## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Level Agreement</td>
<td>3</td>
</tr>
<tr>
<td>Citrix Cloud Services Customer Content and Log Handling</td>
<td>5</td>
</tr>
<tr>
<td>Architectural Overviews</td>
<td>11</td>
</tr>
<tr>
<td>Secure Deployment Guide for the Citrix Cloud Platform</td>
<td>11</td>
</tr>
<tr>
<td>How to Get Help and Support</td>
<td>17</td>
</tr>
<tr>
<td>Third Party Notifications</td>
<td>21</td>
</tr>
<tr>
<td>Terminology</td>
<td>21</td>
</tr>
<tr>
<td>Sign up for Citrix Cloud</td>
<td>22</td>
</tr>
<tr>
<td>Geographical Considerations</td>
<td>39</td>
</tr>
<tr>
<td>Verify your email for Citrix Cloud</td>
<td>44</td>
</tr>
<tr>
<td>Citrix Cloud Service Trials</td>
<td>45</td>
</tr>
<tr>
<td>Extend Citrix Cloud service subscriptions</td>
<td>48</td>
</tr>
<tr>
<td>System Requirements</td>
<td>51</td>
</tr>
<tr>
<td>Internet Connectivity Requirements</td>
<td>52</td>
</tr>
<tr>
<td>Resource locations</td>
<td>55</td>
</tr>
<tr>
<td>Citrix Cloud Connector</td>
<td>57</td>
</tr>
<tr>
<td>Citrix Cloud Connector Technical Details</td>
<td>59</td>
</tr>
<tr>
<td>Cloud Connector updates</td>
<td>65</td>
</tr>
<tr>
<td>Cloud Connector Installation</td>
<td>66</td>
</tr>
<tr>
<td>Cloud Connector Proxy and Firewall Configuration</td>
<td>70</td>
</tr>
<tr>
<td>Identity and access management</td>
<td>72</td>
</tr>
<tr>
<td>Connect Active Directory to Citrix Cloud</td>
<td>74</td>
</tr>
<tr>
<td>Connect Azure Active Directory to Citrix Cloud</td>
<td>79</td>
</tr>
</tbody>
</table>
Citrix Cloud

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

Connect Okta as an identity provider to Citrix Cloud (Technical Preview)

Select a primary resource location

Citrix Workspace platform

Workspace configuration

Add an on-premises Site to Citrix Workspace

Workspace experience

Add administrators to a Citrix Cloud account

Assign users and groups to service offerings using Library

Monitor licenses and active usage for cloud services

Monitor licenses and active usage for Citrix Virtual Apps and Desktops service

Monitor licenses and active usage for Endpoint Management

Register on-premises products with Citrix Cloud

Monitor licenses and usage for on-premises deployments

Notifications

Features for Citrix Partners

Content Collaboration

Create or link a Content Collaboration (ShareFile) account to Citrix Cloud

Set up ShareFile

MDX Service

ITSM Adapter Service

License Usage Insights Service

Technical Details

Get started with the License Usage Insights Service
Use the License Usage Insights Service 200
Update and configure Citrix License Server 207
Frequently Asked Questions 210
Secure Browser service 211
Citrix Virtual Apps Essentials 223
Citrix Virtual Desktops Essentials 256
Citrix Cloud Labs 269
Session Manager 269
Connecting Session Manager to On-Premise XenApp and XenDesktop Deployments 277
Technical Security Overview for Session Manager and On-Premises XenApp and XenDesktop 289
Advanced Concepts 292
On-premises StoreFront Authentication Reference Architectures for Citrix Virtual Apps and Desktops service 292
Access control for SaaS and Web apps in StoreFront–Preview 296
Citrix Cloud

Service Level Agreement

June 14, 2019

Effective date: August 1, 2018

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 99.5% 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 “Un-available.” Services and the measure of availability for each are set forth in the table below. Monthly Uptime percentage measurements exclude downtime resulting from:

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

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

Citrix offers Service Commitments to customers that:

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

Citrix Service Providers (CSPs) are eligible on October 1, 2018.
## Per Service Availability Measures

<table>
<thead>
<tr>
<th>Service</th>
<th>Measure for Monthly Uptime</th>
</tr>
</thead>
<tbody>
<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>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>
<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>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>
<tr>
<td>Citrix Web App Firewall</td>
<td>Time that the web application firewall (WAF) is processing data and applying corresponding security policies</td>
</tr>
<tr>
<td>Intelligent Traffic Management</td>
<td>Time users can access traffic management functionality through DNS queries or HTTP API calls</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: < 99.5%
- 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.

Citrix Cloud Services Customer Content and Log Handling

August 13, 2019

Overview

This article describes the types of Customer Content and Logs that Citrix Cloud services collect. The Citrix Privacy Policy, available at https://www.citrix.com/about/legal/privacy.html, describes how Citrix uses and protects personal information that Citrix collects in connection with the operation of its business (e.g., in Marketing, Sales, Finance and Partner operations). By contrast, this article addresses the collection and handling of Customer Content and Logs in connection with the performance of Citrix Cloud services. In this capacity, Citrix acts as a “data processor” for its customers with respect to the handling of Customer Content. Further information may be found in the Citrix Data Processing Agreement.

The audience for this article is Security Officers, Compliance Officers, and Information Auditors and others whose role includes the handling of cloud data in their organization. This article only applies to Citrix Cloud platform regions, Citrix Virtual Apps and Desktops, Citrix Endpoint Management, and Citrix Content Collaboration services. Details for other services will be included in a future version of this article. This information is subject to change without notice.
The following terms are used in this article:

- **Customer Content** means any data uploaded to Customer’s account for storage or data in Customer’s computing environment to which Citrix is provided access in order to perform Services.
- **Log** means a record of events related to the Services, including records that measure performance, stability, usage, security, and support.
- **Personal Data** means any information relating to an identified or identifiable natural person (as further defined in Article 4 of the EU General Data Protection Regulation) to which Citrix is provided access in order to provide the Services described in this document.

Customer Content and Logs can include Personal Data, including but are not limited to proper names, user IDs, phone numbers, email and IP addresses.

**How Citrix handles Customer Content stored on its systems**

Customers determine the Customer Content that they choose to load to a Citrix-managed service and Citrix processes that data as a data processor for its Customers. Citrix does not have access to Customer Content that might contain Personal Data (for example, Microsoft Office files, databases, and so on) except as requested for support or troubleshooting, other than as described in service-specific sections in this article.

**Geographic location**

Citrix Cloud services are available across multiple regions (for example, EU, US, or Asia Pacific South). However, a customer’s cloud account can only be homed in one region. Once the customer chooses a region, the account cannot be moved between regions.

Logs may be replicated and accessed globally to support the Services, including auditing for performance of the Services, support or troubleshooting, and to allow for cross-region authentication (for example, when an EU-based Administrator needs to access a US-based service).

See [Geographical Considerations](#) for more details.

**Data collected across all Citrix Cloud services**

The Citrix Cloud platform collects the following Log data related to Citrix cloud-based services.

**Inflight and stored user Log data**

- Administrator user name
- Administrator first and last name
• Administrator email address
• Administrator phone number
• Administrator address
• Administrator country
• Administrator password
• End-User principal used to log on by end-users (example: domain\username)
• End-User name
• End-User, first and last name
• Common Active Directory (AD) properties for end-users

Inflight and stored device Log data

• Internet facing IP address used by the administrator to access the service (not stored)
• Active Directory attributes may also be seen in flight

Logging

For administrators, Citrix logs:
• Name (first name, last name, display name)
• Email address

For end-users, Citrix logs:
• Name (first name, last name, display name, and other AD properties containing the name).
• AD properties that typically contain the email address.
• Any AD properties, including custom properties, whose names do not match “email” “telephone” or “address.”

Backup

For all services, all inflight or stored Logs or Customer Content listed in this article may be included in backups. Citrix performs the following types of backups:
• Online backups may be made to any of the following services, depending on the Citrix Cloud service:
  – Azure Blob storage
  – AWS S3
  – AWS Elastic Block Store
  – Azure SQL
• One-way replication of data between Microsoft Azure and Amazon AWS.
• Offline or offsite backups are not made for any service.

Backups may contain any of the data discussed in this article and may be stored in different regions for redundancy.

**Third-party services that may store or process logs on behalf of Citrix**

Citrix may choose, when appropriate, to store or process logs within certain services. These third-party services are subject to change, and not all third party services are utilized by all Citrix Cloud services. Many of these services are US-based. For more details, see [Citrix Services Subprocessors](#).

**Citrix Virtual Apps and Desktops**

Citrix Virtual Apps and Desktops service does not collect, inspect or transfer Customer Content files (for example Microsoft Word and Excel files) from the virtual machines that end-users access. End-users' virtual machines are under customer’s control.

**Stored data**

No Customer Content or Logs are collected in addition to that listed in the section Data collected across all Citrix Cloud services in this article.

**Inflight data**

In addition to the common elements described above, the application and desktop service collects:

- End-user password
- Name of client device

**Citrix Managed Desktops**

Citrix Managed Desktops service does not collect, inspect or transfer Customer Content files (for example Microsoft Word and Excel files) from the virtual machines that end-users access. Responsibility for end-users’ virtual machines in Citrix Managed Azure IaaS is shared between the customer and Citrix. For more information, see [Managed Desktops Technical Security Overview](#).

**Stored data**

No Customer Content or Logs are collected in addition to that listed in the section Data collected across all Citrix Cloud services in this article.
Citrix Cloud

Inflight data

In addition to the common elements described above, the Managed Desktops service collects:

- End-user password
- Name of client device

Citrix Endpoint Management

Citrix Endpoint Management provides regional control planes for locations in US, EU, and Asia Pacific regions. Within each region there may be multiple locations. Some data such as email address may be used across regions (e.g., for auto discover service).

Inflight and stored data

User data inflight and stored:

- Citrix Endpoint Management cookies
- Connection details
- Google enterprise owner email address
- Mobile number (if applicable)

Device data (stored on per-region basis; backups of this data may be stored on other regions):

- Serial Number
- IMEI
- WiFi MAC address
- Bluetooth MAC address
- Memory and storage
- CPU type and speed
- OS version
- IP address
- Screen resolution
- Jailbreak status
- ActiveSync ID

Citrix Content Collaboration

Inflight stored data

User data:
Citrix Cloud

- User Password Hash
- Admin Security Question in its databases
- File and folder names in Logs

Customers may also contribute Personal Data as part of database field data (fields for File Name, Folder Name, and Notes are free-form text).

The document preview engine uses Microsoft Office 365 when customers have the O365 entitlement. Citrix native preview is used in several capabilities like Feedback, Approval, and View with watermark. Signature and workflow features similarly will be processed through Citrix RightSignature in the US. Any Personal Data contained in file names or file content may be processed by the Office 365 or Citrix native preview technologies or Citrix RightSignature.

Regional considerations

Citrix provides separate US and EU instances of the Citrix Content Collaboration control plane; Citrix does not transfer Customer Content between or outside of these regions. See Content Collaboration locations and Storage Zones for more details.

Lab services

Lab services are unsupported, may change over time, and may not necessarily become Citrix Cloud services. For more information, see Citrix Cloud Labs.

Frequently asked questions

Can I opt out from any logging or storage of the Logs mentioned in this article?
No, it is not possible to opt out of logging or storage of Logs. These are required to ensure that our services function optimally.

Are the products detailed in this document compliant with GDPR?
Citrix products and services are designed to facilitate your GDPR compliance by supporting GDPR requirements around data management, access, and security. Citrix has performed data protection impact assessments of its products and Citrix strives to provide functionality that will assist your ongoing compliance efforts. Citrix offers a Data Protection Addendum, including EU Standard Contractual Clauses (Processor), which are available at https://www.citrix.com/buy/licensing/citrix-data-processing-agreement.html.

What about other Citrix Cloud services not mentioned in this document?
Additional services in Citrix Cloud will be included in future revisions of this article.
Citrix Cloud

Architectural Overviews

June 25, 2019

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.


Tech Zone Reference Architectures: https://docs.citrix.com/en-us/tech-zone/design/reference-architectures.html


Secure Deployment Guide for the Citrix Cloud Platform

May 30, 2019


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

- Virtual Apps and Desktops Service Technical Security Overview
- Endpoint Management technical security overview
- Managed Desktops Technical Security Overview
- ShareFile Technical Security Overview
- Secure Browser Service 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.

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 with strong cipher suites.

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 and in the European Union. 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.
Audit and change control

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

Citrix has extensive internal auditing information. If a customer has a concern, they are advised to contact Citrix within 30 days. Citrix will review the audit logs to determine the administrator who performed an operation, the date on which it was performed, the IP address associated with the action, and so on.

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.

Additionally, the machines on which the Cloud Connector software is installed should be inside the customer’s private network and not in the DMZ. For network and system requirements and instructions for installing the Cloud Connector, see 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 will support customers who use other industry standard AV products.

In the customer’s Active Directory (AD) the Cloud Connector’s machine account should be restricted to read-only access. This is the default configuration in Active Directory. Additionally, the customer can enable AD logging and auditing on the Cloud Connector’s machine account to monitor any AD access activity.
**Logging on to the machine hosting the Cloud Connector**

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

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

**Installing additional software on Cloud Connector machines**

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

**Inbound and outbound ports configuration**

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

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

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

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

<table>
<thead>
<tr>
<th>Client Port(s)</th>
<th>Server Port</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>49152-65535/UDP</td>
<td>123/UDP</td>
<td>W32Time</td>
</tr>
<tr>
<td>49152-65535/TCP</td>
<td>135/TCP</td>
<td>RPC Endpoint Mapper</td>
</tr>
<tr>
<td>49152-65535/TCP</td>
<td>464/TCP/UDP</td>
<td>Kerberos password change</td>
</tr>
<tr>
<td>49152-65535/TCP</td>
<td>49152-65535/TCP</td>
<td>RPC for LSA, SAM, Netlogon (*)</td>
</tr>
<tr>
<td>49152-65535/TCP/UDP</td>
<td>389/TCP/UDP</td>
<td>LDAP</td>
</tr>
<tr>
<td>49152-65535/TCP</td>
<td>636/TCP</td>
<td>LDAP SSL</td>
</tr>
</tbody>
</table>
Citrix Cloud

<table>
<thead>
<tr>
<th>Client Port(s)</th>
<th>Server Port</th>
<th>Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>49152 - 65535/TCP</td>
<td>3268/TCP</td>
<td>LDAP GC</td>
</tr>
<tr>
<td>49152 - 65535/TCP</td>
<td>3269/TCP</td>
<td>LDAP GC SSL</td>
</tr>
<tr>
<td>53, 49152 - 65535/TCP/UDP</td>
<td>53/TCP/UDP</td>
<td>DNS</td>
</tr>
<tr>
<td>49152 - 65535/TCP</td>
<td>49152 - 65535/TCP</td>
<td>FRS RPC (*)</td>
</tr>
<tr>
<td>49152 - 65535/TCP/UDP</td>
<td>88/TCP/UDP</td>
<td>Kerberos</td>
</tr>
<tr>
<td>49152 - 65535/TCP/UDP</td>
<td>445/TCP</td>
<td>SMB</td>
</tr>
</tbody>
</table>

Each of the services used within Citrix Cloud will extend 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 listed as Use for subscriptions on the Identity and Access Management page in the Citrix Cloud user interface.

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

Each service within Citrix Cloud extends the list of servers and internal resources that the Cloud Connector might contact in the course of normal operations. Additionally, customers cannot control the data that the Cloud Connector sends to Citrix. For more information about services’ internal resources and data sent to Citrix, consult 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 will always use CAs that are part of the standard Windows Trusted Publisher list.

Each service within Citrix Cloud may 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 will self-manage. Do not disable reboots or put other restrictions on the Cloud Connector. These actions prevent the Cloud Connector from updating itself when there is a critical update.

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

Guidance for handling compromised accounts

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

**How to Get Help and Support**

August 22, 2019

**Creating a Citrix Cloud account**

If you encounter an error when signing up for a Citrix Cloud account, contact [Citrix Customer Service](mailto:).  

**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 signed in to Citrix Cloud in a while or if your password doesn’t meet Citrix Cloud’s requirements, Citrix Cloud automatically prompts you to reset your password before you can sign in. For more information, see Changing your password in this article.
If your company allows users to sign in to Citrix Cloud using their company credentials instead of a Citrix account, click **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, click **Forgot your username or password?** and you can enter your account email address. You’ll receive an email to reset your password. If you do not receive the password reset email, or you need additional assistance, contact **Citrix Customer Service**.

To help you 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.

**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 may also offer help or join the discussion.

You do not need to log in to read forum topics. However, you must log in to post or reply to a topic. To log 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, click the Feedback and Support icon near the top-right of the screen, and then select Open a Ticket.

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

The Citrix Knowledge Center provides a wealth of support content to help you resolve any issues you might experience with Citrix products.

For Citrix Cloud support articles, visit the Citrix Cloud section of the Knowledge Center.
Terminology

September 20, 2018

**Citrix Cloud:** A cloud-based control plane that is owned by Citrix and can be used by customers to provision services in their own data centers or into clouds.

**Citrix Cloud Connector:** Provides communication between the resources in the resource location and the Citrix Cloud. For more details about how the Cloud Connector works and requirements for setting it up, see **Citrix Cloud Connector**.

**Cloud service:** Cloud services provide the features that deliver the services subscribers need to perform their work. This includes creating and managing any infrastructure resources that might be needed.

**Library:** Contains the applications, desktops, or data that make up the offerings made available to subscribers. Administrators use the Library to create and manage their offerings and grant access to subscribers. For more information, see **Assign users and groups to service offerings using Library**.

**Offerings** (provided by the customer for subscribers): Applications, desktops, or data in the Library that a Citrix Cloud administrator assigns to subscribers. Offerings can be created through a Citrix Cloud service, like the Virtual Apps and Desktops service. Subscribers can access only the applications, desktops, and data to which they are assigned.

**Resource location:** Defines the place that contains the resources you use with Citrix Cloud services. Resource locations can reside in a public or private cloud or in your on-premises data center. There is
no limit to the number of resource locations you can create. The resources within a resource location are all within a defined communication or network boundary, where access is available to them from Citrix Cloud and to any other customer infrastructure required to operate. Connection to Citrix Cloud occurs through the Citrix Cloud Connector. For more information, see Resource locations.

**Resources:** The components that are used to provide the infrastructure for the Citrix Cloud services that you use. Resources include hypervisors, servers, network appliances, VDAs for Citrix Virtual Apps and Desktops, and so on. These components typically reside in resource locations in Citrix Cloud. For more information, see Resource locations.

**Subscriber:** A person who uses the Library offerings to which they are assigned by a Citrix Cloud administrator. A subscriber can access their offerings using Citrix Receiver or a workspace available as part of the Citrix Virtual Apps Essentials service.

**Workspace:** Consists of offerings that subscribers can access. Workspaces are available as part of the Citrix Virtual Apps Essentials service. For more information about using workspaces, see Workspace configuration.

**Sign up for Citrix Cloud**

December 5, 2018

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](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.
Sign up as an existing Citrix customer and new to Citrix Cloud

As an existing Citrix customer, this section helps you create a Citrix Cloud account using the right OrgID so you can continue to place orders on the same OrgIDs you’ve been using, without any change to how you have Citrix administrators set up in your company.

Step 1: Sign in with your Citrix.com credentials to create a Citrix Cloud account

Go to https://citrix.cloud.com and sign in with your existing Citrix account. This account is also known as a Citrix.com or My Citrix account.

This is the same account that you use to log in at Citrix.com. You either have a username (also known as web login) and password or an email and password.
What happens if the account is already in use?
If you see this message, it means that another valid administrator from your Citrix account has already created the Citrix Cloud account.

Since a Citrix Cloud account allows admins much greater control on the service, we expect that the first admin who creates the Citrix Cloud account has to explicitly give access to another admin, even if the other admin is already a member of the Citrix account.
Step 2: Pick your Citrix Cloud region

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

Why is this important? Help me decide.

- Asia Pacific South
- European Union
- United States

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

Continue

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.

**Step 3: Verify your email address**

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

To verify your OrgID, use one of the following methods:

- In the top-right corner of the management console, your OrgID is displayed beneath your account name.
- Click on **Account Settings** in the top right menu.
Your OrgID is shown in the Organization ID field.
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.
Sign up as a new Citrix customer

If you are new to Citrix and Citrix Cloud, this section helps you sign up for a new Citrix Cloud account and complete setup.

Step 1: Click to sign up for a new account

Go to https://citrix.cloud.com and click Sign up and try it free.
Step 2: Complete the signup form

Complete all the form fields and click Continue. Remember to use your business email address and business address. Using a personal email address or personal address could cause delays when requesting trials.

Step 3: Pick your Citrix Cloud region

A Citrix Cloud region is a geographical boundary within which Citrix may operate, store, and replicate 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.
Select a home region that best suits your performance and business needs.

Why is this important? Help me decide.

- Asia Pacific South
- European Union
- United States

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

Continue
Step 4: Verify your email address

If you have not verified your email address, you might be asked to verify it.
After you receive the verification email and confirm your email address, your Citrix Cloud account is active.

**Step 5: Pick a password**

Type and confirm your Citrix Cloud password to finish creating your account.
After your account is created, you can sign in to Citrix Cloud.

**Step 6: Invite administrators**

Congratulations, you set up your Citrix Cloud account! Before you start using Citrix Cloud, take a moment to invite at least one other administrators to help you manage your Citrix Cloud account.

To do this from the Citrix Cloud management console, click the menu button and select **Identity and Access Management**. For more information, see [Add administrators to a Citrix Cloud account](#).
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

July 31, 2019

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 the majority of your users and resources will be located.

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

Why is this important? Help me decide.

- Asia Pacific South
- European Union
- United States

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

Continue
**Important:**
You can choose a region only once, when your organization is onboarded. You cannot change your region later.

**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, username, and password.
- Data resulting from traffic directed through your region by any Citrix Cloud 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 there.

**Service presence in each region**

All services are globally available, regardless of the region you select for your organization. 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 located in a region that is different from the one you selected for your organization, certain information (such as authentication data) may 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>Citrix App Layering</td>
<td>Yes</td>
<td>No (Uses US region)</td>
<td>No (Uses US region)</td>
</tr>
<tr>
<td>Application Delivery Management</td>
<td>Yes</td>
<td>No (Uses US region)</td>
<td>No (Uses US region)</td>
</tr>
<tr>
<td>Citrix Content Collaboration</td>
<td>Yes ***</td>
<td>Yes ***</td>
<td>No - Select from US or EU **</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 Endpoint Management</td>
<td>Yes **</td>
<td>Yes **</td>
<td>Yes **</td>
</tr>
<tr>
<td>Citrix Managed Desktops</td>
<td>Yes *</td>
<td>Yes *</td>
<td>Yes *</td>
</tr>
<tr>
<td>SD-WAN Orchestration</td>
<td>Yes</td>
<td>No (Uses US region)</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>
<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>No (Uses US region)</td>
<td>No (Uses US region)</td>
</tr>
<tr>
<td>Citrix Cloud Labs services</td>
<td>Yes</td>
<td>No (Uses US region)</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>
</tbody>
</table>

* Service uses the Citrix Cloud region.

** ** Select from multiple locations across multiple regions. See below.

*** *** StorageZone can be selected from multiple locations. See below.

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

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 StorageZones around the world including choosing a new default zone. You can also specify a default specific to individual users or folders based on the StorageZones that are turned on in the Content Collaboration management console. You can choose from the following locations:

- Japan
FAQ

- Are there performance impacts if I’m in one region and use a service in another region? Citrix Cloud Services are designed to be used on a global basis. For example, customers in the US that have users and Cloud Connectors in Australia will see minimal impact from latency.
- If I’m not in the US or EU, can I still use Citrix Cloud? Yes, you can simply pick the region that is either closest to the majority of your users or that provides the best controls for protecting the integrity of your data.

Verify your email for Citrix Cloud

April 6, 2018

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

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

FAQ

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

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

I haven’t received an email. What do I do? Perform the following steps:
Search your inbox for an email from “Citrix.”
- If it’s not in your inbox, check your folders. If a spam filter or email rule moved the email, it might be in your spam or trash folders.
- Ensure you’re checking the correct email account. Citrix sends the verification email to the email address currently on file for your account. Often, this is the email address you originally signed up with for Citrix Cloud or the one with which you were invited to join the Citrix Cloud account.

Contact Citrix Technical Support

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

Citrix Cloud Service Trials

May 30, 2019

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.

Available Services (13)

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
Citrix Cloud

<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/buy.html.

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

May 20, 2019

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 automatically renewed each month, such as Virtual Apps and Desktops Essentials, and services that do not automatically renew, such as Virtual Apps and Desktops service.

Before expiration

For services that are automatically renewed each month, Citrix Cloud does not send notifications prior to expiration.

For services that are not automatically renewed, 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 services that renew automatically each month and services that don’t renew automatically.
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 you to continue accessing the service for five days. If you don’t extend your subscription during this 5-day grace period, Citrix blocks users from accessing the service. 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 5-day grace period ends, administrators can continue accessing the service for 25 additional days. If you don’t extend your subscription during this period, Citrix blocks administrators from accessing the service.

Non-renewing service subscriptions

For services that don’t renew automatically, 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 services: Users are blocked from access. Administrators are blocked from access after 30 days past the expiration date (5-day grace period plus 25 days of continued access).
- For expired services that don’t renew automatically, 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 90 days after the service expiration date. If you extend your subscription before the 90-day retention period ends, your administrators and users can access the service with your data intact. Your extended subscription starts as follows:

- For monthly services, 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 services that don’t renew automatically, the start date of your extended subscription is the date you purchase the extension.

If you don’t extend your subscription before the 90-day 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 90-day 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 90-day 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/buy.html](https://www.citrix.com/products/citrix-cloud/buy.html).

To complete the purchase, you’ll need your Organization ID, available in the Citrix Cloud management console.
System Requirements

September 20, 2018

Citrix Cloud requires the following minimum configuration:

- An Active Directory domain
- Two physical or virtual machines 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, see Virtual Apps and Desktops System Requirements.

Supported web browsers

- Latest version of Google Chrome
- Latest version of Mozilla Firefox
- Latest version of Microsoft Edge
Internet Connectivity Requirements

September 13, 2019

Citrix Cloud provides administrative functions (through a web browser) and operational requests (from other installed components) that connect to resources within a customer’s deployment. This document defines the requirements and considerations for establishing connectivity between the customer’s resources and Citrix Cloud.

Overview

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.

Required addresses

The following addresses need to be contactable to properly operate and consume the Citrix Cloud services.

Citrix Workspace

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

For Content Collaboration and Citrix Files and Workspace, Citrix recommends whitelisting the domains listed in CTX208318.

Content Collaboration

Citrix resource location / Cloud Connector:

- https://*.sharefile.com
- Additional requirements: ShareFile Firewall Configuration and IP Address (CTX208318)
Citrix Cloud

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

Secure Browser

Citrix resource location / Cloud Connector:
- https://*.citrixworkspacesapi.net
- https://*.cloud.com
- https://*.servicebus.windows.net

Administration console:
- https://*.cloud.com
- https://*.citrixworkspacesapi.net
- https://browser-release-b.azureedge.net

Virtual Apps and Desktops service

Citrix resource location / Cloud Connector:
- https://*.citrixworkspacesapi.net
- https://*.cloud.com
- https://*.blob.core.windows.net
- https://*.nssvc.net
- If Citrix Gateway service is enabled
- https://*.servicebus.windows.net
- https://*.xendesktop.net
- https://*.cloudapp.net

Administration console:
- https://*.citrixworkspacesapi.net
- https://*.cloud.com
- https://*.blob.core.windows.net
- https://*.xendesktop.net

Endpoint Management

Citrix resource location / Cloud Connector:
Citrix Cloud

- https://*.citrixworkspacesapi.net
- https://*.cloud.com
- https://*.blob.core.windows.net
- https://*.servicebus.windows.net
- https://*.cloudapp.net

Administration console:

- https://*.citrix.com
- https://*.citrixworkspacesapi.net
- https://*.cloud.com
- https://*.blob.core.windows.net

Gateway

- https://*.netscalergateway.net

Workspace Environment Management

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

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.

Citrix Cloud Connector

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

For requirements for installing the Cloud Connector, see System requirements. To operate, the Cloud Connector requires outbound connectivity on port 443. After installation, the Cloud Connector might have additional access requirements depending on the Citrix Cloud service with which it is being used.

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.

Resource locations

April 25, 2019

Resource locations contain the resources required to deliver cloud services to your subscribers. You manage these resources from the Citrix Cloud console.

To create a resource location, you install at least two Citrix Cloud Connectors in your domain. The 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:

- Deployment scenarios for Cloud Connectors in Active Directory
- Cloud Connector Technical Details
- Cloud Connector Installation
- Cloud Connector Proxy and Firewall Configuration

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.
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 XenServer
- 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

**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.

**Naming restrictions**

The following characters are not allowed when creating names for resource locations:

- #, $, %, ^, &, ?
- Braces: [ ], { }
- Pipes (|)
- Less-than symbol (<)
- Forward and backward slashes (/, \)

**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 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.

**Example of 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.

**Citrix Cloud Connector**

March 20, 2019

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. Citrix Endpoint Management requires the Cloud Connector for enterprise connectivity to the Endpoint Management service.

**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 `cwconnector.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 `cwconnector.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 or Windows Server 2016. 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**

August 27, 2019

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

**System requirements**

The 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**

Windows Server 2012 R2 or Windows Server 2016 is supported.

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

**.NET requirements**

Microsoft .NET Framework 4.7.2 or later is required.
Server requirements

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

Certificate validation requirements

The Cloud Connector software is signed with a code signing certificate which is validated when the software is installed. All Cloud Connector machines must be configured to trust the root and intermediate certificates to ensure the Cloud Connector software can be installed successfully.

The following certificates must be installed on each Cloud Connector machine:

- https://dlcacerts.digicert.com/DigiCertAssuredIDRootCA.crt

To validate the certificates, all Cloud Connector machines must be able to contact the following addresses:

- http://*.digicert.com
- https://*.digicert.com

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

Active Directory requirements

- Joined to an Active Directory domain that contains the resources and users that you 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 both the parent (root) and domain controllers in the Active Directory infrastructure (to complete the Active Directory workflows) where the Cloud Connector is installed. For more information, see the following Microsoft support articles:
  – How to configure domains and trusts
  – Systems services ports

Network requirements

• Connected to a network that can contact the resources you will use in your resource location. For more information, see Cloud Connector Proxy and Firewall Configuration.
• Connected to the Internet. For more information, see Internet Connectivity Requirements.

Supported Active Directory functional levels

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

<table>
<thead>
<tr>
<th>Forest Functional Level</th>
<th>Domain Functional Level</th>
<th>Supported Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows Server 2008 R2</td>
<td>Windows Server 2008 R2</td>
<td>Windows Server 2008 R2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2012,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2012 R2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Windows Server 2008 R2</td>
<td>Windows Server 2012</td>
<td>Windows Server 2012,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2012 R2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Windows Server 2008 R2</td>
<td>Windows Server 2012 R2</td>
<td>Windows Server 2012 R2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Windows Server 2012</td>
<td>Windows Server 2012</td>
<td>Windows Server 2012,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2012 R2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Windows Server 2012</td>
<td>Windows Server 2012 R2</td>
<td>Windows Server 2012 R2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2016</td>
</tr>
<tr>
<td>Windows Server 2012 R2</td>
<td>Windows Server 2012 R2</td>
<td>Windows Server 2012 R2,</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Windows Server 2016</td>
</tr>
</tbody>
</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.

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:

- 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.
Troubleshoot the Cloud Connector

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

If the Cloud Connector is “disconnected” and the event logs don’t indicate why a the Cloud Connector can’t connect to Citrix Cloud, contact Citrix Support.

If the Cloud Connector is in an “error” state, there might be a problem hosting the Cloud Connector. Install the Cloud Connector on a new machine. If the issue persists, contact Citrix Support.

To troubleshoot common issues with installing or using the Cloud Connector, see CTX221535.

Cloud Connector updates

August 12, 2019

Periodically, Citrix releases updates to increase the performance, security, and reliability of the Cloud Connector. To install these updates timely without unduly affecting your users’ Citrix Cloud experience, you can choose when these updates are installed.

Choose an update schedule

By default, Citrix Cloud installs updates on each Cloud Connector, one at a time, as soon as updates become available. To 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.

©1999-2019 Citrix Systems, Inc. All rights reserved.
3. Under **Choose your update method**, select **Set a maintenance start time** and choose the time of day for installing updates.

The start time you select is applied to all Cloud Connectors regardless of the timezone in which they are located. If you have Cloud 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 Cloud Connectors located in London, Citrix Cloud starts to install the update on those Cloud Connectors at 2:00 AM US Pacific time.

**Unscheduled updates**

Even if you choose a preferred time 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 Cloud Connector is offline for three days following the update release, Citrix Cloud installs the update immediately when the Cloud Connector is back online.
- The update contains a fix for a critical security or feature issue.

**Cloud Connector Installation**

September 4, 2019

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

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

**Information to review before installation**

- **System requirements**: To prepare the machines you’ll use for hosting the Cloud Connector.
- **Antivirus Exclusions** section of the **Endpoint Security and Antivirus Best Practices** 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 perform rigorous testing in a lab environment before applying them to a production environment.
• **Internet 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**

• Do not install the Cloud Connector on an Active Directory domain controller or any other machine critical to your resource location infrastructure. **Regular maintenance** on the Cloud Connector will perform machine operations that will cause an outage to these additional resources.

• Do not download or install other Citrix products on the machines hosting the Cloud Connector.

• Do not download or install the Cloud Connector on machines that are part of other Citrix product deployments (for example, Delivery Controllers in a Citrix Virtual Apps and Desktops deployment).

• Do not 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 the machine needs to be joined to be a different domain, uninstall the Cloud Connector and then re-install it after the machine is joined to the different domain.

• After installation, keep all Cloud Connectors powered on at all times 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 will install the Cloud Connector. The machine should have Windows Server 2012 R2 or Windows Server 2016 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. Launch the Cloud Connector installer. 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 additional 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 over a period of time is not recommended. Download a new Cloud Connector from the Resource Locations page in the Citrix Cloud console.

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

**Supported parameters**

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

- **/Customer**: 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**: Required. The unique identifier for an existing resource location. To retrieve the ID, click the ID button for the resource location on the Resource Locations page in the Citrix Cloud console. If no value is specified, Citrix Cloud uses the ID of the first resource location in the account.
- **/AcceptTermsOfService**: Required. Default value is **Yes**.

A sample command line with all required parameters:

```bash
CWConnector.exe /q /Customer:*Customer* /ClientId:*ClientId* /ClientSecret:*ClientSecret* /ResourceLocationId:*ResourceLocationId* /AcceptTermsOfService:*true*
```
Exit codes

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

Installation Logs

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

Cloud Connector Proxy and Firewall Configuration

April 9, 2019

The Cloud Connector supports connection to the Internet through a web proxy server. Both the installer and the services it installs need connections to Citrix Cloud. 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 Internet Connectivity Requirements. When whitelisting these addresses, wildcards (*) are supported.

The required contactable addresses for Citrix Cloud are specified as FQDNs, not IP addresses. Because IP addresses might change, whitelisting FQDNs ensures that the connection to Citrix Cloud remains stable. Additionally, as Citrix continually improves and augments the Citrix Cloud platform, whitelisting 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. Whitelisting at the subdomain level increases the risk of outage as these functions might use subdomains the customer hasn’t whitelisted. Whitelisting the wildcard domain allows these functions to work without placing an undue burden on the customer to whitelist 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](#).

**Installer**

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

See [How to configure proxy server settings in Windows 8](#) for details of how to configure the proxy settings.

**Services at Runtime**

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

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

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

After executing the command, restart the 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.

**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 whitelisted. 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.
Identity and access management

July 8, 2019

Identity and Access Management

Identity and Access Management defines the identity providers and accounts used for administrators of and subscribers to Citrix Cloud and its offerings.

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

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. The administrator 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 [Add administrators to a Citrix Cloud account](#).

**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.

**Tip:** Add customerservice@citrix.com to your email whitelist to ensure the email doesn’t land in your spam or trash folders.

**Remove administrators**

You can remove administrators from your Citrix Cloud account on the Administrator 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 Cloud Connectors in each forest. Citrix recommends at least two Cloud Connectors to maintain a high availability environment.

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

**Manage subscriber usage**

You can add subscribers to offerings using individual accounts or Active Directory groups. Using Active Directory groups does not require management through Citrix Cloud 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 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**

August 19, 2019

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 or Google Authenticator.

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 Device registration.

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

**Connect Azure Active Directory to Citrix Cloud**

July 8, 2019

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](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 are an XME customer, you will have to grant Microsoft Intune-related read-write permissions.
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 Add administrators to a Citrix Cloud account. 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](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:**


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.

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 Citrix Identity administrators 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 17, 2019

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

By using Citrix Gateway authentication, you can:

- Continue authenticating users through your existing Citrix Gateway so they can access the resources in your on-premises Virtual Apps and Desktops deployment through Citrix Workspace.
- Use the Citrix Gateway authentication, authorization, and auditing (AAA) functions with Citrix Workspace.
- Use features such as pass-through authentication, smart cards, secure tokens, conditional access policies, federation, and many others while providing your users access to the resources they need through Citrix Workspace.
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 Internet Connectivity Requirements.
- Citrix recommends two servers for Cloud Connector high availability. After installation, the Cloud Connectors allow Citrix Cloud to locate and communicate with your Site.

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

Active Directory

Before enabling Citrix Gateway authentication, perform the following tasks:

- Verify that your workspace subscribers have user accounts in Active Directory (AD). Subscribers without AD accounts can’t sign in to their workspaces successfully.
- Ensure that the user properties in your subscribers’ AD accounts are populated. Citrix Cloud requires these properties to establish the user context when subscribers sign in. If these properties aren’t populated, subscribers can’t sign in to their workspace. These properties include:
  - Email address
  - Display name
  - Common name
  - SAM account name
  - User Principal Name
  - OID
  - SID
Connect your Active Directory (AD) to your Citrix Cloud account. In this task, you install the Cloud Connector software on the servers you prepared, as described in the Cloud Connectors section. The Cloud Connectors enable Citrix Cloud to communicate with your on-premises environment. For instructions, see Connect Active Directory to Citrix Cloud.

If you are performing federation with Citrix Gateway authentication, synchronize your AD users to the federation provider. Citrix Cloud requires the AD user attributes for your workspace subscribers so they can sign in successfully.

Requirements

Citrix Gateway advanced policies

Citrix Gateway authentication requires the use of advanced policies on the on-premises Gateway due to deprecation of classic policies. Advanced policies support multi-factor 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**.

   ![Identity and Access Management](#)

   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  Detect

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.
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.
Citrix Cloud

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.
- 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.
- 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.
Default password for multi-factor authentication

If you use multi-factor 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 (Technical Preview)

September 10, 2019

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.

Note:

Okta authentication is currently in Technical Preview. Citrix recommends using technical preview features only in test environments.

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 Internet Connectivity Requirements.

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

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

- okta.com
- okta-eu.com
- oktapreview.com

You can also use Okta custom domains with Citrix Cloud. Review the important considerations for using custom domains in Customize the Okta URL domain on the Okta web site.

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

Okta OIDC web application

To use Okta as an identity provider, you must first create an Okta OIDC web application with client credentials you can use with Citrix Cloud. After you create and configure the application, note the Client ID and Client Secret. You supply these values to Citrix Cloud when you connect your Okta organization.

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

- Create an Okta OIDC web 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 Okta Active Directory agent Deployment on the Okta web site. Afterward, you import your AD users and groups to Okta. When importing, include the SID, UPN, and OID values associated with your AD accounts.

**Note:**

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

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

1. Install and configure the Okta AD agent. For complete instructions, see Install and configure the Okta Active Directory agent on the Okta website.
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, see Import Active Directory Users 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:
      - 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
Citrix Cloud

- 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 into 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

1. Sign into Citrix Cloud at **https://citrix.cloud.com**.
2. From the Citrix Cloud menu, select **Identity and Access Management**.
3. Locate **Okta** and select **Connect** from the ellipsis menu.
4. In **Okta URL**, enter your Okta domain.
5. In **Okta API Token**, enter the API token for your Okta organization.
6. In **Client ID** and **Client Secret**, enter the 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.

Select a primary resource location

December 5, 2018

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 (2) Cloud Connectors.

To decide which resource location you want to use for your primary resource location, consider the following:

- Does the resource location have the best connectivity to your domain?
- Is the resource location the closest to the geographical region in which you use the Citrix Cloud management console? For example, if your Citrix Cloud console is at https://us.cloud.com, the resource location you choose would be the closest one to the US region.

To select a primary resource location

1. From the Citrix Cloud management console, click the menu button and select **Identity and Access Management**.
2. Click **Domains** and then expand the domain containing the resource location you want to use.
3. Click **Set Primary Resource Location** and then select the resource location you want to designate as primary.
4. Click **Save**. Citrix Cloud displays “Primary” next to the resource location you selected.
Note:
Be sure to save your selections in one domain before expanding a different domain. When you expand a domain and then expand another domain, the previously expanded domain collapses and discards any unsaved selections.

Select a different primary resource location

1. From the Citrix Cloud management console, click the menu button and select **Identity and Access Management**.
2. Click **Domains** and then expand the domain that contains the primary resource location you want to change.
3. Click **Change Primary Resource Location** and then select the resource location you want to use.
4. Click **Save**.

Reset a primary resource location

Resetting the primary resource location allows you to remove the “Primary” designation from a resource location without selecting a different one. When you remove the “Primary” designation, any of the Cloud Connectors in the domain can handle user logon operations. As a result, some users might experience slower logons.

1. From the Citrix Cloud management console, click the menu button and choose **Identity and Access Management**.
2. Choose **Domains** and then expand the domain that contains the primary resource location you want to change.
3. Choose **Change Primary Resource Location** and then choose **Reset**. A notification appears, warning you that logon performance might be affected.
4. Select **I understand the potential impact to subscribers** and then click **Confirm Reset**.

Citrix Workspace platform

June 4, 2019

Citrix Workspace platform is a foundational component of Citrix Cloud that enumerates and delivers all your digital workspace resources to the Citrix Workspace user experience.
Important:
The following addresses need to be contactable in order to properly operate and consume Citrix Workspace:

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

For a full listing of Citrix Cloud connectivity requirements, see [Internet Connectivity Requirements](#).

**Workspace overview**

This screenshot is an example of what Citrix Workspace looks like to your users. This interface is evolving and may look different to what they are working with today. For example, it will only include Files if your organization has subscribed to the Content Collaboration service.

For an overview of what's new in Citrix Workspace, see [Citrix Workspace experience](#) and look out for [Citrix Cloud: What's New](#) blogs.

![Citrix Workspace interface](image)

**Note:**

When you first subscribe to the Virtual Apps and Desktops service or the Secure Browser service, the integration to Citrix Workspace is enabled by default. All other new services that your orga-
Citrix Cloud

Organizations subscribe to are disabled by default. You can enable or disable each service from the Service Integrations tab on the Workspace Configuration page. You can disable access to Citrix Workspace for all users in Workspace Configuration > Access.

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 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.

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 service

The Citrix Gateway service (formerly NetScaler Gateway Service) provides secure remote access with Identity and Access Management (IdAM) capabilities, delivering 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.

Content Collaboration service

The Content Collaboration service (formerly ShareFile) provides secure data access, sync, and sharing of files from any device. Follow the steps to set up the Content Collaboration service, then test and share the workspace URL with your subscribers to give them access to Files.

Secure Browser service

The Secure Browser service protects the corporate network from browser based attacks by isolating web browsing. When subscribers (users) navigate to the URL provided by the administrator, their published browsers are shown, along with other apps and desktops that are configured for them 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 the Citrix Gateway service.
Citrix Cloud

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 set up 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.

Workspace configuration

October 8, 2019

This article shows administrators how to configure workspaces for subscribers, who might be using one or more services available from Citrix Cloud.

Important:

The following addresses need to be contactable in order to properly operate and consume Citrix Workspace:

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

For a full listing of Citrix Cloud connectivity requirements, see Internet Connectivity Requirements.

To configure workspaces, from the Citrix Cloud menu, select Workspace Configuration.
Change access to workspace

In Citrix Cloud > Workspace Configuration > Access, the Workspace URL is ready to use.
Notes:
- In Citrix Virtual Apps Essentials, Workspace Configuration is available from the Citrix Cloud menu after you create the first catalog.
- Workspace does not support connections from legacy clients that use a PNAgent URL to connect to resources. If your environment includes these legacy clients, you must instead deploy StoreFront on-premises and enable legacy support. To secure these client connections, use Citrix Gateway on-premises instead of the Citrix Gateway service.

Enable and disable services

You can enable or disable the availability of individual service resources from the Service Integrations tab. By default, the Virtual Apps and Desktops service and the Secure Browser service are enabled after you subscribe to them. All other new services that your organization subscribes to are disabled by default.

Note:
The Citrix App Essentials service, Citrix Desktop Essentials service, and Citrix Virtual Apps and Desktops service display as “Citrix Virtual Apps and Desktops service” in the Service Integrations tab.

To enable workspace integration for a service

1. Go to Workspace Configuration > Service Integrations.
2. Select the ellipsis button next to the service and then select Enable.
3. To disable integration, select the ellipsis button next to the service and then select Disable.
To disable workspace integration for a service

Important:
Disabling workspace integration blocks subscriber access for that service. This does not disable the workspace URL, but subscribers will no longer have access to data and applications from that service in Citrix Workspace.

1. Go to Workspace Configuration > Service Integrations.
2. Select the ellipsis button next to the service and then select Disable.
3. When prompted, click Confirm to acknowledge that subscribers will no longer have access to data or application from the service.
Subscribers will no longer have access to data and applications from this service in Citrix Workspace

Are you sure you want to disable workspace integration for Virtual Apps and Desktops?

Customize the workspace URL

The first part of the workspace URL is customizable. You can change the URL from, for example, https://example.cloud.com, to https://newexample.cloud.com.

Important:

The first part of the workspace URL represents the company or organization using the Citrix Cloud account, and must comply with the Citrix End User Services Agreement. Any misuse of a third party's intellectual property rights including trademarks may result in the revocation and reassignment of the workspace URL and/or the suspension of the Citrix Cloud account.

From the Citrix Cloud menu, go to Workspace Configuration > Access, and select the Edit link next to the workspace URL.

Guidance for new URLs:

- The customizable part of the URL ("newexample") must be between 6 and 63 characters long. If you want to change the customizable part of the URL to fewer than 6 characters, please open a ticket in Citrix Cloud.
- Must consist of only letters and numbers.
- Cannot include Unicode characters.
- When you rename a URL, the old URL is immediately removed and no longer available.
- If you change the workspace URL, your subscribers cannot access their workspaces until the new URL is active (takes about 10 minutes). You’ll also need to tell them what the new URL is and manually update all local Citrix Receiver apps to use the new URL.
You can change the workspace URL only when it is enabled. If the URL is disabled, you must re-enable it first. Re-enabling the workspace URL can take up to 10 minutes to take effect.

**Disable the workspace URL**

You can disable the workspace URL to prevent users from authenticating through Workspace. For example, you might prefer subscribers use an on-premises StoreFront URL to access resources or you want to prevent workspace access during maintenance periods.

Disabling or re-enabling the workspace URL can take up to 10 minutes to take effect. After the workspace URL is disabled, Citrix Cloud parks the domain so it can’t be accessed. Anyone visiting the URL receives a 404 message in their browser.

Disabling the workspace URL has the following effects:

- All service integrations are disabled. Subscribers will no longer have access to data and applications from all services in Citrix Workspace.
- You cannot customize the workspace URL. You must re-enable the URL before you can change it.

**External connectivity**

Provide secure access for your remote subscribers by adding Citrix Gateways or the Citrix Gateway service to the resource locations.

You can add Citrix Gateways from **Workspace Configuration > Access > External Connectivity** or from **Citrix Cloud > Resource Locations**.
Note:

The External Connectivity part of the Workspace Configuration > Access page is not available in Citrix Virtual Apps Essentials. The Citrix Virtual Apps Essentials service uses the Citrix Gateway service, which requires no additional configuration.

Change authentication to workspaces

Change how subscribers authenticate to their workspace in Workspace Configuration > Authentication > Workspace Authentication.
As an administrator, you can choose to have your subscribers (end users) authenticate to their workspaces using Active Directory, Active Directory plus token, or Azure Active Directory. These authentication options are available to any Citrix Cloud service, including access control.

Access control is a feature that delivers access for end users to SaaS, web, and virtual apps with a single sign-on (SSO) experience.

Important:

Switching authentication modes can take up to five minutes and causes an outage to your subscribers during that time. Citrix recommends limiting changes to the authentication methods to periods of low usage. If you do have subscribers logged on to Citrix Workspace using a browser or Citrix Workspace app, please advise them to close the browser or exit the app. After waiting approximately five minutes, they can log back on again using the new authentication method.

Active Directory

By default, Citrix Cloud uses Active Directory to manage subscriber authentication to workspaces. Using Active Directory requires that you have a Citrix Cloud Connector installed in the on-premises Active Directory domain. For more information about installing the Cloud Connector, see Cloud Connector Installation.

Active Directory plus token

For additional security, Citrix Workspace supports a token as a second factor of authentication in addition to Active Directory sign-in.
When you use Active Directory plus token authentication, Workspace prompts all subscribers during every sign-in to enter a token from their enrolled device. Currently, subscribers configured with Active Directory plus token authentication can enroll only one device at a time.

Active Directory plus token authentication has the following requirements:

- A connection between Active Directory and Citrix Cloud, with at least two Cloud Connectors installed in your on-premises environment. For requirements and instructions, see Connect Active Directory to Citrix Cloud.
- In the Citrix Cloud console, Active Directory + Token authentication enabled on the Identity and Access Management page. For more information, see To enable Active Directory plus token authentication.
- Subscribers need access to email to enroll devices.
- During first-time sign-in to Workspace, subscribers follow the prompts to download the Citrix SSO app. The Citrix SSO app generates a unique one-time password on an enrolled device every 30 seconds.

To re-enroll devices

If a subscriber no longer has their enrolled device or needs to re-enroll it (for example, after erasing all content from the device), Workspace provides the following options:

- Subscribers can re-enroll their devices using the same enrollment process described in Device registration. Because subscribers can enroll only one device at a time, enrolling a new device or re-enrolling an existing device removes the previous device registration.
- Administrators can search for subscribers by Active Directory name and reset their device. To do that, go to Identity and Access Management > Recovery.
During the next sign-on to Workspace, the subscriber experiences the first-time enrollment steps described in Device registration.

**Azure Active Directory**

Use of Azure Active Directory (AD) to manage subscriber authentication to workspaces has the following requirements:

- Azure AD with a user who has global administrator permissions.
- A Citrix Cloud Connector installed in the on-premises Active Directory domain. The machine must also be joined to the domain that is syncing to Azure AD.
- VDA version 7.15.2000 LTSR CU VDA or 7.18 current release VDA or higher.
- A connection between Azure AD and Citrix Cloud. For information, see Connect Azure Active Directory to Citrix Cloud. When syncing your Active Directory to Azure AD, the UPN and SID entries must be included in the sync. If these entries are not synchronized, certain workflows in Citrix Workspace will fail.

**Warning:**

- If you are using Azure AD, do not make the registry change described in CTX225819. Making this change may cause session launch failures for Azure AD users.
- Adding a group as a member of another group (nesting) is not supported for federated authentication using Azure AD. If you do assign a nested group to a catalog, members of that group can't access apps from the catalog.

After enabling Azure AD authentication:

- **Manage users and user groups by using Citrix Cloud Library:** Use only the Citrix Cloud Library to manage users and user groups. (Do not specify users and user groups when creating or editing Delivery Groups.)
**Added security:** Users are prompted to sign in again when launching an app or a desktop. This is intentional and provides more security, because the password information flows directly from user’s device to the VDA that is hosting the session.

**Sign-in experience:** Users have a different sign-in experience in Azure AD. Selecting Azure AD authentication provides federated sign-in, not single sign-on. Users sign in to workspace from an Azure sign-in page, however they may have to authenticate a second time when opening an app or desktop from the Citrix Virtual Apps and Desktops service. You can customize the sign-in experience for Azure AD. For information, see the [Microsoft documentation](#). Any sign-in customizations (the logo) made in Workspace Configuration do not affect the Azure AD sign-in experience.

The following diagram shows the sequence of Azure AD authentication.

![Diagram of Azure AD authentication sequence](image)

**Citrix Gateway**

Citrix Workspace supports using an on-premises Citrix Gateway as an identity provider to manage subscriber authentication to workspaces.
Citrix Cloud

Citrix Gateway authentication has the following requirements:

- A connection between your Active Directory and Citrix Cloud. For requirements and instructions, see Connect Active Directory to Citrix Cloud.
- Subscribers must be Active Directory users to sign in to their workspaces.
- If you are performing federation, your AD users must be synchronized to the federation provider. Citrix Cloud requires the AD attributes to allow your users to sign in successfully.
- An on-premises Citrix Gateway:
  - Citrix Gateway 12.1 54.13 Advanced edition or later
  - Citrix Gateway 13.0 41.20 Advanced edition or later
- Citrix Gateway authentication is enabled on the Identity and Access Management page. This action generates the client ID, secret, and redirect URL required to create the connection between Citrix Cloud and your on-premises Gateway.
- On the Gateway, an OAuth IDP authentication policy is configured using the generated client ID, secret, and redirect URL.

For more information, see Connect an on-premises Citrix Gateway as an identity provider to Citrix Cloud.

**Okta (Technical Preview)**

Citrix Workspace supports using Okta as an identity provider to manage subscriber authentication to workspaces.

**Note:**

Okta authentication is currently in Technical Preview. Citrix recommends using technical preview features only in test environments.

Okta authentication has the following requirements:

- A connection between your on-premises Active Directory and your Okta organization.
- An Okta OIDC web application configured for use with Citrix Cloud. To connect Citrix Cloud to your Okta organization, you need to supply the Client ID and Client Secret associated with this application.
- A connection between your on-premises Active Directory domain and Citrix Cloud, with Okta authentication enabled on the Identity and Access Management page.

For more information, see Connect Okta as an identity provider to Citrix Cloud.

**User sign-out experience**
**Important:**

If Citrix Workspace times out in the browser due to inactivity, subscribers remain signed in to Azure AD. This is by design, to prevent a Citrix Workspace timeout from forcing other Azure AD applications to close.

To close Citrix Workspace, use **Settings > Log Off**. That option completes the sign-out process from the workspace and Azure AD. If subscribers close the browser instead of using the **Log Off** option, they might remain signed in to Azure AD.

**Customize the appearance of workspaces**

To customize how subscribers see their workspace, change the settings in **Workspace Configuration > Customize > Appearance** and **Save**.
Changes to the workspace appearance take effect right away. Local Citrix Receiver apps may take around five minutes for the updated user interface to display.

**Note:**

The Workspace Preview does not show a preview if you are currently working with the older “purple” user interface.

<table>
<thead>
<tr>
<th>Logo</th>
<th>Required Dimensions</th>
<th>Max. size</th>
<th>Supported formats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sign-in logo</td>
<td>350 x 120 pixels</td>
<td>2 MB</td>
<td>JPEG, JPG, or PNG</td>
</tr>
</tbody>
</table>
Logos that do not match the required dimensions may appear distorted.

The **Sign-in** logo appears on the workspace sign-in form. You can replace the Workspace logo with your own. The colors and branding of the rest of the sign-in page are not affected.

Changes to the sign-in logo do not impact users who authenticate to their workspace using Azure Active Directory. For more information on how to add company branding to your sign-in page in Azure AD, see the Microsoft documentation.

The **After Sign-in logo** appears at the top left of the workspace.

The **Content Branding** colors change the header background, text and icon color, and the accent color
Citrix Cloud

in the workspace.

**Customize workspace preferences**

Customize how subscribers interact with their workspace in **Workspace Configuration > Customize > Preferences**.

**Allow Favorites**

Allow Favorites is available to customers who have access to Workspace Configuration and the new workspace experience.

**Enabled** (default). Workspace subscribers can add favorite apps (up to a maximum of 250) by selecting the star icon.

**Disabled**. Subscribers can’t select apps as favorites. Favorites are not deleted and can be recovered if you re-enable Favorites.

**Note:**

For some existing customers (new to workspace between December 2017 and April 2018), **Allow**
Favorites defaults to Disabled. The administrator can decide when to enable this feature for their subscribers.

- If a subscriber adds more than the maximum (250) as a favorite, the “oldest favorite” app will be removed (or as close as possible to preserve the most recent favorites).
- Administrators can automatically add favorite apps for subscribers by using KEYWORDS: Auto and KEYWORDS: Mandatory. These settings are available in the Virtual Apps and Desktops service in Manage > Full Configuration > Applications.
  - KEYWORDS: Auto. The application is added as a favorite, however subscribers can remove the favorite.
  - KEYWORDS: Mandatory. The application is added as a favorite, however subscribers cannot remove the favorite. Mandatory apps do not display a star icon.

Automatically Launch Desktop

Automatically Launch Desktop is available to customers who have access to Workspace Configuration and the new workspace experience. This preference only applies to workspace access from a browser.
**Disabled** (default). Prevents Citrix Workspace from automatically starting a desktop when a subscriber signs in. Subscribers must manually launch their desktop after signing in.

**Enabled.** If a subscriber has only one available desktop, the desktop automatically launches when the subscriber signs in to the workspace. The subscriber’s applications aren’t reconnected, regardless of the workspace control configuration.

**Note:**

To enable Citrix Workspace to launch desktops automatically, subscribers accessing the site through Internet Explorer must add the workspace URL to the Local intranet or Trusted sites zones.

**Workspace Timeout**

Use the Workspace Timeout preference to specify the amount of idle time allowed (up to a maximum of 8 hours) before subscribers are automatically signed out of Citrix Workspace. This preference applies to browser access only, and does not apply to access from a local Citrix Workspace app.

**Citrix Workspace Preferences**

Citrix Workspace Preferences is available to customers who have access to Workspace Configuration and the new workspace experience. This preference applies to the way users open apps and desktops.
Citrix Cloud

delivered by Citrix Virtual Apps and Desktops only (service, or on-premises from the Site aggregation feature). It does not apply to, for example, SaaS apps delivered by the Citrix Gateway service. This preference is available to new and existing customers, however the introduction of this feature will not change any settings for existing customers.

- **In a native app** (default). Uses a locally installed version of Citrix Workspace – gives the best experience for the platform the user is on.
- **In a browser**. Uses Citrix Workspace for HTML5 – no client software is required.
- **Let users choose**. Prompts users to detect a locally installed version of Citrix Workspace, or to use Citrix Workspace for HTML5 in their browser where possible.

For the In a native app and Let users choose options, there is an additional check box option to guide users to install the latest version of Citrix Workspace if we weren’t able to detect a local app automatically. Removing this selection makes sense if your users don’t have rights to install software.

**Add an on-premises Site to Citrix Workspace**

March 6, 2019

If you have an on-premises XenApp or XenDesktop deployment, you can add your Site to Citrix Workspace. This process is known as Site aggregation. You can then create workspaces for your users, showing the on-premises applications available to them, and your users can access these applications through Citrix Cloud.

**Supported environments**

Site aggregation is supported for on-premises deployments of the following Citrix products:

- Virtual Apps and Desktops 7 1808 or later
- XenApp and XenDesktop 7.0 through 7.18
- XenApp 6.5

On-premises Sites running older versions of XenApp or XenApp and XenDesktop are not supported for use with Citrix Workspace.
Important:
XenApp and XenDesktop 7.x includes versions which are End of Life. XenApp and XenDesktop Current Releases prior to 7.14 reached End of Life on June 30, 2018. Support for Workspace Site aggregation with End of Life versions of XenApp and XenDesktop 7.x is conditional upon successful enumeration and launch of resources with your existing StoreFront on-premises deployment.
XenApp 6.5 reached End of Life on June 30, 2018. Support for Workspace Site aggregation with End of Life versions of XenApp is conditional on the successful enumeration and launch of resources in your existing StoreFront or Web Interface on-premises deployment.

Task overview

When you add your on-premises Site to Citrix Workspace, the Add Site wizard guides you through the following tasks:

- Discover your Site and select the default resource location. The default resource location specifies the domain and connectivity method for all users who access your Site. During this process, Citrix Cloud performs a connectivity test to verify your Site is reachable and displays your resource locations. If you have resource locations with no Cloud Connectors installed, you can download and install the required software.
- Detect the Active Directory domains in which your Cloud Connectors are installed. For XenApp 6.5, Citrix Cloud also detects if there are any published applications assigned to local user accounts on XenApp servers. To use Citrix Workspace, application users must be able to authenticate with Active Directory. Citrix Cloud provides a list of any local user accounts detected so you can ensure they can authenticate to Citrix Workspace.
- Specify the connectivity you want to use between Citrix Cloud and your Site. For external connectivity, you can use your own Citrix Gateway or use the Citrix Gateway service. To ensure only users on the same network as your Site can access applications, you can specify internal-only access.

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 Internet 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.

Although you can install the Cloud Connectors during the process of your adding your Site to Citrix Workspace, Citrix recommends installing them beforehand to ensure your Site is added with minimal interruption.

Web proxy configuration

If you have a web proxy in your environment, you must ensure the Cloud Connectors can validate connectivity to the XML Service in your Site. To do this, add each XML server to the bypass proxy list on each Cloud Connector. Do not use wildcards; the Cloud Connector supports handling FQDNs only.

1. Add the XML servers to the bypass proxy list:
   a) On the Cloud Connector, click Start and then type Internet Options.
   b) Select the Connections tab and then select LAN Settings.
   c) Under Proxy server, click Advanced.
   d) Under Exceptions, add the FQDN of each XML server in your Site.
2. Import the list so the Cloud Connector services can consume them appropriately. At the command prompt, type netsh winhttp import proxy source=ie.
3. From the Services console, restart all Citrix Cloud services on each machine hosting the Cloud Connector. Alternatively, restart each machine.

Active Directory

Site aggregation supports Sites that use an on-premises Active Directory.

Azure Active Directory configuration

To allow Sites using Azure Active Directory to be added to Citrix Workspace, you must configure your Site to trust XML Service requests. For detailed instructions, refer to the following articles:

• For XenApp and XenDesktop 7.x and Virtual Apps and Desktops 7 1808, see CTX236929.
• For XenApp 6.5, see Configuring the Citrix XML Service Port and Trust.
Important:
If you choose to use Azure Active Directory authentication with Site aggregation, users will be prompted to authenticate to each application they launch.

Active Directory trusts
If you have separate user and resource forests in Active Directory, you must have Cloud Connectors installed in each forest before you add your on-premises Site. When you add your Site, Citrix Cloud detects these forests during the Site discovery process, through the Cloud Connectors. You can then use the forests' users and resources to create workspaces for your users.

Limitations:
- You cannot use separate user and resource forests when you define the default resource location during the process of adding your Site. Because the Cloud Connectors do not participate in any cross-forest trusts that might be established, Citrix Cloud can't discover your Site through the Cloud Connectors in these forests. You can use these forests when you define a secondary resource location that provides a different connectivity option for your users. For more information, see Add IP ranges for different connectivity options.
- Untrusted forests are not supported for Site aggregation. Although Citrix Cloud and Citrix Workspace support users from untrusted forests, these users are not able to use Citrix Workspace after an on-premises Site has been added through Site aggregation. Only users located in the forests that the Site trusts can log in and use Citrix Workspace. If users from an untrusted forest attempt to log in to Citrix Workspace, they receive the error message, “Your logon has expired. Please log on again to continue.”

Internal and external connectivity to workspace resources
During the process of adding your Site to Citrix Workspace, you can specify if you want to provide internal or external access to the resources you make available to users. If you intend to allow only internal users to access your Site through Citrix Workspace, users must be on the same network as the Site to access their applications.

If you intend to allow external users to access these resources, you have the following options:
- Use your existing Citrix Gateway to handle the traffic between your on-premises Site and Citrix Cloud. To use this option, your Citrix Gateway must be configured to use Cloud Connectors as the Secure Ticket Authority (STA) servers before you add your Site to Citrix Workspace. For instructions, see CTX232640.
- Use the Citrix Gateway service if you prefer to allow Citrix to handle the traffic between your Site and Citrix Cloud for you. You can activate a service trial and configure the service when you add
your Site. If you have already signed up for the Citrix Gateway service, Citrix Cloud detects your subscription when you select this option.

Note:
For Citrix Cloud to detect your Citrix Gateway service subscription while adding your Site to Workspace, you must use the same OrgID that you used when you signed up for the Citrix Gateway service. For more information about OrgIDs in Citrix Cloud, see What is an OrgID?

Credentials and ports for Site discovery

During the process of adding your Site to Citrix Workspace, Citrix Cloud discovers your Site and ensures the Controller you specify is available. Before you add your on-premises Site, perform the following tasks:

- Ensure you have Citrix administrator credentials with a minimum of Read Only permissions. During the process of adding your Site to Citrix Workspace, Citrix Cloud prompts you to supply these credentials. Citrix Cloud only reads these credentials for the discovery process. Citrix Cloud does not store these credentials or use them to make changes to your Site.
- **XenApp 6.5 only:** Ensure that port 2513 on the XenApp server is accessible from the Cloud Connector machines in your environment. During the discovery process, the Cloud Connectors contact the Citrix XenApp Remoting Service on the XenApp server you specify. This service listens on port 2513. If this port is blocked, Citrix Cloud can’t discover your deployment.

To enable Site discovery without Site credentials

**XenApp and XenDesktop 7.x and Virtual Apps and Desktops 7 1808 only:** If you don’t want to provide your Site credentials for security reasons, you can enable Citrix Cloud to discover your Site without prompting for Site credentials. Complete this task before you add your Site to Citrix Workspace.

1. Install at least two Cloud Connectors in your Site’s domain.
2. Create an Active Directory security group and add the Cloud Connectors in your domain to it.
3. In Studio, grant the security group Read Only permissions, at a minimum.

**Task 1: Discover your Site**

In this step, you provide the information that Citrix Cloud needs to locate your Site and select your default resource location. The default resource location specifies the domain and connectivity option for all users who access your Site. If you need to install Cloud Connectors in your Site’s domain, you can do so now. If you already have Cloud Connectors installed, you can select them when prompted.

1. From the Citrix Cloud menu, click **Workspace Configuration** and then click **Sites > Add Site.**
2. In **Select type of Site**, select the XenApp or XenDesktop version of the Site you want to add. Citrix Cloud attempts to discover any Cloud Connectors in your domain and displays them in the next tab.

3. In **Discover XenApp Site** or **Discover XenApp and XenDesktop Site**, perform one of the following actions:
   
a) If you have no Cloud Connectors installed in your Site's domain, click **Install Connector**. Citrix Cloud prompts you to download the Cloud Connector software and complete the installation wizard.

   b) If you have Cloud Connectors installed, Citrix Cloud displays the connectors in the domains in which they were detected. Select the resource location you want to add to Citrix Workspace. This resource location becomes the default resource location.

   c) If you have Cloud Connectors installed, but they are not displayed, click **Detect**.

4. In **Enter Server Address**, enter the IP address or FQDN of a Controller in the Site.

5. **XenApp 6.5 only**: Enter the port for the XML Server. If the XML Server port uses SSL, select **Use SSL**.

   ```
   Note:
   For XenApp and XenDesktop 7.x Sites, Citrix Cloud automatically discovers the XML server port.
   ```

6. Click **Discover**.

7. If prompted, type the Citrix Administrator credentials for the Site and click **Continue**. Citrix Cloud performs a connectivity test to verify that your Site is reachable. Discovery might take a few minutes to complete, depending on the type and size of the Site.

8. Click **Continue**.

**Task 2: Verify Active Directory Connection**

In **Verify Active Directory Connection**, Citrix Cloud displays the domains used with your Site and whether or not there are Cloud Connectors installed in those domains. For XenApp 6.5, Citrix Cloud also displays an alert if there are any local user accounts on the XenApp servers assigned to any applications.

If there are no Cloud Connectors in a domain, users in that domain can't use Citrix Workspace to access the applications published there. If only one Cloud Connector is installed, your Site's connection to Citrix Cloud is at risk of an outage, preventing users from using Citrix Workspace. To ensure high availability for your Site, Citrix recommends installing at least two (2) Cloud Connectors in each domain.
**XenApp 6.5:** If there are local user accounts assigned to published applications, these users must be assigned to applications using their Active Directory account instead. Otherwise, they can’t use Citrix Workspace to access their applications. Citrix Cloud provides a downloadable list in CSV format of the applications and the local user accounts assigned to them.

1. To install more Cloud Connectors, click **Install Connector**. If your domain has only one Cloud Connector and you choose to continue without installing more Cloud Connectors, select **I understand that high availability requires having two connectors installed in each domain**.
2. If you have local users assigned to applications in your Site, click **Download user list (.csv)**.
3. Click **Continue**.

**Task 3: Configure connectivity and confirm settings**

In this step, you specify whether you want to allow only external user access or internal-only access to your Site through Citrix Workspace. Internal connectivity requires your users to be on the same network as your Site. For external connectivity, you can use your existing Citrix Gateway or you can use the Citrix Gateway service.

1. In **Configure Connectivity**, under **Select connectivity type**, select one of the following options:
   - **Add Existing Gateway**: Select this option to use your existing Citrix Gateway to provide external access.
   - **Citrix Gateway service**: Select this option to activate a service trial or use your existing subscription with your Site.
   - **Internal Only**: If selected, no other configuration is needed. Click **Continue**.
2. If **Add Existing Gateway** is selected, perform the following actions:
   a) Click **Edit** and type the public URL of the Citrix Gateway.
   b) Verify that Citrix Gateway is configured to use your Cloud Connectors as the STA servers as described in CTX232640.
   c) Click **Test STA**. When the test is successful, click **Continue**. If the test isn’t successful, refer to CTX232517 for troubleshooting steps.
3. If **Citrix Gateway service** is selected, but the service isn’t enabled for your Citrix Cloud account as a service trial or as a purchase, click **Start a 60-day trial**. Citrix Cloud enables the service as a trial for you. If the service was enabled at an earlier time, Citrix Cloud detects the service and displays any remaining trial days, if applicable.
4. Click **Continue**.
5. In **Confirm Site Aggregation**, review the XML port, XML servers, Active Directory domains, and the Connectivity Type you chose earlier.
6. Click **Save and Finish**. The Sites page displays your newly added Site.
Notes:

- Citrix Cloud displays up to five of the XML servers with which it can connect. If you have multiple XML servers in your Site but only one is displayed, Citrix Cloud displays an alert. To troubleshoot this issue, refer to CTX232516.
- If you want to specify different XML servers, click Save and Finish. You can then edit your Site to change these values.

Change your Site configuration

Rediscover your Site

If you add Delivery Controllers to your Site or change XML ports, you can initiate rediscovery to verify your Site is still reachable in Citrix Workspace.

1. On the Sites page, click the ellipsis button for the Site you want to update and click Edit Site.
2. In Server Address, type the IP address or FQDN of a Delivery Controller in your Site and click Rediscover.

Add or modify XML servers

When you add a new Site to Citrix Workspace, Citrix Cloud automatically detects the XML servers in your Site and displays up to five XML servers in your Site configuration. You can add and remove XML servers as needed from your Site configuration, up to the display limit of five XML servers.

To add an XML server

1. On the Sites page, click the ellipsis button for the Site you want to update and click Edit Site.
2. In the XML Servers section, type the XML server port and select Use SSL if needed.
3. Select a connectivity method:
   - Load balanced: This option allows Citrix Cloud to pick a random XML server from the list.
   - Failover: This option allows Citrix Cloud to use the listed XML servers in the order in which they appear in the list. You can re-order the list by dragging and dropping each server as needed.
4. Click Save Changes.

If you experience an error when adding an XML server, refer to CTX232516 for troubleshooting steps.
Add IP ranges for different connectivity options

If you have VDAs or session hosts in different subnets, you can specify IP ranges with a different connectivity type for each one. Each IP range can also have a different resource location associated with it. For example, you might have one IP range for machines located in the EU where users connect internally only, one IP range for machines in the EU where users connect through your existing Citrix Gateway, and one IP range for machines in the US where users connect through the Citrix Gateway service.

1. On the Sites page, click the ellipsis button for the Site you want to update and click Edit Site.
2. In the Connectivity section, click Add an IP range with a different connectivity option.
3. Type an IP range in CIDR format.
4. To create a new resource location for your IP range, perform the following actions:
   a) Select Add a new Resource Location and type a friendly name.
   b) In Select your connectivity, select whether you want to provide internal-only access or allow external access using your existing Citrix Gateway or the Citrix Gateway service.
5. To assign an existing resource location to the IP range, choose Select an existing resource location and then select the resource location you want to use. If you choose a resource location with only one Cloud Connector installed, select I understand that high availability requires having two connectors are installed in a resource location.
6. Click Add.

Add more Active Directory domains

If you install Cloud Connectors in additional domains with Active Directory users in your Site, you can ensure they are added to your Site configuration in Citrix Workspace.

1. On the Sites page, click the ellipsis button for the Site you want to update and click Edit Site.
2. Under Active Directory, click Refresh.

Disable Sites

If you no longer want to make your on-premises Site available to users in Citrix Workspace, you can disable it. You can disable an individual on-premises Site or you can disable all on-premises Sites you’ve added to Citrix Workspace.

When Sites are disabled, users can no longer access the on-premises applications in those Sites through Citrix Workspace, but the configuration for those Sites is preserved. When you re-enable a Site later on, the Site’s default resource location, domain, XML server, and connectivity settings are retained.
**To disable an on-premises Site**

1. On the Sites page, click the ellipsis button for the Site you want to disable.
2. Click Disable. A confirmation message appears.
3. Click Disable.

**To disable all on-premises Sites**

To disable all Sites on the Sites page, you disable the workspace integration for all Virtual Apps and Desktops on-premises Sites. Disabling the workspace integration effectively disables Site aggregation of on-premises Sites. For instructions, see Disable workspace integration for a service.

To re-enable any individual on-premises Sites or to add a new Site later on, you must first re-enable the workspace integration for all Sites on the Service Integrations page.

**Delete a Site from Citrix Workspace**

If you no longer want your on-premises Site configuration in Citrix Workspace, you can delete the Site. When you delete a Site, only the configuration for the Site in Citrix Workspace is removed. Citrix Cloud does not make any changes to your Site.

1. On the Sites page, click the ellipsis button for the Site you want to remove.
2. Click Delete.

**Workspace experience**

September 16, 2019

This article gives an overview of the Citrix Workspace user experience, including recent changes.

**Important:**

The following addresses need to be contactable to properly operate and consume Citrix Workspace:

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

For a full listing of Citrix Cloud connectivity requirements, see Internet Connectivity Requirements.
Citrix Cloud

What’s new in the workspace experience

Okta authentication (Technical Preview)

Subscribers can authenticate to Workspace through Okta.

Citrix Gateway authentication

Subscribers can authenticate to Workspace through an on-premises Citrix Gateway to securely access their resources. They can use features such as RADIUS, pass-through authentication, smart cards, conditional access policies, federation, and many others by integrating them into Workspace using the Gateway’s authentication, authorization, and auditing (AAA) feature.

To ensure a visually consistent sign-in experience for subscribers, you can also customize the Gateway sign-in page to mimic the Workspace sign-in page. For more information, see CTX258331.

Active Directory plus token authentication

For additional security, subscribers can use a token as a second factor of authentication in addition to Active Directory sign-in. Workspace prompts all subscribers during every sign-in to enter a token that’s generated from their enrolled device.

Browser support

Access workspace using Internet Explorer 11, or the latest version of Edge, Chrome, Firefox, or Safari.
Citrix Cloud

Card layout

Apps and desktops in your workspace are represented in a “card” layout. A pop-up window shows more details and actions.

Search

Search everything in your workspace, open apps directly from the search results.

Note:
Search currently requires a minimum of three characters.

Recents

Recents displays recently opened apps, desktops, and files. For apps and desktops, depending on screen size, you see up to 30 (in each). For files, you see up to 15.

Favorites

Select the star icon to add an app to Favorites (max 250). This option is configurable by your administrator, and may not be available.

Settings

Access settings from the drop-down menu. The menu contains the user name. The user name comes from the Active Directory display name. If the display name is left blank (we do not recommend this), the domain and account name display.

Select Account Settings for more options.

- **Activate Citrix Workspace.** Downloads a file that adds this workspace to your local Citrix Receiver app.
Citrix Cloud

- **Change Citrix Workspace.** Opens a page that checks for a local Citrix Workspace app. Not available in Internet Explorer 11.

  **Note:**
  This option is only available with Citrix Virtual Apps and Desktops services. **Change Citrix Workspace** is not available if, for example, you are only using SaaS apps through the Citrix Gateway service.

- **Download Citrix Workspace.** Downloads a Citrix Receiver installation file to your machine. Run the file to install a local Citrix Workspace app for Windows or Mac.

### Citrix Workspace app

Citrix recommends that Workspace subscribers use the latest version of Citrix Workspace app.

You can also access workspaces using Internet Explorer 11, or the latest version of Edge, Chrome, Firefox, or Safari.

Currently, some customers continue to use Citrix Receiver. Citrix Receiver is supported for any of the desktop platforms (Windows, Mac, and Linux). Citrix Receiver for HTML5 and Citrix Receiver for Chrome are also supported.

  **Note:**
  Communication over Transport Layer Security (TLS) 1.0 and 1.1 will be blocked on March 15, 2019. If you are using earlier versions of Citrix Receiver that do not support TLS 1.2, any user trying to connect to Citrix Workspace will **not** be able to connect. Please make sure you update Citrix Receiver or upgrade to Citrix Workspace app by March 15, 2019. For an overview of TLS and SHA2 support with Citrix Receivers, see [CTX23226](#).

For more information about supported features by app platform, refer to the **Workspace app feature matrix**.

### Supported authentication methods for Citrix Workspace app

The following table shows the authentication methods supported by Citrix Workspace app.
Citrix Cloud

<table>
<thead>
<tr>
<th>Citrix Workspace app</th>
<th>Active Directory Authentication</th>
<th>Active Directory plus Token Authentication</th>
<th>Azure Active Directory authentication</th>
</tr>
</thead>
<tbody>
<tr>
<td>Citrix Workspace for Windows</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (Workspace app; Receiver 4.9 LTSR CU2 and later only; Receiver 4.11 CR and later only)</td>
</tr>
<tr>
<td>Citrix Workspace for Linux</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (Workspace app; Receiver 13.8 or and later only)</td>
</tr>
<tr>
<td>Citrix Workspace for Mac</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Citrix Workspace for iOS</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (Workspace app; Receiver 3.13 and later only)</td>
</tr>
<tr>
<td>Citrix Workspace for Android</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

For more information about Workspace app support for specific features, refer to the Workspace app feature matrix.

Currently, some customers continue to use Citrix Receiver. Citrix Receiver is supported for any of the desktop platforms (Windows, Mac, and Linux). Citrix Receiver for HTML5 and Citrix Receiver for Chrome are also supported. For an overview of TLS and SHA2 support with Citrix Receivers, see CTX23226.

**Citrix Receiver and Citrix Workspace app**

This section guides existing customers, who are working with Citrix Receiver, through the change to Citrix Workspace app.

The latest Citrix Workspace experience is available with the following services in Citrix Cloud:

- Virtual Apps Essentials
- Virtual Desktops Essentials
- Virtual Apps and Desktops service (includes Site aggregation from Virtual Apps and Desktops on-premises resources)
- Citrix Gateway service (delivering secure web and SaaS apps)
- Content Collaboration (formerly ShareFile)
Secure Browser service

**New customers.** If you are new to the workspace experience, you’ll get the latest version of the user interface as soon as it is available. You can access the workspace experience from your browser or from a local Citrix Workspace app.

**Existing customers.** If you have been working with an earlier version of Citrix Workspace, it can take around five minutes for the updated user interface to display in local Citrix Workspace apps. You may temporarily see an older version of the user interface. Alternatively, you can click the **Refresh** button in your web browser to update the user interface as needed. If you have been working with Citrix Receiver as your local app, you will need to guide your users to upgrade to Citrix Workspace app to use all the features of the Citrix Cloud services.

The scenarios below illustrate what users are likely to see.

**Citrix Receiver**

If your users are accessing Workspace with Citrix Receiver, with the above service integrations enabled, users will see the “purple” user interface shown below. They will see Virtual Apps and Desktops apps as well as web and SaaS apps from the Citrix Gateway service. Files are not supported in Citrix Receiver and users will not be able to access them this way.

With the same services enabled and **access control** enabled, users will still see the purple user interface, however without web and SaaS apps, as the access control feature is not supported in Citrix Receiver.
Access control is a feature that delivers access for end users to SaaS, web, and virtual apps with a single sign-on (SSO) experience.

**Citrix Workspace app or browser**

When your users upgrade to Citrix Workspace app or use a web browser to access Workspace, they will see the new user interface and can use of all the new functionality including Files.
Azure Active Directory (AAD)

This scenario is for either AAD enabled as the Workspace authentication method. If your users try to log on using Citrix Receiver, they will see a message that the device isn’t supported and to try from a browser instead. Once they have upgraded to Citrix Workspace app, they can access Workspace. For the matrix showing authentication methods supported with Citrix Workspace app, see the table at the end of this article.
**StoreFront (on-premises deployment)**

If you have a StoreFront on-premises environment and users choose to upgrade from Citrix Receiver to Citrix Workspace app, the only change will be the icon to open Citrix Workspace app.

**Government users**

Citrix Cloud Government users will continue to use their “purple” user interface when using the Workspace app or when accessing from a web browser.

**Changes to your service subscription**

If you have changed your service subscription, you may need to refresh the local Workspace app manually. In Citrix Workspace app for Windows:

1. From the Windows system tray, right-click the Citrix Workspace icon, and click **Advanced Preferences > Reset Citrix Workspace**.
2. Open Citrix Workspace app for Windows, then select **Accounts > Add**, and enter the workspace address, for example, `https://example.cloud.com`.

As an alternative to step 2, you can use a browser to enter the workspace URL and sign in. Then, activate Citrix Receiver from **Settings > Account Settings > Activate Citrix Workspace**. Activating Citrix Workspace downloads a file with a `.CR` extension that adds the workspace to your local Citrix Workspace app.

**Changes to authentication**

If you are logged on to Citrix Workspace and your administrator makes a change to the authentication method - for example, from Active Directory to Azure Active Directory - you may see errors in Citrix Workspace. If this happens to you, log off Citrix Workspace and close the browser or Citrix Workspace app. Wait approximately 5 minutes and log back on again. Citrix Workspace should be available to you again. You can log on using the new authentication method.
Authentication with Active Directory plus token

Device registration

Before Workspace subscribers can use two-factor authentication with a token, they must first register their device. During registration, subscribers are presented with a QR code they can scan with an app that follows the Time-Based One-Time Password standard, such as Citrix SSO or Google Authenticator. For a smooth registration process, Citrix recommends downloading and installing this app on the device beforehand.

1. From a computer, open a browser, navigate to the Workspace sign-in page, and click *Don’t have a token?*

![Workspace sign-in page](image)

2. Enter your user name in domain\username format or your company email address and click *Next.*
Citrix Cloud sends you an email with a verification code.
3. After you receive the email, enter the verification code and your Active Directory account password when prompted. Click **Next**.

4. From the authenticator app, scan the QR code or enter the verification code manually.

5. Click **Finish and Sign In** to complete the registration.

After completing registration, subscribers can return to the Workspace sign-in page and enter their Active Directory credentials, along with the token displayed in their authenticator app.
Authentication with Citrix Gateway

When authentication with Citrix Gateway is enabled, subscribers experience the following workflow:

1. The subscriber navigates to the Workspace URL in their browser or launches Workspace app.
2. The subscriber is redirected to the Citrix Gateway logon page and is authenticated using any method configured on the Gateway (for example, RADIUS MFA, smart card, federation, conditional access policies, and so on). You can customize the Gateway logon page so that it looks the same as the Workspace sign-in page using the steps described in CTX258331.
3. After successful authentication, the subscriber’s workspace appears.

Authentication with Okta (Technical Preview)

Note:
This feature is currently available as a technical preview. Citrix recommends using technical preview features only in test environments.

When authentication with Okta is enabled, subscribers experience the following workflow:

1. The subscriber navigates to the Workspace URL in their browser or launches the Workspace app.
2. The subscriber is redirected to the Okta sign-in page and is authenticated using the method configured in Okta (for example, multifactor authentication, conditional access policies, and so on).
3. After successful authentication, the subscriber’s workspace appears.

**Add administrators to a Citrix Cloud account**

September 26, 2019

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

**Invite new administrators**

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

On the **Identity and Access Management** page, click **Administrators**. The console shows all the current administrators in the account.
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**.
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 or not 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.

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**.

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

September 26, 2019

License and Usage 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 **License & Usage** from the console menu.

Note:

This article covers License and Usage features that are common to all supported Citrix Cloud services. Some aspects of License and Usage 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
- Monitor licenses and usage for Endpoint Management service
**Supported regions and cloud services**

License and Usage is available for supported services in the US, EU, and Asia Pacific South regions only.

License and Usage is supported for the following cloud services:

- Virtual Apps and Desktops (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 License and Usage articles referenced at the top of this article.

**License & Usage summary and details**

<table>
<thead>
<tr>
<th>Virtual Apps and Desktops</th>
<th>View Usage Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Licenses</strong></td>
<td></td>
</tr>
<tr>
<td>Assigned / Total</td>
<td>390 / 1,000</td>
</tr>
<tr>
<td>Available</td>
<td>610 (61%)</td>
</tr>
<tr>
<td><strong>Active Use</strong></td>
<td></td>
</tr>
<tr>
<td>Monthly</td>
<td>354 (35.4%)</td>
</tr>
<tr>
<td>Daily</td>
<td>148 (14.8%)</td>
</tr>
</tbody>
</table>

⚠️ 1,000 licenses will expire in 49 days.

The License & Usage 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 License and Usage 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 License and Usage 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 License and Usage 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.
Monitor licenses and active usage for Citrix Virtual Apps and Desktops service

September 9, 2019

License assignment

Citrix Cloud assigns a license when a unique user or unique device launches an app or desktop for the first time.

License & Usage summary

<table>
<thead>
<tr>
<th>Virtual Apps and Desktops</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Licenses</strong></td>
<td><strong>Active Use</strong></td>
</tr>
<tr>
<td>Assigned / Total</td>
<td>Available</td>
</tr>
<tr>
<td>390 / 1,000</td>
<td>610 (61%)</td>
</tr>
<tr>
<td>Available</td>
<td>Monthly</td>
</tr>
<tr>
<td></td>
<td>354 (35.4%)</td>
</tr>
<tr>
<td></td>
<td>Daily</td>
</tr>
<tr>
<td></td>
<td>148 (14.8%)</td>
</tr>
</tbody>
</table>

1,000 licenses will expire in 49 days.

The License & Usage 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.
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.
- **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:

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

<table>
<thead>
<tr>
<th>Username</th>
<th>Domain</th>
<th>Devices</th>
<th>Last Login</th>
<th>Date Assigned</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>
</tr>
<tr>
<td>kianru</td>
<td>Intech</td>
<td>2 Devices</td>
<td>Aug 18, 2016 12:13:45 UTC</td>
<td>Jan 18, 2017</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Device Name</th>
<th>Device ID</th>
<th>Users</th>
<th>Last Login</th>
<th>Date Assigned</th>
</tr>
</thead>
<tbody>
<tr>
<td>GWTD5-Dell XPS</td>
<td>A65AD46A</td>
<td>45 Users</td>
<td>Sep 15, 2016 11:23:40 UTC</td>
<td>Mar 25, 2017</td>
</tr>
<tr>
<td>GWTD5-Surface</td>
<td>A65AD44R</td>
<td>19 Users</td>
<td>Aug 18, 2016 12:13:45 UTC</td>
<td>Jan 18, 2017</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 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.
Citrix Cloud

by logging in and using the cloud service.

**To release multiple assigned licenses**

1. Under **License Activity**, select the **Licensed Users** tab.
2. Click **Release Licenses**.

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

3. From the list, select the users you want to manage and click **Continue**.
Select licenses to release

These 45 users haven't used the service in the last 30 days and their licenses are eligible for release.

Select the licenses you want to release.

<table>
<thead>
<tr>
<th>Username</th>
<th>Last Login</th>
<th>Assigned Since</th>
</tr>
</thead>
<tbody>
<tr>
<td>feltoma</td>
<td>Sep 15, 2016 11:23:40 UTC</td>
<td>Jul 9, 2017</td>
</tr>
<tr>
<td>felainy</td>
<td>Dec 8, 2016 16:23:40 UTC</td>
<td>Mar 25, 2017</td>
</tr>
<tr>
<td>kianru</td>
<td>Sep 15, 2016 11:23:40 UTC</td>
<td>Nov 12, 2017</td>
</tr>
<tr>
<td>mauricele</td>
<td>Sep 15, 2016 11:23:40 UTC</td>
<td>Jul 9, 2017</td>
</tr>
<tr>
<td>smallings</td>
<td>Dec 8, 2016 16:23:40 UTC</td>
<td>Mar 25, 2017</td>
</tr>
<tr>
<td>skyeru</td>
<td>Sep 15, 2016 11:23:40 UTC</td>
<td>Nov 12, 2017</td>
</tr>
<tr>
<td>torpan</td>
<td>Sep 15, 2016 11:23:40 UTC</td>
<td>Nov 12, 2017</td>
</tr>
</tbody>
</table>

4. 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 used the cloud service 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 License.
Monitor licenses and active usage for Endpoint Management

July 24, 2019

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.

License & Usage summary and details

The License & Usage summary provides an at-a-glance view of the following information for each supported service:
• Percentage of total purchased licenses assigned. As the percentage approaches 100%, the percentage goes from green to yellow. If the percentage exceeds 100%, the percentage turns red.

• The ratio of assigned licenses to purchased licenses and the number of available licenses remaining.

• Active usage statistics on a monthly and daily basis:
  – Monthly active use refers to the number of unique users that have used the service in the last 30 days.
  – Daily active use refers to the number of unique users that have used the service in the last 24 hours.

• The time remaining before the cloud service subscription expires. If the subscription expires within the next 90 days, a warning message appears.

Usage trends and license activity

For a detailed view of your licenses, click View Usage Details. You can then see a breakdown of usage trends and individual users and devices that are consuming cloud service licenses.

This breakdown shows you the following information:

• **Total Licenses**: Your total purchased licenses for the cloud service across all entitlements.

• **Previously Assigned**: The cloud service licenses that were already assigned at the beginning of each month. For example, if a user is assigned a license in July, that assignment is counted in the Previously Assigned number for August.

• **Newly Assigned**: The number of cloud service licenses that were assigned during each month. For example, a user who accesses the cloud service for the first time in July is assigned a license. This license is counted in the Newly Assigned number for July.

• **Active Use**: Daily and monthly active usage trends over the previous calendar month and calendar year, respectively.
The License Activity section also displays the following information:

- A list of the individual consumers who have assigned licenses
- The date when licenses were assigned
- The number of enrolled devices and the date of the last check-in for each user

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

After a license is assigned, the license cannot be released, even if the user is no longer accessing the service.

Register on-premises products with Citrix Cloud

August 20, 2019
Prerequisites

Product registration is currently supported for Citrix License Server. To use this feature, you must first enable Call Home and register your License Server with Citrix Cloud from the Citrix Licensing Manager console. For instructions, see Usage and statistics.

Register a product

Product registration requires an 8-digit code that Citrix Cloud generates. Depending on your product, this 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 from the Product Registration page in Citrix Cloud.

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**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Product Type</th>
<th>Registration Date</th>
<th>Remove registration</th>
</tr>
</thead>
<tbody>
<tr>
<td>CITRIX-R2VOL9UV</td>
<td>License Server</td>
<td>May 10, 2019 4:38:31 PM UTC</td>
<td></td>
</tr>
<tr>
<td>CITRIX-FO1808C1</td>
<td>License Server</td>
<td>May 10, 2019 4:38:31 PM UTC</td>
<td></td>
</tr>
<tr>
<td>CITRIX-8TQLGBBF</td>
<td>License Server</td>
<td>May 10, 2019 3:02:25 PM UTC</td>
<td></td>
</tr>
</tbody>
</table>

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

Monitor licenses and usage for on-premises deployments

August 29, 2019

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 **License & Usage** 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 User/Device licensing model.
View on-premises product license usage

Citrix License Server usage insights provides visibility into license usage across your entire Citrix estate. After you enable usage insights for your license servers and register them with Citrix Cloud, you can access usage reporting that helps you:

- Understand how many license servers are deployed and registered, and if they are reporting usage information to Citrix Cloud.
- Get visibility into User/Device license usage for Virtual Apps and Desktops.
- Gain insight into aggregate 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 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.
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

July 20, 2018

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.
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.

Automatic cleanup of notifications

Citrix Cloud automatically deletes notifications older than 90 days, regardless of whether they’ve been read. This ensures the Notifications page remains uncluttered and allows administrators to focus on only the most important notifications.
Citrix Cloud

Features for Citrix Partners

June 20, 2019

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 is shown indicating this account is owned by a Citrix partner. 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
- License and usage 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 then view details around the customer’s basic account information, orders placed by the customer along with entitlement information like services, license counts, expiration dates and so on.

License and usage trends

Partners can view license and usage information from the customer dashboard by clicking the ellipsis button for the customer and selecting **View License & Usage**.

Note:

Citrix Partners can view only the License & Usage summary view and historical active usage trends. They can’t view individual users who consume licenses for a given service.

From the customer page, on the **Usage** tab, click **View Usage Trend** to view a summary that 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.
Virtual Apps and Desktops

Licenses
- Assigned / Total: 28 / 100
- Available: 72 (72%)

Active Use
- Monthly: 0 (0%)
- Daily: 0 (0%)

License Assignment: 19
Active Use: 81
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 actions around it like dismissing the notification. This dismissed notification will not show up for the partner; however, customers will still be able to see the notification in their account after they sign in to Citrix Cloud.
Visibility in customers support tickets will help partners to take actions and resolve issues for their customers ensuring a streamlined and error free experience for their users.

Content Collaboration

September 7, 2018

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 Setup ShareFile.

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

Service Level Agreement

Content Collaboration is designed using industry best practices to achieve cloud scale and a high degree of service availability.
Create or link a Content Collaboration (ShareFile) account to Citrix Cloud

October 11, 2019

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 in to 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 in to **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**.
5. On the **Set up Content Collaboration** page, choose the service region, enter a unique subdomain, and then click **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.
- 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.
3. In **Add Service**, select **Link Account**. The Add Content Collaboration Account page appears with the Link Account tab selected.
4. Select the ShareFile account you want to link and then click Link Account.

**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.
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.

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.

---

**Set up ShareFile**

October 9, 2019

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 into 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 suc-
cessful 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

Follow Citrix ShareFile for Endpoint Management for information on wrapping the ShareFile application and deploying Single Sign-On between Endpoint Management and ShareFile.

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.

MDX Service

September 30, 2019

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

The MDX Service can use MDX version 19.9.5 for wrapping third-party apps.

For information about MDX, the traditional MDX wrapping process using the MDX Toolkit, and a description of signing required assets, see:
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. On the upper right of this page is a blue circle with a plus (+) in it. Mouse over that icon and then click on [Wrap a Mobile App](#).
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**.

![Endpoint Management MDX Service](image)

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.

![Upload an IPA or APK file.](image)

After the .ipa file uploads and is processed successfully, the **Verify App Details** screen appears.
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.

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

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.
Introduction

The IT Service Management (ITSM) Adapter service automates the provisioning and management of Citrix resources in your organization. The Citrix IT Service Management connector (ITSM connector) in ServiceNow provides out-of-the-box workflows for resource management.

This adapter service eliminates the wait time associated with provisioning and managing Citrix virtual assets. This release provides workflows to provision apps and desktops, and reset user sessions.

The ITSM Adapter service is available on the Citrix Cloud platform. This service is available for Citrix Virtual Apps and Desktops (formerly XenApp and XenDesktop) Premium customers.

How the ITSM Adapter Service Works

The ITSM connector in ServiceNow enables communication between ServiceNow and Citrix Cloud. From the ITSM Adapter service, you can process the Catalog requests from ServiceNow. These requests are routed to the Delivery Controller, which provisions and manages the resources in the Site. To enable resource management on your Citrix Virtual Apps and Desktops Sites, the ITSM Adapter redirects you to Site aggregation in Workspace Configuration where you can add your on-premises Sites. ITSM Adapter accesses your Sites through the Citrix Cloud Connector.

The following diagram shows the ITSM Adapter connecting ServiceNow and Citrix Virtual Apps and Desktops Sites and Citrix Virtual Apps and Desktops Service.
**Roles and Permissions**

**User**
- Requests apps and desktops
- Resets sessions

**ServiceNow administrator**
- Downloads and installs the Citrix ITSM connector from the ServiceNow store.
- Provides x_wcs_ctrx_auto_sv.ctrx_auto_admin role to the Citrix Administrator.

**Citrix Administrator**
- Uses the administrator functions in the ITSM connector to setup the connection between ServiceNow and Citrix Cloud.
- Adds the Citrix Virtual Apps and Desktops Sites and Citrix Virtual Apps and Desktops Service through Site aggregation.
- Provides full administrator credentials of the Citrix Virtual Apps and Desktops Sites.
- Provisions apps and desktops for users.
- Resets user sessions.

**Configuring ITSM adapter for ServiceNow**

Setting up the ITSM Adapter involves the following three steps:

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

Log in 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](#).

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

**Prerequisite:** You must have a ServiceNow HI Portal account and be a ServiceNow Administrator to perform the following steps:

1. Download and install the Citrix ITSM connector from the ServiceNow store.

2. On the Citrix ITSM Connector pane, select **Home** and then click **Authenticate**. Type your Client ID and Secret (proxy credentials generated from the Citrix Cloud).
3. Test the connection.

4. Save the configuration. An acknowledgement from ServiceNow appears indicating that the connection is up and running.

**Step 3: Use ITSM Adapter to add Site(s)**

On the Citrix Cloud page, ITSM Adapter is listed under **Available Services**.

1. Click **Request Trial**. The ITSM Adapter page appears.

2. Go to the **Manage** tab.
3. You have to add your on-premises Site(s) to Citrix Workspace to connect with the ITSM Adapter service. Use Site Aggregation to add your Citrix Virtual Apps and Desktops Sites to do this. For more information about adding Citrix Virtual Apps and Desktops Site(s) to Workspace, see Add an on-premises Site to Workspace.

Note:
ITSM Adapter service is available for Citrix Virtual Apps and Desktops Sites and for XenApp and XenDesktop 7.x Sites.

4. After adding one or more Sites using Site Aggregation, return to the ITSM Adapter service to continue.

5. The Citrix Virtual Apps and Desktops Sites appear on the ITSM Adapter service Manage page. If you have subscribed to the Citrix Virtual Apps and Desktops Service, that instance also appears.
6. Full administrator credentials are required to access and modify these Citrix Virtual Apps and Desktops Sites. To do this, select **Manage Credentials** from the dots menu.

![Manage Credentials](image)

7. On the **Manage Credentials** page, provide the full administrator credentials for the Site.

![Manage Credentials Page](image)

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

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

**Related Actions/Information**

- To enable/disable the Citrix Virtual Apps and Desktops Service, click **Enable/Disable Integration** on the dots menu respectively.
- Multiple Sites can use the same Cloud connector to connect to Citrix Cloud.
- ITSM Adapter service can connect to multiple ServiceNow instances.
Sample Scenarios

Request for a Desktop

User Actions

1. Log in to your ServiceNow instance.
2. On the left pane, navigate to Citrix IT Service Management Connector and choose Services.
4. The following services are displayed:
   - Application Provisioning
   - Request a Desktop
   - Reset a session
   Choose Request a Desktop.

5. On the Configuration page, choose the operating system from the list and click Submit.

Administrator Actions
The Citrix Requests page displays the list of requests by the users. Click the icon next to the request ID. The details of the request appear.

Choose the Machine Catalog first and then the Delivery group from the list.

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 click Services.
4. The following services are displayed:
   - Application Provisioning
   - Request a Desktop
   - Reset a session

Choose Application Provisioning.

5. On the Assign Applications to selected users page, the list of users and applications available are listed. Choose the users and the applications you want to assign to them and click Submit.

Administrator Actions

1. The Citrix Requests page displays the list of requests by the users. Click the icon next to the application request ID. The details of the request are displayed.

2. There are two options to complete the app provisioning:
• Add users to Delivery Group—click the lock icon to add the user to the specific delivery group and then click **Update**.

• Add users to Active Directory Group—click the lock icon to add the user to the specific Active Directory group and then click **Update**.

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

**Reset a Desktop Session**

**User Actions**

1. Log in to your ServiceNow instance.

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

3. On the Citrix Automation Catalog page, click **XenApp and XenDesktop**.

4. The following services are displayed:
   - Application Provisioning
   - Request a Desktop
   - Reset a session

Choose **Reset a session**.

5. On the **Reset a session** page, choose the session you want to reset and click **Submit**.

The selected session is signed off and reset.

**Reset an App Session**

**User Actions**

1. Log in to your ServiceNow instance.

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

3. On the Citrix Automation Catalog page, click **XenApp and XenDesktop**.

4. The following services are displayed:
   - Application Provisioning
   - Request a Desktop
   - Reset a session

Choose Reset a session.

5. On the **Reset a session** page, choose the session you want to reset. Click **Submit**.
Note:
Irrespective of provisioning by an administrator or a user, all applications running on the session are reset.

The selected session is signed off and reset.

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:

- 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
• 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**

September 20, 2018

**Step 1: Update Citrix License Server**

The Licensing Usage Insights Service requires Citrix License Server 11.13.1.2 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: 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 17, 2019

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 11.13.1.2 or later.

**About Citrix License Server**

Citrix License Server 11.13.1.2 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.

**Secure Browser service**

August 6, 2019

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:

- Unauthenticated external web apps. Although typically not recommended, unauthenticated external web apps might be used for a simple proof of concept.
• Authenticated external web apps. To publish authenticated external web apps requires a resource location containing at least one Cloud Connector (two or more are recommended). For details, see Citrix Cloud Connector.

The service also offers:

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

What’s new

• June 2019: The Secure Browser can now automatically transfer your published browser to a different region if your current region is reporting an issue. To opt out, you need to disable the Region failover policy. For more information, see the Policy section.
• March 2019: This release contains enhancements that help improve overall performance and stability.
• November 2018: You can enable the Client drive mapping policy to upload and download the files to and from the remote session. For more information, see the Policy section.
• November 2018: Configure a secure browser to automatically connect you to the closest region based on your geolocation. For more information, see Publish a secure browser.
• October 2018: Secure Browser is adapted for use in five languages. For globalization information, seeCTX119253.
• October 2018: Additional region support: Secure Browser supports the Australia East region.
• September 2018: You can now download a custom icon for your published browser. For more information, see Publish a secure browser.
• August 2018: The Citrix Secure Browser service is now integrated with Citrix Workspace. For details, see Integration with Citrix Workspace.
• August 2018: Additional region support: When you publish a secure browser, you can choose among the following regions: US East, US West, Europe West, and Southeast Asia.

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.

For information about purchasing the Citrix Secure Browser service, click **How to Buy** on the Citrix Cloud home page.

**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 should indicate **Enabled**. If it does not, click the ellipsis menu and select **Enable**.
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**

If you haven’t published a secure browser yet, begin with step 3.

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**.

   ![Publish a Secure Browser](image)

   There are no users subscribed to this secure browser. Subscriptions may be managed with the Library.

   Browser versions: Google Chrome on Linux

   Register:

3. Select the type of secure browser to publish: external unauthenticated (default) or external authenticated. Then click Continue. By default, the unauthenticated apps are available to all Workspace subscribers (users) without user assignment. For authenticated apps, you must explicitly add users with Citrix Cloud Library.
4. Enter the name, start URL, and select the region. By default, the icon of the Google Chrome executable is used when you publish a Secure Browser. You can now bring 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.

- Choose among the following regions: 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.
• When you are done, click Publish. When the publishing completes, the Manage tab lists the browser you published.

5. Use the Citrix Cloud Library to add users to the authenticated secure browser you created. Click the right arrow at the end of the row to expand the details pane containing a link to the Library.

6. When you click that link, 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.
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.
Citrix Cloud

For example, if you set an idle timeout of 20 and an idle warning time of 5, a message will be sent to the user if there is no activity in the session for 15 minutes (20 minus 5). If the user does not respond, the session will end five minutes later.

When you’re done, click **OK**.

**Policies**

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, you need to disable the Region failover policy. If you published the browser using the Auto region selection, your secure browser will remain 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 need to navigate to the desired location for storing the file. For example, Anonxxx > ctxmnt > C > Users > UserName > Documents.

  – The dialog box might prompt the user to accept the Permit all access or Read and Write permissions to access the ctxmnt folder.
When you’re done, click OK.

Whitelists

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

Enter whitelist 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 whitelist.

For example, to set https://example.com as a whitelisted URL:

- example.com:* allows connection to this URL from any port.
- example.com:80 allows connection to this URL only from port 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 external web apps URL 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.

Edit

Use the Edit task to change the name, start URL, or region of a published browser. 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.
Citrix Cloud

Monitor usage

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 may 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.

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 should publish HTTPS URLs.

**More information**

See the following resources for additional 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**

August 20, 2019

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 2019VDAs, 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 names.

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
   - Subscription name
   - Location

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 How to attach a data disk to a Windows virtual machine in 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.

Pick a name
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 con-
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.
   - **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

![Choose master image](image)

**How would you like to link your master image?**

- **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**.
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.

   - **Use Azure Managed Disks or unmanaged disks**: Learn more about Azure Managed Disks at https://docs.microsoft.com/en-us/azure/virtual-machines/windows/managed-disks-overview.

   - **Azure Hybrid Use Benefit**: Select whether or not to use existing on-premises Windows
Citrix Cloud

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.

![Workspace link](image)

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.
**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, `\fileserver\share#sAMAccountName#`

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**.
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 identify 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
• 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.
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.

Citrix Virtual Desktops Essentials

May 22, 2019

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:

- 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

© 1999-2019 Citrix Systems, Inc. All rights reserved.
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.

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 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.

- **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.

- **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](https://www.citrix.com/about/citrix-product-guide/).

**System requirements, prerequisites, and compatibility**

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

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.
- 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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
ICP 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.
9. On the **Summary** page, click **Install**.
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.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload the Windows 10 master image to the destination storage account in Azure before you create the machine catalog.</td>
</tr>
</tbody>
</table>

**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.
5. In *Performance*, select *Standard*.
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.
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.

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

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.window.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.

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.

**Citrix Cloud Labs**

February 21, 2018

This is where you can find new, experimental services that feature the latest technologies available. These services could change over time and may not necessarily become Citrix Cloud services. If you experience a problem with a Labs service or would like to provide feedback, please visit our Citrix Cloud - Labs Discussions page.

**Session Manager**

December 6, 2018

Session Manager is a service that can be used in conjunction with the Citrix Virtual Apps and Desktops service to create anonymous, ready-to-use applications reducing the time it takes to launch an application. This service is currently available as a Lab only.

**Getting Started with Session Manager**

The Session Manager service requires you have a Citrix Virtual Apps and Desktops service account within Citrix Cloud and the ability to create an on-premise StoreFront. For more information on how to buy or request a trial of the Citrix Virtual Apps and Desktops service, go to the Citrix Cloud product page.

The applications delivered through this service are pre-launched and delivered by an anonymous StoreFront and published to an anonymous Delivery Group.

**Using Session Manager**

To use Session Manager, you need to configure a few settings with an on-premise StoreFront and Citrix Virtual Apps and Desktops service.

1. Connect a cloud-hosted StoreFront to Citrix Gateway.
2. Create an anonymous on-premise StoreFront.
3. Create an anonymous Delivery Group.
4. Add applications to the anonymous Delivery Group.

Connect a cloud-hosted StoreFront to Citrix Gateway

1. Access the cloud-hosted StoreFront through [https://customername.xendesktop.net/Citrix/StoreWeb/](https://customername.xendesktop.net/Citrix/StoreWeb/).
2. Set up Citrix Gateway as an ICA proxy (no authentication or session policies are needed). This can be configured in the Citrix Virtual Apps and Desktops service by clicking the Manage tab. Under Configuration on the left, click StoreFront and under the right pane select Set Gateway.

4. Bind Citrix Cloud Connectors as Secure Ticket Authority (STA) servers to Citrix Gateway. For more information, see Setting Up StoreFront with Citrix Cloud.
Create an anonymous on-premises StoreFront

1. Install StoreFront 3.6.

2. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.

3. Select the Stores node in the left pane of the Citrix StoreFront management console and in the Actions pane, click Create Store.

4. On the Store Name page, specify a name for your store, select Allow only unauthenticated (anonymous) users to access this store and click Next.
5. Store names appear in Citrix Receiver under users’ accounts so choose a name that gives users information about the content of the store.

6. On the delivery Controllers page, click Add.

7. In the Add Delivery Controller dialog box:
   
a) Specify a name that will help you identify the deployment.
   
b) Point the on-premise StoreFront Store’s Delivery Controllers to the Citrix Cloud Connectors. For transport select HTTP and port 80. The StoreFront machine must be able to directly access the connector through the fully qualified domain name (FQDN).
8. Click OK.

9. Click Next on the Citrix XenApp Services URL section.

10. View the summary and click Create.

The unauthenticated store is now available for use. For more information, see Create an unauthenticated store.

**Create an anonymous Delivery Group**

1. Using the Citrix Virtual Apps and Desktops service in Citrix Cloud, click Delivery Groups on the left pane in Studio. Under Actions on the right, click Create Delivery Group.
2. The Create Delivery Group wizard launches and guides you through the creation of a Delivery Group.

3. Select **Allow any authenticated users to use this Delivery Group**. Then select the **Give access to unauthenticated (anonymous) users: no credentials are required to access StoreFront** option. Click **Next** to complete the steps. For more information, see Create Delivery Groups.
Add applications to the anonymous Delivery Group

By adding applications to an anonymous Delivery Group they can be launched anonymously and can be viewed by all Active Directory users.

1. Click Delivery Groups in the left panel in Studio.
2. Select the Delivery Group that was configured in the previous step.

3. Click Add Applications in the right pane Action menu.

4. Follow the wizard to add applications to the anonymous Delivery Group.
Note:
When selecting an application to prelaunch on the Session Manager UI, make sure that the application is assigned to only one Delivery Groups. The application must not be provided by multiple Delivery Groups. For more information, see Applications.

Manage anonymous Delivery Groups

1. Return to the Session Manager page and click Manage.
2. From the Manage page, you can edit or activate your anonymous Delivery Groups.

If you have questions or need additional information about this Lab, refer to the Discussions site.

Connecting Session Manager to On-Premise XenApp and XenDesktop Deployments

December 5, 2018

You can use Session Manager to create anonymous, ready-to-use applications reducing the time it takes to start an application. The Session Manager Lab can be used to prelaunch anonymous sessions to on-premises XenApp and XenDesktop version 7.12 deployments by following the steps below.

Session Manager uses the Session Manager Proxy service running on a Cloud Connector machine to continuously poll the Broker for session, application, and Delivery Group data. This data is sent to the Session Manager Cloud service and continuously replenishes pools of pre-launched sessions in the on-premises deployment.

Getting Started

You can access the Session Manager Service from the Lab Services section in Citrix Cloud. To get started with connecting your on-premises deployment to the Session Manager Service with a Cloud Connector, click Settings. The Settings tab shows resource locations and Cloud Connectors that you previously configured. If you don’t have any resource locations configured for Citrix Cloud, the following screen appears.
If you created a resource location already, it can take up to 30 seconds for the data to synchronize with the Session Manager when you first access the Labs service. If you do not see your resource locations and Connectors listed, click the Refresh button.

This guide assumes that you do not have a resource location created. If you already have a resource location with connectors that you would like to use for the service, continue to the “Internal StoreFront Configuration” section.

Create a Resource Location in Citrix Cloud

1. On the machine that you would like to use for your Cloud Connector, navigate to the **Resource Locations** page in Citrix Cloud by clicking the menu icon and selecting **Resource Locations**. You can also click the **Add a Resource Location** button on the Session Manager Settings tab.
2. Click **Download** to put the Cloud Connector (CWCCconnector.exe) installer onto your connector machine.

3. Double-click on the Cloud Connector file and follow the installation instructions.

4. After finishing the installation, your **Resource Locations** page shows the connector and resource location:
The Session Manager Settings page now lists your new resource location. It also shows the status of the Session Manager Proxy service running on that particular connector as indicated by the orange ‘warning’ status bar as shown in the following image. You will configure the resource location and the bar will turn green later in the guide.

The Manage page shows that the Session Manager Service does not currently know about any Anonymous Delivery Groups in your resource location.
Internal Storefront Configuration

This section describes how to configure an internal StoreFront store to interact with the Session Manager Service. You can perform this configuration on an existing store, or create a new authenticated or anonymous store that is only used by the Session Manager for better network isolation and security options.

Configure the store to trust the Session Manager

The Session Manager Trusted Issuer in your store establishes trust between Citrix StoreFront and the Session Manager Service. Use the following steps to establish trust.

1. On the StoreFront server, run the command `Add-PSSnapin Citrix` to import the StoreFront PowerShell Snap-In.

2. Run the following command to obtain a reference to your desired Store Service object. Replace the variable “Store” with your store service name.

   ```powershell
   $storeService = Get-STFStoreService | Where-Object { $_.Name -eq ”Store” }
   ```

3. Create a new Session Manager Trusted Issuer, using your customer ID as the tenant ID. Your customer ID is the first 12 characters of your Citrix Cloud customer name. For instance, if your customer name is PrelaunchDemo, your customer ID is PrelaunchDem. The Thumbprint parameter is the thumbprint of the certificate that Session Manager uses to sign tokens bound for the store. Make sure that you copy the thumbprint value correctly from this guide. The Name parameter can be any short string, and is used in StoreFront logging.
4. Add the trusted issuer to the store service configuration:

   ```powershell
   Add-STFSessionManagerTrustedIssuer -StoreService $storeService -SessionManagerTrustedIssuer $trustedIssuer
   ```

5. Restart the StoreFront server with the `iisreset` command, or restart the machine.

### Configure StoreFront Optimal Gateway Settings to Force All Traffic Through Your Netscaler Gateway

The Session Manager requires external access for ICA traffic. This means that the internal StoreFront store must provide an ICA file for external access from the internal Store. To do this, you must force all traffic for apps obtained from this store through Citrix Gateway, even when starting apps internally. This is done with an Optimal Gateway setting on the store.

#### To configure Optimal Gateway settings

1. Configure the Optimal Gateway setting for your store by using the following PowerShell code. The code assumes that your Store name is “Store”. Change the code to suit your specific configuration before running. The gateway ID can be any randomly generated GUID, it only has to match both commands.

   ```powershell
   $gatewayID = "2eba0524-af40-421e-9c5f-a1ccca80715a"
   $logonAddress = "https://myazureurl-eastus.xenapponazure.com"
   $ctxstaPath = "https://XA-Controller.xenapp.local/scripts/ctxsta.dll"
   $siteId = "1"
   $virtualPath = "Citrix\Store"
   $farmName = "Controller"

   Add-DSGlobalV10Gateway -Id $gatewayID -Name MyNewGateway -Address $logonAddress -LogonUsedForHDXObject -SecureTicketAuthorityUrls $ctxstaPath
   Add-DSStoreOptimalGateway -SiteId $siteId -VirtualPath $virtualPath -GatewayId $gatewayID -EnabledOnDirectAccess $true -Farms $farmName
   iisreset
   ```
2. Test the configuration by starting an application from the store and examining the ICA file returned. The **Address** field of the ICA file shows the STA ticket instead of an IP Address. Open the ICA file with Citrix Receiver and confirm that the application starts successfully.

**Gateway Configuration**

You must add the Cloud Connector machine as a Secure Ticket Authority (STA) server to Citrix Gateway. This allows the Session Manager to tunnel through the Citrix Gateway to the on-premises StoreFront server by utilizing STA tickets obtained from the Citrix Cloud STA service.

1. Navigate to the **Citrix Gateway > Virtual Servers** page in the configuration utility.

2. Select the virtual server that you would like to use for tunneling SessionManager traffic to the StoreFront server and click **Edit**.

3. Under **Published Applications**, click **STA Servers** and add your connector to the list of STA Servers that are used by this virtual server. In the image below, the IP address for the connector is 10.0.0.5, and you can see that the connector is sending STA ticketing requests to the Citrix Cloud STA service by checking the **Auth ID** column for CWSSTA.
Session Manager and Broker Configuration

The status bar of the connector in the Session Manager Settings tab is orange. The following steps enable the Session Manager Proxy on the connector to poll the Broker for session data, and allow for the Session Manager to begin pre-launching anonymous sessions.

To configure the Session Manager and Broker service

1. Configure the Broker to trust XML and Prelaunch Requests. To use anonymous prelaunch, the Broker needs to have the `TrustManagedAnonymousXmlServiceRequests` and `TrustRequestsSentToTheXmlServicePort` flags set to true.

   **Note:**
   
   In production environments, configure the XML service to only accept requests originating from trusted StoreFront machines.
   
   Run the following PowerShell commands to enable both of these flags.

   ```powershell
   1. **Add-PSSnapin
   2. Set-BrokerSite -TrustManagedAnonymousXmlServiceRequests $true
   -TrustRequestsSentToTheXmlServicePort $true
   ```

2. Configure the Broker to trust the connector machine as a delegated administrator.
   a) Open **Active Directory Users and Computers** on your domain controller and add the Cloud Connector machine(s) to their own group as shown in the following diagram:
b) In Citrix Studio, select **Configuration > Administrators** and then click **Create Administrator**.

c) Choose the Active Directory group you created in step 2a, select **All** and then click **Next**.

d) In Citrix Studio, select **Configuration > Administrators** and then click **Create Administrator**.
e) On the Role page, select **Help Desk Administrator** for the role and then click **Next**.
Citrix Cloud

f) On the next page, click **Finish** to create the administrator.

**Session Manager Service Configuration**

Return to the Session Manager **Settings** tab to complete the configuration.

1. Click the down arrow icon beside the resource location name to open the Session Manager Settings for this resource location.

2. Enter the following values:
   - **Gateway Address** - use address to Citrix Gateway that was configured in the “Gateway Configuration” portion of this guide. Do not include protocols on this address.
   - **Gateway Port** - The port through which users connect to Citrix Gateway.
   - **Internal Broker URL** - The internal FQDN of the broker. Note this FQDN needs to be resolvable from the Connector machine. For example, *xa-controller.xenapp.local*.
   - **StoreFront Name** - The StoreFront store’s friendly name setting. You can find the name by using the `Get-STFStoreService` PowerShell cmdlet on the StoreFront server.
   - **Internal StoreFront URL** - For example, `https://storefront.xenapp.local/Citrix/Store`
   - **Check to Skip Certificate Validation** - Select this setting if you are using an internal certificate on the StoreFront server that cannot be validated by an external service. Use this in testing environments only.

After 1-2 minutes, the Cloud Connector begins uploading anonymous Delivery Group data to the Session Manager. The connector status bar on the **Settings** page turns green as shown in the image below:
3. Configure the desired prelaunch parameters on your anonymous Delivery Groups.

   a) Click the ellipsis icon to the right of each row to edit Delivery Groups.

   b) Activate the Delivery Group and observe the pre-launching of sessions in Citrix Studio.

You can see three anonymous application sessions running Calculator, matching the configuration found on the Manage page in Session Manager.
Technical Security Overview for Session Manager and On-Premises XenApp and XenDesktop

Session Manager is a product managed by Citrix Cloud. When using the Session Manager Service to prelaunch sessions to an on-premises data center, the Desktop Delivery Controllers (DDC), Storefront servers, Virtual Delivery Agents (VDAs), and any Citrix Gateways used for remote access remain under the customer’s control. The customer has security ownership over these components. You enable the new feature by using the TrustManagedAnonymousXmlServiceRequests setting. The XML Service should only accept incoming requests from trusted Storefront servers when using this setting.

The Session Manager Service uses external ICA connections to internal VDAs to prelaunch sessions, and collects a limited amount of data from the on-premises DDC through the Citrix Cloud Connector to enable prelaunch configuration and monitoring from the cloud. The following diagram illustrates the service and its security boundaries.

XML Service Anonymous Prelaunch Considerations

As part of the Session Manager Service configuration, you must enable both the TrustRequestsSent-
To the XmlServicePort and TrustManagedAnonymousXmlServiceRequests flags. The TrustManagedAnonymousXmlServiceRequests flag allows for the XML Service to accept anonymous prelaunch requests from Storefront. These requests are not validated by the XML Service, and it is important to remember that you allow trusted StoreFront servers only to communicate with the XML service when using either of these settings.

To isolate the XML Service, it is possible to change the XML Service port. Follow the instructions in the article How to Change the XML Port in XenDesktop in the Citrix Support Knowledge Center to change the XML Service port. When the service is running on its own port, it is possible to use network isolation through firewalls or other technologies to keep the XML Service separated from user traffic.

Prelaunched Anonymous Sessions

The session tracking metadata that is stored in the site’s database designates the prelaunched anonymous sessions created in Session Manager. When a user obtains an ICA file for a prelaunched session, the session is converted to a standard anonymous session and can never be reused or connected to again. Standard non-prelaunched anonymous sessions cannot be connected to or modified by the Session Manager Service.

Data Flow

The Citrix Cloud Connector periodically uploads a limited set of metadata that is queried through the broker delegated admin API to allow for prelaunch configuration and monitoring from the Session Manager Service. The data includes Delivery Group names, session counts, application names, and VDA counts. The data is uploaded to an HTTPS server on port 443.

The on-premises Storefront server is configured in a standard external access configuration to channel all ICA traffic through the Netscaler Gateway. The Session Manager Service makes calls to the on-premises Storefront through Netscaler Gateway to enumerate and start anonymous applications. The on-premises Storefront server trusts the Session Manager Service by using a certificate pinning mechanism that ensures requests are valid only for a single tenant and Storefront store. When you configure the internal Storefront for external access, the ICA file obtained from the internal StoreFront contains all of the information necessary to perform the prelaunch sequence from the Session Manager Service.

Data Isolation

The Session Manager Service is a multi-tenant service. The metadata collected from each customer’s Citrix Cloud Connector is stored within this service. The collected metadata, along with configuration information is isolated between tenants. A limited number of authorized Citrix administrators have
internal access to the collected metadata and configuration information for the purposes of maintenance or troubleshooting. External queries for collected customer data and configuration information require unique CWC administrator credentials.

**Citrix Cloud Connector Network Access Requirements**

The Citrix Cloud Connectors require that port 443 is open for outbound traffic to the Internet, and can be hosted behind an HTTP proxy. The communication protocol used in Citrix Cloud for HTTPS is TLS 1.0, 1.1, or 1.2. Within the internal network, the connector will require a Help Desk admin level of delegated administration access to the Broker. You can configure this by using Active Directory Machine Groups and the Administrators settings in Citrix Studio.

**Citrix Gateway Access Requirements**

The Session Manager Service must be able to tunnel through Netscaler Gateway to the internal Store-Front server. You grant access by configuring at least one of the Citrix Cloud Connectors as a STA server for the gateway. The Session Manager Service obtains a STA ticket from the Citrix Cloud STA Server for an internal connection. The ticket is then redeemed by Netscaler Gateway through the Citrix Cloud Connector’s connection to the same cloud-based STA server. Citrix Cloud services with access to the Citrix Cloud STA server can make connections to your internal resources through Netscaler Gateway with this configuration.

**More Information**

See the following resources for additional security information:

- Secure Deployment Guide for Citrix Gateway

**Note:**

This document is intended to provide the reader with an introduction to and overview of the security functionality of Citrix Cloud; and to define the division of responsibility between Citrix and customers with regard to securing the Citrix Cloud deployment. It is not intended to serve as a configuration and administration guidance manual for Citrix Cloud or any of its components or services.
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

May 17, 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 andVDAs registered in that resource location.
8. Session is established between client, Citrix Gateway, and resolved VDA.

External Trusted Domains to Resource Domain

In this scenario, the business partner needs access to resources published to corporate users. The
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.

**Access control for SaaS and Web apps in StoreFront–Preview**

August 16, 2019

The Access Control Sync for StoreFront utility enables administrators to harness the power of Access Control’s enhanced security and web-filtering policies to deliver secure access to SaaS and Web applications through the on-premises StoreFront. When users launch these applications, Access Control’s policies are automatically applied, protecting the users and network from the malware and data leaks.

**Objectives**

Administrators use the utility to provide SaaS and enterprise Web applications in the on-premises StoreFront. This utility must be installed on a Delivery Controller in the on-premises Virtual Apps and Desktops environment. With the utility, administrators can perform the following tasks:

- Display SaaS and Web applications in the on-premises StoreFront.
- Enable access to SaaS and Web apps with single sign-on (SSO), web-filtering policies, and enhanced security control policies through the on-premises StoreFront using Citrix Workspace app.
- View the Access Control analytics on the Analytics tab in Access Control and Citrix Analytics service.

**Prerequisites**

- **Citrix Cloud:**
  - Access Control, Citrix Gateway, Secure Browser, and Citrix Analytics services. To sign up for an Access Control service trial, see Get Started.
  - Gateway Connector, if synchronizing Web applications. For more information, see Citrix Gateway Connector.
  - Before using the utility, you must have SaaS applications already configured and published using the Citrix Gateway service. For more instructions, see Support for Software as a Service apps.
You will need an end user account that is subscribed to the SaaS or Web applications (in the Library in Citrix Cloud) that you want to synchronize with your on-premises StoreFront. When configuring the utility, you will enter the user name and password of this account. After you run the utility, these applications appear in your on-premises store.

- **Citrix XenApp and XenDesktop or Virtual Apps and Desktops:**
  - Citrix XenApp and XenDesktop (7.14 or later) or Virtual Apps and Desktops 7 (1808 or later) on-premises deployment.
  - The Delivery Controller must have Microsoft .NET Framework 4.7.2 or later installed. To download this version, visit [https://dotnet.microsoft.com/download/dotnet-framework/net472](https://dotnet.microsoft.com/download/dotnet-framework/net472).
  - The account you use to run the utility must be at least a Delivery Group Administrator or a custom administrator with permission to publish applications in the Virtual Apps and Desktops Site.

**Limitations**

You can use only Citrix Workspace app to access the synchronized SaaS and Web apps. Access control for your SaaS and Web apps in the on-premises StoreFront is not supported through Workspace for Web.

**Configure Gateway endpoint URL**

To ensure Access Control policies are applied to applications, configure the web.config file on the StoreFront server with the Gateway service endpoint URL that Workspace app uses to retrieve the policies: [https://config.netscalergateway.net/ngs/policy/getcfg.json](https://config.netscalergateway.net/ngs/policy/getcfg.json). The endpoint URL consists of the Gateway FQDN followed by `/ngs/policy/getcfg.json`.

**Note:**

If you don’t have an Access Control entitlement in your Citrix Cloud account or you only want to use single sign-on with your synchronized applications, you don’t need to configure this endpoint URL.

1. Log on to the StoreFront server in your on-premises deployment.
2. Navigate to the web.config file at `C:\inetpub\wwwroot\Citrix\store`.
3. Open the web.config file and locate the `<externalEndpoints>` section.
4. Add a new endpoint called `WebSaaSPolicy` that includes the Gateway service URL where the Workspace app retrieves the Gateway security policies. For example:

   ```xml
   <externalEndpoints>
   ```
<clear />
<endpoint id="WebUI" url="https://sf.aaa.local/Citrix/storeWeb/receiver.html">
  <add capability="WebUI" />
</endpoint>
<endpoint id="WebUIAuthentication" url="https://sf.aaa.local/Citrix/storeWeb/CitrixAuth/Login">
  <add capability="WebUIAuthentication" />
</endpoint>
<endpoint id="WebSaaSPolicy" url="https://config.netscalergateway.net/ngs/policy/getcfg.json">
  <add capability="WebSaaS policy" />
</endpoint>
</externalEndpoints>

5. Save the web.config file.

6. Restart the IIS server. From the command line, enter `iisreset /noforce`.

**Synchronize SaaS and Web applications**

Use the following steps to install and run the Access Control Sync for StoreFront utility. You can only synchronize applications that your end user account is subscribed to in the Citrix Cloud Library.

**Step 1. Download and install the Access Control Sync for StoreFront utility.**

1. Log on to the Delivery Controller and download the utility package on citrix.com. To get the package, navigate to the Downloads > Citrix Virtual Apps and Desktops > Betas and Tech Previews section and download Access control for SaaS and Web apps in StoreFront-Preview.
2. Accept the license agreement and click **Install**.
3. If the User Account Control security dialog appears, click **Yes**.

![User Account Control dialog](C:\citrix-dev\hybridaccesscontrolsyncsetup\AccessControlSync.msi)

Do you want to allow this app from an unknown publisher to make changes to your device?

Publisher: Unknown
File origin: Hard drive on this computer

Show more details

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

4. Click **Finish** to complete the installation.

**Step 2. Synchronize applications using the AccessControlSyncforStoreFront tool.**
1. On the Delivery Controller machine, start the Citrix Access Control Sync for StoreFront application.

2. Configure the following settings:

   - **Citrix Workspace URL**: Enter the URL that you use to access Citrix Workspace. To obtain this URL, select *Workspace Configuration* from the Citrix Cloud menu.
   - **Citrix Workspace Username and Citrix Workspace Password**: Enter the credentials of the end user account that’s subscribed to the SaaS apps you want to synchronize.
   - **Citrix Workspace AD Domain**: Enter the Active Directory domain name. To obtain the domain name, select *Identity and Access Management* from the Citrix Cloud menu and then select *Domains*.
   - **Local Storefront App Prefix (optional)**: Enter a prefix for the SaaS applications that will appear in StoreFront. For example, if the SaaS application name is “test” and you enter “demo” into this field, the utility synchronizes the application as “demo-test”.
   - **Local Delivery Group**: Enter the name of the delivery group containing the users and user groups who can use SaaS applications.

3. Click *Synchronize SaaS Apps*. If you are integrating applications that exist on the machine, the utility deletes them and installs applications with the Access Control policies.

You can check the synchronization process by monitoring the *Status* panel on the form.

To view the Access Control analytics and app usage, go to the *Analytics* tab in Access Control and Citrix Analytics service.