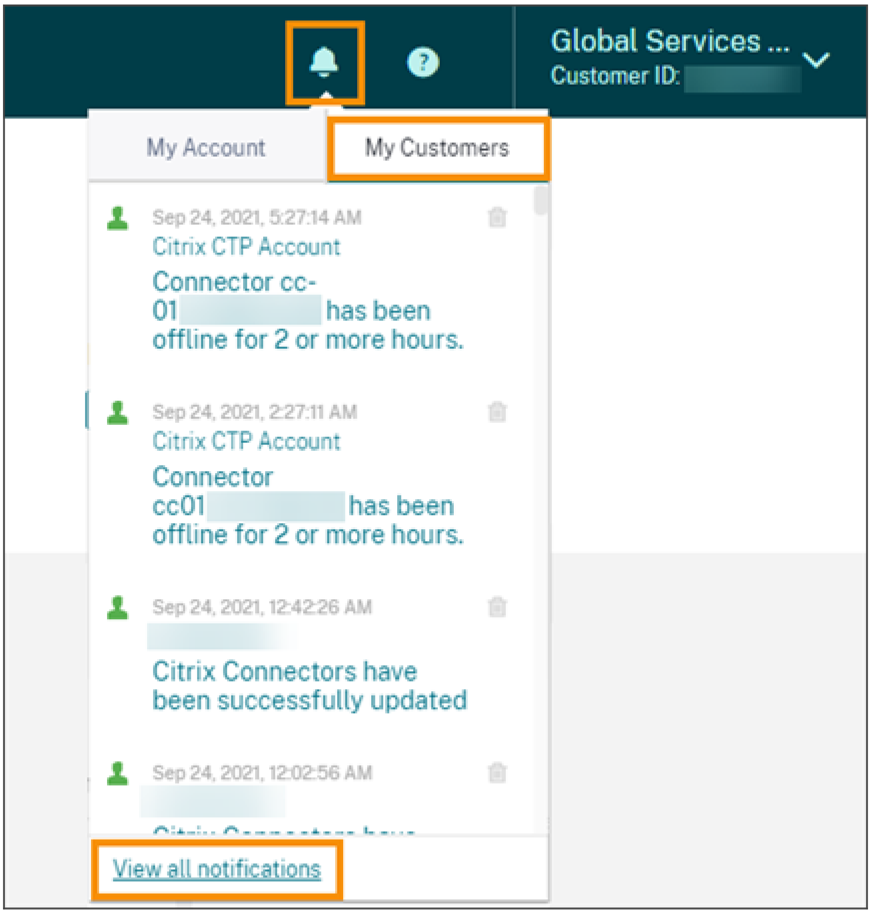
The Licensing feature in Citrix Cloud enables customers of Citrix Service Providers (CSP) to monitor their licenses and usage for supported Virtual Apps and Desktops products. CSPs can sign in under their customer's Citrix Cloud account to view and export this information as well. For more information, see the following articles:

- Customer license and usage monitoring for Citrix Virtual Apps and Desktops service
- Customer license and usage monitoring for Citrix Virtual Apps and Desktops Standard for Azure

Partner visibility into customer's support tickets and notifications

Partners can view the support tickets and notifications for the connected customers. Partners can also filter the customer-specific notification and take action, like dismissing the notification. Dismissed notifications don't show up for the partner. However, customers can still see the notification in their account after they sign in to Citrix Cloud.

To view customer notifications, click the bell icon near the top of the management console, select **My Customers**, and then select **View all notifications**.



Global Services ...
Customer ID: [redacted]

My Account | My Customers

Sep 24, 2021, 5:27:14 AM
Citrix CTP Account
Connector cc-01[redacted] has been offline for 2 or more hours.

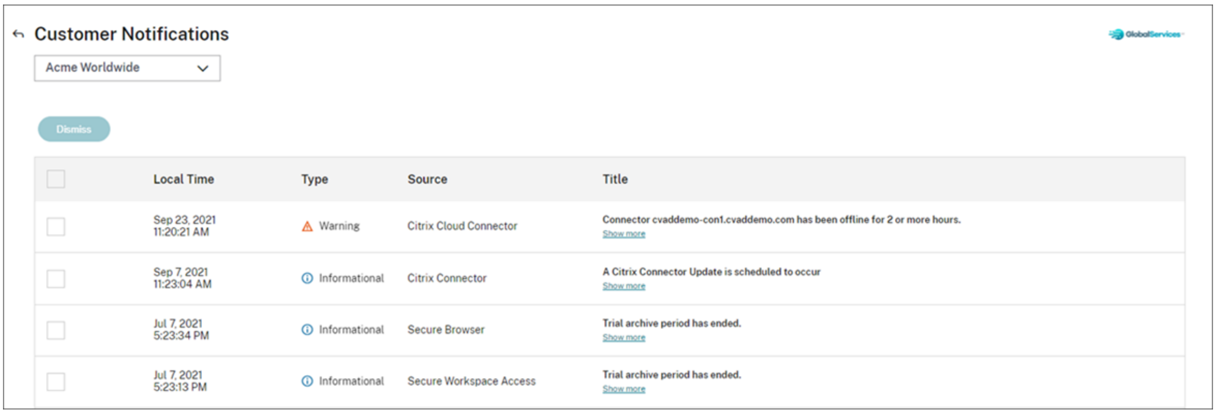
Sep 24, 2021, 2:27:11 AM
Citrix CTP Account
Connector cc01[redacted] has been offline for 2 or more hours.

Sep 24, 2021, 12:42:26 AM
[redacted]
Citrix Connectors have been successfully updated

Sep 24, 2021, 12:02:56 AM
[redacted]
Citrix Connectors have

View all notifications

Select a customer from the drop-down menu to view that customer's notifications.



Customer Notifications

Acme Worldwide

Dismiss

□	Local Time	Type	Source	Title
□	Sep 23, 2021 11:20:21 AM	⚠ Warning	Citrix Cloud Connector	Connector cvaddemo-con1.cvaddemo.com has been offline for 2 or more hours. Show more
□	Sep 7, 2021 11:23:04 AM	ⓘ Informational	Citrix Connector	A Citrix Connector Update is scheduled to occur Show more
□	Jul 7, 2021 5:23:34 PM	ⓘ Informational	Secure Browser	Trial archive period has ended. Show more
□	Jul 7, 2021 5:23:13 PM	ⓘ Informational	Secure Workspace Access	Trial archive period has ended. Show more

Visibility in customer support tickets helps partners resolve issues for their customers, ensuring a streamlined and error free experience for their users.

Federated domains for Citrix Service Providers

Federated domains enable customer users to use credentials from a domain attached to your CSP resource location to sign in to the workspace. This allows you to provide dedicated workspaces to your customer users with a custom workspace URL, such as *customer.cloud.com*. The resource location is still on your partner Citrix Cloud account. You can provide dedicated workspaces alongside the shared workspace that customers can access using your CSP workspace URL (for example, csp-partner.cloud.com). To enable customers to access their dedicated workspace, you add them to the appropriate domains that you manage. After configuring the workspace, customer users can sign in to their workspace and access the apps and desktops that you've made available through the Virtual Apps and Desktops service.

When you remove a customer from a federated domain, the customer's users can no longer access their workspaces using credentials from the partner's domain.

For more information about using federated domains to deliver apps and desktops, see Citrix Virtual Apps and Desktops service for Citrix Service Providers.

Workspace appearance options for Citrix Service Providers

You can configure your workspace colors and logos with custom themes. To learn how to create custom themes, see Customize the appearance of workspaces.

> **Note**
>
> Custom theming is a single-tenant feature. Citrix Service Providers where service provider tenants share a resource location, cloud connectors, and active directory domain (multi-tenant) are not currently supported. Citrix Service Provider tenants that have their own dedicated resource location, cloud connectors and dedicated active directory domain (single-tenant) are fully supported.

Citrix Cloud Services

September 29, 2021

This article lists the services that Citrix offers through Citrix Cloud and links to the product documentation for each service. For descriptions of these services and the Citrix offerings in which they are included, see Service Descriptions for Citrix Services.

Analytics

- Analytics for Security
- Analytics for Performance

- Analytics - Usage

App Builder

Application Delivery Management

Content Collaboration

- Create or link a Content Collaboration (ShareFile) account to Citrix Cloud
- Set up ShareFile

Endpoint Management

Gateway

ITSM Adapter

Managed Desktops (New name: Virtual Apps and Desktops Standard for Azure)

MDX Service

Microapps

SD-WAN Orchestrator

Secure Browser

Secure Internet Access

Secure Workspace Access

Virtual Apps and Desktops

Virtual Apps and Desktops Standard for Azure

Virtual Apps Essentials

Virtual Desktops Essentials

Web App Firewall

Workspace Environment Management

Advanced Concepts

May 17, 2019

The Advanced Concepts section of the Citrix Cloud documentation site provides a selection of technical articles from across the Citrix teams. The articles in this section provide in-depth guidance for deploying key components to help you deliver apps and data in a secure and resilient manner.

For even more in-depth technical articles, reference architectures, and best practices from Citrix technology experts, visit Citrix Tech Zone.

For community support forums for the Citrix Cloud platform and services, see Citrix Discussions.

On-premises StoreFront Authentication Reference Architectures for Citrix Virtual Apps and Desktops service

December 12, 2019

There are various reasons to host Citrix StoreFront inside a customer data center rather than use the Citrix Workspace platform. With the complexity of some environments there is a need to understand how Citrix Cloud components interact with StoreFront and Active Directory when StoreFront is the primary user front-end for the service.

While Citrix Workspace can meet the requirements for most use cases of Citrix Virtual Apps and Desktops, there are some use cases and requirements that will need StoreFront to be hosted in the customer's data center or resource locations.

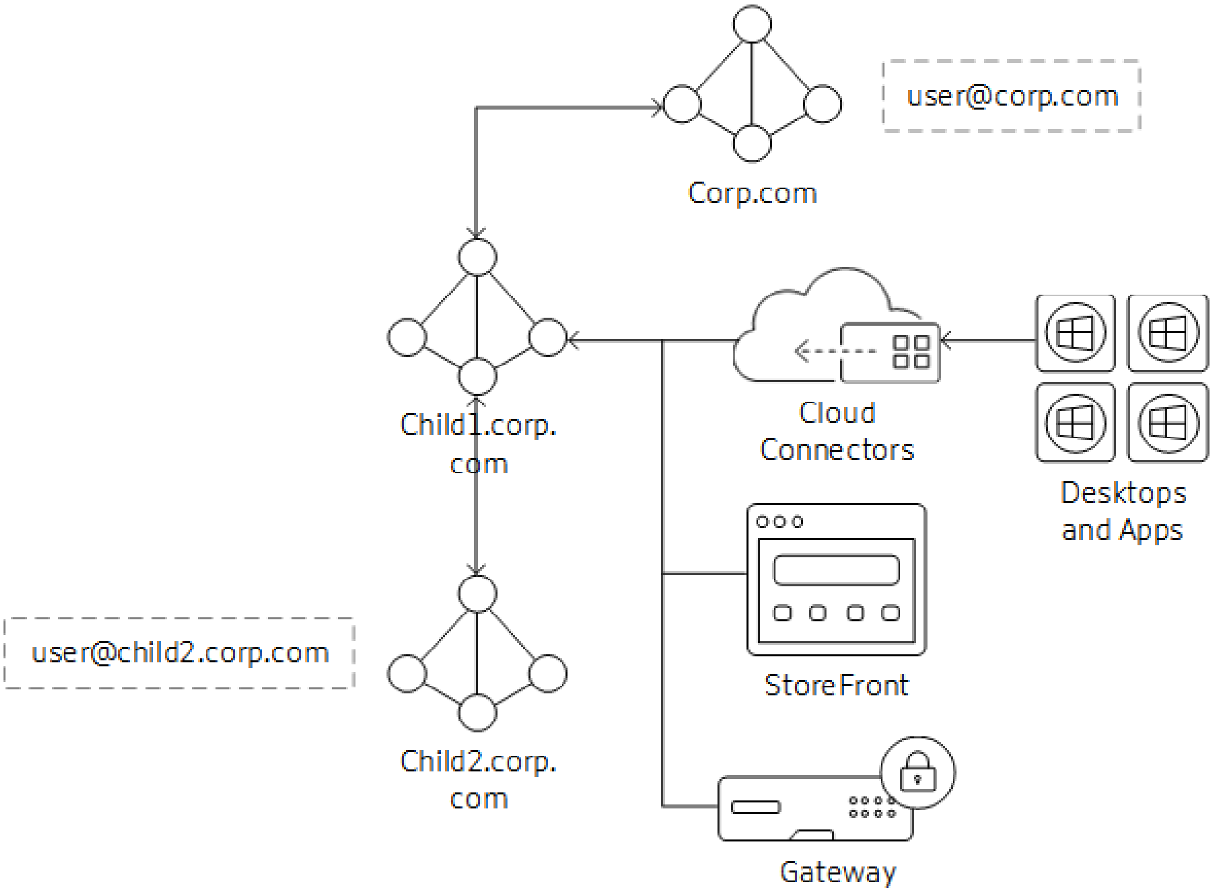
Reasons to maintain on-premises StoreFront

- Support Local Host Cache functionality in Cloud Connectors
- Authentication method such as smart card or SAML is not supported in Citrix Workspace
- Non-default store configurations (web.config changes)
- Hosting multiple store configurations for internal and external users

This article describes high level architectures and how the components interact with various authentication scenarios supported by Active Directory designs. Cloud Connectors will join one of the domains and allow the Virtual Apps and Desktops service to assign Active Directory users and groups of the domain or trusted domains. The Cloud Connectors will also act as Delivery Controllers and STA servers for StoreFront and Citrix Gateway components.

This article assumes StoreFront and Gateway components are hosted together in each data center.

Parent-Child Domains as Resource Domains



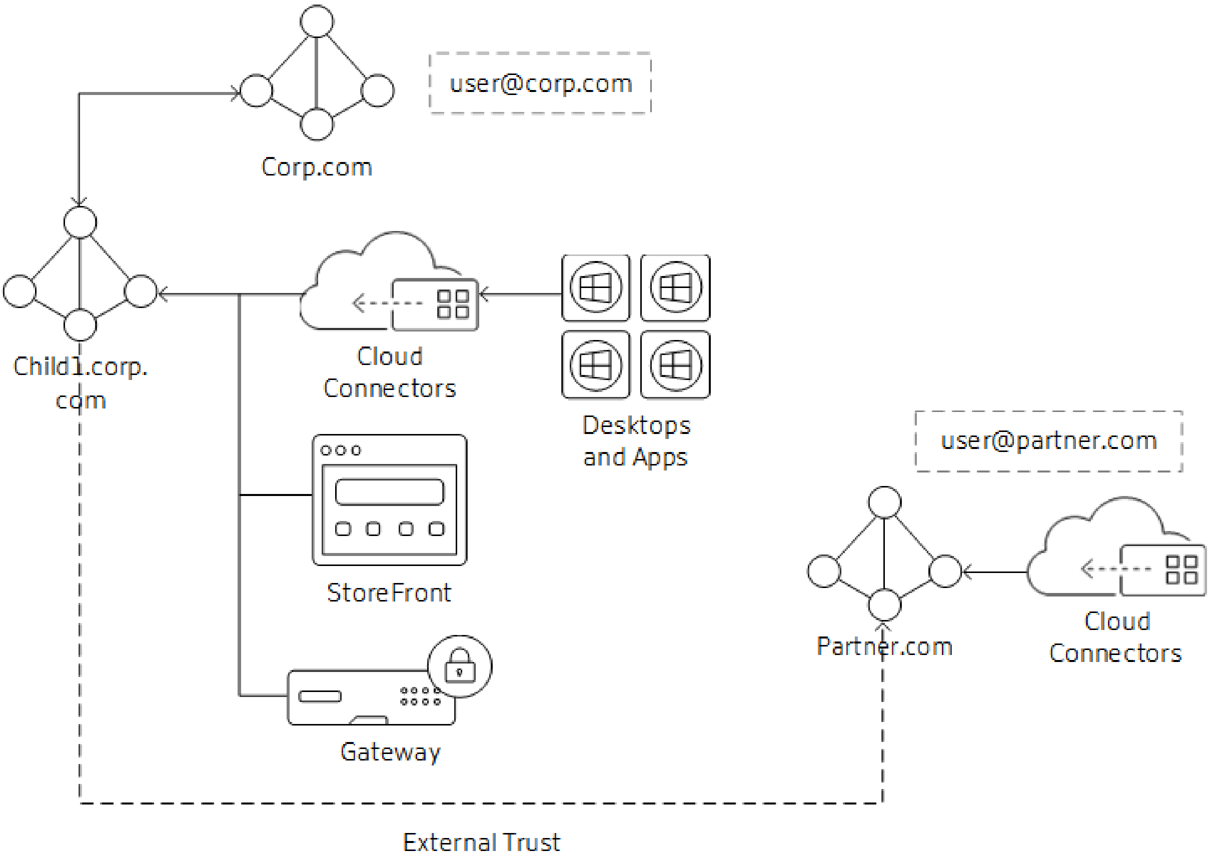
In this scenaio, the child domain is acting as the resource domain for Virtual Desktop Agents (VDAs) and StoreFront instances. The parent domain holds the users that will be accessing the resources in the child domain.

1. Cloud Connectors are joined to child domain only. The two-way transitive trust between child and parent domain allows the Cloud Connectors to communicate with the Global Catalog in the parent domain.
2. StoreFront is joined to the child domain. Store authentication is configured for Username/Password and Pass-through from Citrix Gateway. Username/Password authentication is configured to trust any domain.
3. Citrix Gateway authentication profile is configured for the parent domain to use UPN as the primary logon method. If there are users that need to authenticate from the child domain, the LDAP Authentication profile and policy for the child domain must also be bound to the Gateway vServer.
4. Edit Citrix Gateway Session OS and Web profiles and set Published Applications/Single Sign-On Domain setting blank (may need to set override setting).

Connection Workflow

1. User@corp.com logs on to Citrix Gateway. Gateway looks up the user through the authentication profile and matches the policy action.
2. Credentials are passed through to StoreFront. StoreFront accepts the credentials and passes them to the Cloud Connectors (acting as Delivery Controllers)
3. Cloud Connectors look up the user object details needed by Citrix Cloud.
4. Cloud Connectors pass identity information to Citrix Cloud and identity tokens authenticate the user and enumerate resources assigned to the user.
5. Cloud Connectors return assigned resources to StoreFront for user enumeration.
6. When the user launches an application or desktop, Citrix Gateway generates a STA ticket request using the configured Cloud Connectors.
7. Citrix Cloud brokers manage the sessions between resource domain Cloud Connectors and VDAs registered in that resource location.
8. Session is established between client, Citrix Gateway. and resolved VDA.

External Trusted Domains to Resource Domain



In this scenario, the business partner needs access to resources published to corporate users. The corporate domain is corp.com and the partner domain is partner.com.

1. The corporate domain has an outgoing external trust to the partner domain. Users from the partner domain can authenticate to resources joined to the corporate domain.
2. The Citrix Cloud customer needs two resource locations: one for corp.com Cloud Connectors and the second for partner.com Cloud Connectors. The partner.com Cloud Connectors are needed for Authentication and Identity calls to the domain only; they will not be used for brokering VDAs or sessions.
3. StoreFront is joined to the corp.com domain. Cloud Connectors in the corp.com domain are used as the Delivery Controllers in the store configuration. Store authentication is configured for Username/Password and Pass-through from Citrix Gateway. Username/Password Authentication is configured to trust any domain.
4. The Citrix Gateway authentication profile is configured for the corp.com domain to use UPN as the primary logon method. Configure a second profile and policy for the partner.com domain to use UPN and bind it to the same Gateway vServer as the corp.com domain.
5. Edit Citrix Gateway Session OS and Web profiles and set Published Applications/Single Sign-On Domain setting blank (may need to set override setting).

> **Note:**
>
> Depending on the location of the external trusted domain, the external domain users may experience longer launch times than resource or parent domain users.

Connection Workflow

1. User@partner.com logs on to Citrix Gateway. Gateway looks up the user through the authentication profile that matches the UPN lookup and matches the policy action.
2. Credentials are passed through to StoreFront. StoreFront accepts the credentials and passes them to the Cloud Connectors (acting as the Delivery Controllers).
3. Cloud Connectors perform the lookup for user object details needed by Citrix Cloud.
4. Cloud Connectors pass identity information to Citrix Cloud and identity tokens authenticate the user and enumerate resources assigned to the user.
5. Cloud Connectors return assigned resources to StoreFront for user enumeration.
6. When the user launches an application or desktop, Citrix Gateway generates a STA ticket request using the configured Cloud Connectors, in this case from child1.corp.com.
7. Citrix Cloud brokers manage the sessions between resource domain Cloud Connectors and VDAs registered in that resource location.
8. The session is established between client, Citrix Gateway, and resolved VDA.

Forest Trust / Shortcut Trust to Resource Domains

Forest and shortcut trust domains are only supported if treated as an external domain trust relationship to the resource domain. For forest trusts, you can follow the same steps that are described in the External Trusted Domains to Resource Domain section. This section may change in the future depending on the supportability of native forest trusts between user and resource domains/forests.

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