Citrix Gateway Service
Contents

Release Notes 3
Get started 8
Technical Security Overview 9
Migrate Citrix Gateway to Citrix Gateway service for HDX proxy 13
Support for Citrix Virtual Apps and Desktops 16
Support for Software as a Service apps 18
Support for Citrix Endpoint Management 28
Apps configuration using a template 31
SaaS app server specific configuration 35
Citrix Gateway Connector 48
Gateway Connector dashboard 60
Support for Enterprise web apps 62
FAQ 72
Release Notes

September 30, 2019

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.

**V3.5 (August 19, 2019)**

**Known issues**

- Launching an Enterprise Web app for an NTLM authentication enabled resource from Citrix Workspace fails if both of the following conditions are met:
  - Customer’s data center has a proxy server and that proxy server is configured on the Gateway Connector
  - Web App is configured with no SSO (Don’t use SSO)

  **Workaround:**
  - Publish the Web app as a Basic SSO app or
  - Do not have a proxy server configured on Gateway Connector

  [NGWS-8266]

- If there are SSL intercepting devices in the on premises data center where the Citrix Gateway Connector must be deployed, the connector registration does not succeed if SSL interception is enabled for the following FQDNs.
  - *.nssvc.net
  - *.netscalermgmt.net
  - *.citrixworkspacesapi.net
  - *.citrixnetworkapi.net
  - *.citrix.com
  - *.servicebus.windows.net
  - *.adm.cloud.com
The SSL interception must be disabled for these FQDNs for successful connector registration. [NGSWS-8923]

- Download logs option is available in Gateway Connector from version 401.251. If you are on an earlier version of connector and you upgrade the connector to version 401.251, you cannot download the logs even though the Download Logs link is available. [NGSWS-8438]

**V2019.06.01**

**Fixed issues**

- Edits made in the Access Control page are not propagated to the database because the failed jobs were re-tried incorrectly. [NGSWS-7733]

**V2019.05.01**

**Fixed issues**

- If a customer’s data center has an authentication-enabled proxy server configured for Gateway Connector, the connector fails to register itself with Citrix Cloud. [NGSWS-7231]

- When adding an Enterprise Web app, if the FQDN contains an underscore ( _ ) in the domain name, an error is displayed. [NGSWS-7033]

- If the SSO type for a SaaS app is changed from Don’t use SSO to SAML, the configuration change fails. [NGSWS-7466]

**V2019.04.02**

**What’s new**

- **Kerberos authentication support for Citrix Gateway Connector to outbound proxy** [NGSWS-6410]

  Kerberos authentication is now supported for the traffic from Citrix Gateway Connector to outbound proxy. Gateway Connector uses the configured proxy credentials to authenticate to the outbound proxy.
Fixed issues

- In rare cases, web filtering UI configuration changes do not take effect to the tenant traffic. [NGSWS-7147]
- Memory leaks on ICA service nodes, resulting in a high memory usage. [NGSWS-7014]
- Application fails to launch because Citrix Gateway service node does not send the X-NGS-Session-Id header as part of policy document retrieval request to the CVMs. [NGSWS-6963]
- Authentication and app enumeration on Citrix Gateway service fail if the token size for authentication exceeds 64 KB. [NGSWS-5932]

V2019.04.01

What's new

- **Web/SaaS apps traffic can now be routed via a corporate-network-hosted Gateway-Connector thus avoiding two factor authentication.** If a customer has published a SaaS app that is hosted outside the corporate network, support is now added to authenticate traffic for that app to go through an on premises Gateway Connector.

  For example, consider that a customer has an Okta protected SaaS app (like Workday). The customer may want that even though the actual Workday data traffic is not routed via Citrix Gateway service, the authentication traffic to Okta server is routed through Citrix Gateway service via an on premises Gateway Connector. This helps a customer to avoid a second factor authentication from Okta server as the user is connecting to Okta server from within the corporate network.

  [NGSWS-6445]

- **Disabling Filtering Website Lists and Website Categorization.** Filtering Website Lists and Website Categorization can be disabled if the admin chooses not to apply these functionalities for a specific customer.

  [NGSWS-6532]

- **Automatic geo routing for secure browser service redirects.** Automatic geo routing is now enabled for secure browser service redirects.

  [NGSWS-6926]

Fixed issues

- Web app launch fails for a customer when the value of the CustomerId is in camel case.
• Connection to a Secure Mail server is not possible with FQDN. If the customer configuration has FQDN configured for the mail server, then the connection fails.

• App launch fails after the Gateway Service session times out. The end user needs to re-login to access the apps.

• When renaming a SaaS app, the name changes in the GUI but does not change in the Workspace app. Similarly, when changing or adding an icon of certain SaaS apps and Web apps, the icon updates in the GUI but is not propagated to the Workspace app.

• If Enhanced Security is enabled on a Web app (hosted inside corporate network) and if that app is launched from a native browser, then the app launch is redirected to secure browser service because native browser cannot enforce enhanced security policies.

• An app fails to launch if the app FQDN is in camel case.

• Deleted applications still show up in the cloud library.

• When there is an outbound proxy configured for Gateway Connector and if the proxy has authentication enabled, Gateway Connector cannot perform authentication with the proxy server.

• In race conditions, app configuration does not get propagated intermittently.

• App launch fails intermittently with a “Failed to fetch Policy Document.” error.

• Deleted apps still show up in Workspace app.

• Gateway Service supports form response sizes up to 32k for Web applications with form based SSO which is not sufficient for certain applications. With this fix, Gateway Service now supports form response sizes of up to 64k for Web Applications with form based SSO type.
V2019.03.01

What’s new

- **“Detect” button is added in the “Add a Gateway Connector” page.** The Detect button is used to refresh the list of connectors, allowing the newly added connector to reflect in the Web app connectivity section.
  [CGOP-6358]

- **A new category “Malicious and Dangerous” is added in the “Access Control Web Filtering” categories.** A new category named Malicious and Dangerous in the Access Control Web Filtering categories is added under the Malware and Spam group.
  [CGOP-6205]

Fixed issues

- Sometimes, Gateway Connector crashes when multiple threads access the same resource.
  [CGOP-6359]

- In some cases, delete operation using an administrator credential for a Web or SaaS application that does not have subscribed users or groups fails.
  [CGOP-6310]

- Configurations for Citrix Gateway Connector are lost upon editing Form based SSO parameters.
  [CGOP-6158]

- **Add another app option does not work when you access the option navigating as follows, Edit app>Overview>Add another app.**
  [NGSWS-6089]

- A newly added connector takes too long to show up in the UI.
  [NGSWS-5505]

- Outbound connections from a connector fail when the connector uses the external FQDN value for the connection via an outbound proxy.
  [NGSWS-6451, NGSWS-6431]

- In some cases, app enumeration fails for a customer when the value of the **CC-Customer-Id** field has letters in lower case and in upper case.
  [NGSWS-4924]
• Upon launching an application in a Secure Browser session, the display message incorrectly shows “Connecting to [application id]” instead of “Connecting to “[application name].”

[NGSWS-6061]

• Athena tokens which exceed 64k bytes in size upon decompressing is not supported.

[NGSWS-5932]

Get started

September 30, 2019

This document walks you through how to get started with onboarding and setting up the SaaS apps delivery for the first time. This document is intended for application administrators.

The following are the steps you need to perform to get started:

1. Sign up for Citrix Cloud.
2. Request for the Citrix Gateway service entitlement.
3. Post entitlement, Citrix Gateway service is provisioned under My Services.
4. Access the Citrix Gateway service UI.

Name: Sign up for Citrix Cloud

To start using Citrix Gateway service, you must first create a new Citrix Cloud account or join an existing one that has been created by someone else in your company. For detailed processes and instructions on how to proceed, see Signing Up for Citrix Cloud.

Step 2: Request for the Citrix Gateway service entitlement

To request for the Citrix Gateway service entitlement, on the Citrix Cloud screen, under the Available Services section, click the Request Trial tab present in the Citrix Gateway service tile.
Step 3: **Post entitlement, Citrix Gateway service is provisioned under My Services**

After you receive the Citrix Gateway service entitlement, the Citrix Gateway service tile moves to **My Services** section as shown below.

Step 4: **Access the Citrix Gateway service UI**

Click the **Manage** tab present on the tile to access the Citrix Gateway service UI. After you click the **Manage** tab, an **Overview** screen explaining the available services appears.

**Technical Security Overview**

September 30, 2019

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.
Citrix Gateway Service

- **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 additionally 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 multi-tenant 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.
Citrix Gateway Service

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) may be made available to Citrix Gateway service to perform the following:
  - Access control - The service uses the user’s identity to determine access to SaaS and Enterprise web applications and other resources.
  - Single sign-on - The service may have access to the user’s password in order 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 may configure Gateway Connector with credentials (username + password) for a service account trusted to perform Kerberos Constrained Delegation.
Citrix Gateway Service

Deployment considerations

Citrix recommends that users consult the published best practices documentation for deploying Citrix Gateway services. Additional 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:

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Connector</th>
<th>Form factor</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Authentication: Active Directory</td>
<td>Citrix Cloud Connector</td>
<td>Windows software</td>
</tr>
<tr>
<td>HDX Connectivity</td>
<td>Citrix Cloud Connector</td>
<td>Windows software</td>
</tr>
<tr>
<td>SaaS apps access</td>
<td>Citrix Cloud Connector</td>
<td>N/A</td>
</tr>
<tr>
<td>Enterprise web apps access</td>
<td>Citrix Cloud Connector, Citrix Gateway Connector</td>
<td>N/A</td>
</tr>
<tr>
<td>Enterprise apps and files delivered by Citrix Endpoint Management</td>
<td>Citrix Cloud Connector, Citrix Gateway Connector</td>
<td>N/A</td>
</tr>
</tbody>
</table>

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

September 30, 2019

The following sections guide you in migrating from a Citrix Gateway for HDX proxy and to a fully managed cloud-based HDX proxy powered by 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 may 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 is XenApp and XenDesktop environments.

Figure 2. Deployment with Citrix Gateway service as HDX Proxy
This feature is now included with your XenApp Service, XenDesktop Service, XenApp and XenDesktop Service and Workspace Service entitlements. You can enable this feature.

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

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

Also, please refer to FAQs for any additional information.

To enable this migration, enable Citrix Gateway service for XenApp and XenDesktop service. Once enabled, traffic starts traversing through Citrix Gateway service and an on premises Citrix Gateway will no longer be required.

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

- Customer has subscribed for Citrix cloud service and has purchased XenApp and XenDesktop service.
- 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 XenApp and XenDesktop service users:

1. Sign into Citrix Cloud Services as an admin user.
2. In the **XenApp and XenDesktop Service** menu, choose **Manage > Service Delivery**. The **Service Delivery** screen appears.

3. Click **NetScaler Gateway**.

4. Click **Use cloud hosted Citrix NetScaler Gateway** and click **Save**.

Following are the steps to enable NetScaler 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 **XenApp XenDesktop Service**. Click the ellipses, click **Configure Connectivity**.

4. Choose **NetScaler Gateway Service** in the pop-up window and click **Save**.
Roll back to VPX

To roll back the HDX proxy to an on premises VPX, please follow the below steps.

Following are the steps to roll back the HDX proxy to an on premises VPX for XenApp and XenDesktop service users.

1. Sign into Citrix Cloud Services as an admin user.
2. In the XenApp and XenDesktop Service menu, choose Manage > Service Delivery. The Service Delivery screen appears.
3. Click NetScaler Gateway.
4. Click Use your own NetScaler Gateway in resource location.
5. Enter your NetScaler Gateway URL and click Save.

Following are the steps to roll back the HDX proxy to an on premises VPX for Citrix Workspace users.

1. Sign into Citrix Cloud Services as an admin user.
2. Click the hamburger icon on the top left and choose Workspace Configuration.
4. Click the ellipses, click Configure Connectivity, and click Save.
5. Choose Add Existing NetScaler Gateway in pop-up window and click Add. Click Save.

Support for Citrix Virtual Apps and Desktops

September 30, 2019

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

Citrix Gateway service provides users with secure VPN 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 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.

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.

© 1999-2019 Citrix Systems, Inc. All rights reserved.
4. Choose Citrix Gateway service in pop up window and click Save.

**Support for Software as a Service apps**

September 30, 2019

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.

SaaS apps can be accessed using Citrix Workspace using Citrix Gateway service. The Citrix Gateway service coupled with Citrix Workspace provides a unified user experience for the configured SaaS apps, configured virtual apps, or any other workspace resources.

SaaS apps delivery using Citrix Gateway service provides you an easy, secure, robust, and scalable solution to manage the apps. SaaS apps delivered on the cloud have the following benefits:

- **Simple configuration** – Easy to operate, update, and consume.
- **Single sign-on** – Hassle free logon with Single sign-on.
- **Standard template for different apps** – Template based configuration of popular apps.

**How SaaS apps work with Citrix Gateway service**

1. Customer admin configures SaaS apps using Citrix Gateway service UI (citrix.cloud.com). The admin then adds subscribers (users) for the apps.
2. Admin provides the service URL to the users to access Citrix Workspace.
3. Users subscribed for an app can see the app upon logon to Citrix Workspace.
4. To launch the app, user clicks the enumerated SaaS app icon.
5. SaaS app trusts SAML assertion provided by Citrix Gateway service and the app is launched.

**Note:** Configured SaaS apps are aggregated along with virtual apps and other resources in Citrix Workspace for a unified user experience.
Ways to configure SaaS apps

SaaS apps can be configured and published in the following two ways:

- Template based configuration - For configuration steps, see Configuring and publishing apps using template
- Manual configuration - Configuration steps are as follows.

Configure and publish apps manually

The following configuration takes the Splunk app as an example to configure and publish an app manually:

1. On the Citrix Gateway service tile, click Manage.
2. Click Add a Web/SaaS app tab below the Single Sign On tile.
3. Click Skip to configure Splunk app manually.
4. Select **Outside my corporate network**.

5. Enter the following details in the **App Details** section and click **Save**.

   **Name** – Name of the application.

   **URL** – URL with your customer ID. If SSO fails or when **Don’t use SSO** option is selected, the user is redirected to this URL.

   **Related Domains** - Related domain is auto-populated based on the URL that you have provided. You can add more than one related domain.

   **Icon** – Click **Change** to change the app icon. The icon file size must be 128x128 pixels. If you do not change the icon, the default icon is displayed.
6. In the Enhanced Security section, select **Enable enhanced security** to choose the security options you would like to apply to the application. The following enhanced security options can be enabled for the application.

- **Restrict clipboard access**: Disables cut/copy/paste operations between the app and system clipboard
- **Restrict printing**: Disables ability to print from within the Citrix Workspace app browser
- **Restrict navigation**: Disables the next/back app browser buttons
- **Restrict downloads**: Disables the user’s ability to download from within the app
- **Display watermark**: Displays a watermark on the user’s screen displaying user name and IP address of the user’s machine

Select **Enforce policy on mobile device** to enable the previously mentioned enhanced security options on your mobile device.

**Note:** When **Enforce Policy on Mobile Device** is selected along with **Enable enhanced security**,
the user experience for the application access is negatively impacted for the desktop users and the mobile users.

7. Select your preferred single sign-on type to be used for your application and click Save. The following single sign-on types are available.

- Basic – If your back-end server presents you with a basic-401 challenge, choose Basic SSO.
- Kerberos – If your back-end server presents you with negotiate-401 challenge, choose Kerberos.
- Form-Based – If your back-end server presents you with an HTML form for authentication, choose Form-Based.
- Don’t use SSO – Use Don’t use SSO option when you do not need to authenticate user on the back-end server.

Note: You do not need to enter configuration details for the above SSO types except the form based SSO.

Enter the following Form-based configuration details in the Single Sign On section and click Save.

- **Action URL** - Type the URL to which the completed form is submitted.
- **Logon form URL** – Type the URL on which the logon form is presented.
- **Username Format** - Select a format for the user name.
- **Username Form Field** – Type a user name attribute.
- **Password Form Field** – Type a password attribute.

Note: When Don’t use SSO option is selected, the user is redirected to the URL configured under App details section.

8. Download the metadata file by clicking the link under SAML Metadata. Use the downloaded metadata file to configure SSO on the SaaS apps server.
9. Click Finish.

After you click Finish, the app is added to the library and you are presented with the following three options.

- Add Another App
- Edit App
- Go to the Library

**Assign users or user groups for the published apps**

After an app is published, you can assign users or groups to the app.

1. On the Citrix Cloud screen, click Go to the Library. Alternatively, you can also click Library in the upper left menu.
Notice that the newly added app features in your library.

2. To assign users for the app, hover your pointer over the ellipses on the right, and click **Manage Subscribers**.

3. Click **Choose a domain** list and select a domain. Click **Choose a group or user** and assign users.
Note: A subscribed user can be unsubscribed by selecting the user and clicking the delete icon next to Status.

4. To obtain the Workspace URL to be shared with app users, on Citrix Cloud, click menu icon and navigate to Workspace Configuration.
Manage published apps

You can edit or delete a published app, and add additional subscribers to the published app.

Edit a published app

To edit a published app, perform the following steps:

1. Go to Library and identify the app to be edited.
2. Hover your pointer over the ellipses on the right and click Edit.
3. Edit the entries under App Details section and click Save.
4. Edit the entries under Single Sign On section, click Save, and click Finish.
5. The following screen appears indicating that the app has been modified.

**Delete a published app**

**To delete a published app, perform the following steps:**

1. Go to **Library** and identify the app to be deleted.
2. Click the dot icon on the right and click **Delete**.

**Manage subscribers for published app**

**To adding additional Subscribers, perform the following steps:**

1. Go to **Library** and identify the app to be modified.
2. Hover your pointer over the ellipses on the right, and click **Manage Subscribers**.
Launch a configured app - end-user flow

To launch a configured app, perform the following steps:

1. Log on to Citrix Workspace with AD user credentials. The admin configured app are displayed.
2. Click the app to launch the app. The app is launched and the user is signed-in to the app.

Support for Citrix Endpoint Management

September 30, 2019

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. MAM control traffic goes through the 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
Citrix Gateway Service

users to 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 communication and System requirements.

To configure Citrix Gateway service with Citrix Endpoint Management

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

Apps configuration using a template

September 30, 2019

SaaS apps configuration with single sign-on on Citrix Gateway service is simplified by provisioning a template drop-down menu for popular SaaS apps. The SaaS app to be configured can be selected from the drop-down menu.

The template pre-fills much of the information required for configuring applications. However, the information specific to the customer must still be provided.

Note: The following section has the steps to be performed on Citrix Gateway service for configuring and publishing an app using template. The configuration steps to be performed on the app server is presented in the subsequent section.

Configuring and publishing apps using template - Citrix Gateway service specific configuration

The following configuration takes the Aha app as an example to configure and publish an app using template.

1. On the Citrix Gateway service tile, click Manage.
2. Click **Add a Web/SaaS app** tab below the **Single Sign On** tile.

3. Select the app you want to configure using the **Choose a Template** drop-down and click **Next**.

4. Enter the following details in the **App Details** section and click **Save**.

   **Name** – Name of the application.

   **URL** – URL with your customer ID. If SSO fails or when **Don’t use SSO** option is selected, the user is redirected to this URL.
Icon – Click Change to change the app icon. The icon file size must be 128x128 pixels. If you do not change the icon, the default icon is displayed.

5. In the Enhanced Security section, select Enable enhanced security to choose the security options you would like to apply to the application and click Next. The following enhanced security options can be enabled for the application.

- **Restrict clipboard access:** Disables cut/copy/paste operations between the app and system clipboard
- **Restrict printing:** Disables ability to print from within the Citrix Workspace app browser
- **Restrict navigation:** Disables the next/back app browser buttons
- **Restrict downloads:** Disables the user’s ability to download from within the app
- **Display watermark:** Displays a watermark on the user’s screen displaying username and IP address of the user’s machine

Select Enforce policy on mobile device to enable the aforementioned enhanced security options on your mobile device.

Note: When Enforce Policy on Mobile Device is selected along with Enable enhanced security, the user experience for the application access is negatively impacted for the desktop users and...
6. Enter the following SAML configuration details in the **Single Sign On** section and click **Save**.

   - **Assertion URL** – SaaS app SAML assertion URL.
   - **Audience** – Service provider for whom the assertion is intended
   - **Name ID Format** – Format type of user
   - **Name ID** – Name of the format type of user

**Note:** When **Don’t use SSO** option is selected, the user is redirected to the URL configured under **App Details** section.

7. Download the metadata file by clicking the link under **SAML Metadata**. Use the downloaded metadata file to configure SSO on the SaaS apps server.

8. Click **Finish**.
9. The following screen appears indicating that the app has been added to the Library.

You must also complete the application server specific configuration for configuring and publishing the app using the template. For details on each app server specific configuration, see SaaS app server specific configuration.

**SaaS app server specific configuration**

September 30, 2019

Following are the links to the documents that has guidance on app server specific configuration for configuring and publishing popular SaaS apps using template. Citrix presently supports the following SaaS apps and is continually adding support for more apps.

- **15Five** - Continuous performance management tool to coach employees.
- **10000ft** - Project management tool to plan for growth.
- **4me** - Service management tool for collaboration between internal, external, and outsourced teams.
- **Absorb** - Learning management tool.
- **Accompa** - Requirements management tool to build products.
- **Adobe Captivate Prime** - Learning management system to deliver personalized learning experiences across devices.
- **Aha** - Product roadmap and marketing planning tool to build products and launch campaigns.
- **Alertops** - Collaboration incidence response tool to manage IT incidents.
- **Allocadia** - Marketing performance management tool to manage an organization’s marketing planning process.

- **Anaplan** - Planning tool to help organizations with decision making by connecting data, people, and plans.

- **Andfrankly** - Engagement tool to drive change in the workplace.

- **AppFollow** - Product management tool for accelerating global app growth and increasing customer loyalty.

- **Assembla** - Version control and source code management tool for software development.

- **Automox** - Patch management tool to track, control, and manage the patching process.

- **Azendoo** - Collaboration tool for teams to converse and collaborate.

- **BambooHR** - Human resources management tool to manage employee data.

- **Bananatag** - Tool to track and schedule emails, track files and create email templates

- **Base CRM** - Sales management tool to manage emails, phone calls, and notes.

- **Beekeeper** - Tool to integrate multiple operational systems and communication channels in one secure hub that is accessible from desktop and mobile devices.

- **BitaBIZ** - Absence and vacation planning and communication tool for leave and absence management.

- **BlazeMeter** - Testing suite.

- **Blissbook** - Policy management tool to create employee handbooks.

- **Bluejeans** - Video conferencing solution.

- **Bold360** - Live chat tool for customer engagement.

- **Bonusly** - Employee recognition and reward management tool to recognize team contributions.

- **Box** - Content management and file sharing tool to manage, share and access your content.

- **Branch** - A mobile linking platform powering deep links and mobile.

- **Brandfolder** - Digital asset management tool to store and share digital assets.

- **Buddy Punch** - Time management tool to monitor employee attendance.

- **Bugsnag** - Monitoring tool to manage application stability and report errors and diagnostic data.

- **Buildkite** - Infrastructure tool for continuous integration software development.

- **Bullseye Locations** - Store locator tool to locate a store or dealer on a device.

- **CA Flowdock** - Collaboration tool for teams to converse and collaborate.

- **CakeHR** - Human resources management tool for attendance and performance management.
• **Cardboard** - Collaborative product planning tool to track disorganized information.

• **Citrix Cedexis** - Traffic management tool for large websites to leverage multivendor sourcing of data centers, cloud providers, and content delivery networks.

• **Celoxis** - Project management tool to create project plans, automate work and collaborate.

• **CircleHD** - Training, learning, and collaboration tool to share videos and slides within the organization.

• **Circonus** - Data analytics and monitoring tool to deliver alerts, graphs, dashboards and machine-learning intelligence.

• **Cisco Umbrella** - Cloud security platform to provide the first line of defense against threats on the internet.

• **ClearSlide** - Sales engagement tool to let users share content and sales material for customer interaction.

• **Cloudability** - Cloud cost management platform to improve visibility, optimization, governance across cloud environments.

• **CloudAMQP** - Message queue tool to pass messages between processes and other systems.

• **CloudCheckr** - Cost management, security, reporting and analytics tool to help users optimize their AWS and Azure deployments.

• **CloudMonix** - Tool for cloud and on-premises resources monitoring and automation.

• **CloudPassage** - Visibility and continuous monitoring tool to reduce cyber risk and maintain compliance.

• **CloudRanger** - Tool to streamline your backups, disaster recovery and server control for AWS Cloud.

• **Clubhouse** - Project management tool for software development.

• **Coggle** - Mind mapping web application to create hierarchically structured documents, like a branching tree.

• **Comm100** - Customer service software and communication tool for customer service professionals.

• **Confluence** - Content collaboration tool to help teams collaborate and share knowledge.

• **ConceptShare** - Proofing tool to deliver content faster, quicker, and cheaper.

• **Concur** - Travel and expense management tool to manage expenses on the go.

• **ConnectWise Control** - Business management tool to provide remote support and access.

• **Contactzilla** - Contact management tool to access up to date contact information.
• **ContractSafe** - Contract management tool to track, store, and manage contracts.
• **Convo** - Team communication and collaboration tool for internal conversations.
• **Copper** - CRM tool.
• **Cronitor** - Monitoring tool for cron jobs.
• **Dashlane** - Password management tool that also manages digital wallets.
• **Declaree** - Travel and expense management tool for business travel.
• **Dell Boomi** - Integration tool to connect cloud and on-premises applications and data.
• **DeskPro** - Help desk tool to facilitate ticket management, customer self-help, and customer feedback.
• **Deputy** - Workforce management tool for scheduling and tracking employees’ time, tasks, and communication.
• **DigiCert** - Certificate management and troubleshooting tool for SSL certificates for websites.
• **dmarcian** - Email monitoring tool to filter spam, malware, and phishing.
• **DocuSign** - Online signature tool for different documents, such as insurance, medical, and real estate.
• **DOME9 ARC** - Security and compliance tool to manage public cloud environments.
• **Dropbox** - Cloud storage tool for secure file sharing and storage.
• **Duo** - Security tool to provide secure access to your applications.
• **Easy Projects** - Project Management tool.
• **Edapp** - Learning management tool for workspace learning.
• **EduBrite** - Learning management tool to create, deliver, and track training programs.
• **Ekarda** - Electronic card designing tool.
• **Envoy** - Visitor management tool to manage people and packages.
• **Evernote** - Application for note taking, organizing, task lists, and archiving.
• **Expensify** - Expense management tool for expense report management, receipt tracking, and business travel.
• **ezeep** - Print infrastructure management tool to print from any device, any location to any printer in the Cloud.
• **EZOfficeInventory** - Inventory management tool to track all your assets and equipments.
• **EZRentOut** - Equipment rental tool to track equipment quality and availability.
• **Fastly** - Edge cloud platform to serve and secure applications closer to the users.
- **Favro** - Planning and collaboration tool for organizational flow.
- **Federated Directory** - Cross-company contact directory tool to search through the corporate address books of different companies.
- **Feeder**
- **Feedly** - News aggregation tool to compile news feeds from different sources.
- **Fivetran** - Tool to help analysts replicate data into a cloud warehouse.
- **Flatter Files** - Digital flat file cabinet for drawings and documents to provide a secure and simple way for providing access to content.
- **Float** - Resource planning tool for project scheduling and managing the teams’ utilization.
- **Flock** - Collaboration tool.
- **Formstack** - Online form builder and data collection tool.
- **FOSSA** - Automated open source license scanning and vulnerability management tools built natively into CI/CD.
- **Freshdesk** - Customer support tool to help support the needs of customers.
- **Freshservice** - IT help desk tool to simplify IT operations.
- **FrontApp** - Collaboration tool to manage all conversations in one place.
- **Fulcrum** - Mobile data collection platform that allows you to easily build mobile forms and collect data.
- **G-Suite** - Set of intelligent apps to connect the people in your company.
- **GetGuru** - Revenue empowerment network to empower your revenue teams.
- **GitBook** - Tool to create and maintain your documentation.
- **GitHub** - Web-based hosting service for version control using Git for repositories hosted behind a corporate firewall.
- **GlassFrog** - Software to Holacracy practice.
- **GotoMeeting** - Online meeting software with HD Video Conferencing capabilities.
- **HackerRank** - Provides competitive programming challenges for consumers and businesses.
- **Happyfox** - Online help desk software and web based support ticket system.
- **Helpjuice** - Knowledge management solution to create and maintain knowledge bases.
- **Help Scout** - Customer service software and knowledge base tool for customer service professionals.
- **Hellosign** - Esigning interface to enable signing from anywhere, at any time, on any device.
• Helpdocs - knowledge base software to guide your users when they are stuck.

• Honeybadger - Exception, uptime, and check-in monitoring system in a single platform.

• Harness - Tool for continuous delivery and integration for Java, .NET apps in AWS, GCP, Azure, and Bare Metal.

• HelpDocs - Tool to create an authoritative knowledge base to guide your users when they're stuck.

• Helpmonks - A collaborative email platform for team collaboration.

• Hoshinplan - Tool to visualize your strategic plans and track statuses in one canvas.

• Hosted Graphite - Tool to monitor your website, app, server, and container performance.

• Humanity - Online employee scheduling software to manages shifts, schedules, payroll, and time clocking.

• Igloo - Digital workplace and intranet solution provider to solve IT challenges across your organization.

• Illumio - Security system to prevent spread of breaches inside data center and cloud environments.

• Image Relay - Digital asset management and brand management software to securely organize and share digital files.

• Informatica - Tool for SaaS apps integration and a platform for developing and deploying custom integration services.

• Intelligentcontract - Contract management software.

• iMeet Central - Project management software for marketers, creative agencies, and enterprise businesses.

• InteractGo - Tool to measure real-time and historical data on system performance.

• iQualify One - Learning and management tool to delivers authentic learning experiences.

• InsideView - Data and intelligence solutions to solve sales, marketing, and other business challenges.

• Insightly - Cloud-based customer relationship management (CRM) and project management tools for small and medium size businesses.

• ITGlue - Cloud-based IT documentation platform to help MSPs standardize documentation, create knowledge bases, manage passwords, and track devices.

• Jitbit - Help desk software and ticketing system to manage and track incoming support request emails as well as their associated tickets.

• Kanbanize - Online portfolio Kanban software for lean management.
• **Klipfolio** - Online dashboard platform for building powerful real-time business dashboards for your team or your clients.

• **Jira** - Tool to plan, track, and manage your issues and projects.

• **Kanban Tool** - Visual management software to improve your team performance and boost productivity.

• **Keeper Security** - Password manager and security software to protect your passwords and private information.

• **Kentik** - Tool to leverage big data for network and performance monitoring, DDoS protection, and real-time ad-hoc network flow analytics.

• **Kissflow** - Workflow tool and business process workflow management software to automate your workflow process.

• **KnowBe4** - Tool to provide security awareness training and simulated phishing.

• **KnowledgeOwl** - Knowledge base and authoring tool.

• **Kudos** - Retail, job, project and fulfilment process systems.

• **LaunchDarkly** - Feature management platform to enable dev and ops teams to control the feature lifecycle.

• **Lifesize** - Video conferencing solution.

• **Litmos** - Learning management system for employee training, customer training, compliance training, and partner training.

• **LiquidPlanner** - Online project management software for your business.

• **LeanKit** - Lean-based, enterprise process and work management software to help enterprises visualize work, optimize processes, and deliver faster.

• **LiveChat** - Live chat and help desk software for businesses.

• **LogDNA** - Tool to collect, monitor, parse, and analyze logs from all sources in one centralized logging tool.

• **Mango** - Team collaboration software to consolidate and streamline siloed applications into one single platform.

• **Manuscript** - A writing tool to help you plan, edit, and share your work.

• **Marketo** - Automation software to help marketing teams master the art and science of digital marketing.

• **Meisterplan** - Software that helps organizations create project portfolios.

• **Mingle** - Agile project management and collaboration tool to provide a combined workplace for the entire team.
• **MojoHelpdesk** - Helpdesk software and ticketing system.
• **Monday** - Team management software to plan, track, and collaborate all your work in one tool.
• **Mixpanel** - System to track user interactions with web and mobile.
• **MuleSoft** - Integration software to connect SaaS and enterprise applications in the cloud and on-premise.
• **MyWebTimesheets** - Online time tracking system to track time spent on various projects/jobs/activities.
• **New Edge** - Secure application networking service for Hybrid IT.
• **NextTravel** - Corporate travel management software tool.
• **N2F** - Expense report management tool to manage your business and travel expenses.
• **New Relic** - Digital intelligence platform to measure and monitor the performance of applications and infrastructure.
• **Nmbrs** - Cloud HR and payroll software for businesses.
• **Nuclino** - Collaboration software to collaborate and share information in real-time.
• **Office365** - Microsoft’s cloud-based subscription service.
• **OneDesk** - Project management and helpdesk software to connect with and support your customers.
• **OpsGenie** - Incident management platform for DevOps and IT Ops teams to streamline alerts and incident resolution processes.
• **Orginio** - Online organizational chart creation tool to visualize the organizational structure.
• **Oomnitza** - IT Asset Management platform solution to track and manage assets.
• **Oracle ERP Cloud** - Cloud-based software application suite to manage enterprise functions.
• **Pacific Timesheet** - Web-based timesheet tool for payroll, project hours, and expenses.
• **Pagerduty** - Digital operations management system.
• **Panopta** - Infrastructure monitoring tool.
• **Panorama9** - Cloud-based IT management platform for enterprise network monitoring.
• **ParkMyCloud** - Single-purpose SaaS tool to connects to AWS, Azure Services, or GCP.
• **Peakon** - Tool to measure and improve employee engagement.
• **People HR** - HR software system for all key HR functions.
• **Pingboard** - Tool to build organization charts for organizing teams and workforce planning.
• **Pigeonhole Live** - Interactive Q&A platform.
Citrix Gateway Service

- **Pipedrive** - Sales CRM and pipeline management software.
- **PlanMyLeave** - Leave management system for managing and tracking employee’s leave of absence.
- **PlayVox** - Customer service quality monitoring tool.
- **Podbean** - Podcast service provider.
- **Podio** - Web-based tool to organize team communication, business processes, data and content in project management workspaces.
- **POPin** - Crowd-solving platform and mobile app that operationalizes team engagement for problem-solving
- **Postman** - API development environment.
- **Prescreen** - Applicant tracking tool to publish job vacancies online and offline.
- **ProductBoard** - Product management tool.
- **ProdPad** - Product management software to develop product strategies.
- **Proto.io** - Application prototyping platform to create fully-interactive, high-fidelity prototypes.
- **Proxyclick** - Cloud-based visitor management solution to manage visitors, build their brand image, and ensure the security.
- **PurelyHR** - Leave management tool for accessing employee leave data.
- **Promapp** - Business process management (BPM) tool.
- **Prescreen** - Cloud-based applicant tracking system to publish job vacancies online and offline.
- **QAComplete** - Software test management tool.
- **Qualaroo** - Feedback tool to gain insights from customers.
- **Quality Built, LLC** - Insurance, financial, and construction industry for providing reliable and innovative Third Party Quality Assurance Services.
- **Qubole** - Self-service platform for Big Data analytics built on Amazon.
- **Questetra BPM Suite** - Web-based business process platform for routine workflows.
- **QuestionPro** - Online survey software to create surveys and questionnaires.
- **Quandora** - Question and answer based knowledge management solution.
- **Rackspace** - Managed cloud computing services.
- **ReadCube** - Tool for web, desktop, and mobile reference management.
- **RealtimeBoard** - Whiteboard Collaboration tool for organizations to collaborate beyond formats, tools, locations and time zones.
• **Receptive** - Tool to gather feedback from customers, teams, and the market at one place.

• **Remedyforce** - IT service management and help desk system.

• **Retrace** - Application performance management tool that provides bug tracking, data aggregation and automatic alerts.

• **Robin** - Workplace experience tools to schedule conference meeting rooms and desk bookings.

• **Rollbar** - Real-time error alerting and debugging tools for developers.

• **Really Simple Systems** - Cloud-based CRM software for small businesses to manage their sales and marketing.

• **Reamaze** - Customer support software to support, engage, and convert customers with chat, social, SMS, FAQ, and email on a single platform.

• **Resource Guru** - Resource management software to schedule people, equipment and other resources.

• Retrace - Application performance management to integrate code profiling, error tracking, application logs, and metrics.

• **Roadmunk** - Product roadmap software and roadmap tool to create product roadmaps.

• **Runscope** - Tool to create, manage and execute functional API tests and monitors.

• **Salesforce** – CRM tool to manage customer contact information, integrate social media, and facilitate real-time customer collaboration.

• **Salsify** - Product experience management (PXM) platform.

• **Samanage** - Tool for IT service management.

• **Samepage** - Collaboration software to manage online projects.

• **screencast-o-matic** – Tool to screencast and edit video.

• **ScreenSteps** – Tools to create visual documents centered on screen captures.

• **SendSafely** – Encryption platform for secure exchange of files and emails.

• **Sentry** - Open-source error tracking software.

• **ServiceDesk Plus** - Tool for IT service desk.

• **ServiceNow** - Cloud platform to create digital workflows.

• **SharePoint** – Collaborative platform used for document management and storage.

• **Shufflrr** - Presentation management tool to create, update, share, and broadcast presentations.

• **Sigma Computing** – Analytics tool to explore, analyze, and visualize data.

• **Signavio** – A business process modelling tool.
- **Skeddly** - Tool to automate AWS resources.
- **Skills Base** - Talent management tool to track and document employee's performance and skills.
- **Skyprep** - Learning management system (LMS) to train customers and employees.
- **Slack** - Collaboration tool to communicate and share information.
- **Slemma** - Data analysis tool to create data reports from multiple data sets.
- **Sli.do** - Interaction tool for meetings, events, and conferences.
- **SmartDraw** - Diagram tool used to make flowcharts, organization charts, mind maps, project charts, and other business visuals.
- **SmarterU** - Learning management system (LMS) to train customers and employees.
- **Smartsheet** - Collaboration tool to assign tasks, track project process, manage calendars, and share documents.
- **SparkPost** - Email delivery service.
- **Split** - Bill splitting application.
- **Spoke** - Service desk tool to file service tickets.
- **Spotinst** - SaaS optimization platform that helps companies purchase and manage cloud infrastructure capacity.
- **SproutVideo** - Platform to host business videos.
- **Stackify** - Troubleshooting tool that provides support with a suite of tools including Prefix and Retrace.
- **StatusCast** - Hosted status page to keep your employees and customers aware about downtime and website maintenance.
- **StatusDashboard** - Communications platform for hosting status dashboards and broadcasting incident notifications to customers.
- **Status Hero** - Tool for tracking status updates and daily goals from your team.
- **Statushub** - Platform to host the service status page.
- **Statuspage** - Tool to communicate status and incidents.
- **SugarCRM** - CRM tool for sales-force automation, marketing campaigns, customer support, collaboration, Mobile CRM, Social CRM and reporting.
- **Sumologic** - Data analytics software to provide log management and analytics services.
- **Supermood** - HR platform to gather employee's feedback in real-time.
- **Syncplicity** - Tool to share and synchronize files.
• **Tableau** - Tool to create interactive data visualization.

• **TalentLMS** - Learning management system (LMS) to facilitate online seminars, courses, and other training programs.

• **Tallie** – Tool to capture and upload receipts, generate expense reports, and customize expense details.

• **Targetprocess** - Agile project management software to Scrum, Kanban, SAFe and so on.

• **Teamphoria** - Software to provide real-time employee engagement metrics, employee reviews, and recognition.

• **Tenable.io** - Tool that provides data to identify, investigate, and prioritize the remediation of vulnerabilities and misconfigurations in your IT environment.

• **Testable** - Tool to create behavioral experiments and surveys.

• **TestingBot** - Tool to provide various browser versions for live and automated testing.

• **TestFairy** - Mobile testing platform, to provide companies with video recordings, logs, and crash reports of mobile sessions.

• **TextExpander** - Communication tool to insert snippets of text from a repository of emails, and other content, as you type.

• **TextMagic** - Messaging service to connect with customers.

• **ThousandEyes** - Tool to monitor network infrastructure, troubleshoot application delivery, and map internet performance.

• **Thycotic Secret server** - Account management software tool to manage passwords.

• **TimeLive** – Tool to provide timesheets and track time.

• **Tinfoil Security** - Security solution software to check for vulnerabilities.

• **Trisotech** - Tool that allows customers to discover, model, analyze their digital enterprise.

• **Trumba** - Tool to publish online, interactive, calendars of events.

• **TwentyThree** - Video marketing platform to integrate and add videos to the marketing stack.

• **Ubersmith** - Business management software for usage-based billing, quoting, order management, infrastructure management, and help desk ticketing solutions.

• **Unifi** - Communication and collaboration software with voice, web collaboration, and video conferencing capabilities.

• **UPTRENDS** – Website monitoring solution to track website uptime and performance.

• **UserEcho** - Community forum tool that helps businesses manage customer feedback.
• **UserVoice** - Product feedback management software to enable businesses to make data-driven product decisions.

• **VALIMAIL** - Email authentication software to authenticate legitimate emails and block phishing attacks.

• **Velpic** - Learning management system (LMS) designed to streamline workplace training.

• **VictorOps** - Incident management software to provide DevOps observability, collaboration, and real-time alerting.

• **Vidizmo** - Enterprise live and on-demand video streaming software.

• **Visual Paradigm** - Visual modeling and diagramming online platform for team collaboration.

• **Vtiger** - CRM tool that enables sales, support, and marketing teams to organize and collaborate.

• **WaveMaker** – Software for building and running custom apps.

• **Weekdone** - Tool to create managers’ dashboard and team management service for companies.

• **Wepow** - Tool to connect recruiters, job candidates, and employers through mobile and video interviewing solution.

• **When I Work** - Tool for employee scheduling and time tracking.

• **WhosOnLocation** – Tool to track the flow of people through sites and zones.

• **Workday** - Tool for financial management, human resources, and planning.

• **Workpath** - Tool to manage goals and performance of the organization.

• **Workplace** - Collaboration tool by Facebook to help employees communicate through familiar interface.

• **Workstars** - Platform for social and peer employee recognition programs.

• **Workteam** - Tool to track employee time and attendance.

• **Wrike** - Social project management and collaboration software.

• **XaitPorter** - Document co-authoring software for bids and proposals and other business documents.

• **Ximble** - Tool for employee scheduling and time tracking.

• **XMatters** - Collaboration platform with an alerting software that integrates with other tools creating seamless process and effective communication.

• **Yodeck** - Tool to manage screens remotely, through the web or mobile.

• **Zendesk** - Software to request for customer service and to log support tickets.

• **Ziflow** - Tool for creative production teams.
Citrix Gateway Service

- **Zillable** – Collaboration platform with communication capabilities.
- **Zingtree** - A toolkit for creating interactive decision trees and troubleshooters.
- **Zivver** - Tool that allows secure email and file transfer from your familiar email program.
- **Zoho** - Business application suite.
- **Zoom** - Communication and collaboration software with voice, web collaboration, and video conferencing capabilities.
- **Zuora** - A subscription-based software that enables a company to launch, manage, and transform into a subscription business.

### Citrix Gateway Connector

**September 30, 2019**

Citrix Gateway Connector is a Citrix component which serves as a channel of communication between Cloud services (Citrix Gateway service, ADM, and so on) and on-premises components such as Web servers. It is a virtual appliance compatible with Citrix Hypervisor VMware ESXi, and Microsoft Hyper-V with a small form factor. Citrix Gateway Connector facilitates the remote access to the Enterprise web apps.

#### How it works

Citrix Gateway Connector authenticates and encrypts all communication between Citrix Cloud and your resource locations. The communication between the Citrix Gateway Connector and Citrix Cloud is outbound. All connections are established from the Citrix Gateway Connector to the cloud using the standard HTTPS port (443) and the TCP protocol. No incoming connections are accepted. TCP port 443, with the following FQDNs are permitted outbound:

- *.nssvc.net
- *.netscalermgmt.net
- *.citrixworkspacesapi.net
- *.citrixnetworkapi.net
- *.citrix.com
- *.servicebus.windows.net
- *.adm.cloud.com

**Important:** If there are SSL intercepting devices in the on-premises data center where the Citrix Gateway Connector must be deployed, the connector registration does not succeed if SSL inter-
Citrix Gateway Service

Exception is enabled for these FQDNs. The SSL interception must be disabled for these FQDNs for successful connector registration.

System requirements

Citrix Gateway Connector is a virtual appliance. The VM specification must have at least:

- Number of vCPUs must be exactly 2.
- 4 GB RAM minimum.
- 1 Network Adapter (virtual NIC). You can add an extra virtual NIC upon requirement.
- Firewall:
  - UDP port 53 to DNS server
  - TCP and UDP port 389 to Active Directory Domain Controllers (optional *)
  - TCP port 636 to Active Directory Domain Controllers (optional *)
  - TCP port 3268 to Active Directory Domain Controllers (optional *)
  - TCP port 3269 to Active Directory Domain Controllers (optional *)
  - TCP port 443, with the following FQDNs are permitted outbound:
    - *.nssvc.net
    - *.netscalermgmt.net
    - *.citrixworkspacesapi.net
    - *.citrixnetworkapi.net
    - *.citrix.com
    - *.servicebus.windows.net
    - *.adm.cloud.com
  - TCP ports (***) to Web servers accessed using Citrix Gateway Connector
  - Open port 8443 inbound for web-based management
  - Required to perform domain-based single sign-on to Web applications
  - Ports determined by the customers’ environment – ports 80 and 443 are typical

Recommended: Network with DHCP enabled to simplify the initial configuration.

Continuous availability of the Citrix Gateway Connector

As long as you ensure continuous availability of the Citrix Gateway Connector in each resource location, you can manage the machines where they are installed one at a time to avoid outage periods.
For continuous availability, install multiple Citrix Gateway Connectors in each of your resource locations. Citrix recommends at least two (2) Citrix Gateway Connectors in each resource location. If one Citrix Gateway Connector is unavailable for any period of time, the other Citrix Gateway Connectors can maintain the connection. As long as there is one Citrix Gateway Connector available, there is no loss in communication with Citrix Cloud. Citrix Gateway Connectors can be restricted to upgrade during a specified maintenance window every 24 hour, controlled per Resource Location.

**Load management**

Manage load by installing multiple Citrix Gateway Connectors in each resource location. Since each Citrix Gateway Connector is stateless, the load can be distributed across all available Citrix Gateway Connectors. There is no need to configure this load balancing function. It is automated.

**Ways to install Citrix Gateway Connector**

Citrix Gateway Connector can be installed in one of the following ways:

- By using the Citrix Cloud user interface - Set up resource location and install Citrix Gateway Connector using Citrix Cloud user interface
- While adding an Enterprise Web app - Set-up resource location and download Citrix Gateway Connector while adding Web app

**Set up resource location and install Citrix Gateway Connector using Citrix Cloud user interface**

The following are the steps to set up a resource location and install Citrix Gateway Connector using Citrix Cloud user interface:

1. On top left of the **Citrix Cloud** screen, click the hamburger icon and select **Resource Locations**. Click the plus icon next to **Resource Locations**.
2. Provide a name for the resource location and click **Save**.

3. Double-click the plus icon next to Citrix Gateway Connectors under the newly created resource location.

4. Select the hypervisor and click **Download Image**. Import the locally downloaded image to your hypervisor and create a new virtual machine (Citrix Gateway Connector).
5. Click **Get Activation Code**.

6. The activation code is generated as follows.

7. Once the installation is complete, Click **Detect**.
You can access the Citrix Gateway Connector user interface by using the URL that is displayed in one of the messages on the newly installed Citrix Gateway Connector VM. You can also log on to the Citrix Gateway Connector CLI as an administrator and execute the `show ip` command for viewing the IP address assigned to the Citrix Gateway Connector through DHCP. Then you can open `https://<IP address>:8443` on your browser to access the Citrix Gateway Connector admin user interface.

**Set-up resource location and download Citrix Gateway Connector while adding Web app**

While adding Web app using the **Citrix Gateway service** user interface, you can set up a new resource location and download connectors. To set up a resource location and download connectors, perform the following steps:

1. In the **Web app connectivity** section, select the **Create New** radio button. Provide a name for the resource location and click **Save**.

2. Click **Install Citrix Gateway Connector**.
3. Select the required hypervisor from the **Hypervisor** list, click **Download Image**.

4. Click **Get Activation Code**.
Install a Gateway Connector in Resource Location

Step 1: Install at least two connectors on a hypervisor.

→ Hypervisor  View Minimum Requirements

Citrix Hypervisor  Download Image

Step 2: Get the activation code to enter during the connector install.

Get Activation Code

5. The activation code is generated as follows.

6. Once the installation is complete, Click Detect.

You can access the Citrix Gateway Connector user interface by using the URL that is displayed in one of the messages on the newly installed Citrix Gateway Connector VM. You can also log on to the Citrix Gateway Connector CLI as an administrator and execute the show ip command for viewing the IP address assigned to the Citrix Gateway Connector through DHCP. Then you can open https://<IP address>:8443 on your browser to access the Citrix Gateway Connector admin user interface.
Log on and set up the Citrix Gateway Connector

After the Citrix Gateway Connector installation is complete, look for the following message on the newly installed VM (Citrix Gateway Connector).

Type the mentioned URL in a browser to access the Citrix Gateway Connector user interface. You can also log on to the Citrix Gateway Connector CLI as an administrator and execute the `show ip` command. The command displays the IP address assigned to the Citrix Gateway Connector through DHCP. Then open `<https://IP address:8443>` on your browser to access the Citrix Gateway Connector admin user interface.

1. The user name and password for the following screen is `administrator` for the first time user.

2. Change the password by providing a password of your choice in `Set administrator password` section and click `Continue`.

3. Enter the following configuration details in `System settings` section and click `Continue`.
   - **Connector IP Address** – IP address of Gateway Connector.
   - **Subnet Mask** – Subnet mask of the Gateway Connector IP address.
   - **Default Gateway** – IP address of default gateway.
   - **DNS Server** – IP address DNS server.
   - **Proxy IP** – Your internal proxy server IP address.
   - **Proxy Port** – Port of the proxy server.
4. In the **Single sign on** section, check **Enable Kerberos Single Sign On** for capabilities beyond the basic authentication. Enter the following Kerberos configuration details and click **Continue**.

   - **Active Directory Domain** – Active Directory domain for the users to be granted access.
   - **Service Account Name** – Delegated user name for authentication.
   - **Service Account Password** – Delegated password for Service Account.
5. Finally enter the activation code to register the connector with Citrix Cloud and click **Save and Finish**.
Installation Instructions

- Set administrator password
- System settings
- Single sign on
- Activation code

The activation code registers this connector with Citrix Cloud.

Activation code:
P6c5fa2fd-ea78-4ca5-8e40-4ae18fd4b39

Save and Finish

The following figure displays the Citrix Gateway Connector dashboard.
Gateway Connector dashboard

September 30, 2019

The Gateway Connector dashboard provides key metrics such as CPU usage (packet and management), in-use memory, and TCP connection details.
You can perform the following from the Gateway Connector dashboard.

**Restart the connector**

Click **Restart** to restart the connector from the user interface. You can either do a warm reboot or a complete restart of the Gateway Connector.

**Re-register the connector with Citrix Cloud**

Click **Retry activation code** if you want to install the already registered connector in a different resource location. You must enter the activation code that was provided when you downloaded the Gateway Connector.

**Download support logs**

Click **Download Logs** to download the support logs from the Gateway Connector. The **Download Logs** link is available even during the first time use to help setup the connector.

1. Click **Download Logs**.  
   
   A log file is generated. Generation of log file takes some time. Once the log file if generated, a message with the link to download file appears.

2. Click **Download**. A .tgz file is downloaded.
Citrix Gateway Service

All files in the download folder are in an encrypted format. You must reach out to Citrix Cloud support team for help.

**Important:** Download logs option is available in Gateway Connector from version 401.251. If you are on an earlier version of connector and you upgrade the connector to version 401.251, you still cannot download the logs even though the Download Logs link is available.

**Support for Enterprise web apps**

September 30, 2019

Web apps delivery using Citrix Gateway service enables enterprise specific applications to be delivered remotely as a web-based service. Commonly used web apps include SharePoint, Confluence, OneBug, and so on.

Web apps can be accessed using Citrix Workspace using Citrix Gateway service. The Citrix Gateway service coupled with Citrix Workspace provides a unified user experience for the configured Web apps, SaaS apps, configured virtual apps, or any other workspace resources.

SSO and remote access to web apps are available as part of the following service packages:

- Gateway Service Standard
- Workspace Standard, Workspace Premium or Workspace Premium Plus

**System requirements**

Citrix Gateway Connector – A virtual appliance that facilitates the remote access to the Enterprise web apps. Citrix Gateway Connector is a virtual appliance. The virtual machine specification must at least have:

- Number of vCPUs must be exactly 2.
- 4 GB RAM minimum.
- 1 Network Adapter (virtual NIC). You can add an extra virtual NIC upon requirement.

It is recommended to install the Gateway Connector before configuring the Enterprise web apps for a cleaner approach.

**Important:** If there are SSL intercepting devices in the on premises data center where the Citrix Gateway Connector must be deployed, the connector registration does not succeed if SSL interception is enabled for these FQDNs. The SSL interception must be disabled for these FQDNs for successful connector registration.

For more information on Citrix Gateway Connector, see [Citrix Cloud Gateway Connector](#).
Citrix Gateway Service

How it works

Citrix Gateway service securely connects to the on premises data center using Citrix Cloud Gateway Connector, which is deployed on premises. This connector acts as a bridge between Enterprise web apps deployed on premises and the Citrix Gateway service. These connectors can be deployed in an HA pair and require only an outbound connection.

A TLS connection between the Gateway connector and the Citrix Gateway service in the cloud secures the on premises applications that are enumerated into the cloud service. Web applications are accessed and delivered through Workspace using a VPN-less connection.

The following figure illustrates accessing web applications using Citrix Workspace.

Ways to configure Enterprise web apps

Enterprise web apps can be configured and published in the following two ways:

- Template based configuration - For configuration steps, see Configuring and publishing apps using template
- Manual configuration - Configuration steps are as follows.

Configure and publish Enterprise web apps manually

The following configuration takes the SharePoint app as an example to configure and publish an app manually:

1. On the Citrix Gateway service tile, click Manage.
2. Click Add a Web/SaaS App tab below the Single Sign On tile.
3. Click Skip to configure the SharePoint app manually.
4. Check **Inside my corporate network** radio button.

Enter the following details in the **App Details** section and click **Next**.

**Name** – Name of the application that you are adding.

**URL** – URL with your customer ID. The URL must contain your customer ID (Citrix Cloud customer ID). To get your customer ID, see Sign up for Citrix Cloud. In case SSO fails or you do not want to use SSO, the user is redirected to this URL.

**Related URLs** – Related domain is auto-populated based on the URL that you have provided. You can add more than one related domain.

**Icon** – Click **Change** to change the app icon. The icon file size must be 128x128 pixels. If you do not change the icon, the default icon is displayed.

**Description** – This description that you enter here is displayed to your users in workspace.
5. In the Enhanced Security section, select **Enable enhanced security** to choose the security options you would like to apply to the application. The following enhanced security options can be enabled for the application.

- **Restrict clipboard access:** Disables cut/copy/paste operations between the app and system clipboard
- **Restrict printing:** Disables ability to print from within the Citrix Workspace app browser
- **Restrict navigation:** Disables the next/back app browser buttons
- **Restrict downloads:** Disables the user’s ability to download from within the app
- **Display watermark:** Displays a watermark on the user’s screen displaying user name and IP address of the user’s machine
Select **Enforce policy on mobile device** to enable the previously mentioned enhanced security options on your mobile device.

**Note:** When **Enforce Policy on Mobile Device** is selected along with **Enable enhanced security**, the user experience for the application access is negatively impacted for the desktop users and the mobile users.

6. Now you must connect to a resource location. You can either select an existing resource location or create one. To choose an existing resource location, click one of the resource locations from the list of resource locations, for example My Resource Location, and click **Next**. For guidance on adding a new resource location, click [https://docs.citrix.com/en-us/citrix-gateway-service/gateway-connector.html](https://docs.citrix.com/en-us/citrix-gateway-service/gateway-connector.html)
7. Select your preferred single sign-on type to be used for your application and click **Save**. The following single sign-on types are available.

- **Basic** – If your back-end server presents you with a basic-401 challenge, choose **Basic SSO**.
- **Kerberos** – If your back-end server presents you with negotiate-401 challenge, choose **Kerberos**.
- **Form-Based** – If your back-end server presents you with an HTML form for authentication, choose **Form-Based**.
- **Don’t use SSO** – Use **Don’t use SSO** option when you do not need to authenticate user on the back end server.

**Note:** You do not need to enter configuration details for the above SSO types except the form based SSO.

Enter the following Form-based configuration details in the Single Sign On section and click **Save**.

- **Action URL** - Type the URL to which the completed form is submitted.
- **Logon form URL** – Type the URL on which the logon form is presented.
- **Username Format** - Select a format for the user name.
- **Username Form Field** – Type a user name attribute.
- **Password Form Field** – Type a password attribute.

**Note:** When **Don’t use SSO option** is selected, the user is redirected to the URL configured under **App details** section.
8. Click **Finish**.

   After you click **Finish**, the app is added to the library and you are presented with the following three options.

   - **Add Another App**
   - **Edit App**
   - **Go to the Library**

   ![Image of Citrix Cloud interface with 'Sharepoint2013' added to library]

**Assign users or user groups for the published apps**

After an app is published, you can assign users or groups to the app.

1. On the **Citrix Cloud** screen, click **Go to the Library**. Alternatively, you can also click Library in the upper left menu.

   Notice that the newly added app features in your library.
2. To assign users for the app, hover your pointer over the ellipses on the right, and click **Manage Subscribers**.

3. Click **Choose a domain** list and select a domain. Click **Choose a group or user** and assign users.
4. To obtain the Workspace URL to be shared with app users, on **Citrix Cloud**, click menu icon and navigate to **Workspace Configuration**.

**Note:** A subscribed user can be unsubscribed by selecting the user and clicking the delete icon next to **Status**.
Manage your published apps

You can edit or delete a published app, and add additional subscribers to the published app.

Edit a published app

To edit a published app, perform the following steps:

1. Go to Library and identify the app to be edited.
2. Hover your pointer over the ellipses on the right and click Edit.
3. Edit the entries under App Details section and click Save.
4. Edit the entries under Single Sign On section, click Save, and click Finish.

Delete a published app

To delete a published app, perform the following steps:

1. Go to Library and identify the app to be deleted.
2. Click the dot icon on the right and click Delete.

Manage subscribers for published app

To add additional subscribers, perform the following steps:
1. Go to **Library** and identify the app to be modified.
2. Hover your pointer over the ellipses on the right, and click **Manage Subscribers**.

**Launch a configured app – end-user flow**

**To launch a configured app, perform the following steps:**

1. Log on to Citrix Workspace with AD user credentials.
   The admin configured app are displayed.
2. Click the app to launch the app.
   The app is launched and the user is signed-in to the app.

**FAQ**

September 30, 2019

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

**Can I use my on premise configurations to port into Citrix Cloud?**

No, the underlying infrastructure and mechanisms are different. Please refer to 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](https://docs.citrix.com/en-us/xenapp-and-xendesktop/service/storefront.html)

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

The VPX provided with XenApp and/or XenDesktop service must be used for HDX proxy only (based on EULA) and not for authentication. Authentication on cloud is done using on premise AD via cloud connector or using Azure Active Directory.
Can I use smart control, smart access using cloud services?

The VPX provided with XenApp and XenDesktop service must be used for HDX proxy only (based on EULA) and should 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 premise 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 beta 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.