Citrix Gateway Service

Contents

Release Notes

October 12, 2021

The Citrix Gateway service release to cloud release notes describe the new features, enhancements to existing features, fixed issues, and known issues available in a service release. The release notes include one or more of the following sections:

What's new: The new features and enhancements available in the current release.

Fixed issues: The issues that are fixed in the current release.

Known issues: The issues that exist in the current release and their workarounds, wherever applicable.

V12.1 (October 11, 2021)

What's new

- **Merger of Citrix Gateway service tile into a single Secure Workspace Access in Citrix Cloud**

  The Citrix Gateway service tile and the Secure Workspace Access service tile are merged into the Secure Workspace Access service tile and the Citrix Gateway landing page is modified for the Secure Workspace Access service. Therefore you do not see the **Virtual Apps and Desktops** and the **Add a Web/SaaS app** shortcuts. However, the Citrix Virtual Apps and Desktops customers can enable Citrix Gateway service from **Workspace configuration > Access > External Connectivity**. There is no change in the functionality, otherwise.

  The following Citrix Gateway service features are moved to Secure Workspace Access service.

  - Configuring SaaS and Enterprise web apps
  - Enabling enhanced security controls
  - Configuring contextual policies

  All Secure Workspace Access customers, including Citrix Workspace Essentials and Citrix Workspace Standard, can now use one single Secure Workspace Access tile for configuring SaaS and Enterprise web apps, enhanced security controls, contextual policies, in addition to web filtering policies.

  [ACS-645]

Get started with Citrix Gateway service

October 12, 2021

Customers who are entitled for the Citrix Virtual Apps and Desktops service get the Citrix Gateway service enabled, by default. Customers do not have to request a separate Citrix Gateway service trial. For details, see Sign up for the service.

> **Important:**
>
> On the Citrix Cloud home page, you do not see the Citrix Gateway service tile. The Citrix Gateway service tile and the Secure Workspace Access service tile are merged into the Secure Workspace Access service tile and the landing page is modified for the Secure Workspace Access service. Therefore you do not see the **Virtual Apps and Desktops** shortcut. However, the Citrix Virtual Apps and Desktops customers can enable Citrix Gateway service from **Workspace configuration > Access > External Connectivity**. There is no change in the functionality, otherwise.

Technical Security Overview

September 28, 2020

This document applies to all the features pertaining to Citrix Gateway service hosted in Citrix Cloud, including HDX transport, SaaS apps, and Enterprise Web apps.

Citrix Cloud manages the operation for Citrix Gateway services, replacing the need for customers to manage the Citrix Gateway appliance. Citrix Gateway service is provisioned through Citrix Workspace app.

Citrix Gateway service provides the following capabilities:

- **HDX connectivity for XenApp users** – a globally available service providing secure connectivity from users in any location to virtual apps and desktops.
- **Secure access to SaaS applications** – a unified user experience bringing configured SaaS applications to end-users.
- **Secure access to Enterprise web applications** – a unified user experience bringing configured Enterprise web applications to end-users.
- **Secure access to all apps and files in a digital workspace** – a modern approach to managing all your devices through a single platform, Citrix Endpoint Management. Supported platforms include desktops, laptops, smartphones, tablets, and IoT.

HDX Connectivity: The Virtual Delivery Agents (VDAs) hosting the apps and desktops remain under the customer's control in the data center of their choice, either cloud or on-premises. These components are connected to the cloud service using an agent called the Citrix Cloud Connector.

SaaS apps: Software as a Service (SaaS) is a software distribution model to deliver software remotely as a web-based service. Commonly used SaaS apps include Salesforce, Workday, Concur, GoToMeeting, and so forth.

Enterprise web apps: Enterprise web apps delivery using Citrix Gateway service enables enterprise specific applications to be delivered remotely as a web-based service. Commonly used Enterprise web apps include SharePoint, Confluence, OneBug, and so on. You need Citrix Gateway Connector to access the Enterprise web apps.

SaaS apps and Enterprise web apps are provisioned through Citrix Workspace using Citrix Gateway service. The Citrix Gateway service coupled with Citrix Workspace provides a unified user experience for the configured Enterprise web apps, SaaS apps, configured virtual apps, or any other workspace resources. Along with Secure Access, Citrix Gateway service also protects users from untrusted links embedded in user-generated content.

Endpoint Management integration: When integrated with Citrix Endpoint Management plus Citrix Workspace, Citrix Gateway service provides secure remote device access to your internal network and resources. Onboarding Citrix Gateway service with Endpoint Management is fast and simple. Citrix Gateway service includes full support of Citrix SSO for apps such as Secure Mail and Secure Web.

Data flow

Citrix Gateway service is a globally distributed multitenant service. End-users utilize the nearest Point-of-Presence (PoP) where the particular function they need is available, regardless of Citrix Cloud Control plane geo-selection or location of the applications being accessed. Configuration, such as authorization meta-data is replicated to all PoPs.

Logs used by Citrix for diagnostic, monitoring, business, and capacity planning are secured and stored in one central location.

Customer configuration is stored in one central location and distributed globally to all PoPs.

Data flowing between the cloud and customer premises uses secure TLS connections over port 443.

Encryption keys used for user authentication and single sign-on are stored in hardware security modules.

Data isolation

The Citrix Gateway service stores the following data:

- Configuration data needed for the brokering and monitoring of the customer's applications – data is scoped by customer when persisted.
- TOTP seeds for each user device – TOTP seeds are scoped by customer, user, and device.

Audit and Change Control

Currently Citrix Gateway service does not make auditing and change control logs available to customers. Logs are available to Citrix which can be used to audit activities of end-user and administrator.

Credential handling

The service handles two types of credentials:

- User credentials: End-user credentials (passwords and authentication tokens) might be made available to Citrix Gateway service to perform the following:
  - Secure Workspace Access - The service uses the user's identity to determine access to SaaS and Enterprise web applications and other resources.
  - Single sign-on - The service might have access to the user's password to complete the SSO function to internal web applications using HTTP Basic, NTLM, or forms-based authentication. The encryption protocol used for password is TLS unless you specifically configure HTTP Basic authentication.
- Administrator credentials: Administrators authenticate against Citrix Cloud. This generates a one-time signed JSON Web Token (JWT) which gives the administrator access to the management consoles in Citrix Cloud.

> **Points to note**

- All traffic over public networks is encrypted by TLS, using certificates managed by Citrix.
- Keys used for SaaS app SSO (SAML signing keys) are fully managed by Citrix.
- For MFA, Citrix Gateway service stores per-device keys used to seed the TOTP algorithm.
- To enable Kerberos Single Sign-On functionality, customers might configure Gateway Connector with credentials (user name + password) for a service account trusted to perform Kerberos Constrained Delegation.

Deployment considerations

Citrix recommends that users consult the published best practices documentation for deploying Citrix Gateway services. More considerations regarding SaaS apps and Enterprise web apps deployment, and network connector are as follows.

Selecting the correct Connector: The correct connector must be selected, depending on the use case:

Use Case	Connector	Form factor
User Authentication: Active Directory	Citrix Cloud Connector	Windows software
HDX Connectivity	Citrix Cloud Connector	Windows software
SaaS apps access	Citrix Cloud Connector	N/A

Use Case	Connector	Form factor
Enterprise web apps access	Citrix Cloud Connector, Citrix Gateway Connector	N/A
Enterprise apps and files delivered by Citrix Endpoint Management	Citrix Cloud Connector, Citrix Gateway Connector	N/A

Citrix Cloud Connector network access requirements

For information on Citrix Cloud Connector network access requirements, see https://docs.citrix.com/en-us/citrix-cloud/overview/requirements/internet-connectivity-requirements.html

Citrix Gateway Connector network access requirements

For information on Citrix Cloud Connector network access requirements, see https://docs.citrix.com/en-us/citrix-gateway-service/gateway-connector.html

Citrix Gateway service HDX Connectivity

Using the Citrix Gateway service avoids the need to deploy Citrix Gateway within the customer data centers. To use the Citrix Gateway service, it is a prerequisite to use the StoreFront service delivered from Citrix Cloud.

Customer Best Practices

Customers are recommended to use TLS within their network and not enable SSO for applications over HTTP.

Migrate Citrix Gateway to Citrix Gateway service for HDX Proxy

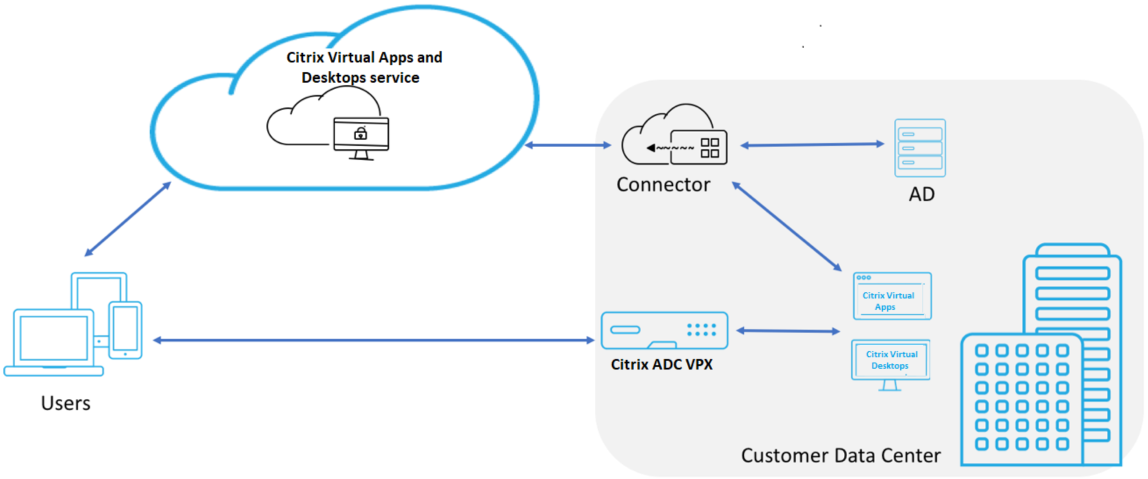
December 2, 2020

You can migrate from a Citrix Gateway for HDX Proxy and to a fully managed cloud-based HDX Proxy powered by the Citrix Gateway service on Citrix Cloud.

Cloud based HDX Proxy

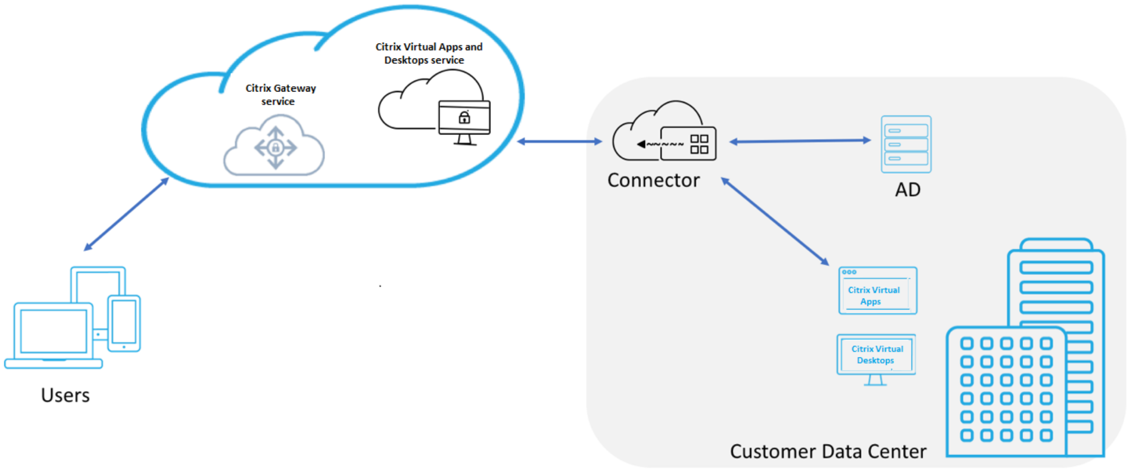
When Citrix Cloud customers purchase Citrix Virtual App Service, Virtual Desktop Service, Virtual App and Desktop Service, or Workspace Service they might use an on-premises Citrix Gateway for secure remote access. The Citrix Gateway is purchased separately.

Figure 1. Deployment with Citrix Gateway as HDX Proxy



Citrix Gateway service is a cloud based HDX Proxy that provides secure remote access through a cloud-based gateway that front-ends virtual apps and desktop environments that are Citrix Virtual Apps and Desktops environments.

Figure 2. Deployment with Citrix Gateway service as HDX Proxy



This feature is now included with your Citrix Virtual Apps service, Citrix Virtual Desktops service, Citrix Virtual Apps and Desktops service, and Workspace Service entitlements. You can enable this feature.

Migration from an on-premises Citrix Gateway to cloud based Citrix Gateway service

On-premises Citrix Gateway appliance is customer managed and cloud based Citrix Gateway service is Citrix managed. This section explains how to migrate from an on-premises Citrix Gateway to cloud hosted Citrix Gateway service for HDX Proxy. Though Citrix Gateway and Citrix Gateway service provide HDX Proxy, the underlying infrastructure and working mechanism is different. However, the steps to enable HDX Proxy on cloud is simple and straight forward with just a few clicks.

To enable this migration, enable the Citrix Gateway service for Citrix Virtual Apps and Desktops. Once enabled, traffic starts traversing through the Citrix Gateway service and an on-premises Citrix Gateway is no longer required.

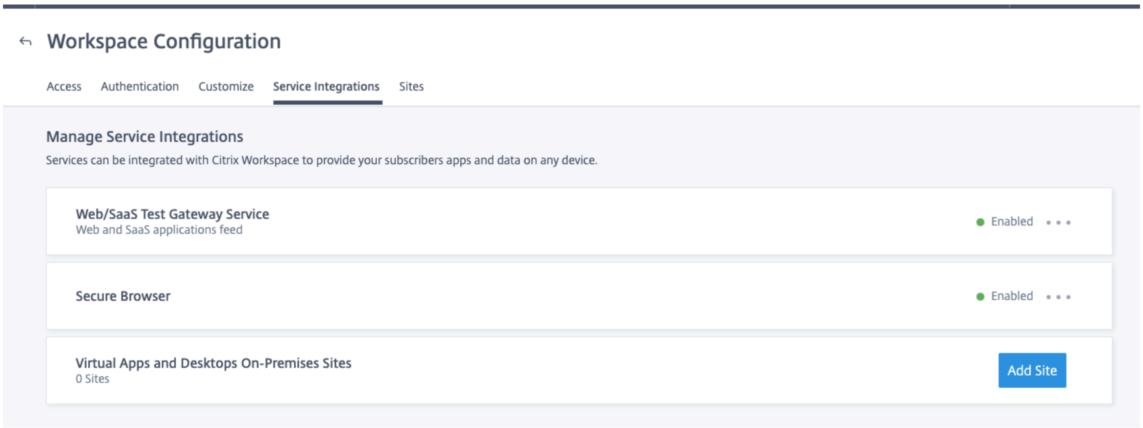
Following are the assumptions made before you begin migration from an on-premises Citrix Gateway to cloud based Citrix Gateway service.

- The customer has subscribed for Citrix Cloud service and has purchased Citrix Virtual Apps and Desktops.
- The customer uses an on-premises Active Directory to authenticate users on cloud.

Enable the Citrix Gateway service

Following are the steps to enable Citrix Gateway service for Citrix Virtual Apps and Desktops service users:

1. Sign into Citrix Cloud Services as an admin user.
2. Click the hamburger icon and choose **Workspace Configuration**.
3. Click **Service Integrations**.
4. Locate the ellipsis next to **Gateway**, click the ellipsis, and then click **Enable**.



Manage Service Integrations

Services can be integrated with Citrix Workspace to provide your subscribers apps and data on any device.

Web/SaaS Test Gateway Service — Web and SaaS applications feed — ● Enabled

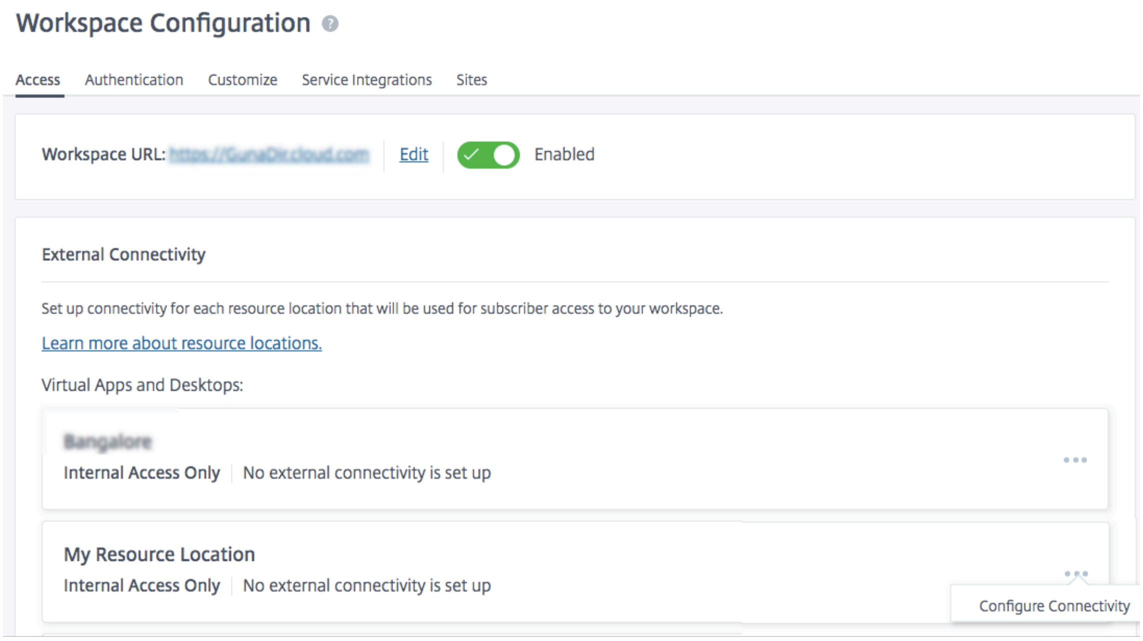
Secure Browser — ● Enabled

Virtual Apps and Desktops On-Premises Sites — 0 Sites

Following are the steps to enable Citrix Gateway Service for Citrix Workspace users.

1. Sign into Citrix Cloud Services as an admin user.

2. Click the hamburger icon and choose **Workspace Configuration**.
3. In the **Access** tab, under **External Connectivity** section, locate the ellipsis next to **My Resource Location** present under **Citrix Virtual Apps and Desktops** service.
4. Click the ellipsis, click **Configure Connectivity**.



Workspace Configuration

Workspace URL: [redacted] Edit ✓ Enabled

External Connectivity

Set up connectivity for each resource location that will be used for subscriber access to your workspace.

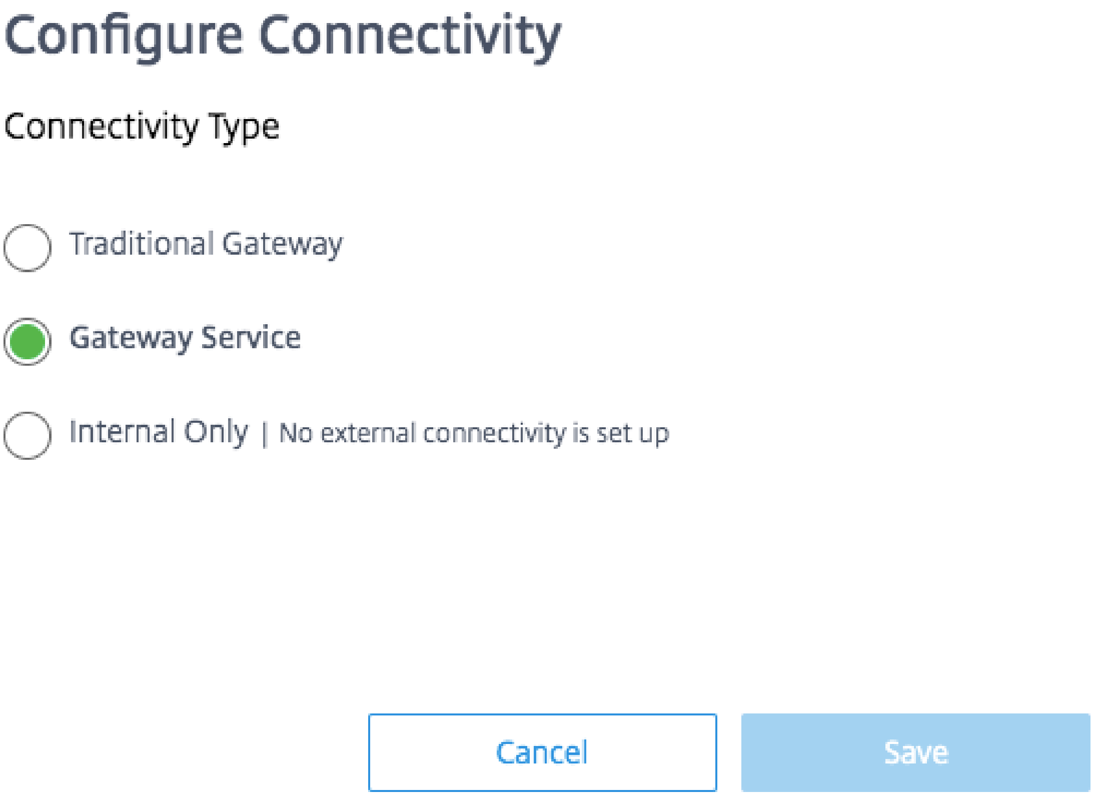
Learn more about resource locations.

Virtual Apps and Desktops:

[redacted]
Internal Access Only | No external connectivity is set up

My Resource Location
Internal Access Only | No external connectivity is set up

5. Choose **Gateway Service** in the pop-up window and then click **Save**.



Configure Connectivity

Connectivity Type

○ Traditional Gateway

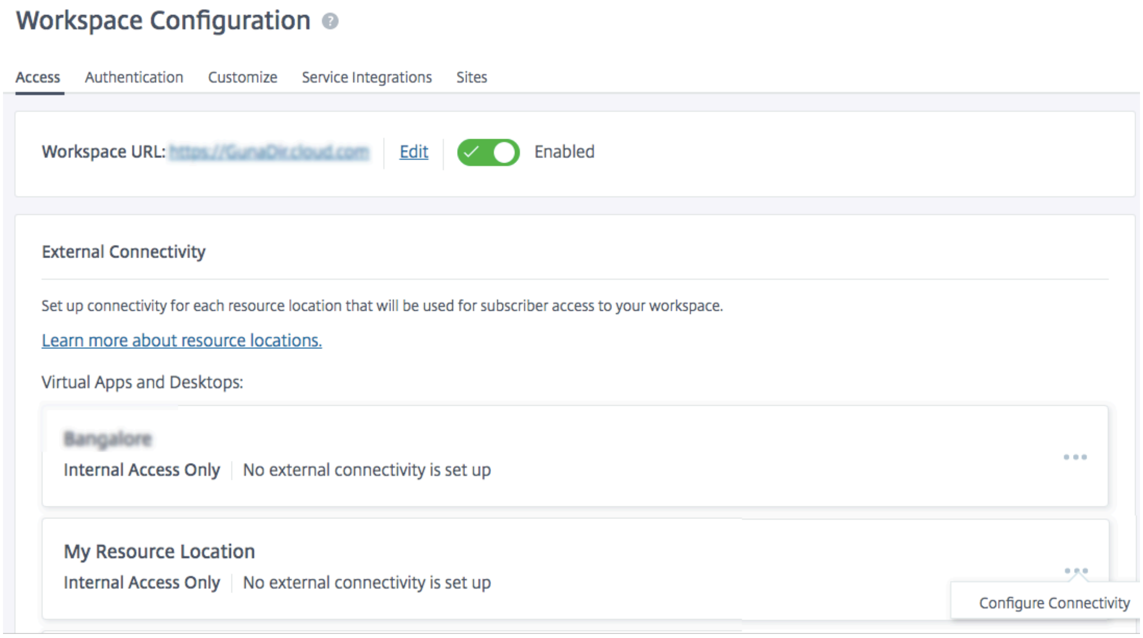
● Gateway Service

○ Internal Only | No external connectivity is set up

Roll back to Citrix Gateway

To roll back the HDX Proxy to an on-premises Citrix Gateway, perform the following.

1. Sign into Citrix Cloud Services as an admin user.
2. Click the hamburger icon on the top left and choose **Workspace Configuration.**
3. In the **Access** tab under **External Connectivity** section, locate the ellipsis next to **My Resource Location** present under **Virtual Apps and Desktops**.



Workspace Configuration

Access | Authentication | Customize | Service Integrations | Sites

Workspace URL: https://GunaDir.cloud.com | Edit | Enabled

External Connectivity

Set up connectivity for each resource location that will be used for subscriber access to your workspace.

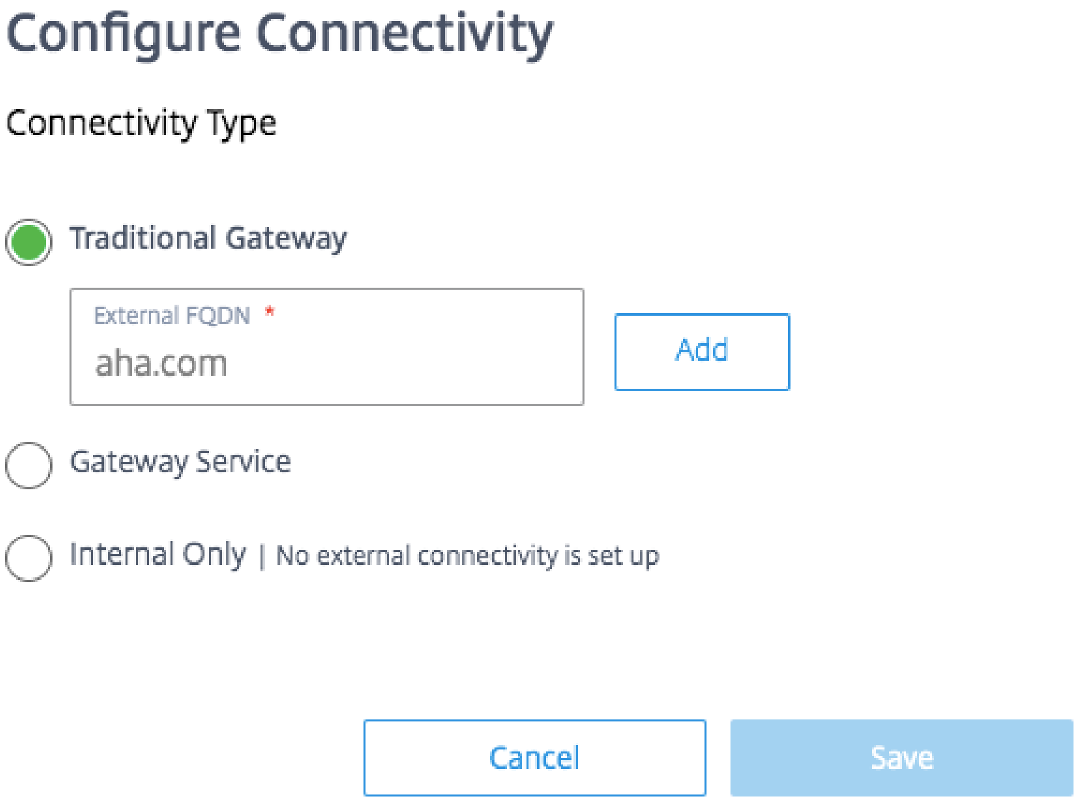
Learn more about resource locations.

Virtual Apps and Desktops:

Bangalore
Internal Access Only | No external connectivity is set up

My Resource Location
Internal Access Only | No external connectivity is set up

4. Click the ellipsis, click **Configure Connectivity**.
5. Choose **Traditional Gateway** and enter the FQDN.



Configure Connectivity

Connectivity Type

● Traditional Gateway

External FQDN *: aha.com

○ Gateway Service

○ Internal Only | No external connectivity is set up

6. Click **Add** and then click **Save**.

HDX Adaptive transport with EDT support for Citrix Gateway service

July 19, 2021

Enlightened Data Transport (EDT) is a Citrix-proprietary transport protocol built on top of UDP. EDT delivers a superior user experience on challenging long-haul connections while maintaining server scalability.
Adaptive Transport is a data transport mechanism for Citrix Virtual Apps and Desktops. Adaptive Transport provides the ability to use EDT as the transport protocol for ICA, and switch to TCP when EDT is not available.
For more information on Adaptive Transport and EDT, see Adaptive Transport documentation.

Prerequisites

- Citrix Virtual Apps and Desktops service
- Virtual Delivery Agent (VDA) 2012 or later
- Citrix Workspace app
  - Windows: version 1912 or later (2105 or later recommended)
  - Linux: version 1912 or later (2104 or later recommended)
  - Mac: version 1912 or later
  - iOS: latest version available in Apple App Store
  - Android: latest version available in Google Play
- UDP port 443 must be allowed for outbound traffic from VDA to Citrix Gateway Service
- Rendezvous protocol must be enabled and working. For details, see the Rendezvous Protocol documentation.
- Ensure Adaptive Transport is enabled. For details, see the Adaptive Transport setting documentation.
- For more information on Adaptive Transport and EDT, see the Adaptive Transport documentation.

Considerations

The following are some of the considerations for using EDT with the Citrix Gateway Service.

- It is highly recommended to enable EDT MTU Discovery. For details, see the Adaptive Transport documentation.
- EDT with Citrix Gateway Service is only available when using Rendezvous. If HDX sessions are being proxied through the Cloud Connector, only TCP is available for data transport.
- When an EDT session establishment fails the session falls back to TCP, causing an increase in the session launch time.

- If you want to continue to proxy HDX sessions through the Cloud Connector, consider disabling Adaptive Transport via the Citrix Studio policy to avoid the potential increase in session launch times introduced by the fallback sequence.
- Citrix recommends using EDT through the Citrix Gateway Service only with VDAs running on Windows 10 and Windows Server 2019. There are limitations on Windows Server 2012 R2 and 2016 that do not allow for an MTU greater than 1024 for DTLS-encrypted sessions, which can affect the performance and user experience.
- With Adaptive Transport, Citrix Gateway service does not Support UDP Audio.

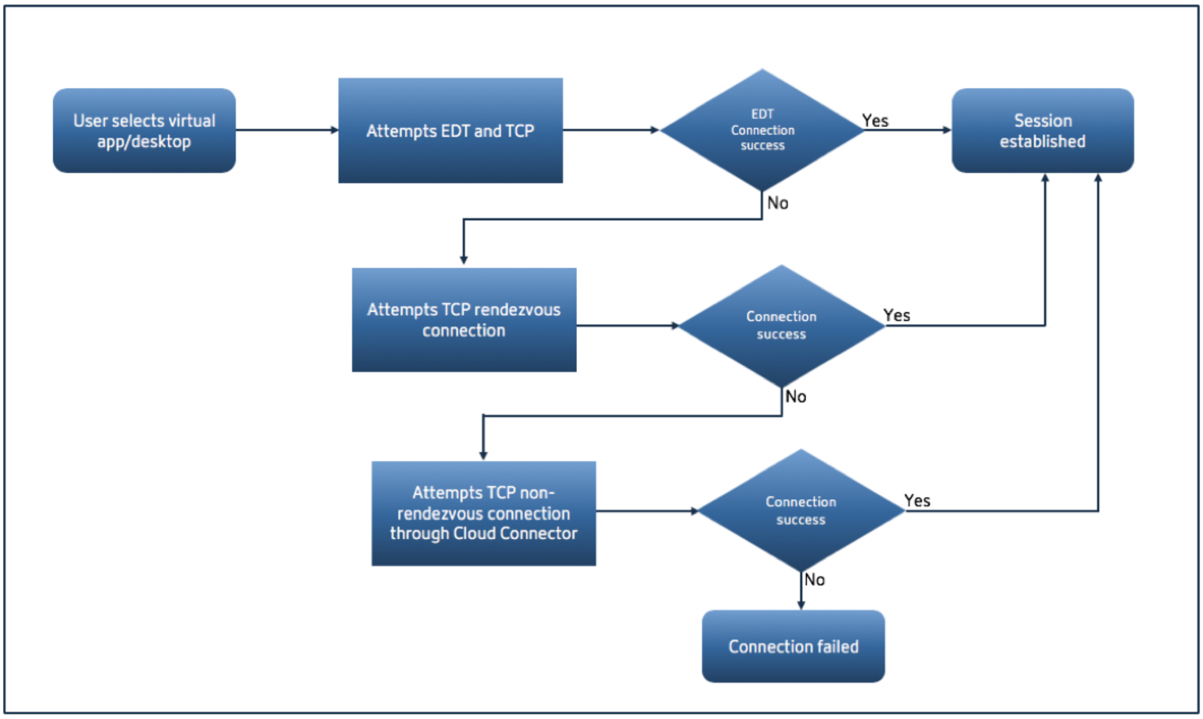
Transport protocol validation

To know if your sessions are using EDT, refer to the following:

- Connection protocol in Citrix Director: https://support.citrix.com/article/CTX220730.
- After you launch an app or a desktop, go to **Citrix Workspace app > Connection Center**, select the appropriate session, click **Properties**, and look at the Transport encryption property. If it shows DTLS, the session is using EDT for transport. If it shows TLS, the session is using TCP for transport.
- If you launched a desktop, you can open a PowerShell or command prompt and run “ `ctxsession -v`” . The Transport Protocols property displays the connection method being used:
  - EDT Rendezvous: “**UDP > DTLS > CGP > ICA**”
  - TCP Rendezvous: “**TCP > SSL > CGP > ICA**”
  - Proxy through Cloud Connector: “**TCP > CGP > ICA**”

Connection fallback

If EDT negotiation fails for any reason, the session falls back to TCP with Rendezvous. And if that fails, then the session falls back to proxying through the Cloud Connectors.



EDT MTU discovery

It is highly recommended to enable EDT MTU Discovery to ensure that each session uses the optimal MTU for that connection.

In case EDT MTU Discovery is disabled or the user's client does not support the feature, the EDT MTU is automatically set to 1380 to avoid fragmentation-related issues.

It is possible for users to connect via a network that requires an MTU lower than 1380, which is mostly seen with mobile networks (3G, 4G) or VPN connections. If this is the case in your environment, and the clients in use by the users do not support EDT MTU Discovery, Citrix recommends that you disable Adaptive Transport until the feature is available in your target client platform.

For more details on EDT MTU Discovery, see Adaptive Transport documentation.

Troubleshooting

The following provides some general troubleshooting guidance.

Sessions connect but are not using EDT:

1. If the sessions are being proxied through the Cloud Connector, make sure that Rendezvous is enabled and that it works properly, as this is a pre-requisite for using EDT with the Citrix Gateway service. For details, see Rendezvous documentation.
2. If the sessions are using TCP Rendezvous:

- Make sure you are using VDA version 2012 or later.
- Check whether Adaptive Transport is enabled in Citrix policies.
- Make sure the appropriate firewall rules are in place to open UDP 443 from the VDA machines to the Citrix Gateway Service. For more details, see the Rendezvous](/en-us/citrix-virtual-apps-desktops-service/hdx/rendezvous-protocol.html) documentation.
- If there is a local firewall enabled in the VDA machine (for example Windows Defender Firewall), make sure that there are no rules blocking UDP 443.
- If using a proxy, only SOCKS5 proxies can be used to proxy EDT. For details, see the Rendezvous documentation.

Sessions connect with EDT but disconnect randomly after some time:

1. Make sure you are using VDA version 2012 or later.

Session fails to connect:

1. Make sure you are using VDA version 2012 or later.
2. If using a client that supports EDT MTU Discovery, ensure that EDT MTU Discovery is enabled. This helps mitigate fragmentation-related issues. For details, see Adaptive Transport documentation.
3. If using a Linux or Android client:
   - Check if Windows or Mac clients are working properly.
   - Check if the CWA version is upgraded to Linux 2104, Android 21.5.0 or later.
   - If you are using an older version of CWA then disable Adaptive Transport and ensure that TCP Rendezvous works properly.
   - Once TCP Rendezvous works, if the session fails to connect after re-enabling Adaptive Transport, see troubleshooting steps mentioned in step **Sessions connect but are not using EDT > If the sessions are using TCP Rendezvous**.

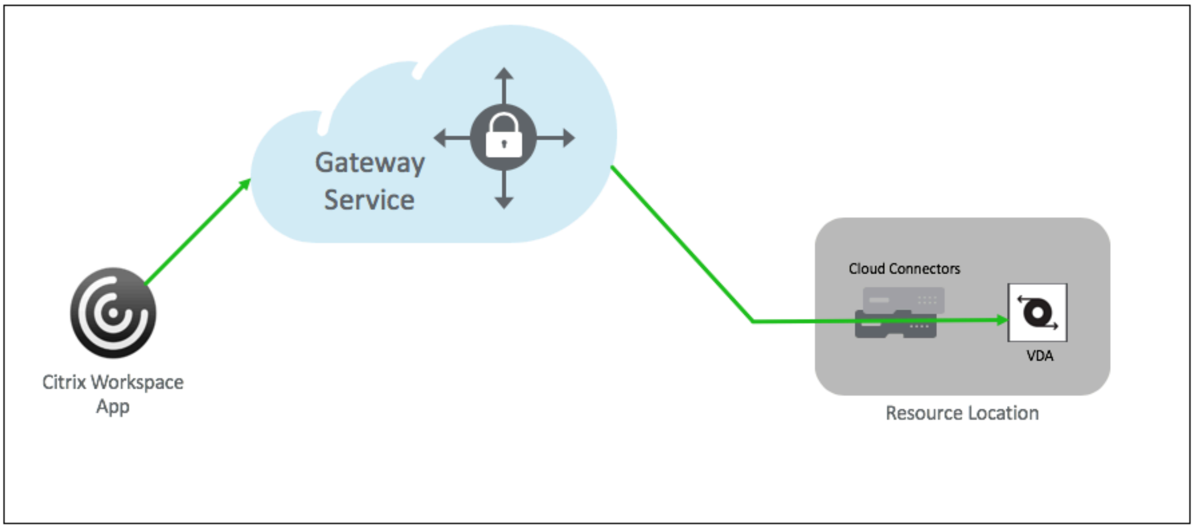
Support for Citrix Virtual Apps and Desktops

December 2, 2020

Citrix Gateway service provides users with secure access to Citrix Virtual Apps and Desktops across a range of devices including laptops, desktops, thin clients, tablets, and smartphones.

Citrix Gateway service enables secure, remote access to Citrix Virtual Apps and Desktops, without having to deploy the Citrix Gateway service in the DMZ or reconfigure your firewall. The entire infrastructure overhead of using Citrix Gateway moves to the cloud and hosted by Citrix.

You enable Citrix Gateway service in Citrix Cloud. After enabling the service, users can access their VDAs from outside their network, as shown in the following diagram.



How it works

Users' endpoints and their on-premises hosted resources VDAs are connected to their nearest respective POPs via Citrix Cloud Connectors. Later, when users select a virtual app or desktop to launch from their Workspace app, the nearest POP hosting that connection identifies the pertinent resource location and directs it to establish a Citrix Cloud Connector session to that POP forming an end-to-end connection and then a virtual session is established.

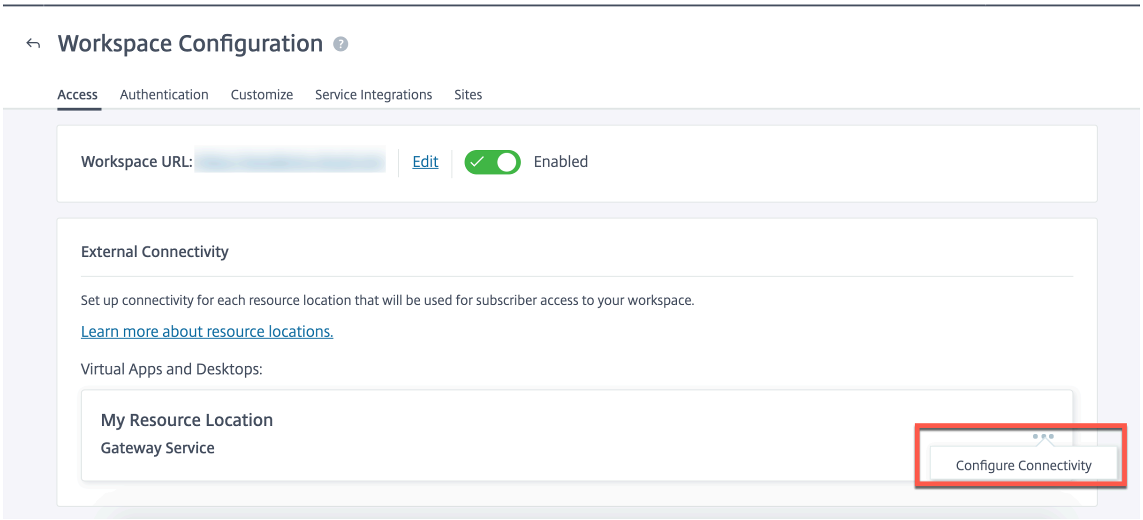
- Sessions are linked via Citrix Gateway service across cloud partner's WANs.
- VDAs and Workspace endpoints rendezvous at the Citrix Gateway service POP closest to the user.
- High quality sessions.

For more details, see Citrix Gateway service for HDX Proxy

Enable the Citrix Gateway service

Following are the steps to enable Citrix Gateway service for Citrix Workspace users.

1. Sign into Citrix Cloud Services as an admin user.
2. Click the hamburger icon and choose Workspace Configuration.
3. In the **Access tab** under **External Connectivity** section, locate ellipses next to **My Resource Location** present under **Citrix Virtual Apps and Desktops Service**. Click the ellipses, click **Configure Connectivity**.



Workspace Configuration

Workspace URL: Edit Enabled

External Connectivity

Set up connectivity for each resource location that will be used for subscriber access to your workspace.

Learn more about resource locations.

Virtual Apps and Desktops:

My Resource Location
Gateway Service

4. Choose Citrix Gateway service in the pop-up window and click **Save**.

Support for Citrix Endpoint Management

September 6, 2021

Citrix Gateway service provides remote device access to your internal network and resources.

Use cases

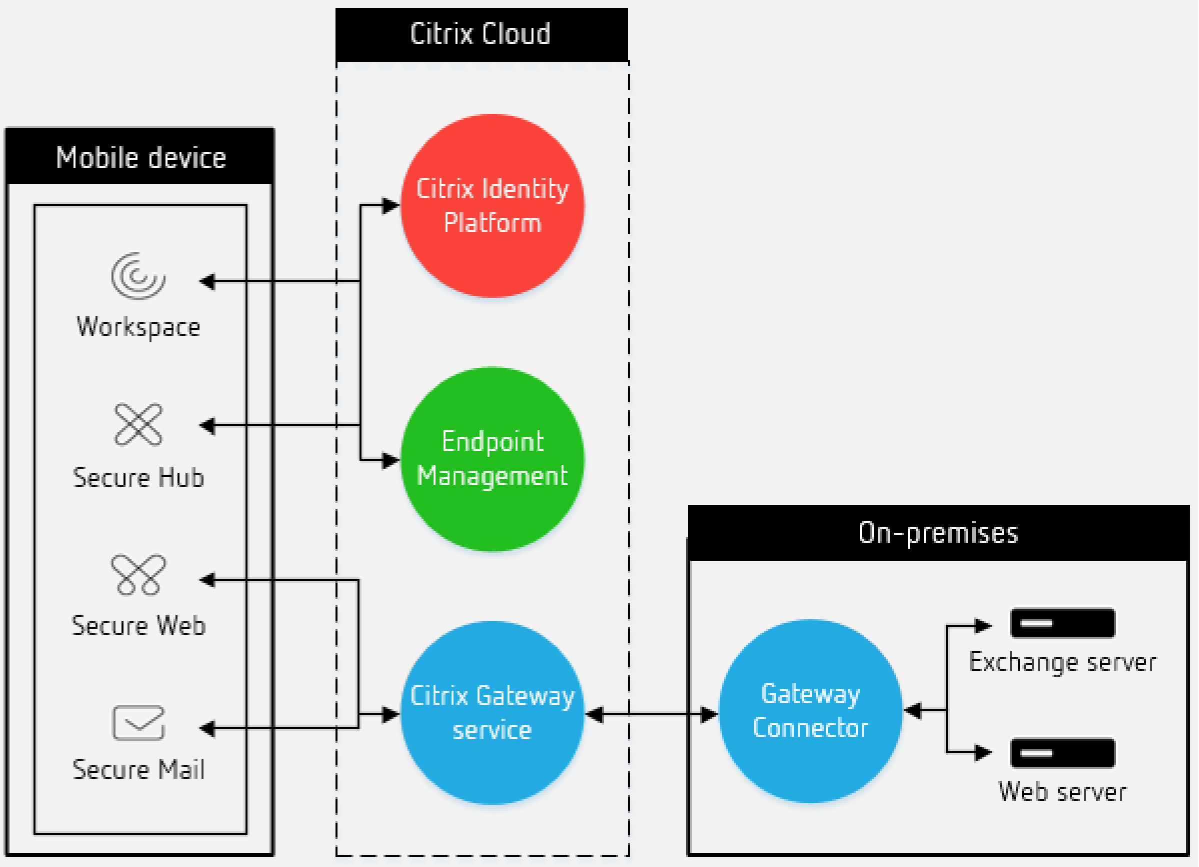
Use the cloud-based Citrix Gateway service with Endpoint Management when:

- You want a maintenance-free service that doesn't require negotiating with network, security, and compliance teams before configuring your corporate network.
- You want to use the unified authentication experience provided by Citrix Cloud. Citrix Gateway service uses the Citrix Identity provider to manage the identity information for all users in your Citrix Cloud account. For more information, see Identity and access management.
- You plan to use Citrix mobile productivity apps, such as Citrix Secure Mail or Secure Web. Citrix Gateway provides an on-demand application VPN connection. Secure Hub initiates that VPN connection on mobile devices to access corporate network sites or resources.

  This variation of a clientless VPN is also known as Tunneled – Web single sign-on (SSO). Connections such as web traffic that tunnel to the internal network use Tunneled – Web SSO. We recommend Tunneled – Web SSO for connections that require single sign-on. For more information, see App network access for Android and App network access for iOS.

Architecture and communication flow overview

The following diagram provides an overview of Citrix Gateway service architecture when used with Endpoint Management.

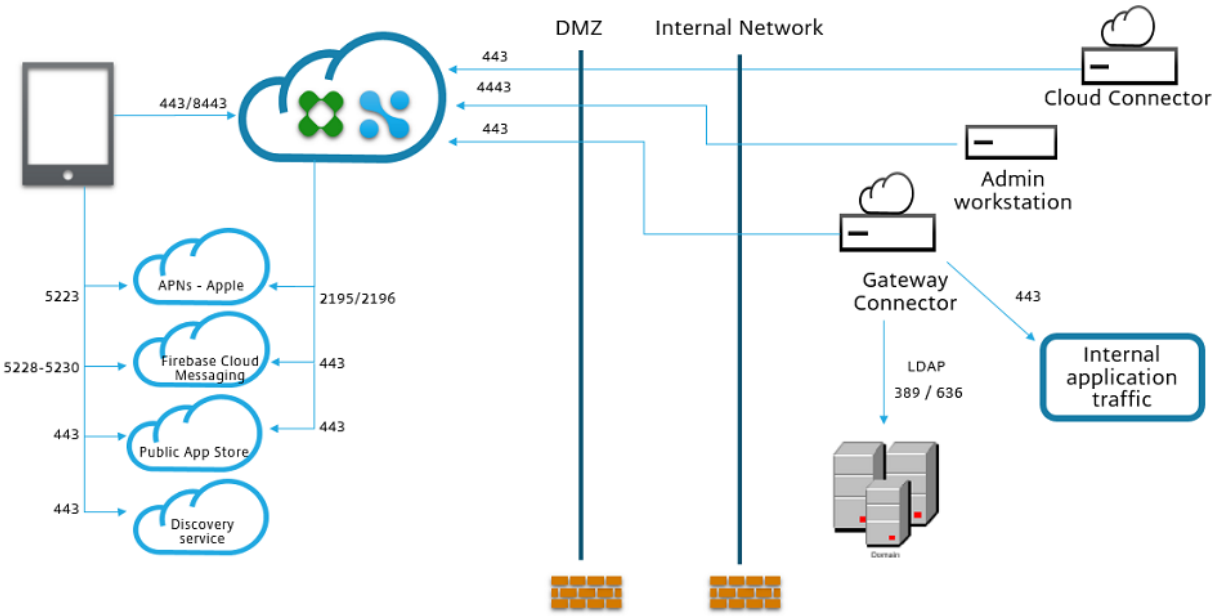


Citrix Gateway service isn't used during device enrollment in Endpoint Management. After enrollment, MDM control traffic goes directly to Citrix Endpoint Management, without going through Citrix Gateway service. Only MAM VPN data traffic is sent to Citrix Gateway service. All traffic sent to Citrix Gateway gets directed to the on-premises Gateway Connector.

The following authentication types are supported for Citrix Gateway service integration with Endpoint Management:

- Basic, Digest, NTLM
- Kerberos Constrained Delegation (KCD) single sign-on
- Form-based single sign-on
- SAML single sign-on

The following diagram shows the Endpoint Management communication flow with Citrix Gateway service.



Prerequisites

- Citrix Workspace experience enabled

  With Citrix Workspace enabled, user enrollment starts in the Workspace app. When Secure Hub detects the Workspace entitlement, Secure Hub completes enrollment. Secure Hub then opens Citrix Workspace where users can access their apps and other resources.

- Citrix Gateway service subscription
  - If you already use on-premises Citrix Gateway and want to switch to Citrix Gateway service, contact your Citrix Sales representative. Switching from on-premises Citrix Gateway to the Citrix Gateway service requires that you reenroll devices.
  - New Endpoint Management customers: Select the Citrix Gateway service during Endpoint Management onboarding.
- Gateway Connector installed on-premises in a resource location
  - Endpoint Management uses the resource location for Gateway Connector only for STA tickets for Secure Mail. Citrix Gateway sends STA traffic to the Gateway Connector in the resource location.
  - Install one or more Gateway Connectors in any one resource location. Endpoint Management doesn't support Gateway Connectors installed in multiple resource locations.
  - Install Gateway Connector in the same or a different resource location than Active Directory. The only role of Active Directory is to use the Citrix Identity provider to authenticate users to the Citrix Gateway service. Citrix Gateway service creates session connections to the Gateway Connector for authenticated users. You can have multiple Active Directories.

  - If the connector isn't available during Citrix Endpoint Management onboarding, you can install it after onboarding.

For more information, see Citrix Gateway Connector and System requirements.

To configure Citrix Gateway service with Citrix Endpoint Management

A preview of the Citrix Gateway service is available for Endpoint Management customers. For more information, see Configure Citrix Gateway use with Endpoint Management.

FAQ

April 22, 2020

This section provides the FAQs on migrating Citrix ADC VPX to Citrix Gateway service for HDX proxy.

Can I use my on-premises configurations to port into Citrix Cloud?

No, the underlying infrastructure and mechanisms are different. See section on enabling Citrix Gateway service.

Can I upload my portal customizations to Citrix Cloud?

This is not possible today. However, there are few customization options with Citrix Cloud. Refer to the following link: https://docs.citrix.com/en-us/xenapp-and-xendesktop/service/storefront.html

I had enabled Multi-Factor or two factor authentication on-premises using VPX. Can I enable this on cloud too?

The VPX provided with XenApp or XenDesktop service must be used for HDX proxy only (based on EULA) and not for authentication. Authentication on cloud is done using on-premises AD via a cloud connector or using Azure Active Directory.

Can I use SmartControl, SmartAccess using cloud services?

The VPX provided with XenApp and XenDesktop Service must be used for HDX proxy only (based on EULA) and must not be used for any other features.

How can I do a phased migration to Citrix Gateway service?

There is no configuration to support hybrid deployment (on-premises Citrix ADC VPX and Citrix Gateway service). However, it is recommended to do a phased migration by enabling Citrix Gateway service by using a trial account (which comes with limited period) and using that for limited set of users or preview users.

What is the minimum license required for Citrix Gateway service?

Any customer using Citrix XAXD service or Citrix Workspace is entitled to use Citrix Gateway service for HDX Proxy.

Locations

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