Citrix Gateway Service

Contents

Release Notes

June 5, 2024

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: New features and enhancements available in the current release.

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

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

April 25, 2024

What's new

- **Citrix Gateway Service for StoreFront - Preview**

Citrix Gateway Service for StoreFront is a cloud-based HDX solution that provides secure remote access to resources accessed from on-premises StoreFront. You can leverage the scalability and reliability of Citrix Cloud (for HDX proxy) without changing your on-premises StoreFront and on-premises NetScaler Gateway environments.

This solution is in preview. For details see Citrix Gateway Service for StoreFront - Preview.

April 24, 2024

What's new

- **Support for loss-tolerant mode for audio policy**

Citrix Gateway Service now supports the latest loss-tolerant mode for audio policy of Citrix Virtual Apps and Desktops. This mode enhances the audio experience for users connecting to networks with high latency and packet loss. Users must use Citrix Virtual Apps and Desktops 7 2402 LTSR or later versions to leverage this functionality.

The loss-tolerant mode for audio policy is based on the EDT Lossy transport protocol. EDT Lossy is a loss-tolerant transport protocol that allows packet loss in transmission without resending multimedia content, resulting in a more real-time experience for users. It is also the preferred mode for audio that ensures superior audio quality compared to EDT during lossy network conditions.

For details on the loss-tolerant mode settings, see Loss tolerant mode for audio.

April 19, 2024

What's new

- **Support for Toronto (Canada) Azure POP**

  Support for the Azure POP in Toronto, Canada is now available.

  POP FQDN: `az-ca-c-rdvz.g.nssvc.net`

  For details, see Geo-location Routing - Preview.

  [CGS-12933]

February 27, 2024

What's new

- **Support for Google Cloud Platform**

  Support for Google Cloud Platform (GCP) POPs along with the existing Azure and AWS POPs are planned in the upcoming service releases.

  Currently, there are 5 GCP POPs that are distributed across geo-locations. With this upcoming support, you can leverage these GCP POPs along with the existing Azure and AWS POPs.

  > **Important:**
  >
  > To ensure continued operations in your Citrix DaaS deployment, complete the instructions specified in Citrix Gateway Service –Points-of-Presence (POPs) before 15th of March, 2024.

February 01, 2024

What's new

- **Support for Toronto (Canada) Azure POP**

  Support for the Azure POP in Toronto, Canada is planned in the upcoming service releases.

  POP FQDN: `az-ca-c-rdvz.g.nssvc.net`

  [CGS-12933]

November 02, 2023

What's new

- **Support for the latest version of reducer for HDX**

  Citrix Gateway Service supports the latest version of the reducer for HDX. Reducer for HDX is a general purpose compressor that works across virtual channels. The latest reducer improves the overall performance of Citrix DaaS with the following capabilities:

  - Reduces the network bandwidth utilization for HDX sessions.
  - Data packets are transmitted in a shorter duration, resulting in a faster response.

  The following software versions support the latest reducer.

  - Citrix Virtual Apps and Desktops 7 2303 (Windows) and later.
  - Citrix Workspace app 2303 (Windows) and later.

  [CGS-16258]

August 29, 2023

What's new

- **Geo-location Routing - Preview**

  Citrix Gateway Service provides a capability to the admins to enable their users to connect to PoPs in a particular region or only through a particular cloud service provider regardless of the users' location. For more information, see Geo-location Routing - Technical preview.

  [CGS-13782]

- **HDX Performance Analytics**

  Citrix Gateway Service supports the HDX performance analytics functionality that enables Citrix Analytics administrators to view performance data related to the Connector-Gateway PoP latency. For more information, see Connector Statistics.

  [CGS-15829]

- **Accelerated Networking**

  The Citrix Gateway Service infrastructure is enhanced to support accelerated networking wherein it uses single root I/O virtualization (SR-IOV) to provide high-performance networking capabilities to users.

  [CGS-15684]

- **Deprecated weak ciphers**

  For the updated list of the deprecated ciphers of Citrix Gateway Service, see Technical security overview.

  [CGS-14234]

Fixed issues

- EDT sessions are disconnected whenever the backend pool is modified in the Azure load balancer.

  [CGS-15808]

November 10, 2022

What's new

- **Rendezvous protocol version V2 support**

  The Citrix Gateway Service now supports Rendezvous protocol version V2 for Citrix Gateway Service on the Google Cloud Platform. For details, see Citrix Gateway Service features supported.

- **Citrix Gateway Service on Google Cloud Platform availabiality in Europe**

  Citrix Gateway Service on the Google Cloud Platform is now available in Europe in the following regions.

  - London
  - Zurich

  For details, see Citrix Gateway Service on Google Cloud Platform.

Known issues

- Rendezvous V2 VDA registration fails if the customer ID is fewer than 6 characters.

  [CGS-15036]

June 30, 2022

What's new

- **Citrix Gateway Service availability on the Google Cloud Platform**

With Citrix Gateway Service support on the Google Cloud Platform (GCP), customers running their workloads on Google Cloud can take the advantage of Google Cloud's high-performing global network using the Citrix Gateway optimal routing feature. The optimal gateway routing feature directs clients to the closest GCP Citrix Gateway Service POP. Also, the Citrix Gateway Service on Google Cloud provides secure connectivity between Citrix Workspace clients and virtualization resources to deliver sessions with the lowest latency and the best user experience possible. For details, see Citrix Gateway Service on Google Cloud Platform.

April 04, 2022

What's new

- **Rebranding changes**
  - Citrix Secure Workspace Access is now rebranded to Citrix Secure Private Access.
  - Citrix Virtual Apps and Desktops service is now rebranded to Citrix DaaS.

What's new

- **Merger of Citrix Gateway Service tile into a single Citrix Secure Private Access in Citrix Cloud**

October 11, 2021

What's new

- **Merger of Citrix Gateway Service tile into a single Citrix Secure Private Access in Citrix Cloud**

  The Citrix Gateway Service tile and Citrix Secure Private Access tile are merged into Citrix Secure Private Access tile and the Citrix Gateway landing page is modified for Citrix Secure Private Access. 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 Citrix Secure Private Access service.

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

Citrix Secure Private Access customers, including Citrix Workspace Essentials and Citrix Workspace Standard, can now use one single Citrix Secure Private 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

April 13, 2023

Customers who are entitled for the Citrix DaaS 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 Citrix Secure Private Access tile are merged into Citrix Secure Private Access tile and the landing page is modified for Citrix Secure Private Access. 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

October 27, 2023

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

Citrix Gateway Service provides the following capabilities:

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.

DTLS 1.2 protocol support: Citrix Gateway Service supports Datagram Transport Layer Security (DTLS) 1.2 for HDX sessions over EDT (UDP-based transport protocol). The following cipher suites are supported:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

TLS protocol support: Citrix Gateway Service supports the following TLS cipher suites:

- TLS1.2-ECDHE-RSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-RSA-AES-256-SHA384
- TLS1-ECDHE-RSA-AES128-SHA
- TLS1.2-AES256-GCM-SHA384
- TLS1-AES-256-CBC-SHA

Endpoint Management integration: When integrated with Citrix Endpoint Management plus Citrix Workspace, the Citrix Gateway Service provides secure remote device access to your internal network and resources. Onboarding the Citrix Gateway Service with Endpoint Management is fast and simple. The 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 use the nearest Point-of-Presence (PoP) where the particular function that they need is available, regardless of Citrix Cloud Control plane geo-selection or the 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 the customer when persisted.
- TOTP seeds for each user device –TOTP seeds are scoped by customer, user, and device.

Audit and Change Control

Currently the 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 the 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 the Citrix Gateway Service to perform the following:
  - Citrix Secure Private 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, the Citrix Gateway Service stores the per-device keys used to seed the TOTP algorithm.
- To enable Kerberos Single Sign-On functionality, customers might configure Connector Appliance 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
Enterprise web apps access	Citrix Cloud Connector, Citrix Connector Appliance	N/A
Enterprise apps and files delivered by Citrix Endpoint Management	Citrix Cloud Connector, Citrix Connector Appliance	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 Service HDX Connectivity

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

Customer best practices

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

Deprecated cipher suites

The following cipher suites are deprecated for enhanced security:

- TLS1.2-AES128-GCM-SHA256
- TLS1.2-AES-128-SHA256
- TLS1.2-AES256-GCM-SHA384
- TLS1.2-AES-256-SHA256
- TLS1.2-DHE-RSA-AES-256-SHA256
- TLS1.2-DHE-RSA-AES-128-SHA256

- TLS1.2-DHE-RSA-AES256-GCM-SHA384
- TLS1.2-DHE-RSA-AES128-GCM-SHA256
- SSL3-DES-CBC3-SHA
- TLS1-ECDHE-RSA-AES256-SHA
- TLS1-AES-256-CBC-SHA
- TLS1-AES-128-CBC-SHA
- TLS1-ECDHE-ECDSA-AES256-SHA
- TLS1-ECDHE-ECDSA-AES128-SHA
- TLS1-DHE-RSA-AES-256-CBC-SHA
- TLS1-DHE-RSA-AES-128-CBC-SHA
- TLS1-DHE-DSS-AES-256-CBC-SHA
- TLS1-DHE-DSS-AES-128-CBC-SHA
- TLS1-ECDHE-RSA-DES-CBC3-SHA
- TLS1.2-ECDHE-RSA-AES-128-SHA256
- TLS1.2-ECDHE-ECDSA-AES128-SHA256
- TLS1.2-ECDHE-ECDSA-AES256-GCM-SHA384
- TLS1.2-ECDHE-ECDSA-AES128-GCM-SHA256

Geo-location Routing - Preview

June 12, 2024

Citrix Gateway Service provides a capability to the admins to enable their users to connect to a specific region (POPs). Doing so ensures that the user traffic is directed to the specific region irrespective of the user's location.

> **Note:**
>
> Sign up for the preview using https://podio.com/webforms/27328175/2108260.

The following table lists the regions and the POPs in that region that support Geo-location based traffic routing:

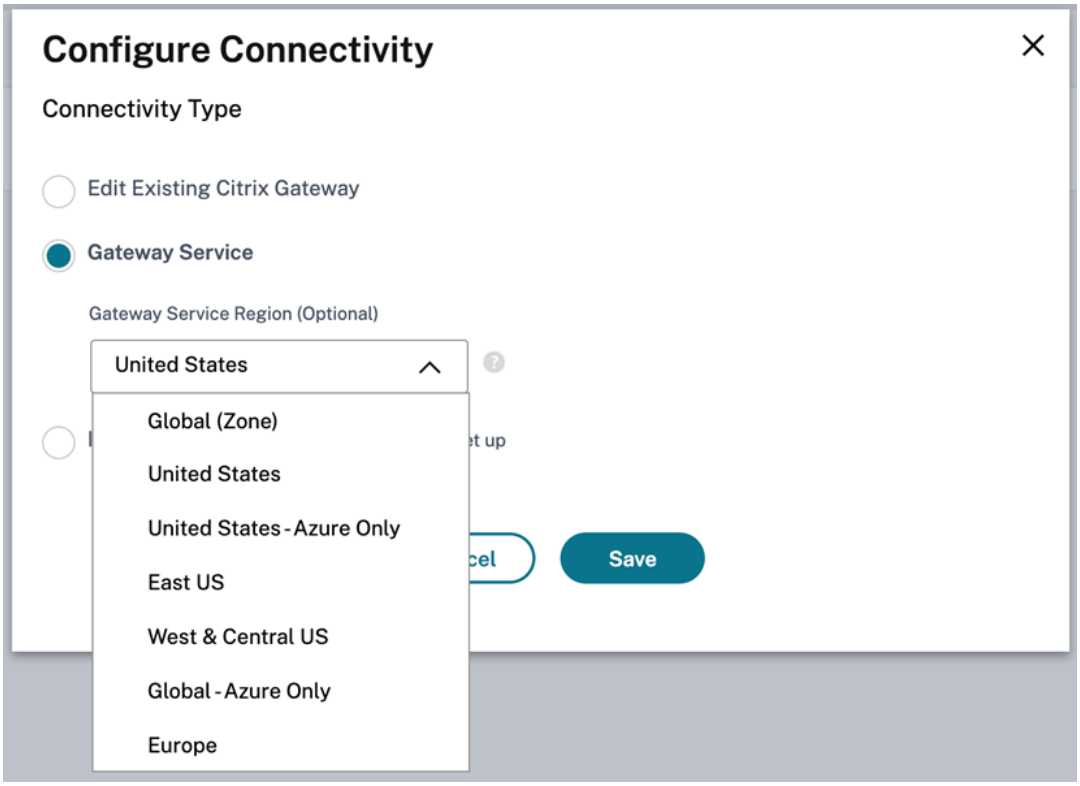
Geo-location	POPs
United States - East	Azure-US-East, AWS US East, AWS-US-North-Central
United States - Central and West	Azure-US-West, AWS-US-West, Azure-US-South-Central

Geo-location	POPs
United States	Azure-US-South-Central, Azure-US-East, Azure-US-West, AWS-US-East, AWS-US-West, AWS-US-North-Central
United States - Azure only	Azure-US-East, Azure-US-West, Azure-US-South-Central
Europe	AWS-Europe-Central, Azure-Europe-West, Azure-Europe-North
Australia	Azure-Australia-East, AWS-Australia-East
Global - Azure only	Azure-US-East, Azure-US-West, Azure-US-South-Central, Azure-Brazil-South, Azure-Europe-West, Azure-Europe-North, Azure-Australia-East, Azure-Asia-South-East, Azure-Japan-East, Azure-India-South, Azure-UAE-North, Azure-South-Africa, Azure-Hong Kong, Azure-Toronto-Canada

How to configure

You can configure a specific region for the user traffic from the **Resource locations** or **Workspace Configuration** page on Citrix Cloud.

1. Sign in to Citrix Cloud.
2. Click the hamburger menu and select **Resource Locations** or **Workspace Configuration**.
    a) On the **Resource Locations** page, select a location and click **Gateway**. The **Configure Connectivity** screen appears.
    b) In the **Workspace Configuration** page, in External Connectivity, select a location and click the ellipsis. The **Configure Connectivity** screen appears.



3. In **Gateway Service Region (Optional)**, select the region to which you want to route your customer traffic.

   > **Notes:**
   >
   > If you do not select any region, then **Global** is selected, by default. When the region is **Global**, the traffic is diverted to the POP that is in the closest proximity to the customer.
   >
   > In rare scenarios, if there is an outage, and all the POPs of a specific region are not available, then the configuration falls back to **Global** instead of blocking the traffic.

4. Click **Save**.

Migrate NetScaler Gateway to Citrix Gateway Service for HDX Proxy

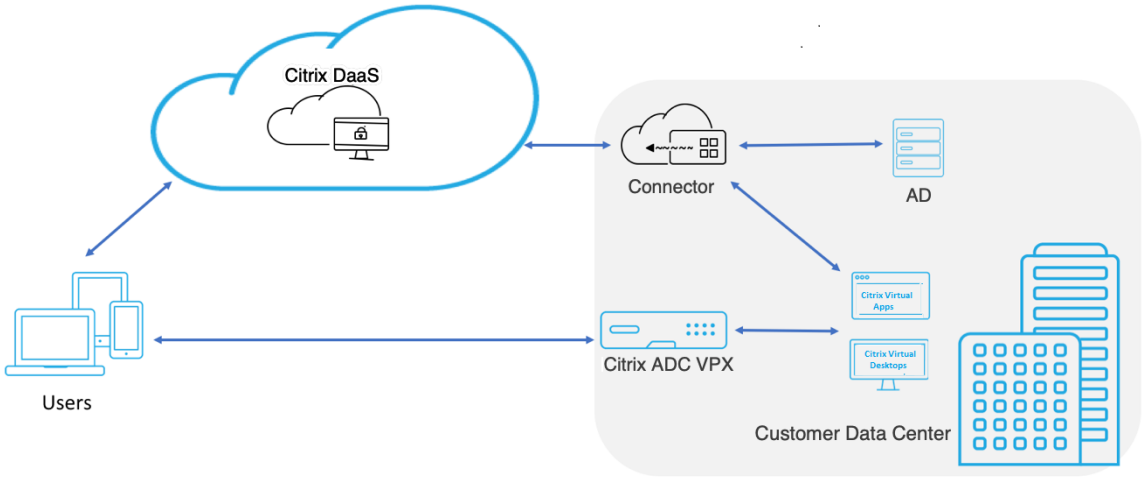
August 24, 2023

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

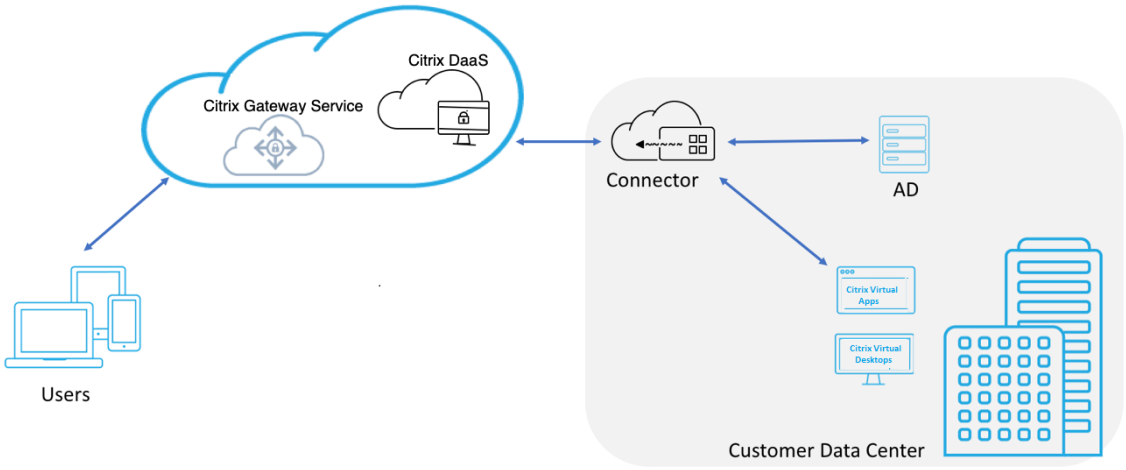
Customers who are entitled for the Citrix DaaS get the Citrix Gateway Service enabled, by default. Customers do not have to request a separate Citrix Gateway Service trial.

Figure 1. Deployment with NetScaler 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 DaaS environments.

Figure 2. Deployment with Citrix Gateway Service as HDX Proxy



This feature is now included with your Citrix DaaS and Workspace Service entitlements. You can enable this feature.

Migration from an on-premises NetScaler Gateway to cloud based Citrix Gateway Service

The NetScaler Gateway appliance is customer managed and cloud based Citrix Gateway Service is Citrix managed. This section explains how to migrate from an on-premises NetScaler Gateway to cloud-hosted Citrix Gateway Service for HDX Proxy. Though NetScaler 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 DaaS. Once enabled, traffic starts traversing through the Citrix Gateway Service and an on-premises NetScaler Gateway is no longer required.

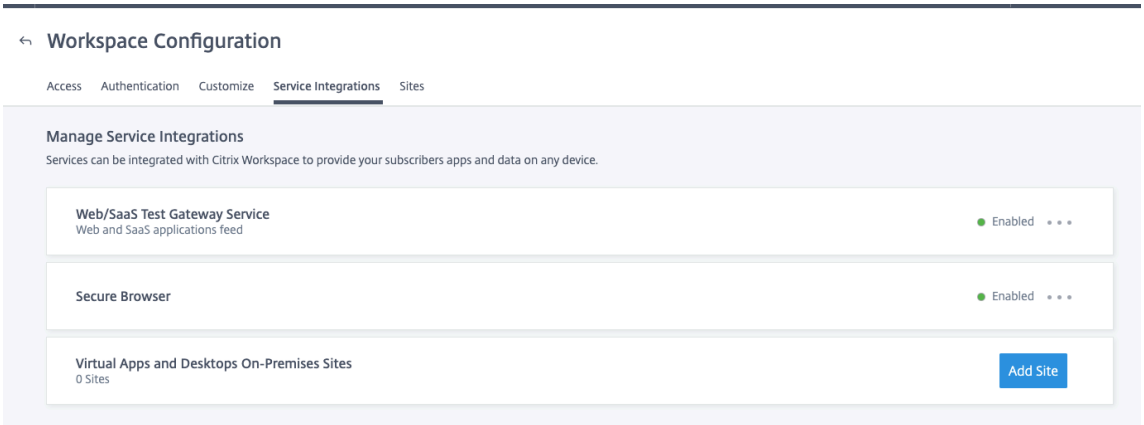
Following are the assumptions made before you begin migration from an on-premises NetScaler Gateway to cloud based Citrix Gateway Service.

- The customer has subscribed for Citrix Cloud Service and has purchased Citrix DaaS.
- 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 DaaS users:

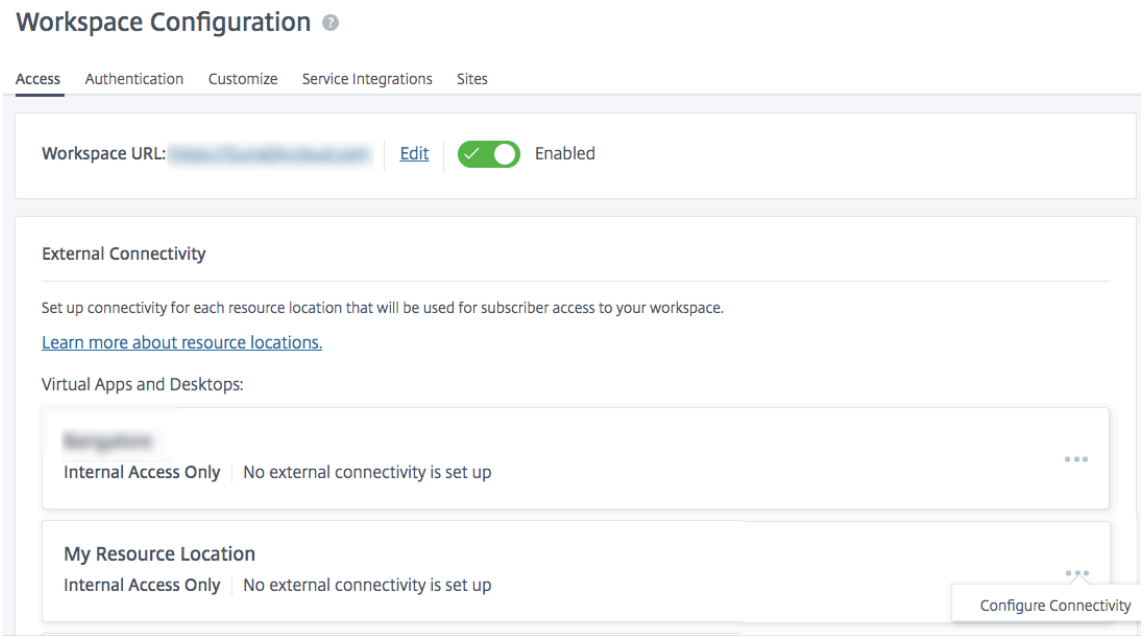
1. Sign into Citrix Cloud Services as an admin user.
2. Click the hamburger icon and choose **Workspace Configuration**.
3. Click **Service Integrations**.
4. Locate the ellipsis next to **Gateway**, click the ellipsis, and then click **Enable**.



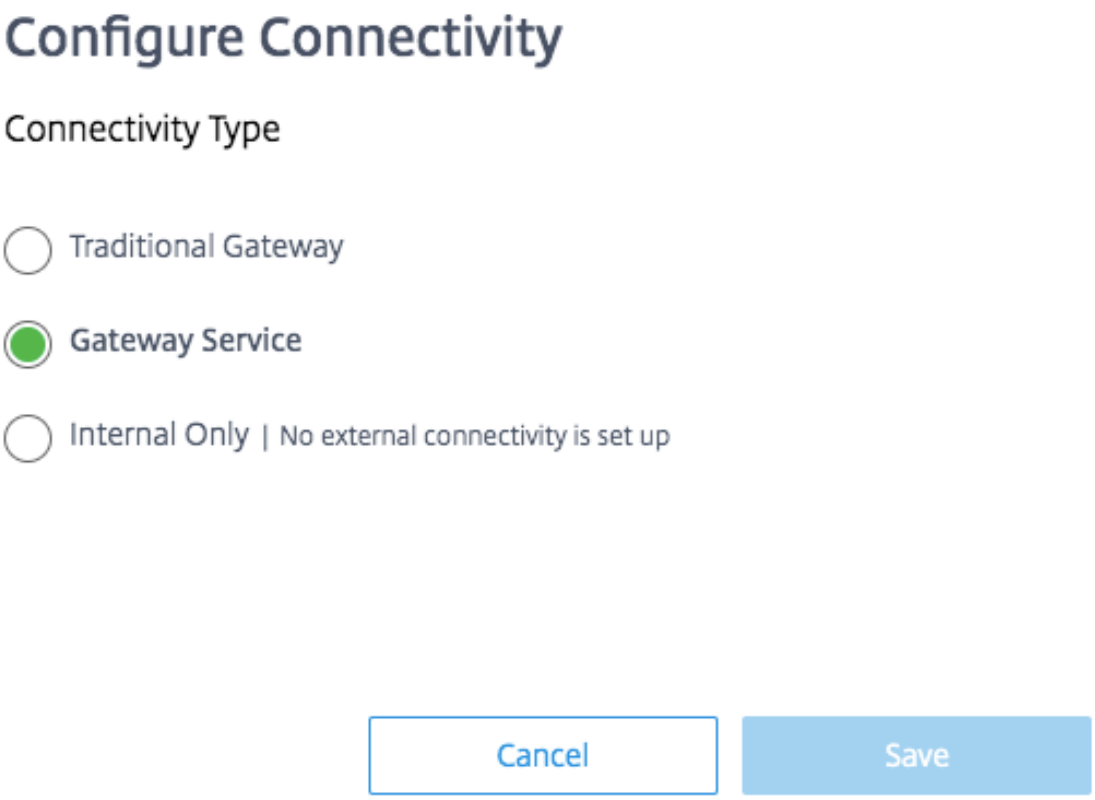
Following are the steps to enable the Citrix Gateway Service for Citrix Workspace users.

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** under **Citrix DaaS**.
4. Click the ellipsis, click **Configure Connectivity**.



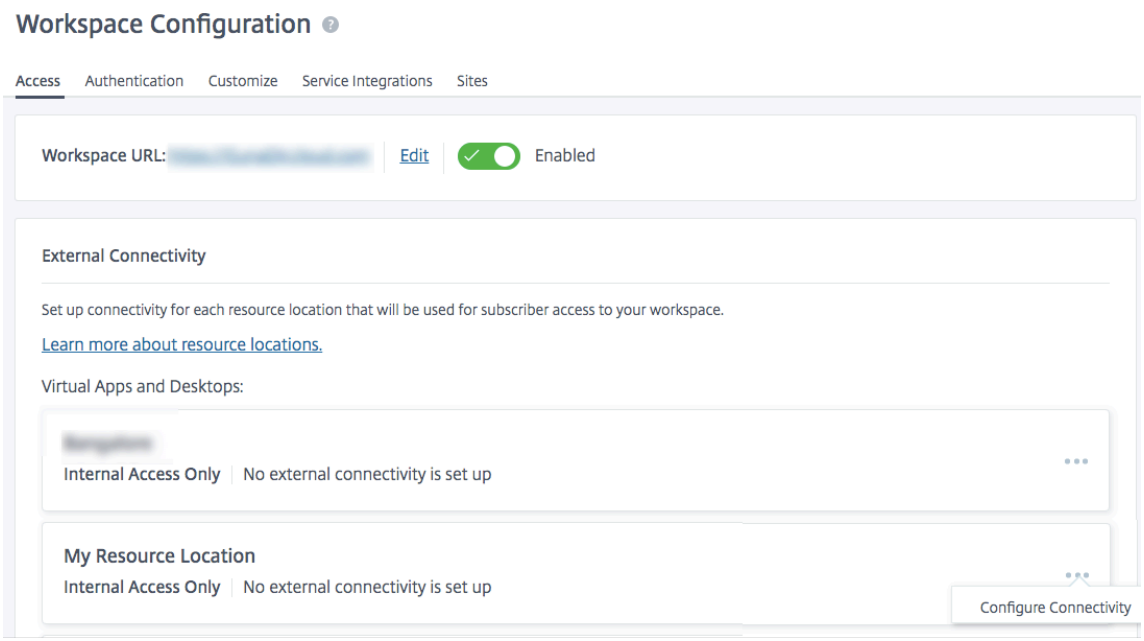
5. Choose **Citrix Gateway Service** in the pop-up window and then click **Save**.



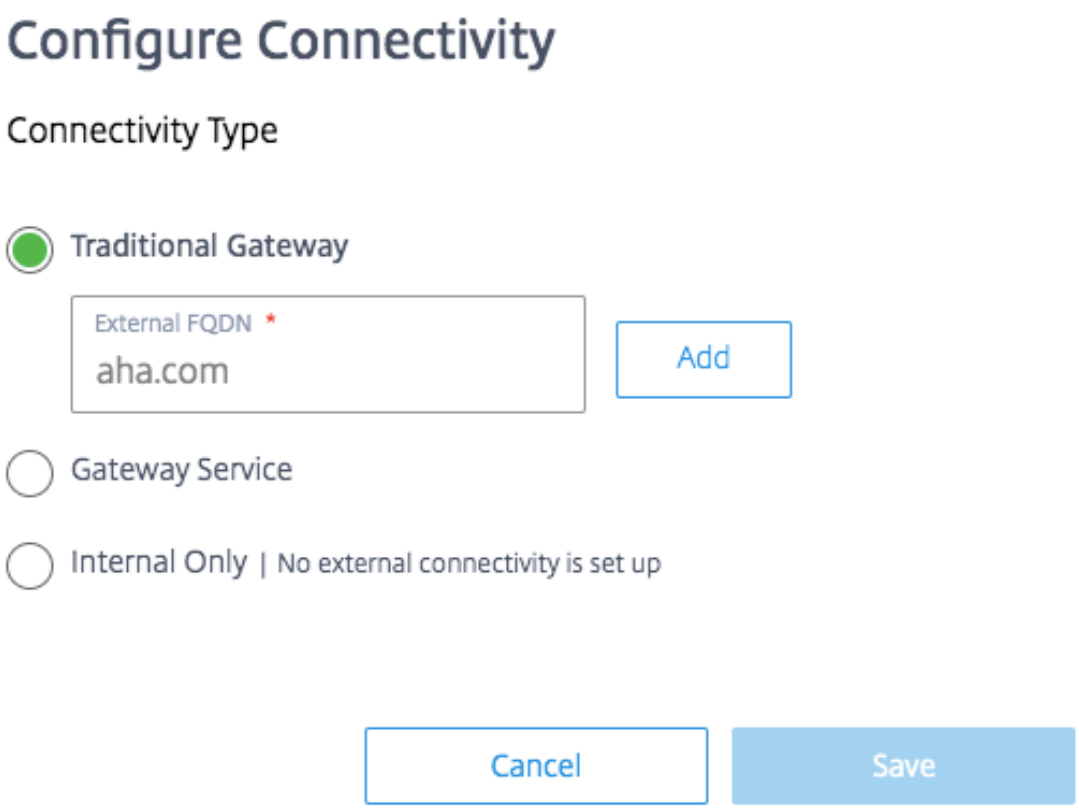
Roll back to NetScaler Gateway

To roll back the HDX Proxy to an on-premises NetScaler 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** under **Citrix DaaS**.



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



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

HDX Adaptive transport with EDT support for Citrix Gateway Service

April 13, 2023

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 DaaS
- 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.

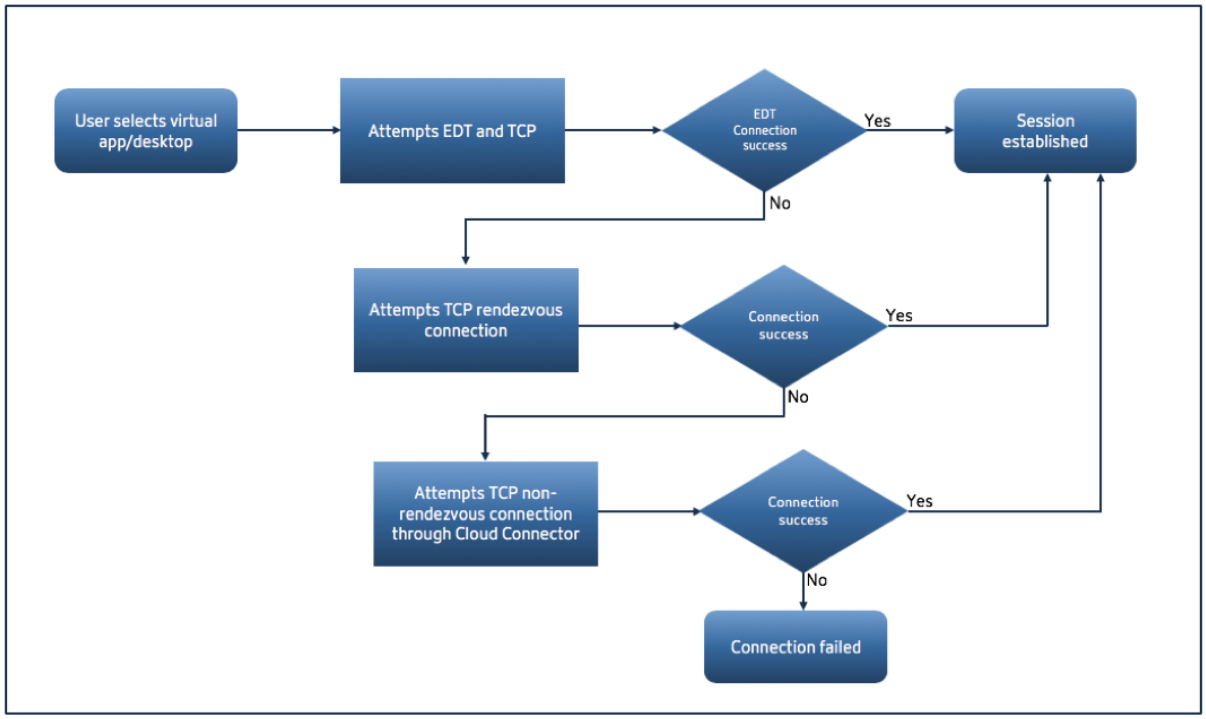
Transport protocol validation

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**.

Citrix Gateway Service on Google Cloud Platform

June 9, 2023

With Citrix Gateway Service support on the Google Cloud Platform (GCP), customers running their workloads on Google Cloud can take advantage of Google Cloud's high-performing global network using the Citrix Gateway optimal routing feature. The optimal gateway routing feature directs clients to the closest GCP Citrix Gateway Service POP. Also, the Citrix Gateway Service on Google Cloud provides

secure connectivity between Citrix Workspace clients and virtualization resources to deliver sessions with the lowest latency and the best user experience possible.

Currently, Citrix Gateway Service for GCP is available in the following regions.

- United States
  - Los Angeles
  - Oregon
  - South Carolina
- Europe
  - London
  - Zurich

> **Note:**
>
> - GCP POPs are only available for Citrix DaaS customers who have purchased subscriptions from the Google Cloud Marketplace and running their workloads on Google Cloud.
> - Citrix Gateway Service account - Customers who are entitled for Citrix DaaS 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.

Prerequisites

- Citrix Cloud account. For details see, Sign up for Citrix Cloud.

Citrix Gateway Service features supported

The following are some of the features supported by the Citrix Gateway Service for GCP.

TCP HDX Proxy - Currently, only TCP HDX Proxy is supported. Virtual Apps and Desktops launch is supported only via the TCP protocol.

Rendezvous V1 - When using the Citrix Gateway Service, the Rendezvous protocol version V1 allows VDAs to bypass the Citrix Cloud Connectors to connect directly to gateway POP for data-path traffic. For details, see Rendezvous V1.

Rendezvous V2 - The Rendezvous protocol version V2 supports bypassing the Citrix Cloud Connectors for both control traffic and HDX session traffic. For details, see Rendezvous V2.

> **Important:**
>
> EDT support is not yet enabled for GCP.

How to enable Citrix Gateway Service

Customers who are entitled for Citrix DaaS 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.

Limitations

Currently, GCP in available only in the United States and Europe regions. GCP customers from other regions might observe high latency issues.

References

- Citrix Cloud Connector connectivity requirements –For details, see Cloud Connector common service connectivity requirements.
- Scale and size considerations for Cloud Connectors. For details, see Scale and size considerations for Cloud Connectors.

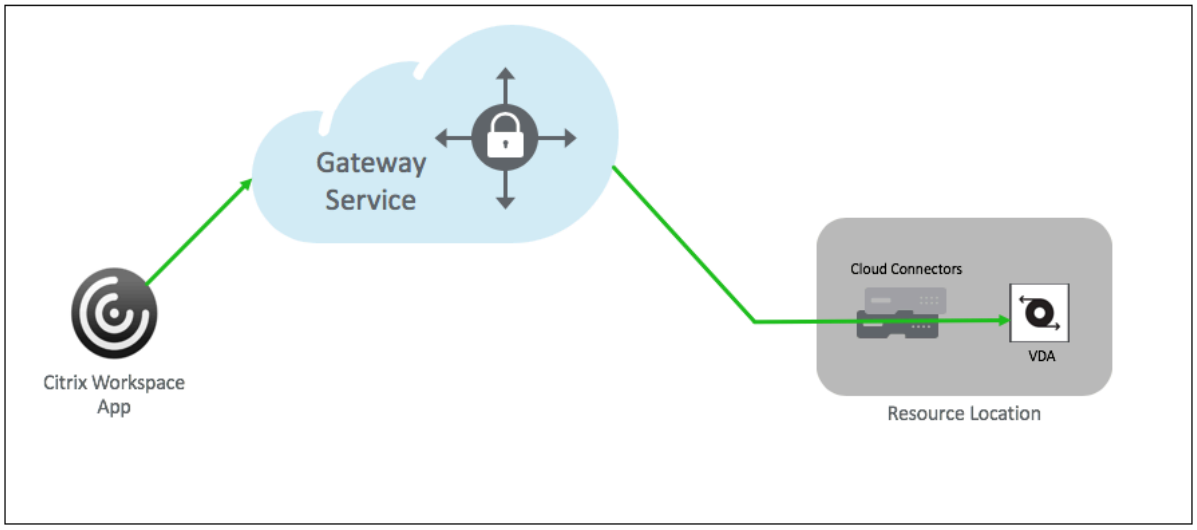
Support for Citrix Virtual Apps and Desktops

April 13, 2023

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.

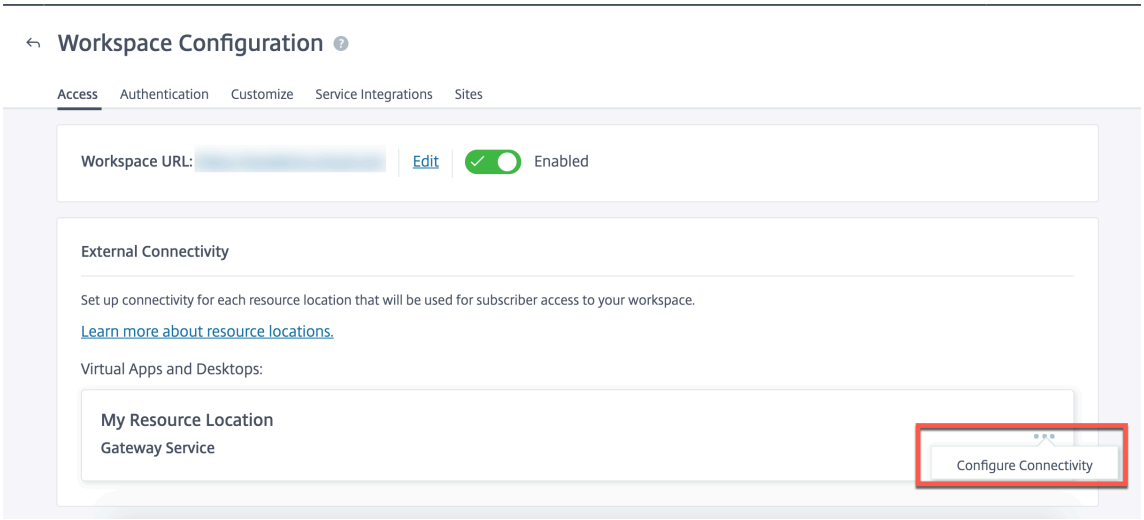
- Sessions are linked via Citrix Gateway Service across cloud partner's WANs.
- VDAs and Workspace endpoints rendezvous at the Citrix Gateway Service POP closest to the user.
- High quality sessions.

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 DaaS**. Click the ellipses, click **Configure Connectivity**.



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

Citrix Gateway Service for StoreFront - Preview

June 5, 2024

> **Important information:**
>
> - This document describes the steps that you can perform to deploy Citrix Gateway Service for StoreFront in a scenario where you prefer to use the on-premises NetScaler Gateway for authentication and on-premises StoreFront for enumeration.
> - The Citrix Gateway Service for StoreFront solution is in preview and must not be used in a production environment. Features in preview are recommended to be used in non-production environments only and to give customers an opportunity to share feedback. Cloud Software Group does not accept support cases for features in preview but welcomes feedback for improving them. Cloud Software Group might act on feedback based on its severity, criticality, and importance in its sole discretion.
> - No service commitment is offered for any trial, preview, labs, or beta service.
> - Citrix Gateway Service for StoreFront is currently not supported in Citrix Cloud Japan and Citrix Cloud Government environments.

Overview

Citrix Gateway Service for StoreFront is a cloud based HDX solution that provides secure remote access to resources accessed from on-premises StoreFront. You can leverage the scalability and relia-

bility of Citrix Cloud (for HDX proxy) without changing your on-premises StoreFront and on-premises NetScaler Gateway environments.

Consider that you are a Citrix DaaS customer using on-premises StoreFront as your enterprise application store and on-premises NetScaler Gateway for remote access. If you are looking for an option to leverage a cloud-hosted remote access solution (HDX proxy) while maintaining on-premises StoreFront as your user portal and on-premises NetScaler Gateway for authentication, Citrix Gateway Service for StoreFront is for you.

Citrix Gateway Service handles the HDX proxy launches using a Windows-based Cloud Connector in your resource location.

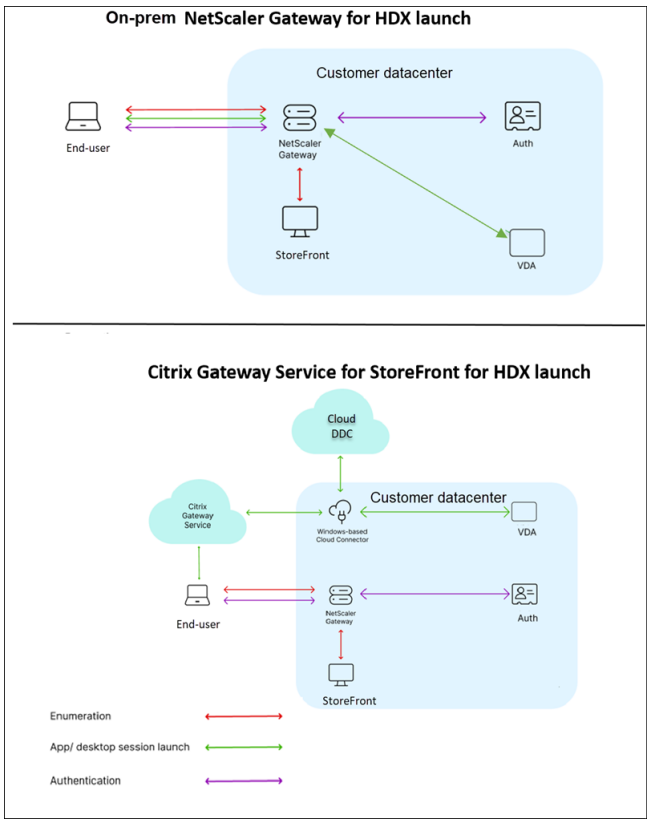
> **Notes:**
>
> - You can sign up for the preview using https://podio.com/webforms/28961380/2348524.
> - You can provide your feedback using https://podio.com/webforms/29573332/2436458.

Citrix Gateway Service for StoreFront supports the following use cases:

- Authentication and session management: Two-factor authentication (LDAP, SAML) along with basic EPA scans
- HDX: HDX over TCP
- Smart Access

The following use cases are not supported:

- Non-HDX use cases such as RDP proxy, VPN, PC over IP (PCoIP).
- Classic authentication policies



Benefits

- Citrix Cloud onboarding is faster and seamless.
- Retains the benefits of on-premises StoreFront for enumeration and on-premises NetScaler Gateway for authentication.
- Customers can maintain their NetScaler and StoreFront customizations.
- Citrix DaaS customers can use their existing on-prem NetScaler Gateway URL.
- Ensures high resiliency because of the multi-cloud and multi-geo architecture of Citrix Gateway Service.
- HDX proxy performance and scale requirements are now managed by Citrix Gateway Service. They are no longer customer-managed.

Pre-requisites

- Use NetScaler 13.1 version and above. For details, refer to NetScaler documentation.
- Use an on-prem StoreFront version 2311 or later with Citrix DaaS configured. For details, refer to StoreFront System requirements.
- Onboard Citrix Cloud and install Citrix Cloud Connector. Cloud Connector in your on-premises environment is used to establish connectivity with your on-premises StoreFront from Citrix

Gateway Service. You can use an existing Cloud Connector or deploy a new one. If your connector upgrade is disabled, contact Support to get it enabled.

For details about the Citrix Cloud Connector requirements, see Citrix Cloud Connector requirements. For details about the sizing requirements, see Size and scale considerations for Cloud Connectors.

- Configure a network time protocol (NTP) server to avoid time skews. For details, see How to synchronize system clock with servers on the network.

> **Note:**
>
> Only a Windows-based Cloud Connector is supported. Connector Appliance is not supported.

Deploy Citrix Gateway Service for StoreFront

Citrix Gateway Service for StoreFront deployment involves the following steps:

1. On-premises NetScaler Gateway for authentication
2. On-premises StoreFront configuration for enumeration

1. On-premises NetScaler Gateway for authentication

On-premises NetScaler Gateway directly facilitates authentication and establishes connectivity with on-premises StoreFront. With this approach, you can continue using the existing on-premises resources for authentication, enumeration, and pre-launch.

Deploy on-premises NetScaler Gateway at the perimeter of your organization's internal network to provide a secure single point of access to Citrix Virtual apps and Desktops.

2. On-premises StoreFront configuration for enumeration

This section describes the following on-premises StoreFront configurations to be performed after Citrix Gateway Service for StoreFront is deployed.

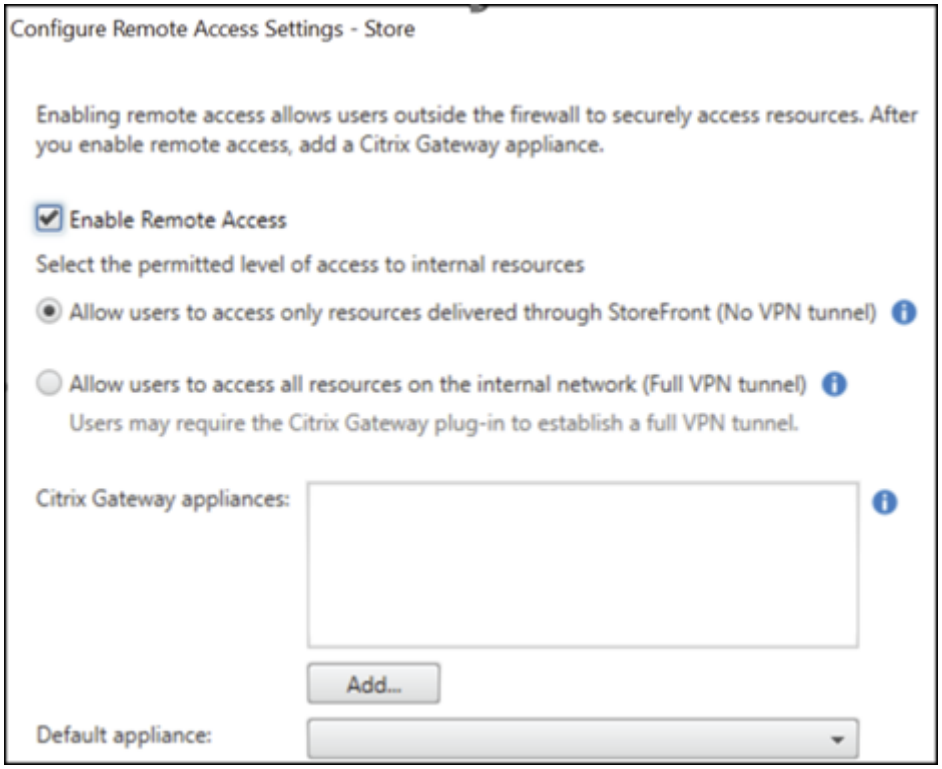
1. Enable remote access to the StoreFront store
2. Add on-premises NetScaler Gateway
3. Configure a store to use Citrix Gateway Service for StoreFront
4. Establish a launch path

1. Enable remote access to the StoreFront store

1. Select **Stores** on the right pane of the on-premises StoreFront GUI.
2. In the **Results** pane, select a store and click **Configure Remote Access Settings**.
3. Select the **Enable Remote Access** option.

2. Add on-premises NetScaler Gateway This step enables access to the stores from Citrix Gateway Service for users connecting from public networks.

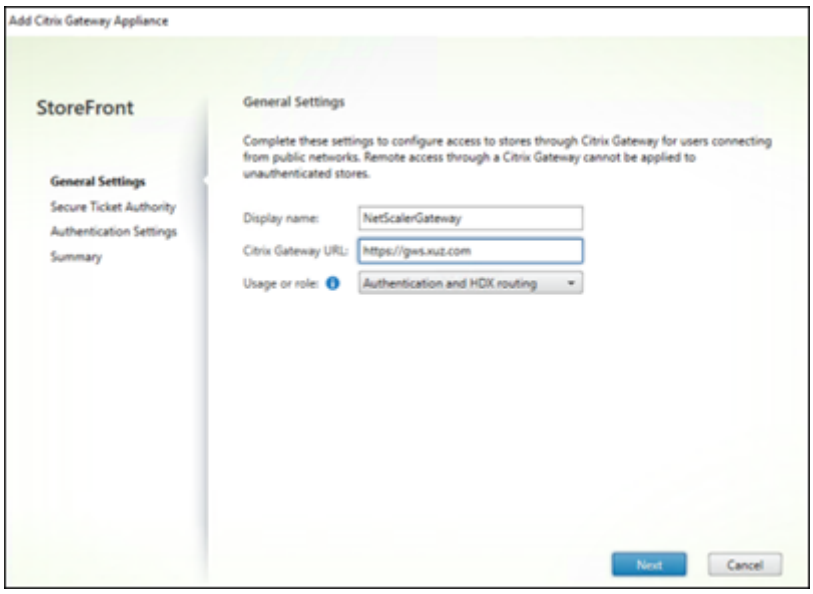
1. Click **Add** in the **Citrix Gateway appliances** section.



2. On the **General Settings** page, configure the following settings:

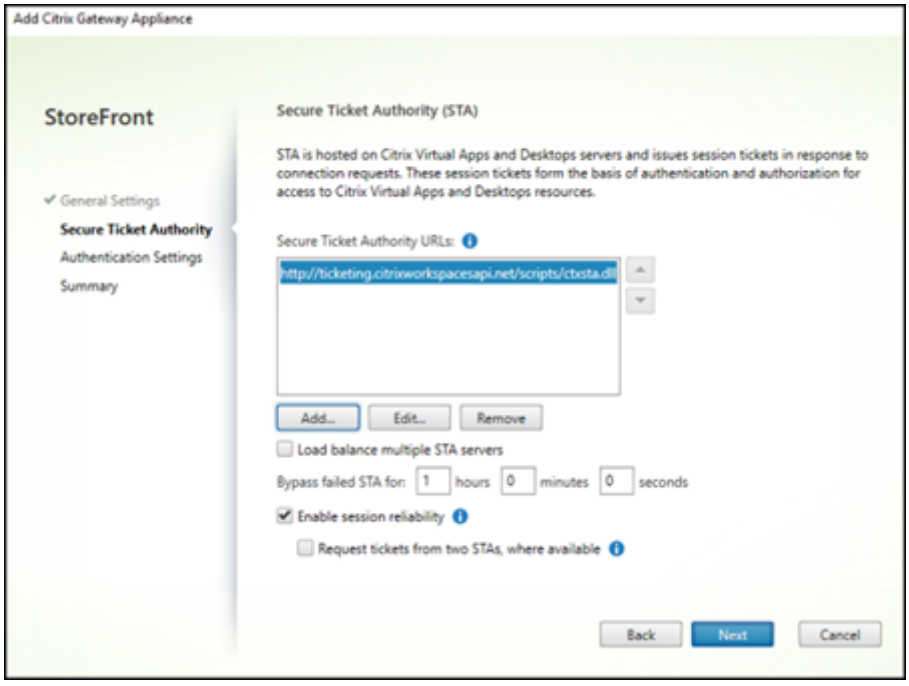
   - **Display name**: The name of the on-premises NetScaler Gateway.
   - **Citrix Gateway URL**: FQDN of the on-premises NetScaler Gateway.
   - **Usage or role**: Select Authentication and HDX routing.

> **Note:**
>
> In this section, "NetScalerGateway"is used as the name of the on-premises NetScaler Gateway. You will require this name later when running a PowerShell command, to enable Citrix Gateway Service for StoreFront.

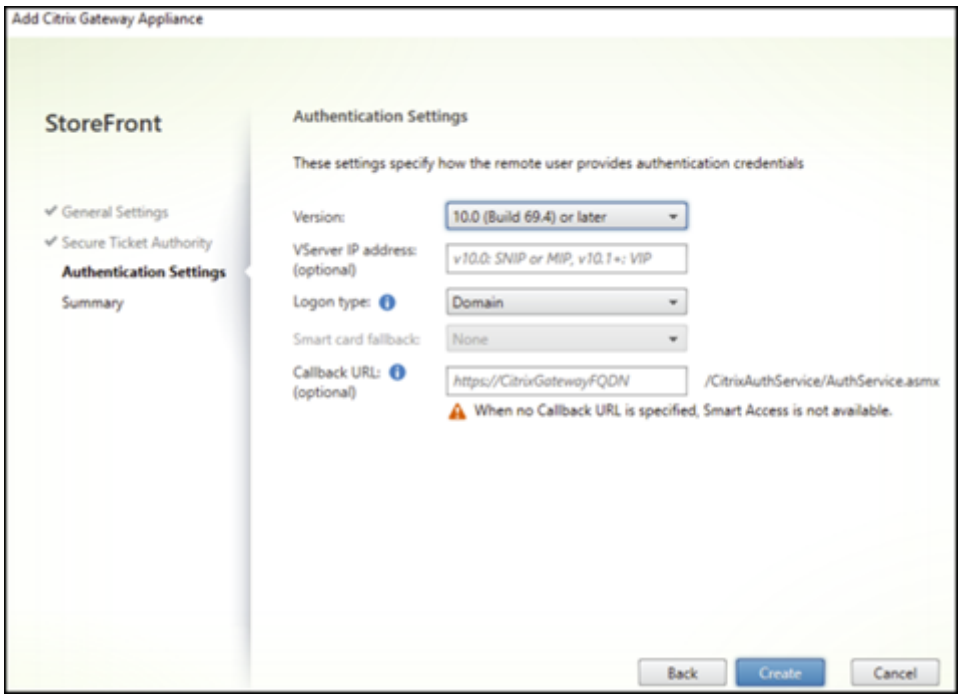


3. On the **Secure Ticket Authority (STA)** page, add the STA URL that redirects you to the connector that proxies your requests to the Cloud STA service. Select **Load balance multiple STA servers** if more than one STA URL is configured.

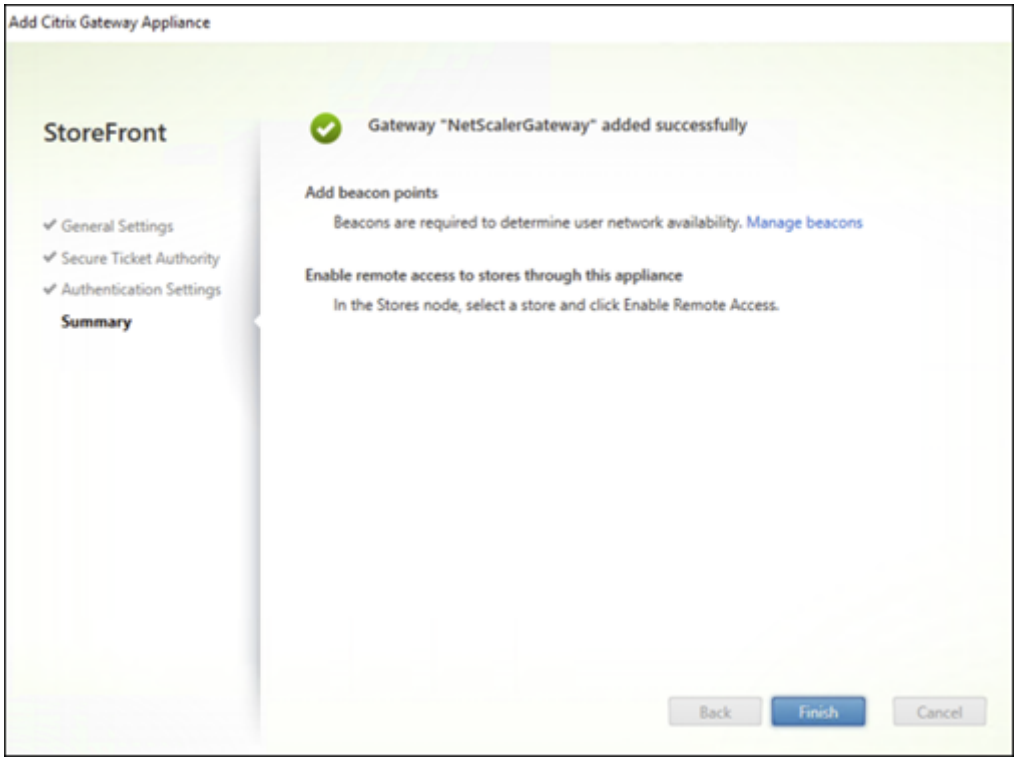
> **Note:**
>
> Ensure that the **Enable session reliability** checkbox is selected.



4. On the **Authentication Settings** page, select the version of your on-premises NetScaler Gateway, the virtual server, and logon type and then click **Create**.

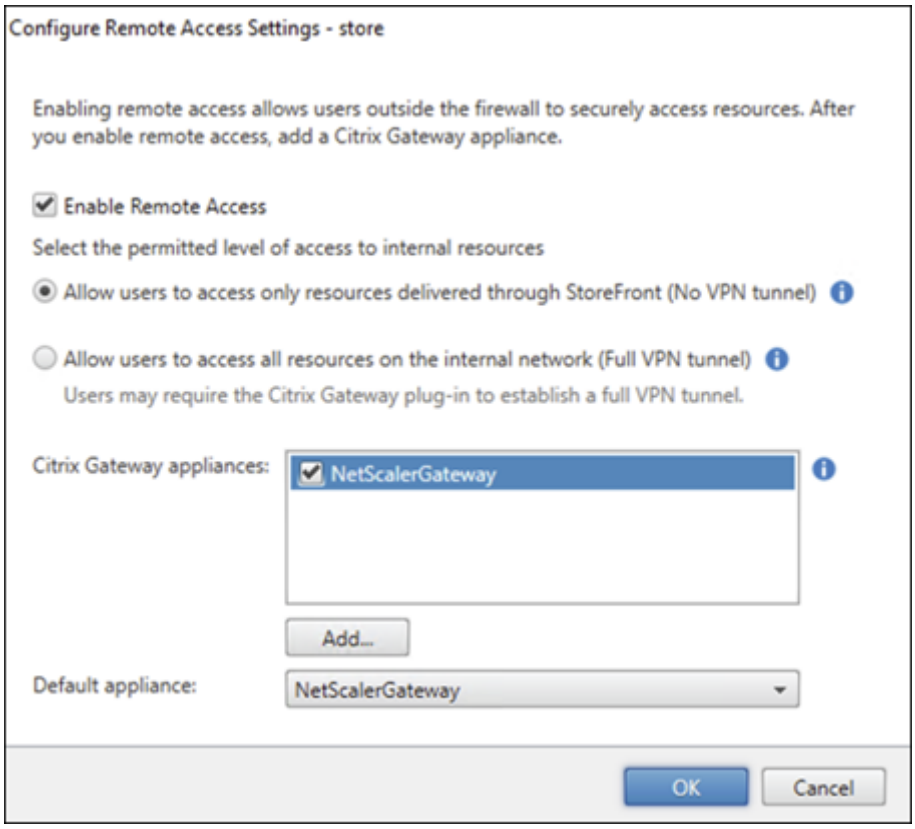


5. On the **Summary** page, you see a notification that the on-premises NetScaler Gateway has been added successfully. Click **Finish**.



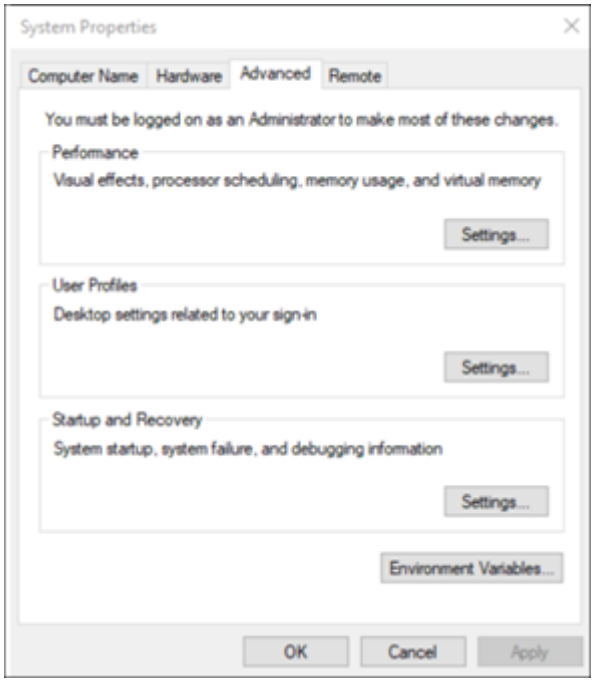
3. Configure a store to use Citrix Gateway Service for StoreFront This step enables you to associate on-premises NetScaler Gateway to your store.

1. On the **Store > Configure Remote Access Settings** page, select your on-premises NetScaler Gateway and set it as your default appliance.
2. Click **OK**.

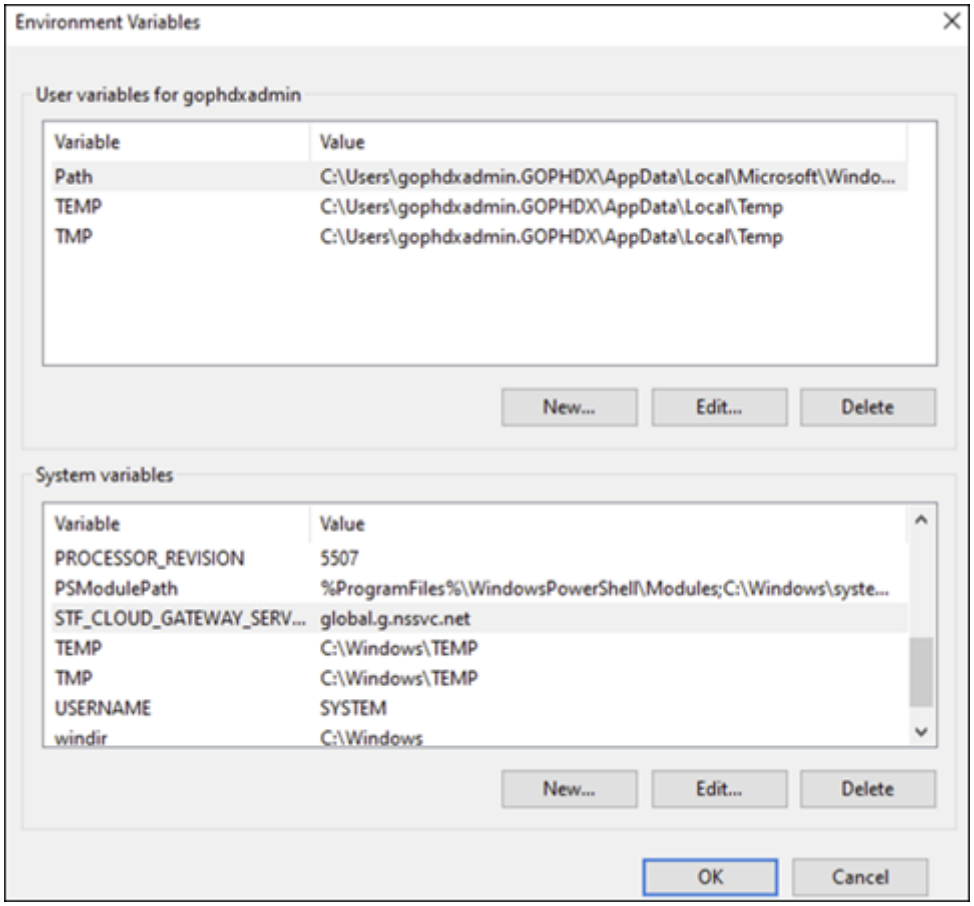


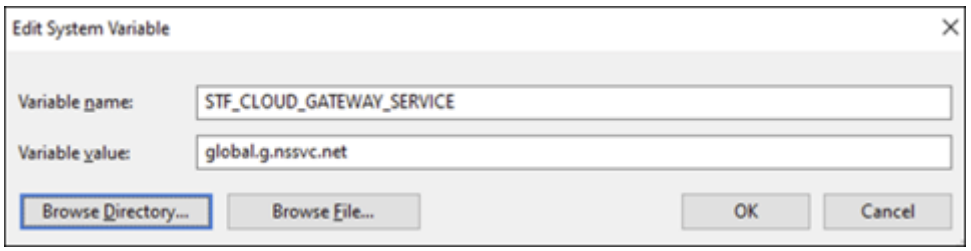
4. Establish a launch path Enable the Citrix Gateway Service FQDN to establish a path for HDX launch.

1. Navigate to **System Properties** on your device (On your command prompt, run the `sysdm.cpl` command).
2. Go to the **Advanced** tab and click **Environment Variables**.



3. Add the user variables and system variables. Assign a name and value to the variables. For this deployment, the value must be `global.g.nssvc.net`.
4. Click **OK**.





5. Open your command prompt as an administrator and run the `IISRESET` command.

Use the following PowerShell command to enable the Cloud Gateway Service for StoreFront functionality for your deployment:

```
Set-STFRoamingGateway -Name "NetScalerGateway"-IsCloudGateway $true
```

Use the following PowerShell command to verify the status of your Citrix Gateway Service for on-premises StoreFront deployment.

```
Get-STFRoamingGateway | Format-Table Name, IsCloudGateway

 Name          IsCloudGateway
# ----          --------------
# NetScalerGateway     True
<!--NeedCopy-->
```


Security requirements

For best practices on NetScaler security, see the NetScaler secure deployment guide.

Troubleshooting

Ensure that you enable the log levels to capture the Citrix Gateway Service for StoreFront logs.

To enable logs using the NetScaler GUI:

1. Navigate to **Configuration > System > Auditing**.
2. In the **Auditing** page, under **Settings**, click **Change Auditing Syslog Settings**.
3. In **Log Levels**, select **ALL**.

> **Note:**
>
> Ensure to restore the log level settings after troubleshooting.

Authentication

- To troubleshoot authentication issues, see Troubleshoot authentication, authorization and auditing issues.
- For information about data collection, see How to collect data for ADC Gateway, Storefront, and VDA issues.

EPA

- **Issue**: EPA client is already present, but the user is prompted to download it:

  Possible causes: Version mismatch or corrupt files

  Run Developer Tools and validate if the plug-in list file contains the same version as that of NetScaler and your client machine. Ensure that the Citrix EPA client version is the same as the one on the client machine.

  Workaround: Update the EPA client on the on-premises NetScaler Gateway GUI by navigating to **Citrix Gateway > Global Settings > Update client libraries**. For details about the EPA client versions, see the EPA plug-in libraries page on Citrix Downloads.

- Revert EPA settings (Always, Yes, No) after the user has selected an option.

  Workaround:

  - On the client machine, navigate to `C:\Users<user_name>\AppData\Local\Citrix\AGEE`.

- Open the `config.js` file and set "trustAlways"to "null". For example, "trustAlways" :null.

For instructions about EPA configurations, refer to the following articles:

- Configure pre-auth and post-auth EPA scan as a factor in nFactor authentication
- Configure NetScaler Gateway preauthentication EPA scan for the domain check
- Advanced Endpoint Analysis Scans

Session launch

For information about how to diagnose session launch failures, see Session launch diagnostics.

General Support log collection procedures

- **Technical support bundle:** For details, see How to collect the technical support bundle from VPX appliances for insight analysis.
- **Trace files**: For details, see How to record a packet trace on NetScaler.
- Contact Support for guidance.

Other references

- StoreFront Always On tracing
- EPA log collection
- Support

Known issues and limitations

- HDX session launch fails if the Enable session reliability option is disabled on on-premises StoreFront.
- Citrix Gateway Service for StoreFront does not support dual STA.
- Applications launched through Citrix Workspace fail to load from iOS devices.

  Workaround: Run the following CLI commands through the Netscaler ADM configuration job before you launch the applications through Citrix Workspace.


```
bind policy patset ns_aaa_relaystate_param_whitelist "
    citrixauthwebviewdone://" -index 1 -charset ASCII

bind policy patset ns_aaa_relaystate_param_whitelist "citrixsso
    ://" -index 2 -charset ASCII

bind policy patset ns_aaa_relaystate_param_whitelist "citrixng://
    " -index 3 -charset ASCII
<!--NeedCopy-->
```

Upcoming enhancements

The following enhancements are planned in the upcoming releases:

- HDX over EDT
- Local Host Cache Support
- Rendezvous protocol
- DDC (On-premises)
- Multistore support

FAQ

October 27, 2023

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 Citrix DaaS 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 SmartAccess and SmartControl features are not available with Citrix Gateway Service. However, you can achieve these requirements using Citrix Device Posture service (for EPA scans) and Citrix Adaptive Authentication service.

How can I do a phased migration to the 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 the 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 the Citrix Gateway Service?

Any customer using Citrix DaaS or Citrix Workspace is entitled to use Citrix Gateway Service for HDX Proxy.

What happens after the bandwidth quota is exhausted?

You can check the bandwidth Usage on the License Usage dashboard on Citrix Cloud. Once the bandwidth quota is exhausted, it is business as usual with no disruptions. However, customers must buy more bandwidth for which they can contact the Citrix sales representatives.

Citrix DaaS Advanced and Advanced Plus customers are entitled to the following licenses:

- User licensing: 1 GB per user per month
- Concurrent user licensing: 2 GB per user per month

Citrix DaaS Premium and Premium Plus customers are entitled to the following licenses:

- User licensing: 5 GB per user per month
- Concurrent user licensing: 10 GB per user per month

Where can I view the metrics of connections established through Citrix Gateway service?

The Connector statistics dashboard of the Citrix Analytics for Performance UI provides a comprehensive view of the resource consumption on the selected connector during the last 24 hours and a view of the synthetic latency calculated from the connector to the Citrix Gateway Service PoPs in your virtual apps and desktops environment. For more information, see Connector Statistics.