Citrix Cloud
Connect Okta as an identity provider to Citrix Cloud 133
Connect SAML as an identity provider to Citrix Cloud (Technical Preview) 138
Select a primary resource location 145
Manage Citrix Cloud administrators 146
Assign users and groups to service offerings using Library 152
Monitor licenses and active usage for cloud services 156
Monitor licenses and active usage for Citrix Virtual Apps and Desktops service (User/Device) 160
Monitor licenses and peak usage for Citrix Virtual Apps and Desktops service (Concurrent) 167
Monitor licenses and active usage for Citrix Virtual Apps and Desktops Standard for Azure service 170
Monitor licenses and active usage for Endpoint Management 174
Register on-premises products with Citrix Cloud 179
Monitor licenses and usage for on-premises deployments 181
Notifications 186
Citrix Workspace 188
Citrix Cloud for Partners 192
Content Collaboration 201
Create or link a Content Collaboration (ShareFile) account to Citrix Cloud 202
Set up ShareFile 207
IT Service Management (ITSM) Adapter 210
License Usage Insights Service 227
Technical Details 227
Get started with the License Usage Insights Service 228
Use the License Usage Insights Service 229
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update and configure Citrix License Server</td>
<td>236</td>
</tr>
<tr>
<td>Frequently Asked Questions</td>
<td>238</td>
</tr>
<tr>
<td>MDX Service</td>
<td>240</td>
</tr>
<tr>
<td>Secure Browser service</td>
<td>248</td>
</tr>
<tr>
<td>Citrix Virtual Apps Essentials</td>
<td>264</td>
</tr>
<tr>
<td>Citrix Virtual Desktops Essentials</td>
<td>296</td>
</tr>
<tr>
<td>Advanced Concepts</td>
<td>309</td>
</tr>
<tr>
<td>On-premises StoreFront Authentication Reference Architectures for Citrix Virtual Apps and Desktops service</td>
<td>309</td>
</tr>
</tbody>
</table>
Citrix Cloud

May 26, 2021

Citrix Cloud is a platform that hosts and administers Citrix 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.

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.

- 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.

Citrix Cloud services

Microapps

Microapps service helps you deliver relevant, actionable notifications from your applications directly into users’ workspaces. Build integrations from your application data sources to pull actions into Workspace. Microapps can write back to source systems, so users can address these actions without leaving their workspace. Users save time and can focus on their primary work because they don’t have to switch to other applications to interact with key business systems in your organization.

For more information, see the Microapps service documentation.

Virtual Apps and Desktops service

Citrix Virtual Apps and Desktops service (formerly XenApp and XenDesktop Service) offers a virtual app and desktop solution, provided as a cloud service, giving employees the freedom to work from anywhere on any device while cutting IT costs. Deliver Windows, Linux, web, and SaaS applications or full virtual desktops from any cloud: public, on premises or hybrid.

To learn more about this service, see Citrix Virtual Apps and Desktops service.
**Citrix Cloud**

**Endpoint Management**

Citrix Endpoint Management (formerly XenMobile Service) is a solution for managing endpoints, offering mobile device management (MDM) and mobile application management (MAM) capabilities. With Endpoint Management, you manage device and app policies and deliver apps to users.

To learn how to set up this service, see [Endpoint Management](#).

For Endpoint Management customers with the workspace experience enabled, users who open Secure Hub and click **Add Apps** are directed to the workspace. For more information, see [Secure Hub](#).

**Citrix Secure Browser**

The Citrix Secure Browser service isolates web browsing to protect the corporate network from browser-based attacks. It delivers consistent, secure remote access to internet hosted web applications, with no need for user device configuration. Administrators can rapidly roll out secure browsers, providing instant time-to-value. By isolating internet browsing, IT administrators can offer end users safe internet access without compromising enterprise security. For more information, see [Secure Browser service](#).

**Citrix Gateway**

Citrix Gateway (formerly NetScaler Gateway Service) allows secure, contextual access to the apps and data you need to do your best work.

To learn more about this service, see [Citrix Gateway Service](#).

**Citrix Analytics**

Citrix Analytics collects data across Citrix portfolio products and generates actionable insights, enabling administrators to proactively handle user and application security threats, improve app performance, and support continuous operations.

To learn more about this service, see [Citrix Analytics](#).

**Citrix Application Delivery Management**

Citrix Application Delivery Management (formerly NetScaler Management and Analytics Service) provides an easy and scalable solution to manage Citrix networking deployments on-premises or on the cloud from a single, unified, and centralized cloud based console. It provides all the capabilities required to quickly set up, deploy, and manage application delivery in Citrix networking deployments and with rich analytics of application health, performance, and security.

To learn more about this service, see [Citrix Application Delivery Management](#).
**Citrix Content Collaboration**

The advanced access, collaboration, workflows, rights management, and integration features of ShareFile are now available in the Citrix Content Collaboration component set in our secure, contextual, integrated Citrix Workspace.

To learn more about this service, see [Citrix Content Collaboration](#).

**Citrix SD-WAN Orchestrator**

Citrix SD-WAN Orchestrator is a cloud hosted, multi-tenant management SaaS offering, which Citrix partners could leverage to offer managed SD-WAN services to their customers. It provides a single-pane of glass management platform for Citrix partners to manage multiple customers centrally, with suitable role based access controls.

To learn more about this service, see [Citrix SD-WAN Orchestrator](#).

**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](#).

**Service Level Agreement**

April 20, 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.
Citrix Cloud

- 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**

<table>
<thead>
<tr>
<th>Service</th>
<th>Measure for Monthly Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Analytics for Performance</td>
<td>Time users can access and improve apps and desktops performance.</td>
</tr>
<tr>
<td>Citrix Analytics for Security</td>
<td>Time users can detect and mitigate user access and activity risks.</td>
</tr>
<tr>
<td>Citrix Application Delivery Management service</td>
<td>Average time the Service is available across all POPs.</td>
</tr>
<tr>
<td>Citrix Content Collaboration</td>
<td>Time users can enumerate files and folders associated with their account or download files that are hosted in Citrix-managed StorageZones.</td>
</tr>
</tbody>
</table>
Citrix Cloud

<table>
<thead>
<tr>
<th>Service</th>
<th>Measure for Monthly Uptime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Endpoint Management</td>
<td>Time users can access their Citrix delivered mobile apps and enrolled devices through the Service.</td>
</tr>
<tr>
<td>Citrix Gateway Service for HDX Proxy</td>
<td>Time users can access their app or desktop session through the Service.</td>
</tr>
<tr>
<td>Citrix Intelligent Traffic Management</td>
<td>Time users can access traffic management functionality through DNS queries or HTTP API calls.</td>
</tr>
<tr>
<td>Citrix SD-WAN Orchestrator</td>
<td>Time users can access their SD-WAN Orchestrator account and manage their SD-WAN network through the Service.</td>
</tr>
<tr>
<td>Citrix Secure Workspace Access</td>
<td>Time users can access their SaaS or internal web app through the Service.</td>
</tr>
<tr>
<td>Citrix Virtual Apps service</td>
<td>Time users can access their app or desktop session through the Service.</td>
</tr>
<tr>
<td>Citrix Virtual Desktops service</td>
<td>Time users can access their app or desktop session through the Service.</td>
</tr>
<tr>
<td>Citrix Virtual Apps and Desktops service</td>
<td>Time users can access their app or desktop session through the Service.</td>
</tr>
<tr>
<td>Citrix Workspace</td>
<td>Same as above for component services, but includes availability for each. Credits may be prorated if a claim relates to less than all components.</td>
</tr>
</tbody>
</table>

**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

May 7, 2021


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.
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
  • ShareFile StorageZones

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.

<table>
<thead>
<tr>
<th>Client Port</th>
<th>Server Port</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>49152-655535/UDP</td>
<td>123/UDP</td>
<td>W32Time</td>
</tr>
<tr>
<td>49152-655535/TCP</td>
<td>135/TCP</td>
<td>RPC Endpoint Mapper</td>
</tr>
<tr>
<td>49152-655535/TCP</td>
<td>464/TCP/UDP</td>
<td>Kerberos password change</td>
</tr>
<tr>
<td>49152-655535/TCP</td>
<td>49152-655535/TCP</td>
<td>RPC for LSA, SAM, Netlogon (*)</td>
</tr>
<tr>
<td>49152-655535/TCP/UDP</td>
<td>389/TCP/UDP</td>
<td>LDAP</td>
</tr>
<tr>
<td>49152-655535/TCP</td>
<td>636/TCP</td>
<td>LDAP SSL</td>
</tr>
<tr>
<td>49152-655535/TCP</td>
<td>3268/TCP</td>
<td>LDAP GC</td>
</tr>
<tr>
<td>49152-655535/TCP</td>
<td>3269/TCP</td>
<td>LDAP GC SSL</td>
</tr>
<tr>
<td>53, 49152-655535/TCP/UDP</td>
<td>53/TCP/UDP</td>
<td>DNS</td>
</tr>
<tr>
<td>49152-655535/TCP</td>
<td>49152-655535/TCP</td>
<td>FRS RPC (*)</td>
</tr>
<tr>
<td>49152-655535/TCP/UDP</td>
<td>88/TCP/UDP</td>
<td>Kerberos</td>
</tr>
<tr>
<td>49152-655535/TCP/UDP</td>
<td>445/TCP</td>
<td>SMB</td>
</tr>
</tbody>
</table>

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.
Citrix Cloud

<table>
<thead>
<tr>
<th>Connection Direction</th>
<th>Connector Appliance Port</th>
<th>External Port</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inbound</td>
<td>443/TCP</td>
<td>Any</td>
<td>Local Web UI</td>
</tr>
<tr>
<td>Outbound</td>
<td>49152-65535/UDP</td>
<td>123/UDP</td>
<td>NTP</td>
</tr>
<tr>
<td>Outbound</td>
<td>53, 49152-65535/TCP/UDP</td>
<td>53/TCP/UDP</td>
<td>DNS</td>
</tr>
<tr>
<td>Outbound</td>
<td>67/UDP</td>
<td>68/UDP</td>
<td>DHCP and broadcast</td>
</tr>
</tbody>
</table>

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

April 26, 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](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.

Use the dashboard to learn more about the following conditions:
• The current health status of all Citrix Cloud services, grouped by geographical region
Citrix Cloud

- 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.

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.

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.
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.

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

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.
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**.
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:
• Notification email with subscription options

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](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**

3. Sign in with your Citrix account
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.

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 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)
Sign up for Citrix Cloud

November 30, 2020

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

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 enables users to potentially impact service, it’s important to control who accesses the Citrix Cloud 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.

**Step 1: Visit the sign-up page**


**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**.

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?

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

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

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.

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

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.
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.

**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

2. If you are an administrator for multiple customer organizations, select one from the list.
3. From the top-right menu, select My Profile.
4. In Authenticator app, select Set up authenticator app.

Citrix Cloud sends you an email with a verification code.
5. After you receive the email, enter the 6-digit verification code and your Citrix Cloud password and select Verify.
6. 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.
7. Under **Verify your authenticator app**, enter the code from your authenticator app and select **Verify code**.

8. 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**.
9. Select **Finish** to complete the enrollment.

After successful enrollment, the Authenticator app section displays a green check mark and the My Profile page displays your configured recovery methods.
The next time you sign in with your Citrix Cloud administrator credentials, Citrix Cloud prompts you for the verification code from your authenticator app.
Manage your device enrollment

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

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

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 top-right corner of the management console, beneath your account name.
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

April 21, 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.
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.

<table>
<thead>
<tr>
<th>Service</th>
<th>US</th>
<th>EU</th>
<th>Asia Pacific South</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Cloud control plane</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Citrix Analytics</td>
<td>Yes</td>
<td>Yes</td>
<td>No (Uses US region)</td>
</tr>
<tr>
<td>Application Delivery Management</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Citrix Content Collaboration</td>
<td>Yes***</td>
<td>Yes***</td>
<td>No - Select from US or EU **</td>
</tr>
<tr>
<td>Citrix Endpoint Management</td>
<td>Yes**</td>
<td>Yes**</td>
<td>Yes**</td>
</tr>
<tr>
<td>SD-WAN Orchestrator</td>
<td>Yes</td>
<td>Yes</td>
<td>No (Uses US region)</td>
</tr>
<tr>
<td>Secure Browser Service</td>
<td>Yes*</td>
<td>Yes*</td>
<td>Yes*</td>
</tr>
<tr>
<td>Citrix Virtual Apps and Desktops service</td>
<td>Yes*</td>
<td>Yes*</td>
<td>Yes*</td>
</tr>
</tbody>
</table>
## Citrix Cloud

<table>
<thead>
<tr>
<th>Service</th>
<th>US</th>
<th>EU</th>
<th>Asia Pacific South</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Virtual Apps and Desktops Standard for Azure</td>
<td>Yes ⚫</td>
<td>Yes ⚫</td>
<td>Yes ⚫</td>
</tr>
<tr>
<td>Citrix Virtual Apps Essentials</td>
<td>Yes ⚫</td>
<td>Yes ⚫</td>
<td>Yes ⚫</td>
</tr>
<tr>
<td>Citrix Virtual Desktops Essentials</td>
<td>Yes ⚫</td>
<td>Yes ⚫</td>
<td>Yes ⚫</td>
</tr>
<tr>
<td>Web App Firewall</td>
<td>Yes</td>
<td>Yes</td>
<td>No (Uses US region)</td>
</tr>
<tr>
<td>Citrix Workspace</td>
<td>Yes ⚫</td>
<td>Yes ⚫</td>
<td>Yes ⚫</td>
</tr>
<tr>
<td>Workspace Environment Management</td>
<td>Yes</td>
<td>Yes</td>
<td>No (Uses US region)</td>
</tr>
<tr>
<td>Networking services</td>
<td>Yes</td>
<td>No (Uses US region)</td>
<td>No (Uses US region)</td>
</tr>
<tr>
<td>License Usage Insights (CSPs only)</td>
<td>Globally replicated</td>
<td>Globally replicated</td>
<td>Globally replicated</td>
</tr>
<tr>
<td>Citrix Gateway Access Nodes/POP</td>
<td>Multiple WW nodes; traffic routed as needed to ensure the best experience</td>
<td>Multiple WW nodes; traffic routed as needed to ensure the best experience</td>
<td>Multiple WW nodes; traffic routed as needed to ensure the best experience</td>
</tr>
<tr>
<td>Citrix Secure Internet Access Nodes/POP</td>
<td>Multiple WW nodes; traffic routed as needed to ensure the best experience</td>
<td>Multiple WW nodes; traffic routed as needed to ensure the best experience</td>
<td>Multiple WW nodes; traffic routed as needed to ensure the best experience</td>
</tr>
</tbody>
</table>

* Service uses the Citrix Cloud region.

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

*** StorageZone can be selected from multiple locations. See Content Collaboration locations and StorageZones 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.

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

For ShareFile Enterprise accounts created outside of Citrix Cloud, your StorageZone 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 Zones that are turned on in the Content Collaboration management console. Choose from the following locations:
Citrix Cloud

- 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:
Citrix Cloud

- 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

January 26, 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.

**Fast facts about service trials**

<table>
<thead>
<tr>
<th>Citrix Cloud Trial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of subscribers allowed</td>
</tr>
<tr>
<td>Maximum Length</td>
</tr>
<tr>
<td>Availability</td>
</tr>
<tr>
<td>Resource location</td>
</tr>
<tr>
<td>User session length</td>
</tr>
<tr>
<td>Local Microsoft Active Directory integration</td>
</tr>
<tr>
<td>Choice of resource locations</td>
</tr>
<tr>
<td>Deploy to on-premises</td>
</tr>
<tr>
<td>Virtual Apps and Desktops service</td>
</tr>
<tr>
<td>Endpoint Management*</td>
</tr>
<tr>
<td>Customizable</td>
</tr>
</tbody>
</table>

*Trial not currently available.
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.
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

April 22, 2021

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.
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.

**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 1st 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’ll need your Organization ID, available in the Citrix Cloud management console.
System and Connectivity Requirements

June 10, 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](https://trust.citrixnetworkapi.net) (for retrieving a code)
- [https://trust.citrixworkspacesapi.net/](https://trust.citrixworkspacesapi.net/) (for confirming the license server is registered)
- [https://cis.citrix.com](https://cis.citrix.com) (for data upload)
- [https://core-eastus-release-a.citrixworkspacesapi.net](https://core-eastus-release-a.citrixworkspacesapi.net)
- [https://core.citrixworkspacesapi.net](https://core.citrixworkspacesapi.net)
- [ocsp.digicert.com port 80](https://ocsp.digicert.com:80)
- [crl3.digicert.com port 80](https://crl3.digicert.com:80)
- [crl4.digicert.com port 80](https://crl4.digicert.com:80)
- [ocsp.entrust.net port 80](https://ocsp.entrust.net:80)
- [crl.entrust.net port 80](https://crl.entrust.net: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.
Citrix Cloud

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.

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

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, seeCTX221535.

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
Citrix Cloud

* **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 How to configure 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 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-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
    - Customers using Citrix Virtual Apps Essentials need to use https://*.xendesktop.net instead.
Citrix Cloud

- **https://*.*.nssvc.net**
  - Customers who can’t enable all subdomains can use the following addresses instead:
    * [https://*.*.g.nssvc.net](https://*.*.g.nssvc.net)
    * [https://*.*.c.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://*.*.citrixworkspacesapi.net)
- [https://*.*.citrixnetworkapi.net](https://*.*.citrixnetworkapi.net)
- [https://*.*.cloud.com](https://*.*.cloud.com)
- [https://[customerid].xendesktop.net](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](https://*.*.xendesktop.net) instead.
- [https://*.*.nssvc.net](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://*.*.g.nssvc.net)
    * [https://*.*.c.nssvc.net](https://*.*.c.nssvc.net)
- For in-product messages including new features and critical communications: [https://citrix-cloud-content.customer.pendo.io/](https://citrix-cloud-content.customer.pendo.io/)

**Citrix Workspace service connectivity**

- [https://*.*.cloud.com](https://*.*.cloud.com)
- [https://*.*.citrixdata.com](https://*.*.citrixdata.com)
- For in-product messages including new features and critical communications: [https://citrix-cloud-content.customer.pendo.io/](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](http://*.cloud.com)
  - *[.citrixworkspacesapi.net](http://*.citrixworkspacesapi.net)
Citrix Cloud

- 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
Citrix Cloud

- 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**

June 8, 2020

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

May 26, 2021

**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.

**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 web site.

*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 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 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 web site.
  - http://crl3.digicert.com
  - http://crl4.digicert.com
  - http://ocsp.digicert.com
  - http://crl.microsoft.com
  - http://oneocsp.microsoft.com
• Communication with the following addresses is enabled:
  - https://*.digicert.com
• The following certificates are installed:
  - https://dl.cacerts.digicert.com/DigiCertAssuredIDRootCA.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

**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.

<table>
<thead>
<tr>
<th>Forest Functional Level</th>
<th>Domain Functional Level</th>
<th>Supported Domain Controllers</th>
</tr>
</thead>
</table>

**Federal Information Processing Standard (FIPS) support**

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

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Description</th>
<th>Runs As</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Cloud Agent System</td>
<td>Handles the system calls necessary for the on-premises agents. Includes installation, reboots, and registry access. Can only be called by Citrix Cloud Services Agent WatchDog.</td>
<td>Local System</td>
</tr>
<tr>
<td>Citrix Cloud Services Agent WatchDog</td>
<td>Monitors and upgrades the on-premises agents (evergreen).</td>
<td>Network Service</td>
</tr>
</tbody>
</table>

© 1999-2021 Citrix Systems, Inc. All rights reserved.
<table>
<thead>
<tr>
<th>Service Name</th>
<th>Description</th>
<th>Runs As</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Cloud Services Agent Logger</td>
<td>Provides a support logging framework for the Citrix Cloud Connector services.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Cloud Services AD Provider</td>
<td>Enables Citrix Cloud to facilitate management of resources associated with the Active Directory domain accounts in which it is installed.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Cloud Services Agent Discovery</td>
<td>Enables Citrix Cloud to facilitate management of XenApp and XenDesktop legacy on-premises Citrix products.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Cloud Services Credential Provider</td>
<td>Handles storage and retrieval of encrypted data.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Cloud Services WebRelay Provider</td>
<td>Enables HTTP Requests received from WebRelay Cloud service to be forwarded to On-Premises Web Servers.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix CDF Capture Service</td>
<td>Captures CDF traces from all configured products and components.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Config Synchronizer Service</td>
<td>Copies brokering configuration locally for high availability mode.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Connection Lease Exchange Service</td>
<td>Enables Connection Lease files to be exchanged between Workspace app and Cloud Connector for Service Continuity for Workspace</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix High Availability Service</td>
<td>Provides continuity of service during outage of central site.</td>
<td>Network Service</td>
</tr>
</tbody>
</table>
# Citrix Cloud

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Description</th>
<th>Runs As</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix ITSM Adapter Provider</td>
<td>Automates provisioning and management of virtual apps and desktops.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix NetScaler Cloud Gateway</td>
<td>Provides internet connectivity to on-premises desktops and applications without the need to open in-bound firewall rules or deploying components in the DMZ.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Remote Broker Provider</td>
<td>Enables communication to a remote Broker service from local VDAs and StoreFront servers.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix Remote HCL Server</td>
<td>Proxies communications between the Delivery Controller and the Hypervisor(s).</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix WEM Cloud Authentication Service</td>
<td>Provides authentication service for Citrix WEM agents to connect to cloud infrastructure servers.</td>
<td>Network Service</td>
</tr>
<tr>
<td>Citrix WEM Cloud Messaging Service</td>
<td>Provides service for Citrix WEM cloud service to receive messages from cloud infrastructure servers.</td>
<td>Network Service</td>
</tr>
</tbody>
</table>

## Deployment scenarios for Cloud Connectors in Active Directory

If you have a single domain in a single forest, installing Cloud Connectors in that domain is all you need to establish a resource location. 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:
Citrix Cloud

- 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**

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

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

**Event logs**

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

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 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.

Cloud Connector Proxy and Firewall Configuration

May 26, 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
Citrix Cloud

Cloud remains stable. Additionally, 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.

Installer

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

Services at Runtime

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

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

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

After executing the command, restart the 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. Additionally, 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 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 the address for the Network Service account is configured using netsh or a similar tool.

Cloud Connector Installation

May 26, 2021

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

The installation occurs with the privileges of the user who initiates 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 that will 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 re-install 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) is not supported. If you clone a machine with the Cloud Connector installed, the Cloud Connector services will not run and the machine cannot connect to Citrix Cloud.

Interactive installation

To create your first resource location

1. Log on as an administrator to the machine where you’ll install the Cloud Connector. The machine must have Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019 installed, be joined to a domain, and have outbound Internet access.
2. Visit https://citrix.cloud.com and sign in with the credentials you received in the email from Citrix Cloud. The Citrix Cloud management console appears.
3. From the menu button in the upper left corner, select Resource Locations.
4. On the Resource Locations page, click Download to download the Cloud Connector software.
5. Right-click the Cloud Connector installer and select Run as administrator. The installer performs an initial connectivity check to ensure you can connect to Citrix Cloud.
6. When prompted, sign in to Citrix Cloud.
7. Follow the wizard to install and configure the Cloud Connector. When the installation finishes, the installer performs a final connectivity check to verify Connector-to-Cloud communication.
8. Repeat these steps on other machines you want to use as Cloud Connectors.

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

**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 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:

```json
{
    "customerName": "*CustomerID*",
    "clientId": "*ClientId*",
    "clientSecret": "*ClientSecret*",
}
```
A sample command line that installs using the parameter file:

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

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

**Note:**

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

**Troubleshooting**

**Connectivity checks**

You can attempt to diagnose and fix issues encountered during installation using the Cloud Connector Connectivity Check utility. The utility can be used to:

- Test whether Citrix Cloud and its related services are reachable
- Configure proxy settings on the Cloud Connector

**Installation error**

If you install the 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 on to the machine as an administrator to install the Cloud Connector. To avoid this error, run the Cloud Connector software as an administrator by right-clicking the installer and selecting Run as administrator.

**Installation Logs**

Installation logs are located at `%LOCALAPPDATA%\Temp\CitrixLogs\CloudServicesSetup`. Logs are also added to `%ProgramData%\Citrix\WorkspaceCloud\InstallLogs` after installation.
Exit codes

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

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.
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–!`.

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.

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**

May 12, 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:
Citrix Cloud

- 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

- [x] Set a maintenance start time:

  - Select Hour:
  - Select a Timezone:

[ Cancel ] [ Confirm ]
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

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 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.

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.
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
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.

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.

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.

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.
4. Copy the VHD 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.
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.

### 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](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.psl
```

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.

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.

**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.

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.

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

   The **Create new password** webpage opens.

3. Create a password for your Connector Appliance UI and click **Set password**.
The password you set must meet the following requirements:

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

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

4. Sign in with the password you just set.

The **Connector Appliance administration page** opens.
5. (Optional) If you use one or more web proxies, you can add the proxy addresses here. Only unauthenticated proxies are 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**.
The webpage provides a code to use to register with Citrix Cloud. This code expires in 15 minutes.

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.
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.
Generating a diagnostic report

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

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

**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:

   ![GRUB Menu](image)

   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>
     ```
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**

March 2, 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.

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 that’s running in your resource location at any time. 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.

---

Note:
This information is not available for Connector Appliances.

---

**Identity and access management**

May 26, 2021
Identity and Access Management defines the identity providers and accounts used for Citrix Cloud administrators and workspace subscribers.

Identity providers

By default, Citrix Cloud uses the Citrix identity provider to manage the identity information for all users in your Citrix Cloud account. You can change this to use one of the following identity providers:

- On-premises Active Directory
- Active Directory plus token
- Azure Active Directory
- Citrix Gateway
- Okta

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

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. This 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 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 will stay 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 will 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 loca-
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. The resource location you select as "primary" should have Citrix 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.

**Connect Active Directory to Citrix Cloud**

May 26, 2021

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

**Note:**

Some workspace authentication methods require a connection between your AD and Citrix Cloud. For more information, see Change authentication to workspaces.

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

4. Launch the Cloud Connector installer and follow the installation wizard.
5. From the **Connect to Active Directory** page, click **Detect**. After verification, Citrix Cloud displays a message that your Active Directory is connected.

6. Click **Return to Authentication**. The **Active Directory** entry is marked **Enabled** on the **Authentication** tab.

**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

August 20, 2020

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

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 multi-factor authentication for a higher level of security against the possibility of stolen sign-in credentials.
- Use a branded sign-in page, so your users know they’re signing in at the right place.
- Use federation to an identity provider of your choice including ADFS, Okta, and Ping, among others.

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.

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

Important:

You must be a Global Admin in Azure AD to complete this task.

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. These read-only permissions 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 information, see Consenting to delegated permission prompts.
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 multi-factor authentication, world-class security features, federation to 20 different identity providers, and self-service password change and reset, among many other features. Turning these features on for your Azure AD users enables Citrix Cloud 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 read-only 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 read-only permissions to Citrix Cloud and allow Citrix Cloud to reconnect to Azure AD on your behalf.

**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 will fail. 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.

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

September 4, 2020

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](https://www.citrix.com/) 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.
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 need to 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
Citrix Cloud

- 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 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


**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**.

3. Enter the FQDN of your on-premises Gateway and click **Detect**.
Configure your On-Premises Gateway as an Identity Provider for Workspace

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

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

FQDN: citrix.com

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

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 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 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:
   b) On the Create Authentication Policy page, enter the following information:
      • In Name, enter a friendly name for the policy.
      • In Action Type, select LDAP.
      • In Action, select the LDAP authentication server you created earlier.
      • In Expression, enter TRUE.
   c) Click Create to save the configuration.

3. Create the Authentication Policy Label:
   b) In Name, enter a friendly name for the authentication policy label.
   c) In Login Schema, select LSCHEMA_INT.
d) Under **Policy Binding**, in **Select Policy**, select the LDAP advanced authentication policy you created earlier.

e) In **GoTo Expression**, select **END**.

f) Click **Bind** to finish the configuration.

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

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**

July 21, 2020

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](#).
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 website.

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

Okta OIDC web application

To use Okta as an identity provider, you must first create an Okta OIDC web application with client credentials you can use with Citrix Cloud. 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 application
- 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 website. Afterward, you import your AD users and groups to Okta. When importing, include the SID, UPN, and OID values associated with your AD accounts.

*Note:*

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

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

1. Install and configure the Okta AD agent. For complete instructions, refer to the following articles on the Okta website:
   - Install the Okta Active Directory agent
   - Configure Active Directory import and account settings
Configure Active Directory provisioning settings

2. Add your AD users and groups to Okta by performing a manual import or an automated import. For more information about Okta import methods and instructions, refer to Manage Active Directory users and groups on the Okta website.

Create an Okta OIDC web application

1. From the Okta management console, under Applications, select Applications.
2. Click Add Application and then click Create New App.
3. In Sign in method, select OpenID Connect and then click Create. The Platform default value (Web) is unchanged.
4. Enter an application name.
5. In Login redirect URIs, enter https://accounts.cloud.com/core/login-okta.
6. In Logout redirect URIs, enter your Workspace URL from Citrix Cloud.
7. Click Save.

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. From the Okta application configuration page, in General Settings, click Edit.
2. In Allowed grant types, select the following options:
   - Authorization Code
   - Refresh Token
   - Implicit (Hybrid)
   - Allow ID Token with implicit grant type
   - Allow Access Token with implicit grant type
3. Click Save.
4. Allow user or group access to the application:
   a) From the Assignments tab, select Assign and then select Assign to People or Assign to Groups.
   b) Select the users or groups you want to have access to workspaces. To allow access for all users, select Assign to Groups and then select Everyone.
5. Click Done.
6. 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:
Citrix Cloud

- Display Name: cip_sid
- Variable Name: cip_sid
- Description: AD User Security Identifier
- Attribute Length: Greater than 1
- Attribute Required: Yes

d) Click 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) Click 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) Click Save.

7. 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) On the Settings tab, select Edit Mappings.
   d) Map the following attributes:
      - 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) Click Save Mappings.
   f) Click Apply updates now.

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. Click 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**

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 credentials for your Okta application. 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 (Technical Preview)**

May 27, 2021

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

**Notes:**

- This feature is currently in Technical Preview. Citrix recommends using technical preview features only in test environments.
- This article describes setting up SAML 2.0 in Citrix Cloud with Active Directory only. If you plan to use single sign-on (SSO) with SAML 2.0, see [How to Integrate Azure AD with SAML 2.0 Tech Preview (CTX312150)](https://citrix.cloud.com).

**Prerequisites**

Using SAML authentication with Citrix Cloud has the following requirements:

- SAML provider that supports SAML 2.0
Citrix Cloud

- 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:

- SecurityIdentifer (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. **Identity and Access Management**, configure SAML authentication in Citrix Cloud. This task involves configuring the SAML metadata from Citrix Cloud in your SAML provider and then configuring the metadata from your SAML provider in Citrix Cloud to create the SAML connection.

4. **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

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:

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

   ![SAML Metadata Example]

   ```xml
   <EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="https://app.example.com/saml/metadata/80733d0b-0579-414d-b4e1-4ff034893419"
   allowUnsatisfiable="true" allowUnsatisfiableSignature="true" artifactResolutionWindow="120000">
   ...
   </EntityDescriptor>
   </ds:SOAPMessage>
   
   ![Certificate Image]
   
   ![Signature Image]
   ```

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.
   - **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**.
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 enforce authentication at the selected context as well as more strict contexts. Select Exact to enforce authentication at the selected context only. For example, if you select the Transport Layer Security (TLS) context and the Minimum level, Citrix Cloud accepts SAML responses with the context of TLS, X.509 Certificate, Integrated Windows Authentication, and Kerberos. Responses using the User Name and Password and Password Protected Transport contexts are rejected. 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**.

### 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](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.
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.

Manage Citrix Cloud administrators

May 21, 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.

**Invite new administrators**

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

![Citrix Cloud interface](image)

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

![Administrators page](image)

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:

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.

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](image)

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.
**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
To add subscribers to the offering, choose a domain and then select the users or groups you want to add.

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**
  - yourdomain.com

- **Step 2: Choose a group or user**
  - Search...

Selected 2 of 3 Subscriber(s)  
[Remove Selected] Cancel

<table>
<thead>
<tr>
<th></th>
<th>Type</th>
<th>Subscriber</th>
<th>Status</th>
</tr>
</thead>
</table>
|  | USER | James Tennant  
Domain:yourdomain.com | Subscribed |
|  | USER | Michael Tennenbaum  
Domain:yourdomain.com | Subscribed |
|  | GROUP | TechGroup  
Domain:yourdomain.com | 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.

Monitor licenses and active usage for cloud services

November 24, 2020

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:
Citrix Cloud

- 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

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

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.

- **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.

**Monitor licenses and active usage for Citrix Virtual Apps and Desktops service (User/Device)**

October 15, 2020

**License assignment**

Citrix Cloud assigns a license when a unique user or unique device launches an app or desktop for the first time.
The Licensing summary 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.
- 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, whichever is less.
  - Daily active use refers to the number of unique users or devices that have used the service in the last 24 hours, whichever is less.
- 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. Citrix Cloud uses the lesser of these counts to measure assigned licenses and active use.

For example, 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.

If 10 unique users and 20 unique devices used the service in the last 30 days, Citrix Cloud calculates monthly active use based on the lesser number (10). Likewise, if 30 unique users and 15 unique devices were counted in the last 24 hours, Citrix Cloud calculates daily active use based on the lesser number (15).
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, under Usage Trends, 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 native Workspace app or Receiver client instead.
- **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.
- **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:
Citrix Cloud

- A list of the individual users who have assigned licenses, including associated devices.

  **License Activity**

<table>
<thead>
<tr>
<th>36 Licensed Users</th>
<th>9 Licensed Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release Licenses</strong></td>
<td><strong>Search by User..</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Username</th>
<th>Domain</th>
<th>Devices</th>
<th>Last Login</th>
<th>Date Assigned</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>mauricele</td>
<td>acmeworldwide</td>
<td>2 Devices</td>
<td>Sep 15, 2016 11:23:40 UTC</td>
<td>Mar 25, 2017</td>
<td>***</td>
</tr>
<tr>
<td>ikianru</td>
<td>Initech</td>
<td>2 Devices</td>
<td>Aug 18, 2016 12:13:45 UTC</td>
<td>Jan 18, 2017</td>
<td>***</td>
</tr>
</tbody>
</table>

- A list of the devices that have assigned licenses, including associated users.

<table>
<thead>
<tr>
<th>36 Licensed Users</th>
<th>9 Licensed Devices</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Release Licenses</strong></td>
<td><strong>Search by Device..</strong></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Device ID</th>
<th>Users</th>
<th>Last Login</th>
<th>Date Assigned</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>GWDT5-Dell XPS</td>
<td>A65AD46A</td>
<td>45 Users</td>
<td>Sep 15, 2016 11:23:40 UTC</td>
<td>Mar 25, 2017</td>
<td>***</td>
</tr>
<tr>
<td>GWDT5-Surface</td>
<td>A65AD44R</td>
<td>19 Users</td>
<td>Aug 18, 2016 12:13:45 UTC</td>
<td>Jan 18, 2017</td>
<td>***</td>
</tr>
</tbody>
</table>

- 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.

© 1999-2021 Citrix Systems, Inc. All rights reserved. 165
To release multiple assigned licenses

1. Under License Activity, select Release Licenses.

   ![License Activity Table]

   - **username1**: acmeworldwide, **Devices**: 2 Devices, **Last Login**: Sep 15, 2016 11:23:40 UTC, **Date Assigned**: Mar 25, 2017
   - **username2**: Initext, **Devices**: 2 Devices, **Last Login**: Aug 18, 2016 12:13:45 UTC, **Date Assigned**: Jan 18, 2017

2. From the list, select the users you want to manage and select Continue to Devices.

   ![Release Licenses Screen]

   - There are 45 users that haven’t logged in the last 30 days and are eligible for release.

3. Select the devices you want to manage and select Continue to Release.
4. Review the licenses you’ve selected and select Release Licenses.
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.
b) To release a single device, click the ellipsis button and select Release Device.

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)

March 30, 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.
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 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.
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.

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

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

You can download usage information for a standard or specified interval.

The information includes meter usage for:
Citrix Cloud

- 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.
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.

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 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

<table>
<thead>
<tr>
<th>Endpoint Management</th>
<th>View Usage Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Licenses</strong></td>
<td><strong>Active Use</strong></td>
</tr>
<tr>
<td>62% (USED)</td>
<td>40 (40%)</td>
</tr>
<tr>
<td>62 / 100</td>
<td>36 (36%)</td>
</tr>
<tr>
<td>AVAILABLE</td>
<td>MONTHLY</td>
</tr>
<tr>
<td>38 (38%)</td>
<td>DAILY</td>
</tr>
</tbody>
</table>

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:
Citrix Cloud

- 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

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**.

2. From the list, select the users you want to manage and select **Continue**.
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**.

4. Review the user you selected and select **Continue**.

5. When prompted to confirm the release, click **Release**.

---

**Register on-premises products with Citrix Cloud**

May 26, 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 currently 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 with Citrix Cloud**.

**Connectivity requirements**

To register your on-premises products successfully, ensure the following addresses are contactable:

- [https://trust.citrixnetworkapi.net](https://trust.citrixnetworkapi.net) (for retrieving a code)
- [https://trust.citrixworkspacesapi.net/](https://trust.citrixworkspacesapi.net/) (for confirming the license server is registered)
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.

Register a product

1. From the Citrix Cloud menu, select Identity and Access Management.
2. Select API Access > Product Registrations and then select Register.
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**.

3. When prompted, select **Remove**.

### 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
Citrix Cloud
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.

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.
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 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.
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.

Notifications

February 24, 2020

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 click **Dismiss**. Dismissing notifications removes them from your list and Citrix Cloud updates the notifications count when you return to the console home page.

Administrators receive their own notifications in Citrix Cloud. So, dismissing notifications doesn’t prevent other administrators from viewing their notifications.
Citrix Cloud

**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.

Citrix Workspace

May 5, 2021
Citrix Workspace is a complete digital workspace solution that delivers secure access to the information, apps, and other content that is relevant to a person’s role in your organization. Users subscribe to the services you make available and can access them from anywhere, on any device. Citrix Workspace helps you organize and automate the most important details that your users need to collaborate, make better decisions, and focus on their work.

For a complete description of each Citrix Workspace edition and included features, see the Citrix Workspace Feature Matrix.

**Get started**

Citrix Workspace includes a step-by-step walkthrough to help you deliver workspaces quickly. Each step guides you through the Citrix Cloud console with instructions for tasks like configuring your identity provider, selecting your workspace authentication, and enabling other services that come with Workspace. The walkthrough also provides quick access to technical information needed for assembling your deployment team, and configuring your infrastructure and resources. For an overview of the tasks and the information needed as you progress in your deployment, see Get Started with Citrix Workspace.

**Microapps**

Microapps helps you deliver relevant, actionable notifications from your applications directly into users' workspaces. Users save time and can focus on their primary work when they don’t have to switch between applications to interact with key business systems in your organization. Build integrations from your application data sources to pull actions into Workspace. Microapps write back to source systems, so users can address these actions without leaving their workspace.

For more information, see the Microapps service documentation.

**Citrix Virtual Apps Essentials service**

Citrix Virtual Apps Essentials offers secure access to virtual Windows apps. This service includes a workspace URL, enabled by default, usually in the format: https://yourcompanyname.cloud.com. Follow the steps to set up Citrix Virtual Apps Essentials, then test and share the workspace URL link with your subscribers to give them access to their apps.

**Citrix Virtual Desktops Essentials service**

Citrix Virtual Desktops Essentials offers secure access to Windows 10 virtual desktops. This service includes a workspace URL, enabled by default, usually in the format: https://yourcompanyname.cloud.com. Follow the steps to set up Citrix Virtual Desktops Essentials, then test and share the workspace URL link with your subscribers to give them access to their desktops.
Citrix Cloud

**Citrix Virtual Apps and Desktops service**

The Citrix Virtual Apps and Desktops service offers secure access to virtual apps and desktops. This service includes a workspace URL, enabled by default, usually in the format: https://yourcompanyname.cloud.com. Follow the steps to set up the Citrix Virtual Apps and Desktops service, then test and share the workspace URL link with your subscribers to give them access to their apps and desktops. Your subscribers can access the workspace URL without any additional configuration.

**Citrix Endpoint Management**

For Endpoint Management customers with the workspace experience enabled, users who open Secure Hub and click **Add Apps** are directed to the Workspace apps store instead of the Secure Hub store. This feature is available only to **new customers**. Migration for existing customers is not supported. To use this feature, perform the following tasks:

- To deploy the Workspace experience to new devices, add them to the Workspace delivery group. For more information, see [Citrix Endpoint Management integration with Citrix Workspace](#).
- Enable the Password Caching and Password Authentication policies. For more information on configuring policies, see [MDX Policies at a glance](#).
- Configure Active Directory authentication as AD or AD+Cert. These are the two modes that we support. For more information on configuring authentication, see [Domain or domain plus security token authentication](#).
- Enable Workspace integration for Endpoint Management. For more information on workspace integration, see [Workspace Configuration](#).

**Important:**

After this feature is enabled, ShareFile SSO occurs through Workspace and not through Endpoint Management. We recommend that you disable ShareFile integration in the Endpoint Management console before you enable Workspace integration.

**Citrix Gateway**

Citrix Gateway (formerly the NetScaler Gateway Service) provides secure remote access with Identity and Access Management (IdAM) capabilities. Citrix Gateway delivers a unified experience to SaaS (Software as a Service) apps, and virtual apps and desktops. Follow the steps to set up the Citrix Gateway service, then test and share the workspace URL with your subscribers to give them remote access. For more information on configuring SaaS apps within the Citrix Gateway service, see [Support for Software as a Service Apps](#).
Citrix Content Collaboration

Citrix Content Collaboration (formerly ShareFile) provides secure data access, sync, and file sharing from any device. We bring business-class file sharing, streamlined workflows, and real-time collaboration together in one location so that users can work the way they want.

1. Ensure you have entitlement to Content Collaboration.
2. Link Citrix Workspace to your Content Collaboration account. For more information, see About Content Collaboration including the Create or link a Content Collaboration (ShareFile) account to Citrix Cloud article.
3. Enable Content Collaboration in Citrix Workspace. See Deploy and enable Citrix Content Collaboration in Citrix Workspace in the Citrix Content Collaboration doc set. If you have this process set up, you see the Files tab in the left-side navigation in Citrix Workspace UI.

Electronic signature

Citrix delivers electronic signature capability using Citrix RightSignature. An electronic signature, sometimes known as an e-signature, is the same as your handwritten signature on a paper document, except electronic — a mark on an electronic contract or document you make to demonstrate your intent to agree to the terms of that document. For more information about RightSignature, see RightSignature FAQs.

Users can send for signature directly from Citrix Workspace with the Citrix RightSignature integration with Citrix Content Collaboration. See the ShareFile RightSignature Integration Follow these steps:

1. Ensure you have entitlement to Content Collaboration and RightSignature.
2. Link Citrix Workspace to your Content Collaboration account and enable Content Collaboration in Citrix Workspace. For more information, see About Content Collaboration including the Create or link a Content Collaboration (ShareFile) account to Citrix Cloud article, and Deploy and enable Citrix Content Collaboration in Citrix Workspace in the Citrix Content Collaboration doc set. If you have this process set up, you see the Files tab in the left-side navigation in Citrix Workspace UI.
3. Enable RightSignature for end users. See Add Users to RightSignature support article. If you have this process set up, you see the Send for Signature tile from any file opened from Files in Citrix Workspace UI.

Citrix RightSignature is also available as a stand-alone solution. To get started, see RightSignature. For Electronic signature in Content Collaboration, see Citrix Content Collaboration - Electronic signature.

Secure Browser service

The Secure Browser service protects the corporate network from browser-based attacks by isolating web browsing. When subscribers navigate to the URL provided by the administrator, their published
browsers are shown, along with other apps and desktops that are configured in other Citrix Cloud services. Follow the steps to set up the Secure Browser Service, then test and share the workspace URL with your subscribers to give them access to a secure browser.

**Example use case**

Your organization currently manages a mix of Microsoft Office apps through the Citrix Virtual Apps and Desktops service, and SaaS apps, such as Workday, through Citrix Gateway.

You also have legacy apps from an on-premises Virtual Apps and Desktops deployment. You can now deliver all these apps into a single integrated user experience.

The user can access their workspace with all the apps they need from a browser or app - the Citrix Workspace app. You can customize the experience in a simplified console (Workspace Configuration) in Citrix Cloud, and choose how you want users to authenticate.

For this use case, complete the setup for the individual services first. Switch to Workspace Configuration to carry out further customization and configuration to the overall behavior of the Workspace user experience. Workspace Configuration (in the Sites tab) is also where you connect up your on-premises Virtual Apps and Desktops deployment to the Workspace user experience (known as Site aggregation). Share the Workspace URL with your users for clientless access, and guide them to install the Citrix Workspace app for the best experience.

**Citrix Cloud for Partners**

May 12, 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). Each Citrix Cloud account is associated with a Citrix ORGID that can be viewed in the Citrix Cloud account details.

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.
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.

**Licensing trends**

Partners can view licensing information from the customer dashboard by clicking the ellipsis button for the customer and selecting **View Licensing**.

---

**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. 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.
Inviting a customer to connect

Partners connect with customers in three simple steps:

1. Partner retrieves their invitation link from the customer dashboard.
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.

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.

**Sharing account information with partners**

**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

---

**Partner visibility into customer’s support tickets and notifications**

Partners can view the support tickets and notification 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.
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.

Content Collaboration

November 13, 2020

Content Collaboration allows you to share, sync, and secure content from the cloud and on-premises storage services.

For information about creating Content Collaboration accounts in Citrix Cloud, see Create or link a Content Collaboration (ShareFile) account to Citrix Cloud.

For information about setup tasks, see Set up ShareFile.

For information about deploying Content Collaboration and using Citrix Files in Citrix Workspace, see Citrix Content Collaboration.

For information about using Citrix Files on each supported platform, see Citrix Files in the User Help Center.

Service Level Agreement

Content Collaboration is designed using industry best practices to achieve cloud scale and a high degree of service availability.

For complete details about Citrix’s commitment for availability of Citrix Cloud services, see Service Level Agreement
Create or link a Content Collaboration (ShareFile) account to Citrix Cloud

June 9, 2021

To get started with Content Collaboration, you can take advantage of the following options:

- If you’re new to Content Collaboration and want to try it out, you can request a trial.
- If you already have a ShareFile account but haven’t purchased any new entitlements, you can connect your account to Citrix Cloud.
- If you’ve purchased ShareFile or Workspace entitlements, you can create a new account in Citrix Cloud and assign your entitlements to that account.
- If you’ve purchased the ShareFile or Workspace entitlements, you can connect your existing ShareFile account to Citrix Cloud to assign your new entitlements.

Request a trial

Use the following steps if you don’t have a Content Collaboration account and want to try out the service.

1. Sign into Citrix Cloud using your Citrix credentials.
2. From the Citrix Cloud console, under My Services, locate the Content Collaboration tile.
3. In Add Service, select Request a Trial.

The Add Content Collaboration Account page appears with the Request Trial tab selected.

4. In the GEO Location section, select the service region you want to use and acknowledge that the location can’t be changed after requesting the trial.
5. In the Select a subdomain section, enter the unique subdomain you want to use.
6. Click Request Trial. Citrix Cloud sends you an email after your Content Collaboration account is created.
7. Under **My Services**, click **Manage** on the Content Collaboration tile to continue to the Content Collaboration Admin Overview.

**Create a new Content Collaboration account and assign entitlements**

Use the following steps if you've purchased Content Collaboration entitlements and want to create a new account and assign the entitlements to that account.

1. Sign into **Citrix Cloud** using your Citrix Cloud credentials.
2. From the Citrix Cloud console, under **My Services**, locate the Content Collaboration tile and click **Manage**.

![My Services](image)

The Assign Content Collaboration Entitlements page appears and displays any new Content Collaboration entitlements purchased under your Citrix OrgID.

3. Select the entitlements you want to apply to the account and click **Continue**.
4. Under **Account Name**, select a new account you want to assign to the entitlement and click **Assign**.

![Assign Content Collaboration Entitlements](image)

5. On the **Create a Content Collaboration account** page, under **Account Details**, enter the following information:
a) In Step 1: GEO Location, select the service region for your account. If you select the USA region, choose whether you plan to store Protected Health Information (PHI) in the account.
b) In Step 2: Identity Provider, select the identity provider you want to use for end-user access to your account. If your identity provider isn’t supported, you can elect to have Citrix store your user directory.
c) In Step 3: Select Storage Zone, select the default storage zone for your account.

6. Select Create Account.

**Link an existing ShareFile account**

To link an existing ShareFile account to your Citrix Cloud account, the following requirements must be met:

- You must have administrator permissions in both Citrix Cloud and ShareFile.
- Your ShareFile administrator permissions must include Access company account permissions.
- The email address that you use to sign in to Citrix Cloud must match the email address on record for ShareFile.

If any of these requirements aren’t met, Citrix Cloud might not be able to locate your ShareFile account for assignment. If you need help with these requirements, contact Citrix Support.

**To link your Content Collaboration account to Citrix Cloud (no new entitlements)**

Use the following steps if you haven’t purchased new entitlements and want to link your existing ShareFile account to Citrix Cloud.

1. Sign in to Citrix Cloud using your Citrix credentials.
2. From the Citrix Cloud console, under My Services, locate the Content Collaboration tile.
4. Select the ShareFile account you want to link and then click **Link Account**.

![Add Content Collaboration Account](image)

**Important:**

If no accounts are displayed, verify that you are an administrator for ShareFile and that your email address for Citrix Cloud matches your email address for Content Collaboration. For additional assistance, contact [Citrix Support](#).

**To link your ShareFile account and assign entitlements**

Use the following steps if you’ve purchased new ShareFile or Workspace entitlements to assign and manage your entitlements in Citrix Cloud.

1. Sign in to Citrix Cloud using your Citrix credentials.

2. From the Citrix Cloud console, under **My Services**, locate the Content Collaboration tile and click **Manage**. The Assign Content Collaboration Entitlements page appears and displays the new entitlements you have purchased.

3. Select the entitlements you want to apply to the account and then click **Continue**.

![Assign Content Collaboration Entitlements](image)

4. Select the account you want to apply to the selected entitlements.
Important:
If no accounts are displayed, verify that you are an administrator for Content Collaboration and that your email address for Citrix Cloud matches your email address for ShareFile. For additional assistance, contact Citrix Support.

When the **We didn’t find any Content Collaboration accounts** message appears, see **To link to an account never connected to Citrix Cloud** and complete the steps.

5. Select **I understand that entitlements assigned to an account cannot be reversed.**

6. Click **Assign.** The Assign Content Collaboration Entitlements page displays the account assigned to the entitlement.

7. Click **Manage** to continue to the Content Collaboration Admin Overview.

**To link to an account never connected to Citrix Cloud**

Use the following steps if you have never linked an account to Citrix Cloud.

1. Sign in to Citrix Cloud using your Citrix credentials.

2. From the Citrix Cloud console, under **My Services**, locate the Content Collaboration tile and click **Manage.** The **We didn’t find any Content Collaboration accounts** message appears.

3. Select **Link another account.**

4. Select the Content Collaboration account you want to link and then click **Link Account.**
Set up ShareFile

May 26, 2021

After you create or link your ShareFile account, perform the following tasks:

1. Provision administrators.
2. Provision users.
3. Import Active Directory users into ShareFile.
4. Configure authentication.

Provisioning Administrators

The first thing you need to do is provision administrators. When your account was created, it was provisioned with a master administrator account. This was the first administrator added to your Citrix Cloud account. In addition to this administrator, you can provision additional administrators. Any additional administrator provisioned within Citrix Cloud will be added to ShareFile with administrator access.

Provisioning Users

To begin using your new ShareFile account, you must add users and configure authentication. In the Citrix Cloud environment, you will want to enable SSO between the different components. In order to provide a seamless experience to your end users, you will use SAML to authenticate against your Active Directory user accounts.

Importing Active Directory Users into ShareFile

The ShareFile User Management Tool (UMT) makes it easy for you to add your Active Directory users into ShareFile. You can use the tool to provision user accounts and create distribution groups from Active Directory (AD).

Importing users from Active Directory can take some time and be resource intensive. To help with this, you can schedule the tool to run at selected times. In addition to the initial import, you can also use the tool to keep your ShareFile users synchronized with your AD users.

For more information about the UMT, see User Management Tool for Policy-Based Administration.

Configuring Authentication

After you have imported your users in to ShareFile, you must configure authentication. When using the Citrix Cloud environment, you will want to use SSO. SSO will be done using the SAML protocol.
In this environment you have two options for configuring SAML – either using ADFS or via Endpoint Management SAML authorization.

**Configuring Authentication with ADFS**

You can integrate your ShareFile account with Active Directory (AD) to enable single sign-on for users with AD credentials. ShareFile supports Security Assertion Markup Language (SAML) for single sign-on. You configure ShareFile to communicate with a SAML-based federation tool running in your network. User logon requests are then redirected to Active Directory. You can use the same SAML Identity Provider that you use for other web applications. For more information, see [ShareFile Single Sign-On SSO](#).

**Configuring Authentication to your Active Directory with Endpoint Management**

You can configure Endpoint Management and Citrix Gateway to function as a SAML identity provider for ShareFile. In this configuration, a user logging on to ShareFile using a web browser or other ShareFile clients is redirected to the Endpoint Management environment for user authentication. After successful authentication by Endpoint Management, the user receives a SAML token that is valid for logon to their ShareFile account. For more information, see [Single Sign On for ShareFile with Citrix Gateway](#).

**Accessing ShareFile**

Now that you have configured your users and authentication, you should look at how ShareFile will be accessed. There are two specific types of access you need to look at: administrator access and user access.

**Administrator Access**

As administrator, you may need to make changes to your ShareFile configuration or manage your account.

**Accessing the Content Collaboration Administrator UI through Citrix Cloud**

You can access the Content Collaboration Web UI directly through the Citrix Cloud. Access through the Citrix Cloud provides a slightly trimmed down version of the ShareFile Web UI. It contains everything you need to configure access for your users and set up your account.

To access the Content Collaboration Administrator UI from the Citrix Cloud console, select **My Services > Content Collaboration** from the Citrix Cloud menu.
Accessing the ShareFile Administrator UI Directly

There may be some ShareFile administrator settings that you are unable to access using the Citrix Cloud version of the console. If you need additional functionality, your ShareFile account can be accessed directly through the regular ShareFile login page. You can access the login page by going to https://YourSubdomain.sharefile.com.

Note:
This is not the recommended method for accessing the ShareFile Administrator UI in a Citrix Cloud environment.

User Access

There are three options on how users will access their data in ShareFile. Data can be accessed directly using the Web UI. The other two options depend on what other applications you have enabled. If you have Citrix Virtual Apps and Desktops or Endpoint Management enabled, users can access their data through one of those applications.

Accessing ShareFile through the Web UI

End users can access ShareFile directly by going to http://YourSubdomain.sharefile.com.

Accessing ShareFile with Citrix Virtual Apps and Desktops

Accessing ShareFile with Citrix Virtual Apps and Desktops will be done using Citrix Files for Windows. Citrix Files allows you to access your files in ShareFile directly through a mapped drive providing a native Windows Explorer experience.

Using Citrix Files for Windows

On Citrix Virtual Apps and Desktops you will be using Citrix Files for Windows. Citrix Files for Windows can be preinstalled on your desktop image before deploying to end users. You can install the app once and have it propagated to all of the Citrix Virtual Apps and Desktops sessions in your environment. For more information about using Citrix Files for Windows, see the following articles:

- Citrix Files on Citrix Virtual Apps and Desktops
-CTX228273: Install and use Citrix Files for Windows

Accessing ShareFile with Endpoint Management

For information on wrapping the ShareFile application and deploying Single Sign-On between Endpoint Management and ShareFile, see Citrix ShareFile for Endpoint Management.
Overview

ITSM Adapter is a Citrix Cloud service that provides an easy way to extend ServiceNow’s capabilities into your Citrix environments. Citrix Virtual Apps and Desktops allows organizations to be more flexible and end users to be more productive with anywhere, any device access. The ITSM Adapter service further provides workflows for IT teams to easily automate and manage their Citrix environments, allowing them to focus on strategic projects.

To ensure that ITSM Adapter can interact with ServiceNow, add one of the following IP addresses to the Allow list of your ServiceNow instance:

<table>
<thead>
<tr>
<th>ITSM Adapter region</th>
<th>IP address</th>
</tr>
</thead>
<tbody>
<tr>
<td>US</td>
<td>52.158.218.132/30</td>
</tr>
<tr>
<td>EU</td>
<td>20.54.214.12/30</td>
</tr>
<tr>
<td>Asia Pacific</td>
<td>20.195.2.68/30</td>
</tr>
</tbody>
</table>

What’s new

- April 2021: We have made an enhancement to automatically generate a refresh token and an access token when you register a ServiceNow instance in Citrix Cloud. This enhancement frees you from using a separate tool to generate the tokens. For more information, see Step 4: Register a ServiceNow instance with Citrix Cloud.

- April 2021: We have synchronized the Citrix alert policies that you set in the Citrix Virtual Apps and Desktops service to ServiceNow under Citrix IT Service Management Connector > Settings > Alert Policies. With the webhook monitor enabled for an alert policy, alerts meeting the policy are listed in ServiceNow under Citrix IT Service Management Connector > Alerts. You can also create incidents and assign them to specific assignees. To disable an alert policy in ServiceNow, click Disable Monitor. For more information, see Access Citrix alerts from within ServiceNow.

- November 2020: We have simplified the deployment of the ITSM Adapter service.

- November 2020: The ITSM Adapter service adds the Reporting dashboard for presenting request statistics.
- November 2020: The ITSM Adapter service adds the **Add users to Application Group(s)** tab for ServiceNow administrators to select when processing application access requests.

- November 2020: Access to a specific application can be limited to certain users in an Active Directory group. To facilitate the need, the ITSM Adapter service lists all Active Directory groups that can access a specific application on the **Add users to Active Directory Group(s)** tab. ServiceNow administrators can add a user to such an Active Directory group when processing application access requests.


- June 2020: The ITSM Adapter service implements the User Principal Name (UPN) to give Active Directory (AD) users an email address-like format to sign on with.

**How the ITSM Adapter service works**

The following diagram shows the ITSM Adapter service connecting ServiceNow and the Citrix Virtual Apps and Desktops environments.

The ITSM connector is a plug-in installed in ServiceNow. It enables communication between ServiceNow and Citrix Cloud. The ITSM Adapter service, hosted on Citrix Cloud, processes requests from ServiceNow. The requests are routed to Delivery Controllers, which provision and manage resources in both on-premises and cloud sites. To enable resource management for your on-premises Citrix Virtual Apps and Desktops sites, go to Citrix Cloud and add your on-premises sites through **site aggregation**. Before adding on-premises sites, ensure that **Citrix Gateway service** is available for your Citrix Cloud account. For users that already subscribe to the Citrix Virtual Apps and Desktops service, the service instance is automatically listed on the **Manage** tab of the ITSM Adapter service on Citrix Cloud. The ITSM Adapter service accesses your sites through the Citrix Cloud Connector.

**Roles and permissions**

**User**

- Requests apps and desktops
Citrix Cloud

- Resets sessions

**ServiceNow administrator**

- Downloads and installs the Citrix ITSM connector from the ServiceNow store.
- Provides the `x_cion_citrix_it_s.ctx_itsm_admin` role for users to configure the ITSM connector in ServiceNow.

**Citrix administrator**

- Uses the administrator functions in the ITSM connector to set up the connection between ServiceNow and Citrix Cloud.
- Adds on-premises Citrix Virtual Apps and Desktops sites through site aggregation.
- Provides full administrator privileges on user domains and Delivery Controllers of the Citrix Virtual Apps and Desktops sites.
- Provisions apps and desktops for users.
- Resets user sessions.

**Configuring ITSM Adapter for ServiceNow**

Configuring the ITSM Adapter service for ServiceNow involves the following three steps:

1. Subscribe to the Citrix Cloud service
2. Configure the ITSM Connector for ServiceNow
3. Add on-premises sites to Citrix Workspace through site aggregation
4. Register a ServiceNow instance with Citrix Cloud

**Step 1: Subscribe to the Citrix Cloud service**

Sign on to Citrix Cloud using your Citrix credentials or sign up for a new account. For more information about signing up for Citrix Cloud, see [Sign up for Citrix Cloud](#).
The ITSM Adapter service is hosted on Citrix Cloud. Click **Manage** to proceed.

**Tip:**

The **Manage** button is available after user accounts are assigned the entitlement. Before that, **Request Demo** shows.

**Step 2: Configure the Citrix ITSM connector for ServiceNow**

You must have a ServiceNow HI Portal account and be a ServiceNow administrator to perform the steps in this section.

1. Ensure that you have activated the ServiceNow Orchestration plug-in.
2. Download and install the Citrix ITSM connector from the ServiceNow store.
3. On the **Citrix IT Service Management Connector** pane, select **Home** and then click **Authenticate**. Type your Client ID and Secret (proxy credentials generated from the Citrix Cloud).
4. Test the connection.

5. Save the configuration. An acknowledgment from ServiceNow appears indicating that the connection is up and running.

**Step 3: Add on-premises sites to Citrix Workspace through site aggregation**

**Note:**
If you already subscribe to the Citrix Virtual Apps and Desktops service, the service instance is automatically listed on the Manage tab of the ITSM Adapter service on Citrix Cloud. Only on-premises sites require manual manipulation. You can add on-premises sites to Citrix Workspace through site aggregation.

1. Go to Citrix Cloud and access the ITSM Adapter service.
2. Click the blue Manage button. The Overview tab appears.

3. Click the Manage tab. The Manage tab presents the ServiceNow instances and the Citrix Virtual Apps and Desktops sites that are connected to the current Citrix Cloud account. If the on-premises site you want is not listed, add it through site aggregation.
For information on how to register a ServiceNow instance with Citrix Cloud, see Step 4: Register a ServiceNow instance with Citrix Cloud.

4. To access and modify a Citrix Virtual Apps and Desktops site, select **Manage Credentials** from the dots menu.

5. On the **Manage Credentials** page, provide the full administrator credentials for the site.

6. Click **Test** to check the connection.

   The site is now running and connected to the ITSM Adapter service.

7. Click **Save**.
Step 4: Register a ServiceNow instance with Citrix Cloud

This step is optional.

1. Click **Register ServiceNow Instance**.

2. Fill in the field values.

   ![Register ServiceNow Instance with Citrix Cloud](image)

   **Note:**
   When you create an OAuth endpoint for external clients to access your instance, set the Redirect URL field to the value prompted in the note message. In this example, `https://us-stage.itsm.cloudburrito.com`.

3. In the **Register a ServiceNow instance with Citrix Cloud** dialog, click **Connect**. The instance login page appears.
4. Type credentials for your ServiceNow instance and click **Log in**. A page appears, requesting a permission for the OAuth endpoint to connect to your ServiceNow account on the specified ServiceNow instance.

5. Click **Allow**.

6. Click **Register ServiceNow Instance** again. The refresh token and access token fields are automatically filled.
7. Click **Test** to verify that you have installed the ITSM connector successfully. The **Save** button is available after the test completes successfully.

8. Click **Save** to save the instance.

**Related actions and information**

- To enable or disable managing a Citrix Virtual Apps and Desktops service site, click the dots menu next to the service site and choose **Enable Integration** or **Disable Integration**, respectively.
- One site can use multiple Cloud Connectors to connect to Citrix Cloud.
- The ITSM Adapter service can connect to multiple ServiceNow instances.
An ITSM Connector can connect to only one ServiceNow instance.

Sample scenarios

Request for a desktop

User actions

1. Log in to your ServiceNow instance.
2. In the left pane, navigate to Citrix IT Service Management Connector and choose Services.
3. On the Citrix IT Service Management Connector Services page, click Citrix Virtual Apps and Desktops. The following services appear:
   - Provisioning applications
   - Request a desktop
   - Reset a session
4. Choose Request a desktop.
5. On the Request a desktop page, use the search tool in the Configuration area to look for available machine catalogs.
6. Select a target operating system. Click **Order Now**.

---

**Administrator actions**

The **Requests** page displays the list of requests by users.
1. Click the icon next to the request ID and then **Open Record**. The details of the request appear.

![Image of Open Record button](image.png)

2. Choose the machine catalog first and then the delivery group from the list.

3. Click **Update**.

The requested desktop is now provisioned and assigned to the user.

**Request for apps**

**User actions**

1. Log in to your ServiceNow instance.

2. On the left pane, navigate to **Citrix IT Service Management Connector** and choose **Services**.

3. On the Citrix IT Service Management Connector Services page, click **Citrix Virtual Apps and Desktops**. The following services appear:
   - Provision applications
   - Request a desktop
   - Reset a session

4. Choose **Provision applications**.

5. On the **Provision applications** page, available users and applications are listed. Choose users and the applications you want to assign to them. Click **Order Now**.
Administrator actions

1. The **Requests** page displays the list of requests by users. Click the icon next to the application request ID and then **Open Record**. The details of the request appear.

2. There are three options to complete app provisioning:
   - **Add users to Delivery Group(s)**: Click the lock icon to add users to a specific delivery group and then click **Update**.
   - **Add users to Application Group(s)**: Click the lock icon to add users to a specific application group and then click **Update**.
   - **Add users to Active Directory Group(s)**: Click the lock icon to add users to a specific Active
Directory group and then click **Update**.

The selected apps are now provisioned and assigned to the user.

**Reset a session**

**User actions**

1. Log in to your ServiceNow instance.
2. In the left pane, navigate to **Citrix IT Service Management Connector** and choose **Services**.
3. On the **Citrix IT Service Management Connector Services** page, click **Citrix Virtual Apps and Desktops**. The following services appear:
   - Provision applications
   - Request a desktop
   - Reset a session
4. Choose **Reset a session**.
5. On the **Reset a session** page, select a desktop or app session of the current user and click **Order Now** to log off from the session.

**Note:**

Regardless of whether provisioned by an administrator or a user, all applications running in the session are reset.
Access Citrix alerts from within ServiceNow

On the Monitor tab of the Citrix Virtual Apps and Desktops service, you can set alert policies to monitor the running status of your environment.

The alert policies are also available in ServiceNow under Citrix IT Service Management Connector > Settings > Alert Policies.

You can open an alert policy of your choice and click Enable Monitor. After that, alerts meeting the policy can be listed in ServiceNow under Citrix IT Service Management Connector > Alerts.
The following screen capture shows alerts presented in ServiceNow.

You can also create incidents and assign them to specific assignees for alert handling.
If the monitor is disabled, alerts meeting the specific policy are not synchronized to ServiceNow.

License Usage Insights Service

November 28, 2018

The License Usage Insights (LUI) Service in Citrix Cloud is a free cloud service that helps Citrix Service Providers (CSP) understand and report on product usage.

The LUI service makes it easy for Citrix Service Provider partners to understand which Citrix products are in use and at what capacity. Only CSP partners have access to the LUI service.

The License Usage Insights service enables you to:

- Automatically collect and aggregate product usage information from Citrix license servers
- 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 usage and ADC VPX allocations data to CSV

Technical Details

September 26, 2018

Before using the License Usage Insights (LUI) service, consider the following items:
Citrix Cloud

- Only Windows-based and VPX-based license servers are supported.
- It may take up to 24 hours for a newly updated license server to appear in the LUI service.
- When usage data is uploaded from a license server, it’s processed and stored in a secure fashion such that it can be accessed at a later date by the LUI service. This process might take up to 24 hours to complete.
- By default, usernames associated with Virtual Apps and Desktops license checkouts will be securely phoned home to Citrix.
- Usernames are phoned home so CSP partners can take full advantage of LUI 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.
- For partners sensitive to uploading username information, this functionality can be disabled on the Citrix License Server using the username anonymization feature.

Supported Citrix products

The License Usage Insights (LUI) service provides usage information for the following Citrix products:

- Virtual Apps and Desktops
- ADC VPX
- CloudPortal Services Manager (CPSM)

To use the LUI service with CloudPortal Services Manager, CPSM 11.5 Cumulative Update 4 must be installed in your deployment. This update includes Call Home features that enable the LUI service to display deployment status and license usage information. For more information, see CTX220717.

Get started with the License Usage Insights Service

April 27, 2021

Step 1: Update Citrix License Server

The Licensing Usage Insights Service requires Citrix License Server 11.16.3.0 or later. Before you start using the service, download the latest Citrix License Server software and upgrade your license servers. Upgrading in-place is simple and fast. For more information about the latest Citrix License Server, refer to the Citrix Licensing documentation.
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 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 with Citrix Cloud.

Step 4: 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 Use the License Usage Insights Service.

Use the License Usage Insights Service

December 5, 2018

Product selection

To view licensing details for a different product, click the arrow next to the product name and select the product you want to view.
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 the LUI service.

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, LUI displays the “Reporting” status and includes a timestamp of the most recent upload.
Usage collection

Usage collection helps you understand product usage through automated data collection and aggregation. There’s no need to deploy additional tools.

The service 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.

To create a customer breakdown of Virtual Apps and Desktops 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.

**Usage reporting for CloudPortal Services Manager**

For CloudPortal Services Manager (CPSM) usage, the LUI service includes the Services and Customers views.

The Services view is your primary view to understand the total CPSM license usage across all of your customers. License usage data is grouped by service, mapping directly to how you report CPSM licenses. When drilling down through a specific service, the total usage is broken down to clearly show which customers are contributing towards that usage.
The Customers view presents similar data as the Services view, but in a different format. This view helps you understand which services a specific customer is using or consuming. When you select a specific customer, you can dig deep into the CPSM services that customer is using.

**Free user management**

LUI 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.
**Note:**
Free users for CloudPortal Services Manager (CPSM) are only viewable in the LUI service. Managing free CPSM users occurs within the CPSM console.

**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.
**Export usage and allocations data**

You can export the following types of data as a CSV file from the LUI service:

- 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.
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**.

**Update and configure Citrix License Server**

May 26, 2021

The Citrix License Server is a critical component of the License Usage Insights (LUI) service. To use the LUI service, your Citrix License Servers must be updated to version 11.16.3.0 or later.

**About Citrix License Server**

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.

**Upgrade your Citrix License Servers to use the License Usage Insights service**

Complete the following tasks:

1. Download the latest license server.
2. Upgrade your current license server.
3. Repeat the upgrade process for each of your license servers.
4. Start using the LUI service.

**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 LUI 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.

For partners sensitive to uploading username information, username anonymization can be enabled. When active, username anonymization will convert readable usernames into unique strings using a secure and irreversible algorithm prior to upload.

The LUI service will use 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
   <?xml version="1.0" encoding="utf-8"?>
   <Configurations>
   ```
3. Save the file.

License server information included in uploads

When CSP home is activated on a Citrix License Server, it uploads the following information daily:

- Information about the license server: License server version
- Information about licenses on the license server:
  - License files installed on the server
  - License file expiration dates
  - Product feature and edition entitlement information
  - License quantities
- Information about 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.zip.

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.

Frequently Asked Questions

August 29, 2018
• **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 [Using the License Usage Insights Service](#).

• **Is the LUI service available to Citrix customers or partners that are not Citrix Service Providers?** No. The LUI service is only available to Citrix Service Provider partners with an active partner agreement.

• **Can I disable license server phone home?** No. Under the Citrix Service Provider license agreement, all Citrix 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 the LUI service?** No. The LUI service 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.

• **Which Citrix products does the LUI service support?** The LUI service currently supports the following Citrix products:
  - Virtual Apps and Desktops product usage.
  - Citrix ADC VPX allocations.
  - CloudPortal Services Manager Call Home. CPSM 11.5 Cumulative Update 4 is required to use the LUI service with your CPSM deployment. For more information, see [CTX220717](#).

• **How much does the License Usage Insights service cost?** The LUI service comes with Citrix Cloud, free of charge.

• **How do I get help with the License Usage Insights service?** Open a support ticket from within Citrix Cloud:
  1. Sign in to Citrix Cloud.
  2. Click the **Feedback and Support** icon near the top-right of the screen.
  3. Select **Open a ticket** and complete the form.
A member of Citrix Technical Support will follow up and assist you.

- **How do I provide feedback about the License Usage Insights service?** To give feedback about the LUI service:
  1. Sign in to Citrix Cloud.
  2. Click the **Feedback and Support** icon near the top-right of the screen.
  3. Select **Feedback & Suggestions**. The Citrix Cloud suggestions page opens in a separate browser tab or window.
  4. In **Tell us about your suggestion**, start typing a title for your feedback. As you type, additional fields appear so you can provide more details.
  5. Click **Post idea**. Your feedback appears on the Citrix Cloud suggestions page where others, including the Citrix Cloud team, can read it, comment on it, and vote for it.

**MDX Service**

April 23, 2021

You can use the MDX Service to prepare iOS and Android mobile apps by wrapping the apps with MDX, an app container technology. The MDX Service is used to wrap apps created within your organization. You can then manage the apps with Citrix Endpoint Management.

The MDX Service can use MDX version 20.10.5 for wrapping third-party apps.
Announcements

- **WKWebView Issues and Citrix SSO**

  Citrix started supporting WKWebView for mobile productivity apps as of version 20.11.x, after Apple ended support for apps using UIWebView. WKWebView is an Apple framework that replaced the previously used UIWebView framework. Due to technical limitations and the complexities of WKWebView, some tunneling issues may occur with some websites.

  Citrix may be able to provide analysis and suggest modifications to the way you render your website on a best-effort basis. Ultimately, however, if you are experiencing issues, we recommend that you use the Citrix SSO app for VPN tunneling.

  For details about Citrix SSO, see [Citrix Gateway clients](#).

- A Mobile Application Management (MAM) SDK is available to replace areas of MDX functionality that aren’t covered by iOS and Android platforms. For more details about the MAM SDK (Preview), see the Citrix Developer section on [Device Management](#). You can find more information as well in this [Citrix blog post](#).

  The SDK is available for download when you sign on to [Citrix downloads](#).

- The MDX wrapping technology is scheduled to reach end of life (EOL) in September 2021. To continue managing your enterprise applications, you must incorporate the MAM SDK.

  For more details about wrapping iOS apps, see [To wrap an iOS app](#)

  For more details about wrapping Android apps, see [To wrap an Android app](#)

  For information about MDX, the traditional MDX wrapping process using the MDX Toolkit, and a description of signing required assets, see:

    - [About the MDX Toolkit](#)
    - Wrapping iOS mobile apps
    - Wrapping Android mobile apps

Data retention policy

The data retention policy for the MDX Service is as follows:

- **App binaries (IPA and APK files)**: 90 days.
- **Wrapped app (MDX files)**: 90 days (available for downloads).
- **Certificate and keystore files**: Deleted immediately after wrapping.
- **iOS mobile provisioning profile**: Deleted immediately after wrapping.
**Getting started with the MDX Service**

Follow these steps to start using the MDX Service. To provide feedback on your experience, use your Citrix ID to join the [MDX Service discussion forum](#).

1. Sign up for Citrix Cloud by requesting a trial if you do not already have a Citrix Cloud account. For details on signing up, see [Sign up for Citrix Cloud](#).
2. Click on the hamburger menu on the upper-right corner of the page and then click **Library**.
3. On the upper-right of this page is a blue circle with a plus (+) in it. Mouse over that icon and then click **Wrap a Mobile App**

   ![Library](#)

**To use the MDX Service**

To use the MDX Service, upload the application package binary and the required signing assets. Then, verify the app details and modify the attributes, as necessary. You can then download the wrapped application package.

To start, on the MDX Service Overview page, at the bottom of the screen, click **Start**.
Then, follow the steps for wrapping either an iOS or an Android app.

**To wrap an iOS app**

1. Upload the .ipa file for the app. The time required for the upload to complete depends on the file size. The allowed file size limit for the .ipa file is 209 MB. If you have an app that is over this limit, then use the MDX Toolkit.
2. On the **Verify App Details** screen, enter the following information:

   a) (Optional) Change the **App Name**, **Minimum OS Version**, and **Maximum OS Version**.

   b) Enter a **Description** (required).

   c) Select an MDX SDK version with which to wrap the app.

   d) Upload the following iOS signing assets:

      - **Provisioning Profile**
      - **Certificate**
      - **Certificate Password**

      To collect the iOS provisioning profile and certificate information, see the “MDX Service or MDX Toolkit” section in the Endpoint Management Certificates article on [Endpoint Management Certificate Administration](#).

      After the MDX Service uses the signing assets to modify the app, the **Create Mobile App** screen appears.
3. (Optional) On the **Create Mobile App** screen, change the bundle ID of the mobile app, and then click **Next**. The wrapping process begins.

4. After the wrapping process finishes, download the wrapped MDX application package (`.mdx` file).

   You can also download the file later from the **Jobs** tab.
To wrap an Android app

1. Upload the .apk file for the app. The time required for the upload to complete depends on the file size. The allowed file size limit for the .ipa file is 209 MB. If you have an app that is over this limit, then use the MDX Toolkit.

![Wrap a Mobile App](image1.png)

2. After the .apk file is uploaded to the MDX Service and is processed successfully, the Verify App Details screen appears.

![Verify App Details](image2.png)

3. On the Verify App Details screen, enter the following information:
   a) (Optional) Change the App Name, Minimum OS Version, and Maximum OS Version.
   b) Enter a Description (required).
   c) Select an MDX SDK Version with which to wrap the app.

4. On the Create Mobile App screen, upload the following Android signing assets:
   - Keystore
   - Keystore Password
   - Alias Name
   - Alias Password
To collect the Keystore and Alias Name information, follow the steps in CTX220480.

5. Click **Next** to begin the wrapping process.

6. Download the wrapped MDX application package (.mdx file).

You can also download the file later from the **Jobs** tab.
Known Issues

Known issues in MDX Service 20.10.5

- You can’t wrap iOS apps developed on macOS 10.14 and later using the MDX Service. To add iOS apps with MAM SDK or MDX functionality, prepare the app with the MAM SDK or wrap the apps using the on-premises MDX Toolkit. [CXM-90666]

Secure Browser service

May 26, 2021

The Citrix Secure Browser Service isolates web browsing to protect the corporate network from browser-based attacks. It delivers consistent, secure remote access to internet hosted web applications, with no need for user device configuration. Administrators can rapidly roll out secure browsers, providing instant time-to-value. By isolating internet browsing, IT administrators can offer end users safe internet access without compromising enterprise security.

Users log on through Citrix Workspace (or Citrix Receiver) and can open web apps in the configured web browser. The website does not directly transfer any browsing data to or from the user device, so the experience is secure.

The Secure Browser service can publish secure browsers for use with:

- **Shared Passcode external web apps.** If you publish a browser with shared passcode authentication, users must enter the passcode to launch an app.

- **Authenticated external web apps.** When you publish authenticated external web apps and launch the apps using Citrix Workspace, the Secure Browser service requires a resource location containing at least one Cloud Connector (two or more are recommended). For details, see Citrix Cloud Connector. For authenticated apps, you must add users with Citrix Cloud Library.

- **Unauthenticated external web apps.** When you publish unauthenticated external web apps and launch the apps using Citrix Workspace, the Secure Browser service requires a resource location containing at least one Cloud Connector (two or more are recommended). For details, see Citrix Cloud Connector.

  Although typically not recommended, unauthenticated external web apps might be used for a simple proof of concept.

For more information, see Publish a secure browser.

The service also offers:

- Integration of published apps with Citrix Workspace
• Integration of published apps with on-premises StoreFront
• Simple URL allow list function for security
• Usage monitoring
• Controls for clipboard use, printing, kiosk mode, region failover, and client drive mapping

What’s new

• March 2021:
  – **Secure Browser supports authentication with Azure Active Directory.** Users can now sign in to Secure Browser apps from Citrix Workspace using Azure Active Directory credentials. For more information, see Integration with Citrix Workspace.
  – **Secure Browser lets you monitor and log off users’ active sessions.** Secure Browser provides user name, session ID, client IP, authentication type, application name, session start time, and session duration information about users' active sessions. You can view basic information about each active session and disconnect the session if needed. For more information, see Monitor active sessions.
• Releases in 2020: All releases of 2020 contain enhancements that help improve overall performance and stability.

Get started

Here's a video about getting started with Secure Browser.
1. Sign in to Citrix Cloud. If you don’t have an account, see Sign up for Citrix Cloud. You can request a 30-day trial of the Citrix Secure Browser Service.

2. In the **Secure Browser Service** tile, click **Request Trial**.

3. In a few moments, you’ll receive an email (the email associated with your Citrix Cloud account). Click the **Sign-in** link in the email.

4. After you’re in Citrix Cloud again, click **Manage** on the **Secure Browser Service** tile.
5. On the **Welcome to Secure Browser** page, click **Let’s Get Started**. You’re guided to publish your first secure browser.


**Integration with Citrix Workspace**

Secure Browser can be integrated with Citrix Workspace. To ensure that it’s integrated:

1. Sign in to **Citrix Cloud**.
2. In the upper left menu, select **Workspace Configuration**.
3. Select the **Service Integrations** tab.
4. The Secure Browser service entry indicates **Enabled**. If it does not, click the ellipsis menu and select **Enable**.
Citrix Cloud

You can authenticate using Active Directory or Azure Active Directory. If you choose Azure Active Directory, the on-premises domain containing your Active Directory Domain Controllers must contain one (preferably two) Cloud Connectors. For more information, see:

- Change authentication to workspaces
- Connect Azure Active Directory to Citrix Cloud

Integrate with your on-premises StoreFront

Citrix Virtual Apps and Desktops customers with an on-premises StoreFront can easily integrate with the Secure Browser Service to provide the following benefits:

- Aggregate your published secure browsers with your existing Citrix Virtual Apps and Desktops apps for a unified store experience.
- Use native Citrix Receivers for enhanced end user experience.
- Strengthen security for Secure Browser launches by using your existing multifactor authentication solution integrated with your StoreFront.

For details, see CTX230272 and the StoreFront configuration documentation.

Publish a secure browser

1. If you’re not already in Citrix Cloud, sign in. In the Secure Browser Service tile, click Manage.

2. On the Manage tab, click Publish a Secure Browser.

3. Select the type of secure browser to publish: shared passcode, authenticated, or unauthenticated. Then click Continue.
By default, users must launch apps with shared passcode authentication using launch.cloud.com. Citrix Workspace and the Citrix Cloud Library do not support apps with shared passcode.

To use Citrix Workspace, you must publish authenticated apps and explicitly assign subscribers (users) or groups in the Citrix Cloud Library. The unauthenticated apps are available to all Workspace subscribers without user assignment.

4. Configure these settings:

- **Name:** Type a name for the app you are creating.
- **Start URL:** Specify the URL that opens when users start an app.
- **Region:** Choose the location/region for the server. Available regions are West US, East US, Southeast Asia, Australia East, and West Europe.
  
  If you select **Auto**, your Secure Browser connects you to the closest region based on your geolocation.

- **Passcode:** If you selected a browser with shared passcode authentication, enter the passcode to provide an enhanced secure access to your app. The passcode must be at least 8 alphanumeric characters long. Ensure that you save the passcode and share it with the users. Users must enter the passcode when they launch an app using launch.cloud.com.
• **Icon:** By default, the icon of the Google Chrome executable is used when you publish a Secure Browser. You can now choose your own icon to represent a published browser.

  Click **Change icon > Select icon** to upload the icon of your choice, or choose **Use default icon** to use the existing Google Chrome icon.

  5. When you are done, click **Publish.** When the publishing completes, the **Manage tab** lists the browser you published.

  • If you published the authenticated secure browser, you must use the Citrix Cloud Library to add users or groups. Click the right arrow at the end of the row to expand the details pane containing a link to the Library.

    ![Manage published secure browsers](image)

    When you click the link provided, you are guided to the Library display containing your secure browser. Click the ellipsis on the tile containing the secure browser and click **Manage Subscribers.** For information about adding subscribers, see **Assigning users and groups to service offerings using Library.**

    **Manage published secure browsers**

    The **Manage** tab lists the published secure browsers. To access management tasks, click the ellipsis at the end of an entry’s row, and then select the task.

    ![Manage published secure browsers](image)

    If you select a menu entry, and then decide not to change anything, cancel the selection by clicking the **X** outside the dialog box.
Time-outs

Time-out settings include:

- **Idle Timeout**: The number of minutes a session can remain idle before it is ended due to inactivity.
- **Idle Warning Time**: The number of minutes before ending a session that a warning message is sent to the user.

Setting an idle timeout of 20 and an idle warning time of 5 displays a message if there is no activity in the session for 15 minutes (20 minus 5). If the user does not respond, the session ends five minutes later.

When you’re done, click **OK**.
Settings on the policies page control the following:

- **Clipboard**: Enabling the Clipboard policy allows copy and paste operations to and from the remote session. (The Clipboard button is removed from the Citrix Workspace app toolbar.) By default, this setting is disabled.

- **Printing**: Enabling printing saves the remote webpage as a PDF and transfers it to the user’s device. The user can then press Ctrl-P and select the Citrix PDF printer. By default, this setting is disabled.

- **Non-kiosk**: Enabling non-kiosk mode restores the interface to the remote browser. The user can then access the address bar and create multiple tabs and windows. (Disabling non-kiosk
mode removes the remote browser’s navigation controls and address bar.) By default, this setting is enabled (non-kiosk mode is on).

- **Region failover:** The Region failover policy automatically transfers your published browser to a different region if your current region is reporting an issue. To opt out, disable the Region failover policy. If you published the browser using the **Auto** region selection, your secure browser remains enrolled in the policy. By default, this setting is enabled.

- **Client drive mapping:** Enabling the Client drive mapping policy allows the user to upload and download files to and from the remote session. This feature is available only for sessions launched with the Citrix Workspace app. By default, this setting is disabled.
  - Users must save downloaded files only on the `ctxmnt` disk in the `Anonxxx` directory. To do that, users must navigate to the desired location for storing the file. For example, `Anonxxx > ctxmnt > C > Users > User Name > Documents`.
  - The dialog box might prompt the user to accept the **Permit all access** or **Read and Write** permissions to access the `ctxmnt` folder.

- **URL parameters:** Enabling URL parameters allows you to change a new session’s starting URL when users launch an app. For this policy to take effect, configure a local proxy server to identify suspicious websites and redirect them to Secure Browser. By default, this setting is disabled. For more information, see [Proof of Concept Guide: URL Redirection to Secure Browser with Citrix ADC in Azure](#).
- **Hostname tracking:** Use host name tracking to enable Secure Browser to log host names during a user's session. This policy is disabled by default. This information is shared with Citrix Analytics. For more information, see [Citrix Analytics](#).

When you’re done, click **OK**.

### Allow lists

Use the **Whitelists** task to restrict users to visiting only allowed URLs within their published Secure Browser session. This feature is available for external authenticated web apps.

Enter allow list entries in the form `hostname:port number`. Specify each entry on a new line. Asterisks are supported as wildcards. Browser requests must match at least one entry in the allow list.

For example, to set `https://example.com` as an allowed URL:

- `example.com:*` allows connection to this URL from any port.
- `example.com:80` allows connection to this URL only from port 80.
- `*:80` allows access to this URL from any port and from any links to other URLs and ports. The `*.*` format allows access to all external web apps from the published app. This format is the default setting for the web apps **External Whitelist** field.

When you’re done, click **OK**.

Advanced web filtering capabilities are available through integration with the Access Control service. Learn more at **Use case: Selective access to apps.**

© 1999-2021 Citrix Systems, Inc. All rights reserved.
You can configure URL filtering to control access methods based on pre-defined categories associated with risk models. URL filtering options include:

- **None** - Allows all categories.
- **Lenient** - Maximizes access while still controlling risk from illegal and malicious websites. Includes the following categories:
  - **Adult**: Grotesque, sex education, porn, nudity, sexual services, adult search and links, swimsuits and lingerie, adult magazines and news, sexual expression (text), fetish, and dating.
  - **Computing and Internet**: remote proxies, private IP addresses, peer-to-peer file sharing, and torrents.
  - **Gambling**: Sweepstakes, prizes, lotteries, and gambling in general.
  - **Illegal and harmful**: Terrorism, extremism, hate, slander, weapons, violence, suicide, illegal drugs, medication, illegal activities, marijuana, and advocacy in general.
  - **Malware and spam**: Hacking, malware, spam, spyware, botnets, infected sites, phishing sites, keyloggers, mobile malware, phone bots, malicious and dangerous websites.
Citrix Cloud

- **Moderate** - Minimizes risk while allowing more categories with low probability of exposure from unsecure or malicious sites. Includes the following categories:
  - **Adult**: Grotesque, sex education, porn, nudity, sexual services, adult search and links, swimsuits and lingerie, adult magazines and news, sexual expression (text), fetish, and dating.
  - **Business and industry**: Auctions.
  - **Computing and Internet**: Advertisements, banners, remote proxies, private IP addresses, peer-to-peer file sharing, and torrents.
  - **Downloads**: Mobile app stores, storage services, downloads, and program downloads.
  - **Email**: Web-based mail and email subscriptions.
  - **Finance**: Cryptocurrency.
  - **Gambling**: Sweepstakes, prizes, lotteries, and gambling in general.
  - **Malware and spam**: Hacking, malware, spam, spyware, botnets, infected sites, phishing sites, keyloggers, mobile malware, phone bots, malicious and dangerous websites.
  - **Messaging, chat, and telephony**: Instant messages and web-based chat.
  - **News, entertainment, and society**: Wordpress (posts and uploads), unsupported URLs, occult, no content, miscellaneous, horoscope, astrology, fortune telling, drinking, religions, personal webpages, blogs, and online games.
  - **Social networking**: Photo search and sharing sites, IT bulletin boards, and bulletin boards.

- **Strict** - Minimizes the risk of accessing unsecured or malicious websites. End users can still access websites with low risk. Includes the following categories:
  - **Adult**: Grotesque, sex education, porn, nudity, sexual services, adult search and links, swimsuits and lingerie, adult magazines and news, sexual expression (text), fetish, and dating.
  - **Business and industry**: Auctions.
  - **Computing and Internet**: Advertisements, banners, dynamic DNS, mobile apps, publishers, parked domains, remote proxies, private IP addresses, peer-to-peer file sharing, and torrents.
  - **Downloads**: Mobile app stores, storage services, downloads, and program downloads.
  - **Email**: Web-based mail and email subscriptions.
  - **Finance**: Cryptocurrency and financial products.
  - **Gambling**: Sweepstakes, prizes, lotteries, and gambling in general.
  - **Illegal and harmful**: Terrorism, extremism, hate, slander, weapons, violence, suicide, illegal drugs, medication, illegal activities, marijuana, and advocacy in general.
  - **Jobs and resumes**: Employment, career advancement, and LinkedIn (updates, mail, connections, and jobs).
  - **Malware and spam**: Hacking, malware, spam, spyware, botnets, infected sites, phishing sites, keyloggers, mobile malware, phone bots, malicious and dangerous websites.
- **Messaging, chat, and telephony**: Instant messages and web-based chat.
- **News, entertainment, and society**: Wordpress (posts and uploads), accommodations, travel and tourism, unsupported URLs, politics, fashion and beauty, arts and cultural events, reference, recreation and hobbies, local communities, miscellaneous, drinking, popular topics, special events, news, society and culture, online magazines, online games, life events, occult, no content, horoscope, astrology, fortune telling, celebrity, streaming media, entertainment, venues, activities, personal webpages and blogs, and religions.
- **Social networking**: Social networks in general, YikYak (posts), Twitter (posts, mail, and follows), Vine (uploads, comments, and messages), Google+ (photo and video uploads, posts, video chat, and comments), Instagram (uploads and comments), YouTube (shares and comments), Facebook (groups, games, questions, video upload, photo uploads, events, chat, apps, posts, comments, and friends), Tumblr (posts, comments, photo, and video uploads), Pinterest (pins and comments), IT bulletin boards, and bulletin boards.

When you’re done, click **Ok**.

**Edit**

Use the **Edit** task to change the name, start URL, region of a published browser, or the passcode. When you’re done, click **Publish**.

**Delete**

Use the **Delete** task to remove a published secure browser. When you select this task, you’re prompted to confirm the deletion.
The **Monitor** tab provides information about users’ real-time sessions. You can monitor and disconnect one or several active sessions.

To stop a single session, select the session and click the ellipsis menu at the end of an entry’s row. Click **Log off session** and confirm your changes.

To disconnect multiple sessions, select the active sessions in the list and click the **Log off** button on the top of the page. After you confirm your changes, Secure Browser immediately disconnects all selected sessions.

The **Usage** tab shows the:

- Number of initiated sessions
- Number of hours used

To create a spreadsheet containing usage details, click **Export to CSV** and select a timeframe.
Technical security overview

Secure Browser Service is a SaaS product managed and operated by Citrix. It allows access to web applications via an intermediate web browser hosted in the cloud.

Cloud service

The Citrix Secure Browser Service consists of web browsers running on Virtual Delivery Agents (VDAs) along with the management console used to manage and connect users to these VDAs. Citrix Cloud manages the operation of these components, including the security and patching of operating systems, web browsers, and Citrix components.

While using Secure Browser service, hosted web browsers track user’s browsing history and perform caching of HTTP requests. Citrix uses mandatory profiles and ensures that this data is deleted when the browsing session ends.

Secure Browser service is accessed with an HTML5-compatible web browser. The service does not provide any downloadable clients. All traffic between the browser being used and cloud service is encrypted using industry-standard TLS encryption. Secure Browser supports TLS 1.2 only.

Egress traffic for Secure Browser uses specific IP addresses to protect the internal network. For the list of accepted IP addresses, see Knowledge Center article CTX286379.

Web applications

Citrix Secure Browser Service is used to deliver web applications owned by the customer or a third party. The owner of the web application is responsible for its security, including patching the web server and application against vulnerabilities.

Security of the traffic between Secure Browser and the web application depends on the encryption settings of the web server. To protect this traffic as it flows over the Internet, administrators publish HTTPS URLs.

More information

See the following resources for more security information:

- Citrix Security site: https://www.citrix.com/security
- Citrix Cloud documentation: Secure Deployment Guide for the Citrix Cloud Platform

Additional resources

For developers: Preview API for Secure Browser Service
Citrix Virtual Apps Essentials

May 26, 2021

Citrix Virtual Apps Essentials allows you to deliver Windows applications and shared hosted desktops from Microsoft Azure to any user on any device. The service combines the industry-leading Citrix Virtual Apps service with the power and flexibility of Microsoft Azure. You can also use Virtual Apps Essentials to publish Windows Server desktops.

Server OS machines run multiple sessions from a single machine to deliver multiple applications and desktops to multiple, simultaneously connected users. Each user requires a single session from which they can run all their hosted applications.

The service is delivered through Citrix Cloud and helps you to deploy your application workloads within your Azure subscription with ease. When users open applications from the workspace experience, the application appears to run locally on the user computer. Users can access their apps securely from any device, anywhere.

Virtual Apps Essentials includes the workspace experience and the Citrix Gateway service, in addition to its core management services. Your app workloads run in your Azure subscription.

Deployment architecture

The following diagram shows an architectural overview of a basic Virtual Apps Essentials cloud deployment:
You can also allow users to connect to your on-premises data center. Connections between the Azure cloud and your on-premises data center occur through a VPN connection. Users connect through Virtual Apps Essentials to your license server, file servers, or Active Directory over the VPN connection.
Deployment summary

Follow these steps to deploy Citrix Virtual Apps Essentials:

- Buy Citrix Virtual Apps Essentials from the Azure Marketplace.
- Prepare and link your Azure subscription.
- Create and upload your master image.
- Deploy a catalog, publish apps and desktops, and assign subscribers

What’s new

- December 2018: Cloud-hosted StoreFront removed

Cloud-hosted StoreFront is no longer available for use with Virtual Desktops Essentials. Customers who purchased Virtual Desktops Essentials (formerly XenDesktop Essentials) before December 2017 can use Citrix Workspace as described in this article to provide subscriber access to desktops.

- August 2018: New product names

If you’ve been a Citrix customer or partner for a while, you’ll notice new names in our products and product documentation. If you’re new to this Citrix product, you might see different names for a product or component.

The new product and component names stem from the expanding Citrix portfolio and cloud strategy. This article uses the following names.

- Citrix Virtual Apps Essentials: XenApp is part of our workspace strategy, where many types of apps come together in the preferred place to access work tools. As part of a unified, contextual, secure workspace, XenApp Essentials is now Citrix Virtual Apps Essentials.

- Citrix Workspace app: The Citrix Workspace app incorporates existing Citrix Receiver technology as well as the other Citrix Workspace client technologies. It has been enhanced to deliver more capabilities to provide end users with a unified, contextual experience where they can interact with all the work apps, files, and devices they need to do their best work.

- Citrix Gateway: The NetScaler Unified Gateway, which allows secure, contextual access to the apps and data you need to do your best work, is now Citrix Gateway.

In-product content might still contain former names. For example, you might see instances of earlier names in console text, messages, and directory/file names. It is possible that some items (such as commands and MSIs) might continue to retain their former names to prevent breaking existing customer scripts.

Related product documentation, other resources (such as videos and blog posts), and other sites (such as Azure Marketplace) might still contain former names. Your patience during this
transition is appreciated. For more detail about our new names, see https://www.citrix.com/about/citrix-product-guide/.

- May 2018: **Building additional images from the Virtual Apps Essentials interface**

  After creating a production image from the Azure Resource Manager interface, you can create additional images through Azure, as needed. Now, as an optional alternative to creating additional images through the Azure interface, you can build a new master image from the Virtual Apps Essentials interface. For details, see Prepare and upload a master image.

- May 2018: **Monitor display enhancements**

  The Monitor display now includes usage information about applications and top users. For details, see Monitor the service.

**System requirements**

**Microsoft Azure**

Citrix Virtual Apps Essentials supports configuring machines only through Azure Resource Manager. Use Azure Resource Manager to:

- Deploy resources such as virtual machines (VMs), storage accounts, and a virtual network.
- Create and manage the resource group (a container for resources that you want to manage as a group).

To provision and deploy resources in Microsoft Azure, you need:

- An Azure account.
- An Azure Resource Manager subscription.
- An Azure Active Directory global administrator account in the directory associated with your subscription. The user account must have Owner permission for the Azure subscription to use for provisioning resources. For more information about how to set up an Azure Active Directory tenant, see How to get an Azure Active Directory tenant.

**Citrix Cloud**

Virtual Apps Essentials is delivered through the Citrix Cloud and requires a Citrix Cloud account to complete the onboarding process. You can create a Citrix Cloud account on the Citrix Cloud Sign Up page before going to Azure Marketplace to complete the transaction.

The Citrix Cloud account you use cannot be affiliated with an existing Citrix Virtual Apps and Desktops service or Citrix Virtual Desktops Essentials service account.
Virtual Apps Essentials console

You can open the Virtual Apps Essentials administration console in the following web browsers:

- Google Chrome
- Internet Explorer

Known issues

Virtual Apps Essentials has the following known issues:

- On Windows Server 2019 VDAs, some application icons might not appear correctly during configuration and in the users’ workspace. As a workaround, after the app is published, use the Change icon feature to assign a different icon that displays correctly.
- If you use Azure AD Domain Services: Workspace logon UPNs must contain the domain name that was specified when enabling Azure AD Domain Services. Logons cannot use UPNs for a custom domain you create, even if that custom domain is designated as primary.
- When you configure users for a catalog and select a domain, you can see and choose the users from the Builtin\users group.
- Creating the catalog fails if the virtual machine size is not available for the selected region. To check the virtual machines that are available in your area, see the chart at Products available by region on the Microsoft website.
- You cannot create and publish multiple instances of the same app from the Start menu at the same time. For example, from the Start menu you publish Internet Explorer. Then, you want to publish a second instance of Internet Explorer that opens a specific website on startup. To do so, publish the second app by using the path for the app instead of the Start menu.
- Virtual Apps Essentials supports linking a subscription by using an Azure Active Directory user account. Virtual Apps Essentials does not support Live.com authenticated accounts.
- Users cannot start an application if there is an existing Remote Desktop Protocol (RDP) session on the VDA. This behavior only happens if the RDP session starts when no other users are logged on to the VDA.
- You cannot enter a license server address longer than server.domain.subdomain.
- If you perform multiple sequential updates to capacity management, there is a possibility that the updated settings do not properly propagate to the VDAs.
- If you use a non-English web browser, the text appears as a combination of English and the browser language.

How to buy the service

Note:

The information in this section is also available as a PDF. That content contains earlier product
Buy Citrix Virtual Apps Essentials directly from the Azure Marketplace, using your Microsoft Azure account. Citrix Virtual Apps Essentials requires at least 25 users.

The service is delivered through Citrix Cloud and requires a Citrix Cloud account to complete the onboarding process. See System requirements > Citrix Cloud for details.

When buying Citrix Virtual Apps Essentials, ensure that you enter correct information for all details, including address fields, to ensure fast processing of your order. Before you configure Virtual Apps Essentials, ensure that you complete the following in the Azure Marketplace:

- Provide contact information and your company details.
- Provide your billing information.
- Create your subscription.

To configure the customer and pricing:

1. In Select a customer, select the customer name.
2. Under Pricing, in Number of users, type the number of users who have access to Virtual Apps Essentials.
3. Under Price per month, select the agreement check box and then click Create.

The summary page appears and shows the details of the resource.

After your account is provisioned, click Manage through Citrix Cloud.

**Important:**
Wait for Microsoft Azure to provision your service. Do not click the Manage through Citrix Cloud link until provisioning is complete. This process can take up to four hours.

When you click the link, Citrix Cloud opens in the web browser, and you can begin the configuration process described below.

**Prepare your Azure subscription**

Choose your Azure subscription to be the host connection for your VDAs and related resources. These resources can incur charges based on your consumption.

**Note:**
This service requires you to log on with an Azure Active Directory account. Virtual Apps Essentials does not support other account types, such as live.com.

To prepare your Azure subscription, configure the following in Azure Resource Manager:

1. Create a resource group and provide:
   - Resource group name
2. In Azure Resource Manager, create a virtual network in the resource group and provide a name for the network. You can leave all other default settings. You create a storage account when you create the master image.

3. Use an existing domain controller or create one. If you create a domain controller:
   
a) Use the A3 Standard or any other size Windows Server 2012 R2 virtual machine in the Resource Group and virtual network. This virtual machine becomes the domain controller. If you plan to create multiple domain controllers, create an availability set and put all the domain controllers in this set.
   
b) Assign a private static IP address to the network adapter of the virtual machine. You can assign the address in the Azure portal. For more information, see Configure private IP addresses for a virtual machine using the Azure portal on the Microsoft documentation website.
   
c) [Optional] Attach a new data disk to the virtual machine to store the Active Directory users and Groups and any Active Directory logs. For more information, see Attach a managed data disk to a Windows VM by using the Azure portal. When you attach the disk, select all the default options to complete the settings.
   
d) Add the domain controller virtual machine’s private IP address to the virtual network DNS server. For more information, see Manage DNS servers used by a virtual network (Classic) using the Azure portal (Classic).
   
e) Add a public DNS server in addition to the Microsoft DNS server. Use the IP address 168.63.129.16 for the second DNS server.
   
f) Add the Active Directory Domain Services role to the domain controller virtual machine. When this step is complete, promote the domain controller virtual machine to a domain controller and DNS.
   
g) Create a forest and add some Active Directory users. For more information, see Install a new Active Directory forest on an Azure virtual network.

If you prefer to use Azure Active Directory Domain Services instead of a domain controller, Citrix recommends reviewing the documentation Azure Active Directory Domain Services for Beginners on the Microsoft website.

**Link Your Azure subscription**

In Citrix Cloud, link your Citrix Virtual Apps Essentials to your Azure subscription.

1. Sign in to **Citrix Cloud**. In the upper left menu, select **My Services > Virtual Apps and Desktops**.
2. On the **Manage** tab, click **Azure Subscriptions**.
3. Click **Add Subscription**. The Azure portal opens.
4. Log on to your Azure subscription with your global administrator Azure credentials.
5. Click Accept to allow Virtual Apps Essentials to access your Azure account. The subscriptions available in your account are listed.
6. Select the subscription you want to use and then click Link.
7. Return to the Virtual Apps Essentials console to see the subscription in a linked state.

After you link your Azure subscription to Virtual Apps Essentials, upload your master image.

**Prepare and upload a master image**

Catalog creation uses a master image to deploy VMs containing applications and desktops. This can be a master image you prepare (with applications and VDA installed), or an image prepared by Citrix. For production deployments, Citrix recommends preparing and using your own master image. Citrix-prepared images are intended only for pilot or test deployments.

The first production image must be prepared from the Azure Resource Manager interface. Later, you can create additional images through Azure, as needed.

As an alternative to creating additional images through the Azure interface, you can build a new master image from the Virtual Apps Essentials interface.

- This method uses a previously created master image. You can obtain the network settings from an existing catalog or manually specify them.
- After you use an existing master image to create a new image, you connect to the new image and customize it, adding or removing apps that were copied from the template. The VDA is already installed, so you don’t have to do that again.
- This method lets you stay with the Essentials service. You don’t need to navigate to Azure to create the new image, and then return to the Essentials service to import the image.

For example, let’s say you have a catalog named HR that uses a master image containing several HR apps. Recently, a new app released that you want to make available to the HR catalog users. Using the build-an-image feature in Virtual Apps Essentials, you select the current master image as a template to create a new master image. You also select the HR catalog so that the new master image uses the same network connection settings. After the initial image setup, install the new app on the new image. After testing, update the HR catalog with the new master image, making it available to that catalog’s users. The original HR master image is retained in the My Images list, in case it’s ever needed again.

The following sections describe how to prepare and upload a master image through the Azure interface. For details about building an image from within Virtual Apps Essentials, see Prepare a master image in Virtual Apps Essentials.
**Procedure summary**

1. Prepare a master image VM in Azure or Virtual Apps Essentials.
2. Install apps on the master image.
3. Install a Citrix VDA on the master image.
4. Upload the master image from Azure Resource Manager to Virtual Apps Essentials (if needed).

Citrix recommends installing the latest Current Release (CR) of the server VDA or the latest Cumulative Update (CU) for Server VDA 7.15 Long Term Service Release (LTSR) on Windows Server 2016 or Windows Server 2012 R2 machines. If you have a Windows Server 2008 R2 machine, you must install server VDA 7.15 LTSR (latest CU recommended), which is also available on the download page. See Lifecycle Policy for Citrix Cloud Virtual Apps and Desktops Service to learn about the lifecycle policy for CR and LTSR VDAs.

**Create a master image VM in Azure**

1. Sign in to the Azure portal.
2. Click Create a Resource in the navigation pane. Select or search for a Windows Server 2008 R2, Windows Server 2012 R2, or Windows Server 2016 entry. Click Create.
3. On the Create virtual machine page, in panel 1 Basics:
   a) Enter a name for the VM.
   b) Select a VM disk type (optional). Create a standard disk.
   c) Enter the local user name and password, and confirm the password.
   d) Select your subscription.
   e) Create a new resource group or select an existing resource group.
   f) Select the location.
   g) Select the resource group and location.
   h) Choose whether you will use a Windows license that you already own.
i) Click **OK**.

4. On the **Create virtual machine** page, in panel 2 Size, choose the virtual machine size:
   a) Select a VM type, then indicate the minimum number of vCPUs and minimum memory. The recommended choices are displayed. You can also display all choices.
   b) Choose a size and then click **Select**.
5. On the **Create virtual machine** page, in panel 3 Settings:
   a) Indicate whether you want to use high availability.
   b) Provide the virtual network name, subnet, public IP address, and network security.
   c) Optionally, select extensions.
   d) Enable or disable auto-shutdown, monitoring (boot diagnostics, guest OS diagnostics, diagnostics storage account).
   e) Enable or disable backup.
   f) Click **OK**.

6. In panel 4 Summary, click **OK** to begin creation of the VM.

Do not Sysprep the image.
Install apps on the master image

On the master image VM you just created, add the apps that will be available to users when they log on with the workspace URL. (Later, after you create the catalog that uses this master image, you’ll specify exactly which of these apps will be available to the users you specify.)

1. Connect to the master image VM after you create it and while it is running.
2. Install applications.

Install a VDA on the master image

1. Connect to the master image VM (if you’re not already connected).
2. You can download a VDA for Server OS by using the Downloads link on the Citrix Cloud navigation bar. Or, use a browser to navigate to the Citrix Virtual Apps and Desktops service download page. Download a VDA for Server OS onto the VM. (See guidance above for VDA version information.)
3. Launch the VDA installer by double-clicking the downloaded file. The installation wizard launches.
4. On the Environment page, select Create a master image using MCS and then click Next.
5. On the Core Components page, click Next.
6. On the Delivery Controller page, select Let Machine Creation Services do it automatically and then click Next.
7. Leave the default settings on the Additional Components, Features, and Firewall pages, unless Citrix instructs you otherwise. Click Next on each page.
8. On the Summary page, click Install. Prerequisites begin to install. When prompted to restart, agree.
9. The VDA installation resumes automatically. Prerequisite installation completes and then the components and features are installed. On the Call Home page, leave the default setting (unless Citrix instructs you otherwise), and then click Next.
10. Click Finish. The machine restarts automatically.
11. To ensure that the configuration is correct, launch one or more of the applications you installed.
12. Shut down the VM. Do not Sysprep the image.

Upload the master image

In this procedure, you upload the master image from Azure Resource Manager to Virtual Apps Essentials.

1. If you are not already in Citrix Cloud, sign in. In the upper left menu, select My Services > Virtual Apps and Desktops
2. On the Manage tab, click Master Images.
3. Click Add Master Image.
4. On the **Add an image** page, specify the location of the image by selecting the subscription, resource group, storage account, VHD, and region.
5. Enter a name for the master image.
6. Click **Save**.

The service verifies the master image. After verification, the uploaded image appears under **Master Images > My Images**.

**Tip:** As an alternative to uploading the master image before creating the catalog, you can import a master image from Azure Resource Manager when you create the catalog.

**Prepare a master image in Virtual Apps Essentials**

This method uses an existing master image as a template (and optionally, connection details from an existing catalog) to build another master image. You can then customize the new master image. This procedure is completed entirely through the Virtual Apps Essentials interface.

1. Sign into **Citrix Cloud**, if you haven’t already. In the upper left menu, select **My Services > Virtual Apps and Desktops**.
2. Click **Manage** and then select the **Master Images** tab.
3. Click **Build Image**.
4. On the **Build Image** page, in the **Select an image** panel, select a master image. Specify a name for your new image. Click **Next**.
5. In the **Specify network connectivity settings** panel, you can either use the settings from an existing catalog, or you can specify the settings. The settings are: subscription, virtual network, region, subnet, domain, and VM instance type. (If you don’t have a catalog, you must enter the settings.)
   
   If you select **Copy settings from a catalog**, select the catalog. The network connection settings display, so you can visually verify that you want to use them with your new master image. Enter your service account username and password to join the domain. Click **Save**.

   If you select **Enter new settings**, select values in the appropriate settings fields. Enter your service account username and password to join the domain. Click **Save**.
6. Click **Start Provisioning**.
7. When the new image has been created, it appears in the **Manage > Master Images** list with a status of **Input Required**. Click **Connect to VM**. An RDP client downloads. Use RDP to connect to the newly created VM. Customize the new image by adding or removing applications and other software. As with all master images, do not Sysprep the image.
8. When you’re done customizing your new image, return to the Manage > Master Images page and click Finish for your new master image. The new image is then sent to the verification process.

9. When the verification process completes, the new image appears in the My Images list with a status of Ready.

Later, when you create a catalog, and select Link an existing image on the Choose master image page, the new image appears among the Image Name choices.

Deploy a catalog, publish apps and desktops, and assign subscribers

A catalog lists the apps and desktops that you choose to share with selected users.

If you’re familiar with other Citrix app and desktop delivery products, a catalog in this service is similar to combining a machine catalog and a delivery group. However, the machine catalog and delivery group creation workflows in other services are not available in this service.

Deploying a catalog and sharing apps with subscribers is a multi-step process.

- Create a catalog
- Publish apps and assign subscribers for that catalog
- Test and share the workspace link your subscribers will use

Create a catalog

When creating a catalog, have Azure Active Directory account credentials and your subscription name available.

1. If you are not already in Citrix Cloud, sign in. In the upper left menu, select My Services > Virtual Apps and Desktops.
2. On the Manage tab, click Catalogs and then Add Catalog.
3. Provide information in the following panels. Click Save when you’re done with each panel. A warning sign appears in a panel’s header if required information is missing or invalid. A check mark indicates that the information is complete.
1. Type a 2-38 character name for the catalog. (Letters and numbers only, no special characters.) This name is visible only to administrators.

2. Select **Domain Joined** if it isn't already selected. A domain-joined deployment allows VDAs to join Active Directory. Later, you provide an Azure virtual network that is connected to your domain. If you don’t have a domain, you can use Azure Active Directory Domain services.

3. Click **Save**.

**Link your Azure subscription**

1. Select your Azure subscription. When you link a new Azure subscription, the Azure sign-in page appears for authentication of your Azure credentials. After signing in, accept the service consent to manage your subscription. Then, you can link a subscription. Virtual Apps Essentials requires you to log on with an Azure Active Directory account. Other account types (such as live.com) are not supported.

2. Select your resource group, virtual network (VNET), and subnet. The VNET determines the Azure...
region where your resources are deployed. The subnet must be able to reach your domain controller.

3. Click **Save**.

### Join local domain

1. Enter domain information:
   - **Fully Qualified Domain Name**: Enter the domain name. The name must resolve from the DNS provided in the virtual network.
   - **Organizational Unit**: (optional) Ensure that Active Directory contains the specified OU. If you leave this field blank, machines are placed in the default Computers container.
   - **Service Account Name, Password, and Confirm Password**: Enter the User Principal Name (UPN) of the account that has permissions to add machines to the domain. Then enter and confirm the password for that account.

2. Click **Save**.

You can test connectivity through the virtual network by creating a VM in your Azure subscription. The VM must be in the same resource group, virtual network, and subnet that you use to deploy the catalog. Ensure that the VM can connect to the internet. Also ensure that you can reach the domain by joining the VM to the domain. You can test using the same credentials that were used for deploying this catalog.

### Connect to a resource location
Each resource location must have two or more Cloud Connectors, which communicate with Citrix Cloud. The service handles the Cloud Connector deployment automatically when a catalog deploys. The two Windows Server VMs are created in Azure Resource Manager and then a Cloud Connector is installed automatically on each server.

If the selected resource location is available, connection occurs automatically. Simply click **Save**.

To create a resource location, enter a name for it.

- To create Cloud Connectors in a specific Azure resource group, click **Edit** next to **Azure Resource Group** to change the resource location. Otherwise, the service uses the resource group you specified when you linked your Azure subscription.
- To put the Cloud Connectors into a separate OU, click **Edit** next to **Organizational Unit** to change the OU. Otherwise, Virtual Apps Essentials uses the resource group you specified when you linked your Azure subscription.

**Choose a master image**

1. Select one of the following:

   - **Link an existing image**: Use this option if you previously imported a custom image and want to use it with this catalog. Select the image and optionally, a region.
   - **Import a new image**: Use this option if you want to use a custom image with this catalog, but have not yet imported it. Select the subscription, resource group, storage account, and VHD. Enter a friendly name for the image.
   - **Use a Citrix prepared image**: Use this option to test the service without using your own custom image. These images are suitable only for demonstration environments, and are not recommended for production. Select a prepared image.
2. Click **Save**.

**Pick storage and compute type**

1. Configure the following items:
   - **Standard or premium disks**: Standard disks (HDD) are backed by magnetic drives. They are preferable for applications where data is accessed infrequently. Premium disks (SDD) are backed by solid state drives. They are ideal for I/O-intensive applications.
overview.

- **Azure Hybrid Use Benefit:** Select whether or not to use existing on-premises Windows Server licenses. Enabling this feature and using existing on-premises Windows Server images uses Azure Hybrid Use Benefits (HUB). For details, see https://azure.microsoft.com/pricing/hybrid-use-benefit/.

  HUB reduces the cost of running VMs in Azure to the base compute rate, because it waives the price of additional Windows Server licenses from the Azure gallery. You need to bring your on-premises Windows Servers images to Azure to use HUB. Azure gallery images are not supported. On-premises Windows Client licenses are currently not supported. See Azure Hybrid Benefit for Windows Server on the Microsoft web site.

- **Pick a virtual machine size:** Select a worker role (for example, task, office, knowledge, power). The worker role defines the resources used. When you specify a worker role, the service determines the correct load per instance. You can select an option or create your own custom option.

  2. Click **Save**.

Manage costs with power management settings
1. Enter the following information:

   - **Scale settings:**
     - **Minimum number of running instances:** The service ensures that this many VMs are powered on all the time.
     - **Maximum number of running instances:** The service does not exceed this number of VMs.
     - **Maximum concurrent users:** The service does not allow concurrent users beyond this limit.
     - **Capacity buffer:** Enables extra sessions to be ready for demand spikes, as a percentage of current session demand. For example, if there are 100 active sessions and the capacity buffer is 10%, the service provides capacity for 110 sessions.
As the total session capacity changes, the number of running instances for this catalog scales up or down. The number of running instances always stays within the configured minimum and maximum values. A lower capacity buffer percentage can result in a decreased cost. However, it might also result in some sessions having an extended logon time if several sessions start concurrently.

- **Schedule for peak time:** Select this option if you want a different number of VMs running during peak times than in non-peak times. Select the days of the week for the peak time, start and end times, and time zone. Specify the minimum number of running instances during peak time.

- **Idle or disconnected session time-out:** Set the time for when the session ends. User sessions end automatically if the session remains idle or is disconnected for the specified time period. Shorter time-out values allow unused VDAs to power off and save costs.

2. Click **Save**.

### Deploy the catalog

After you complete the configuration panels, click **Start Deployment** to start the catalog creation. Creating a catalog can take 1 to 2 hours (or longer, if you specified a large number of VMs).

When a catalog is created:

- A resource group (and a storage account in that resource group) for the workload machines are created automatically in Azure.
- The VMs are named Xenappxx-xx-yyy, where xx is derived from an environmental factor and yy is an ordinal number.

### Publish apps and assign subscribers for a catalog

To complete the catalog after it is deployed, you must publish one app or desktop, and assign at least one subscriber.

The image you used to create the catalog includes the applications (or desktop) that you can publish. You can select applications from the Start menu or specify a directory path on the machine.

1. If you are not already in **Citrix Cloud**, sign in. In the upper left menu, select **My Services > Virtual Apps and Desktops**.
2. On the **Manage** tab, click **Catalogs**.
3. In the ellipsis menu (...) for the catalog that was created, select **Manage Catalog**.
4. Select **Publish Apps and Assign Subscribers**. The following page displays.
5. In the **Publish Apps and Assign Subscribers** dialog box, click **Publish**. The Publish to catalog-name page contains three choices. Complete at least one. Optionally, you can then choose another (for example, to publish both apps and desktops using this catalog).

6. To publish apps located on the Start menu:
   a) Select **Publish from Start Menu**.
   b) Select the applications from the list.

7. To publish apps by specifying their location and other information:
   a) Select **Publish using Path**.
   b) Enter each application's name and path (for example, c:\Windows\system1\app.exe).
   c) Optionally, enter a description that will appear in the user's workspace, command line parameters, and working directory.
   d) To change the icon that represents the published app, click **Change icon** and then navigate to the location of the icon. A message appears if the selected icon cannot be extracted. In that case, you can retry or continue using the existing icon.
e) Click **Publish App**.

8. To publish a desktop:
   a) Select **Publish desktop**.
   b) Enter the name of the desktop.
   c) Optionally, enter a description that will appear in the user’s workspace.
   d) Click **Publish Desktop**.
After you add apps or desktops, they appear in the list under the selectors. To delete an app or desktop you added, select the button to the left of the entry (or click the trash icon next to the entry) and then click **Remove**. Later, if you want to unpublish an app or desktop, select the button to the left of the entry and then click **Unpublish**.

9. In the **Publish Apps and Assign Subscribers** dialog box, click either **Manage App Subscribers** or **Manage Desktop Subscribers**.

10. Select a domain and then search for a user or user group.

11. User assignments for apps and desktops are separate. To assign a user access to both apps and desktops, assign that user with **Manage App Subscribers** and with **Manage Desktop Subscribers**.
After you add a user or group, it appears in the list under the selectors. To delete a user or group you selected, click the trash can icon next to the entry and click **Remove**. Later, if you want to remove users, select the button to the left of the entry and then click **Remove Selected**.

---

**Test and share the workspace link**

After you deploy a catalog, publish apps, and assign subscribers, you’re provided the link that your subscribers use to access the apps and desktops you published for them.

1. If you are not already in **Citrix Cloud**, sign in. In the upper left menu, select **My Services > Virtual Apps and Desktops**.
2. On the **Manage** tab, click **Catalogs**.
3. In the ellipsis menu (…) for the catalog, select **Manage Catalog**.
4. Select **Test and Share Workspace Link**.

In the following graphic, the workspace link appears in the circled area. Share this link with your subscribers. The right portion of the page lists the workspace URL, plus information about the catalog’s master image, resource location, Azure subscription, and domain.

See **Workspace experience** for more information.

---

**Update master images and catalogs**

To update or add applications, update the virtual machine that you used to create the catalog’s master image.
Citrix Cloud

Update the master image

1. Power on the master image VM. Powering on the machine does not affect the master image installed in Azure Resource Manager.
2. Install any updates or applications on the VM.
3. Shut down the VM.
4. In the Virtual Apps Essentials console, add the new image that includes the path to the VM’s VHD image.

Update a catalog with a new image

1. If you are not already in Citrix Cloud, sign in. In the upper left menu, select My Services > Virtual Apps and Desktops.
2. On the Manage tab, click Catalogs.
3. Click the ellipsis menu for the catalog and then click Update Catalog Image.
4. Select either Link an existing image or Import a new image. Enter the information that is appropriate for your choice.
5. In Time until automatic log-off, choose the amount of time before the session ends.
6. Click Update.

When you start the catalog update, users can continue to work until the initial processing completes. Then, users receive a warning message to save their work and close applications. After closing all active sessions on the VDA, the update finishes on that VDA. If users do not log off in the amount of time given, the session closes automatically.

Update the number of VDAs in a catalog

1. If you are not already in Citrix Cloud, sign in. In the upper left menu, select My Services > Virtual Apps and Desktops.
2. Click the Manage tab.
3. On the Catalogs tab, select a catalog.
4. On the Capacity tab, under Select scale settings, click Edit.
5. Change the Maximum number of running instances value to the desired VDA count for the catalog.
6. Click Save.

Monitor machine states

When you select a catalog, the Machines tab on the catalog summary page lists all of the machines in that catalog. The display includes each machine’s power and registration states, and the current
You can turn maintenance mode on or off for a machine. Turning on maintenance mode prevents new connections from being made to the machine. Users can connect to existing sessions, but they cannot start new sessions. You might want to place a machine in maintenance mode before applying patches.

If you turn on maintenance mode for one or more machines, Smart Scale is temporarily disabled for all machines in that catalog. Either of the following actions will enable Smart Scale again:

- Click **Enable Smart Scale** in the warning at the top of the screen. This action automatically turns off maintenance mode for all machines in the catalog that have maintenance mode turned on.
- Explicitly turn off maintenance mode for each machine that currently has maintenance mode turned on.
Monitor the service

1. If you are not already in Citrix Cloud, sign in. In the upper left menu, select My Services > Virtual Apps and Desktops.
2. Click the Monitor tab.

Session information

To monitor the overall performance of Citrix Virtual Apps Essentials:

1. Select the catalog that you want to monitor. You can view information on sessions, logon duration, and other information.
2. Choose a session and then:
   - Disconnect the session
   - Log off from the session
   - Send a message
3. Click each session to view extra details about the session such as processes, applications running, and more.
Usage information

Usage information shows aggregated data for all catalogs (rather than a specified catalog).

- **Usage Overview** displays the total number of application launches and the number of unique users who launched apps over the past six weeks.
- **Top Apps** lists the most frequently used apps for the current and previous months. Hovering over an entry displays the number of times that application was launched.
- **Top Users** lists the top ten users for the current and previous months, with the number of times they launched applications.

Weekly data intervals are Monday (UTC 00:00) through the query time. Monthly data intervals are the first day of the month (UTC 00:00) through the query time.

Profile Management

Profile Management ensures that personal settings apply to users' virtual applications, regardless of the location of the user device.

Configuring Profile Management is optional.

You can enable Profile Management with the profile optimization service. This service provides a reliable way for managing these settings in Windows. Managing profiles ensures a consistent experience by maintaining a single profile that follows the user. It consolidates automatically and optimizes user profiles to minimize management and storage requirements. The profile optimization service requires minimal administration, support, and infrastructure. Also, profile optimization provides users with an improved log on and log off experience.

The profile optimization service requires a file share where all the personal settings persist. You must specify the file share as a UNC path. The path can contain system environment variables, Active Directory user attributes, or Profile Management variables. To learn more about the format of the UNC text string, see To specify the path to the user store.

You configure Profile Management in Citrix Cloud.

To configure Profile Management

1. If you are not already in Citrix Cloud, sign in. In the upper left menu, select My Services > Virtual Apps and Desktops.
2. On the Manage tab, click Catalogs.
3. Click the name of the catalog.
4. Click More Settings.
5. In Set up Profile Management in Azure subscription, enter the path to the profile share. For example, \fileserv#r\share#sAMAccountName#

© 1999-2021 Citrix Systems, Inc. All rights reserved.
6. Click **Save**.

When enabling Profile Management, consider further optimizing the user’s profile by configuring folder redirection to minimize the effects of the user profile size. Applying folder redirection complements the Profile Management solution. For more information, see Microsoft Folder Redirection.

**Configure the Microsoft RDS License Server**

Citrix Virtual Apps Essentials accesses Windows Server remote session capabilities that would typically require a Remote Desktop Services client access license (RDS CAL). The VDA must be able to contact an RDS license server to request RDS CALs. Install and activate the license server. For more information, see Activate the Remote Desktop Services License Server. For proof of concept environments, you can use the grace period provided by Microsoft.

With this method, you can have Virtual Apps Essentials apply the license server settings. You can configure the license server and per user mode in the RDS console on the master image. You can also configure the license server using Microsoft Group Policy settings. For more information, see License your RDS deployment with client access licenses (CALs).

**To configure the RDS license server using Group Policy settings**

1. Install a Remote Desktop Services License Server on one of the available VMs. The VM must always be available. The Citrix service workloads must be able to reach this license server.
2. Specify the license server address and per user license mode using Microsoft Group Policy. For details, see Specify the Remote Desktop Licensing Mode for an RD Session Host Server.
3. If you purchased CAL licenses from Microsoft Remote Access, you do not have to install the licenses. You can purchase licenses from Microsoft Remote Access in the Azure Marketplace, along with Virtual Apps Essentials.

**To configure the RDS license server**

1. If you are not already in **Citrix Cloud**, sign in. In the upper left menu, select **My Services > Virtual Apps and Desktops**.
2. On the **Manage** tab, click **Catalogs**.
3. Select the catalog and then select **More Settings**.
4. In Enter the FQDN of the license server, type the fully qualified domain name of the license server.
5. Click **Save**.
Citrix Cloud

Connect users

Workspace experience

Virtual Apps Essentials in Citrix Cloud enables the workspace experience for each customer. After you create the first catalog, Virtual Apps Essentials configures the workspace URL automatically. The URL is the one from which users can access their applications and desktops. The workspace URL appears in the catalog details panel on the Summary tab. Virtual Apps Essentials does not support on-premises StoreFront deployments.

After creating a catalog, you can use Workspace Configuration to customize the workspace URL and the appearance of workspaces. You can also enable the preview version of federated authentication using Azure Active Directory.

Enabling federated authentication using Azure Active Directory includes the following tasks:

- Set Azure AD as your identity provider. For more information, see Connect Azure Active Directory to Citrix Cloud.
- Enable Azure AD for authentication to the Citrix Workspace experience.

For more information, see Workspace configuration.

Citrix Gateway service

To allow users secure access to their published apps, Virtual Apps Essentials uses the Citrix Gateway service. This service does not need any configuration by you. Each user is limited to 1-GB outbound data transfer per month. You can purchase a 25 GB add-on from the Azure Marketplace. The charge for the add-on is on a monthly basis.

Cancel Virtual Apps Essentials

You can incur Azure charges from Virtual Apps Essentials because of the following elements:

- Virtual Apps Essentials subscription
- Azure resource created by Virtual Apps Essentials

The Microsoft Azure charge for the Virtual Apps Essentials service is on a monthly basis. When you purchase Virtual Apps Essentials, you are charged for the current month. If you cancel your order, your service will not renew for the next month. You continue to have access to Virtual Apps Essentials until the end of the current month by using Citrix Cloud.

Your Azure bill can contain multiple line items for Virtual Apps Essentials, including:

- Virtual Apps Essentials service subscription
- Citrix Gateway service add-on, if purchased
- Microsoft Remote Access fee
Citrix Cloud

- Azure resource created when using Virtual Apps Essentials

Cancel Virtual Apps Essentials in Azure

To cancel your Virtual Apps Essentials subscription, delete the order resource in the Azure portal.

1. Sign in to the Azure portal.
2. Click All Resources.
3. In the Type column, double-click to open Citrix Virtual Apps Essentials.
4. Click the trash icon. The delete process starts.

Delete the Azure resources created by Virtual Apps Essentials

In Citrix Cloud, delete the catalogs and images associated with your account. Also, remove the subscription links and ensure the removal of the Cloud Connector VMs from Citrix Cloud.

If you are not already in Citrix Cloud, sign in. In the upper left menu, select My Services > Virtual Apps and Desktops.

To delete catalogs

1. On the Manage tab, click Catalogs.
2. In the ellipsis menu (…) next to the catalog you want to remove, select Delete Catalog.
3. Repeat the previous step for each catalog you want to delete.

To remove master images

1. On the Manage tab, click Master Images.
2. Select an image and click Remove.
3. Repeat the previous step for each master image you want to delete.

To remove links to Azure subscriptions

1. On the Manage tab, click Subscriptions.
2. Click the trash icon next to the subscription. The Azure portal opens.
3. Sign in to your Azure subscription, using your global administrator Azure credentials.
4. Click Accept to allow Virtual Apps Essentials to access your Azure account.
5. Click Remove to unlink the subscription.
6. Repeat the preceding steps for other linked Azure subscriptions.
**To ensure removal of the Citrix Cloud Connector VMs**

1. In the upper left menu, select **Resource Locations**.
2. Identify the Cloud Connector VMs.
3. Sign in to the **Azure portal**.
4. Delete the VMs from the **Resource** page in Azure.

**Partner resources**

This service is now available through the Microsoft Cloud Solution Provider channel. For details, see [Microsoft CSP enablement for Citrix Essentials](#).

**Get help**

If you have problems with Virtual Apps Essentials, open a ticket by following instructions in [How to Get Help and Support](#).

**More information**

- For information about using Citrix policies in a Virtual Apps Essentials environment, see [CTX220345](#).
- To troubleshoot catalog creation failures, see [CTX224151](#).

**Upgrade to Citrix Virtual Apps and Desktops Standard for Azure**

Learn how to [upgrade from Citrix Virtual Apps Essentials to Citrix Virtual Apps and Desktops Standard for Azure](#).

**Citrix Virtual Desktops Essentials**

May 26, 2021

Citrix Virtual Desktops Essentials allows management and delivery of Windows 10 virtual desktops from Microsoft Azure.

Virtual Desktops Essentials is designed specifically for the Azure Marketplace. Citrix and Microsoft partner to deliver an integrated experience for Virtual Desktops Essentials and Azure IaaS. This partnership gives you a single interface to deliver a complete Windows 10 digital workspace from Azure.

Using Virtual Desktops Essentials, you can:
Citrix Cloud

- Deploy and secure Windows 10 virtual desktops on Azure
- Deliver best-in-class user experience by using Citrix HDX capabilities
- Provide secure access on any device by using Citrix Workspace app
- Manage and administer the deployment from Microsoft Azure and Citrix Cloud

Citrix Virtual Desktops Essentials simplifies Windows 10 deployment. You can deploy desktops quickly, manage at scale, and deliver a rich user access experience from a single management plane.

You manage the Windows 10 desktops using Studio and monitor sessions using Director. Users connect to their Windows 10 virtual desktops by logging on with Citrix Workspace app.

After you configure Citrix Virtual Desktops Essentials, you provide your users with a URL to Citrix Workspace. Users connect to their desktops through the Citrix Workspace app on their devices, with the URL you provide. When users log on to the Citrix Workspace app, the Windows 10 desktop icon appears in the workspace window.

**Important:**

Virtual Desktops Essentials includes a Citrix Workspace URL, usually in the format https://<yourcompanyname>.cloud.com. After you set up Virtual Desktops Essentials, test and share the workspace URL link with your subscribers to give them access to their desktops. Virtual Desktops Essentials does not support on-premises StoreFront.

For details about the workspace, see Workspace configuration.

The diagram shows an architectural overview of a Virtual Desktops Essentials deployment.

© 1999-2021 Citrix Systems, Inc. All rights reserved.
What’s new

December 2018: **Cloud-hosted StoreFront removed**

Cloud-hosted StoreFront is no longer available for use with Virtual Desktops Essentials. Customers who purchased Virtual Desktops Essentials (formerly XenDesktop Essentials) before December 2017 can use Citrix Workspace as described in this article to provide subscriber access to desktops.

August 2018: **New product names**

If you’ve been a Citrix customer or partner for a while, you’ll notice new names in our products and product documentation. If you’re new to this Citrix product, you might see different names for a product or component.

The new product and component names stem from the expanding Citrix portfolio and cloud strategy. This article uses the following names.

1. **Citrix Virtual Desktops Essentials**: The technology that made XenDesktop the industry leader is now Citrix Virtual Desktops, and it brings VDI into a modern, contextual, secure app that allows the preferred way to securely access all your work applications. XenDesktop Essentials is now Citrix Virtual Desktops Essentials.

2. **Citrix Workspace app**: The Citrix Workspace app incorporates existing Citrix Receiver technology as well as the other Citrix Workspace client technologies. It has been enhanced to deliver additional capabilities to provide end users with a unified, contextual experience where they can interact with all the work apps, files, and devices they need to do their best work.

3. **Citrix Gateway**: The NetScaler Gateway, which allows secure, contextual access to the apps and data you need to do your best work, is now Citrix Gateway.

In-product content might still contain former names. For example, instances of earlier names in console text, messages, and directory/file names. It is possible that some items (such as commands and MSIs) might continue to retain their former names to prevent breaking existing customer scripts.

Related product documentation and other resources (such as videos and blog posts) that are linked from this product’s documentation might still contain former names. Your patience during this transition is appreciated. For more detail about our new names, see [https://www.citrix.com/about/citrix-product-guide/](https://www.citrix.com/about/citrix-product-guide/).

**How to buy Virtual Desktops Essentials**

For detailed information about buying or canceling Virtual Desktops Essentials, download How to buy or cancel the Virtual Desktops Essentials Service.
System requirements, prerequisites, and compatibility

Virtual Desktops Essentials requires certain complementary products and components and specific account permissions for installation, configuration, and operation.

Microsoft Azure

Virtual Desktops Essentials is designed to support Microsoft Azure exclusively. Your Azure environment must meet certain minimum requirements to support Virtual Desktops Essentials:

- An Azure subscription with an enterprise agreement, or a Microsoft CSP Azure subscription.
- Windows Server Active Directory or Azure Active Directory Domain Service.
- An Azure Active Directory tenant.

Important:

Microsoft requires the Azure Active Directory tenant in the Azure subscription to deploy Windows 10 desktops. You can use the Azure Active Directory tenant or another active directory to identify authorized users.

- An Active Directory domain controller.
- An Azure Resource Manager (ARM) virtual network and subnet in your preferred region. Configure the virtual network with a custom domain name server (DNS) entry pointing to the domain controller. The virtual network must have one subnet that is large enough to hold the desktops. Use the same virtual network for the DNS entry and desktop subnet.
- An Azure Active Directory user with contributor (or greater) permissions within the subscription.
- One virtual machine that has Microsoft Windows 10 installed, including your required customizations and apps.

Citrix Cloud Connector

Citrix Cloud Connector authenticates and encrypts communications between Citrix Cloud and your resource locations. With Virtual Desktops Essentials, your resources are located in Microsoft Azure. Citrix Cloud requires that you install the Citrix Cloud Connector on two Windows server VMs to ensure continuous availability of your resource locations.

For more information about Cloud Connectors, see Citrix Cloud Connector

Citrix Cloud

- A Citrix Cloud account.
Citrix Cloud

- Access to the Citrix Virtual Apps and Desktops service within Citrix Cloud, which is enabled as a part of your Virtual Desktops Essentials purchase.
- (Optional) One Citrix ADC VPX configured in ICA Proxy mode, for access from outside the corporate network.
  - ICA Proxy enables secure access to the applications and desktops offered to your users.
  - For information about setting up the Citrix ADC VPX, see Deploying Citrix NetScaler VPX on Microsoft Azure.

Known issues

- The Citrix Help Desk Administrator custom access role does not work correctly. As a workaround, use the Cloud Administrator role, or enable Full access. [BRK-3589]
- If you use Azure AD Domain Services: Workspace logon UPNs must contain the domain name that was specified when enabling Azure AD Domain Services. Logons cannot use UPNs for a custom domain you create, even if that custom domain is designated as primary.

Step 1: Connect your Azure subscription to Virtual Desktops Essentials

1. Sign in to the Azure portal.
2. In Azure, open a domain-joined Windows Server virtual machine and then open a web browser.
3. In the web browser on the VM, sign in to Citrix Cloud. The Virtual Apps and Desktops service opens.
4. From the upper left menu, select Resource Locations.
6. Double-click the downloaded program to start the installer.
7. When prompted, enter your Citrix Cloud credentials. Follow the on-screen instructions to install and configure the Citrix Cloud Connector.
8. Repeat steps 4 through 7 on at least one more server VM, to install another Cloud Connector.

During installation, the Cloud Connector accesses Citrix Cloud to authenticate, validate the installer permissions, and then download and configure the services that the Cloud Connector provides. The installation uses the privileges of the user who initiated the installation.

After installation, Citrix Cloud registers your domain in Identity and Access Management. For more information, see Identity and Access Management.

Step 2: Create a host connection

Before you start, ensure that you have your Azure Active Directory credentials and your subscription ID available. The Azure AD user who creates the host connection must be a native cloud user in the Azure
AD or synchronized for the enterprise domain. The user account cannot be an invited or delegated Microsoft account.

1. Sign in to Citrix Cloud.
2. In the upper left menu, select My Services > Virtual Apps and Desktops.
3. Click Manage. The Studio management console opens.
4. Select Configuration > Hosting in the Studio navigation pane.
5. Click Add Connection and Resources in the Actions pane.
6. On the Add Connection and Resources page:
   a) In Connection type, select Microsoft Azure.
   b) In the Azure environment, select Azure Global and then click Next.
7. In Connection Details:
   a) In Subscription ID, type the Azure subscription ID.
   b) In Connection name, type a name for the connection and then either:
      i. Click Create new and then follow the procedure Option 1: To create a connection.”
      ii. Click Use existing and continue configuring the settings. Follow the procedure Option 2: Use an existing host connection.”

Option 1: Create a connection

1. Sign in to Azure with the subscription contributor (or greater) account.
2. Azure creates the host connection automatically. In Studio, a green check mark with the word Connected appears on the Add Connection and Resources page.
3. Click Next.
4. On the Region page, select the region where your virtual network resides, and then click Next.
5. On the Network page:
   a) Type a name for the resources.
   b) Select the virtual network for the resource group.
   c) Select the subnet that applies to the resource group and then click Next.
6. On the Summary page, click Finish. The host connection to the Microsoft Azure Resource Manager is complete.

Option 2: Use an existing host connection

After you click Use existing, the Existing Service Principal Details page appears:

1. In Subscription ID, type the Microsoft Azure subscription ID.
2. In Subscription name, type the name of the Azure subscription.
3. Click OK.
4. On the Connection page:
a) Click **Create a new Connection**, type your Microsoft Azure subscription ID and a connection name (optional), and then click **Create new**. The Microsoft authentication dialog box appears.

If you want to use a connection that you created at another time, choose **Use an existing connection**. Then, select the connection.

b) Type the user name and password for the Microsoft Azure Active Directory user. Citrix Cloud creates a service principal with the rights to create and manage machines for this subscription.

5. On the **Region** page, select the Azure region where your Microsoft Azure resource group is located.

6. On the **Network** page:
   a) Type a name for the resources. If you typed a connection name, use it as the name for the Resources name.
   b) Choose the virtual network for your Microsoft Azure resource group.
   c) Select the subnets to use for this connection. If only one subnet exists, it is selected by default.

### Step 3: Create a pool of Windows 10 desktops

In preparation for hosting the desktops, install the Citrix Virtual Delivery Agent (VDA) software on the Windows 10 virtual machine. The VDA:

- Enables the machine to register with Virtual Desktops Essentials.
- Establishes and manages the connection between the machine and the user device.
- Verifies that a Citrix license is available for the user or session.
- Applies any configured policies for the session.
- Communicates session information to Virtual Desktops Essentials.

**To install the VDA on the base image**

1. Start the Windows 10 image.
3. Start the VDA installation.
4. On the **Environment** page, click **Create a master image using MCS**.
5. On the **Additional Components** page, select all of the components except **Enable Citrix App-V**.
6. On the **Delivery Controller** page, enter the locations of your Cloud Connector virtual machines. Click **Next** and confirm any warning messages.
7. On the **Features** page, keep the default settings and click **Next**.
8. Click Next to accept the default settings on the remaining pages.
10. Restart the virtual machine and sign back in.
11. Confirm that the settings have taken effect.
12. Shut down the virtual machine. Shutting down the virtual machine is required for VDA registration.

Create a Storage Account

In Microsoft Azure, you need a storage account to host the base image virtual hard disk. You can host the drive in an existing storage account or create a storage account.

Important:
Upload the Windows 10 master image to the destination storage account in Azure before you create the machine catalog.

To create a storage account for images

1. In the Microsoft Azure navigation pane, click Storage accounts.
2. On the Storage accounts page, click Add.
3. In Name, provide a name.
6. For Replication, Storage service encryption, and Subscription, leave the default settings.
7. In Resource group, click one of the following:
   a) Click Create new to create a resource group. Type the name of the group.
   b) Click Use existing to use an existing resource group. Select a group.
8. To have the storage account appear on the dashboard, click Pin to dashboard.
9. Click Create.

After you create a storage account, create a blob container and then name it to reflect the virtual hard disk, such as “VHDs.”

To create a blob container for image VHDs

1. In the Microsoft Azure navigation pane, click Storage accounts and navigate to the storage account that you created previously.
2. In the center navigation pane, under BLOB SERVICE, click Containers.
3. In the details pane, click Container.
4. In the New container pane, give the container a name.
5. In Access type, select Blob and then click Create. The new blob container appears in the pane.
6. Copy the blob URL and save it in a text file. The URL is used later to upload the converted VHD.

Create a machine catalog for Citrix Virtual Desktops Essentials

Machine catalogs are collections of virtual desktops that you manage as a single entity. These virtual desktops are the resources you provide to your users. All the machines in a catalog have the same operating system and the same VDA installed.

Typically, you create a master image and use it to create identical virtual machines in the catalog.

1. Sign in to Citrix Cloud. In the upper left menu, select My Services > Virtual Apps and Desktops.
2. Select the Manage tab.
3. Click Machine Catalogs in the Studio navigation pane.
4. Click Create Machine catalog in the Actions pane.
5. On the Operating System page, Desktop OS is the only option available. Select it and then click Next.
6. On the Desktop Experience page:
   a) Select I want users to connect to the same (static) desktop each time they log on.
   b) Select Yes, create a dedicated virtual machine and save changes on the local disk.
7. On the Master Image page:
   a) Navigate to and select the VHD in the blob storage you created previously. The structure of the navigation tree aligns with the Azure hierarchy:
      • Resource group
      • Storage accounts
      • Containers
      • Virtual hard disks (VHDs)
      • Image names
   b) Keep the default selection in Select the minimum functional level for this catalog.
8. On the Storage and License Types page, select the destination storage type and your license preference.
9. On the Virtual Machines page, select the number of virtual machines and the Azure virtual machine size.
10. On the Network Interface Cards page, select a network adapter to associate with the Azure subnet name for your Citrix machines. You can also click Add Card to add another network adapter.
11. On the Computer Accounts page:
    a) Click Create new Active Directory accounts.
    b) Choose the domain for the computer accounts.
    c) Navigate to the organizational unit (OU) for the new machines.
    d) Type an account naming scheme for the new machines. Include two number signs (##) to increment numbers automatically. Select number or letters. The pound signs translate
to the naming scheme. For example, mymachcatalog## becomes mymachcatalog01 or mymachcatalogAB.

12. On the Domain Credentials page, click Enter Credentials and then in the Windows Security dialog box, type your user name and password. This account is used to create the computer accounts.

13. On the Summary page, type a name for the catalog and a description for administrators.

14. Click Finish.

The virtual machines are created and a new storage account appears in the Microsoft Azure dashboard. While Machine Catalog Services deploys the virtual machines, a preparation virtual machine with a VHD is created temporarily in Azure.

To identify the image name in Microsoft Azure

1. Sign in to the Azure portal.
2. In the Dashboard navigation pane, click All resources. A list of subscriptions appears.
3. Choose the subscription.
4. Click All settings.
5. Click Resource groups.
6. Select the resource group.
7. Select the Windows 10 virtual machine that contains the Citrix VDA.
8. Click All settings.
9. Click Disks.
10. Select the OS disk. The first text box in the OS disk window contains the URL for the image, which is structured as shown in the following example. You can obtain the storage account name and image name from the URL. For example: https://<storage account name>.blob.core.windows.net/vhds/<image name>.
11. On the Machines page, the templates listed are retrieved directly from your Azure subscription.

Step 4: Assign Windows 10 desktops to your users

A Delivery Group is a collection of machines selected from one or more machine catalogs. The Delivery Group specifies which users can use those machines.

1. Select Delivery Groups in the Studio navigation pane and then select Create Delivery Group in the Actions pane.
2. Specify how many machines that you want to make available to the Delivery Group. The number you specify cannot exceed the number of available machines in your machine catalog.
3. On the Delivery Type page, choose Desktops.
4. On the Users page, choose the option to leave user management to Citrix Cloud. Selecting this option allows you to use Citrix Cloud to manage who can access machines in the Delivery Group.
(You can also add users through Studio.)

5. On the **Summary** page, provide a name and (optionally) a description for the Delivery Group.

After completing these steps, edit the delivery group to configure access for users. You can add or remove users and change user settings.

**Add or remove users in a Delivery Group through Studio**

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **Users** page, to add users, click **Add**, and then specify the users you want to add. To remove users, select one or more users and then click **Remove**. You can also select or clear the check box that enables or disables access by unauthenticated users.
4. Click **OK**.

**Change user settings in a Delivery Group through Studio**

The name of this page can appear as either **User Settings** or **Basic Settings**.

1. Select **Delivery Groups** in the Studio navigation pane.
2. Select a group and then click **Edit Delivery Group** in the Actions pane.
3. On the **User Settings** (or **Basic Settings**) page:
   a) In **Description**, type the text that the workspace displays to users.
   b) Set the time zone to match the Azure time zone.
   c) Select **Enable Delivery Group**.
   d) Set the maximum number of desktops per user.
4. Click **OK** to save settings.

**Add user access through the Citrix Cloud**

1. Sign in to Citrix Cloud and then click **View Library**.
2. On the desktops tile, click ellipsis (…) in the right corner.
3. Search for the users groups that are allowed access to the Delivery Group and add them to the list.
4. When finished, click the X to close the window.

Your Windows 10 virtual desktops are assigned to the groups added to the subscribers list.

**Step 5: Configure Citrix ADC VPX in Azure (optional)**

The Citrix ADC VPX virtual appliance is available as an image in the Microsoft Azure Marketplace. When you deploy Citrix ADC VPX on Microsoft Azure Resource Manager, you can use the Azure cloud comput-
Citrix Cloud

You can use Citrix Gateway load balancing and traffic management features for your business needs.

You can deploy Citrix ADC VPX instances on Azure Resource Manager in one of two ways:

- A standalone instance.
- A high availability pair in active-active or active-standby modes.

If you have users who connect from a remote location, configure Citrix ADC VPX in Azure to create secure connections between Citrix Workspace app and Windows 10 desktops.

When the deployment is complete, use the Remote Desktop Protocol (RDP) to connect to one of the Cloud Connector machines. When you connect, you continue to the Citrix ADC VPX configuration from the Citrix Gateway administration console.

For complete configuration information, see Deploying Citrix ADC VPX instance on Microsoft Azure.

After you configure Citrix ADC VPX in Azure, enable Citrix Gateway in Citrix Cloud.

To configure the Citrix Gateway settings for secure access

1. Log on to the management console using the Citrix Gateway administrator credentials. You do not need to configure more IP addresses. Click Skip.
2. In Host Name, DNS IP Address, and Time Zone, use the IP address and the DNS settings of the virtual network. The settings are on your Active Directory domain controller.
3. Click Done. You do not have to restart Citrix ADC VPX now.
4. On the Configuration tab, click Licenses and upload the necessary licenses to configure Citrix Gateway.
5. After the licenses upload, restart the appliance.
6. When the virtual machine restarts, log on again by using Citrix Gateway credentials.

Configure Citrix Virtual Desktops Essentials settings in Citrix Gateway

After you configure the previous settings, run the Quick Configuration Wizard in Citrix Gateway. For more information, see Configuring Settings with the Quick Configuration Wizard.

Configure Citrix Gateway for high availability and load balancing

In a Microsoft Azure deployment, a high availability configuration of two Citrix Gateway virtual machines is achieved by using the Azure load balancer. The load balancer distributes client traffic across the virtual servers configured on both the Citrix Gateway instances.

If the client traffic originates from the internet, deploy an external load balancer between the internet and the Citrix Gateway instances to distribute client traffic. For more information about this configuration, see Configure a high-availability setup with a single IP address and a single NIC.
You can also add inbound port 80 to the Citrix Gateway network security group to configure Citrix Gateway by using its public IP address. After the configuration is complete, you can delete the inbound port 80 rule to secure access to the management console.

**Step 6: Connect users**

Citrix Workspace delivers the service to user devices. In the Citrix Cloud console, select **Workspace Configuration** from the upper left menu.

After you create the first catalog, Virtual Desktops Essentials configures the workspace URL automatically. This URL appears under the catalog details. You can customize the workspace URL and the appearance of workspaces. You can also enable the preview version of federated authentication using Azure Active Directory. For details, see **Workspace configuration**.

1. In the Citrix Cloud console, select **Workspace Configuration** in the upper left menu. Select the **Service Integrations** tab. The service is listed.
2. Test your connection by logging on to the workspace URL with your domain credentials and starting a desktop.
3. Provide the URL to your users, which they can copy. Users can type or paste that URL in the address bar of their browser or Citrix Workspace app to access desktops.

**Remote access using Citrix ADC VPX**

1. In the Citrix Cloud console, click **Manage** and then click **Service Delivery**.
2. Enable **Citrix Gateway**.
3. Select **Use your own Citrix Gateway** in the resource location.
4. Type the Citrix Gateway address in the text field. Do not include a protocol. You can include a port number.
5. Enable session reliability, if you want that feature.
6. Save.
7. Test your connection by logging on to the workspace URL with your domain credentials and starting a desktop.
8. Provide the URL to your users, which they can copy. Users can type or paste the URL in the address bar of their browser or Citrix Workspace app to access desktops.

**Partner resources**

This service is also available through the Microsoft Cloud Solution Provider channel. For details, see **Microsoft CSP enablement for Citrix Essentials**.
Upgrade to Citrix Virtual Apps and Desktops Standard for Azure

Learn how to upgrade from Citrix Virtual Desktops Essentials to Citrix Virtual Apps and Desktops Standard for Azure.

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 scenario, 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.
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.