



StoreFront 2402

Contents

StoreFront 2402 Long Term Service Release Overview	5
What's new	6
What's new in 2402 (initial release)	6
Known issues in 2402	11
New UI for on-premises stores (Technical Preview)	12
Install, set up, upgrade, and uninstall	23
Plan your StoreFront deployment	23
User access options	27
System requirements	33
Install StoreFront	39
Citrix Customer Experience Improvement Program	43
Citrix Analytics service	45
Securing StoreFront with HTTPS	55
Secure your StoreFront deployment	60
Email-based account discovery	71
Create a new deployment	73
Join an existing server group	74
Upgrade StoreFront	75
Reset a server to factory defaults	80
Uninstall StoreFront	81
Configure authentication and delegation	82
Configure authentication	83
Smart card authentication	85

Domain pass-through authentication	90
Pass-through from Citrix Gateway	92
SAML authentication	96
User name and password authentication	102
Federated Authentication Service Configuration	110
Configure and manage stores	111
Create store	113
Configure a Store	120
Remove a store	121
Export store provisioning files for users	122
Advertise and hide stores to users	122
Kerberos delegation	124
Manage the resources made available in stores	125
Manage remote access to stores through Citrix Gateway	146
Certificate Revocation List (CRL) checking	148
Configure two StoreFront stores to share a common subscription datastore	157
Manage favorites for a store	159
Store subscription data using Microsoft SQL Server	164
Enable or disable favorites	183
Citrix Virtual Apps and Desktops configuration	184
Advanced store settings	186
Configure optimal HDX routing for a store	193
Subscription synchronization	198
Configure session settings	201

ICA file signing	203
Citrix Workspace app configuration	204
Manage a website	205
Create a website	206
Configure website	209
Category Settings	211
Customize appearance	215
Featured app groups	217
Authentication methods	221
Website shortcuts	223
Citrix Workspace app deployment	225
Configure session settings	228
Workspace control	231
Client Interface Settings	234
App Protection	236
Remove website	237
Configure Workspace app website	237
Configure server groups	238
Integrate with Citrix Gateway and NetScaler ADC	240
Configure Citrix Gateways	241
Import a Citrix Gateway	249
Load balancing with NetScaler ADC	257
Configure Citrix Gateway and StoreFront for Delegated Forms Authentication (DFA)	270
Authenticate using different domains	273

Configure beacon points	283
Create a single FQDN used internally and externally	285
Export and import the StoreFront configuration	287
End user guide	296
StoreFront SDK	304
Troubleshoot StoreFront	314
Third Party Notices	317

StoreFront 2402 Long Term Service Release Overview

April 17, 2024

StoreFront is an enterprise app store that aggregates applications and desktops from [Citrix Virtual Apps and Desktops](#) sites and [Citrix DaaS](#) into a single easy to use store for users.

Within StoreFront you can configure one or more stores. Each store has its own configuration including:

- The list of resource feeds that StoreFront queries to enumerate the apps and desktops available to the user.
- The appearance of the website used to access the store.
- What [authentication methods](#) users use to log on.
- External access via a NetScaler gateway.

Users can use locally installed [Citrix Workspace app](#) or Citrix Workspace app for HTML5 in a web browser to access StoreFront stores. For more information see [User access options](#).

To get started, [Plan your StoreFront deployment](#), view the [System requirements](#) and [Install StoreFront](#).

What's new

Know more about the new features, fixed issues, and known issues in this release using the following links.

[What's new](#)

Earlier releases

To know more about earlier releases, refer [here](#).

For steps to upgrade from an earlier release, see [Upgrade](#).

Support lifecycle

The product lifecycle strategy for StoreFront Current Releases (CR) and Long Term Service Releases (LTSR) is described in [Lifecycle Milestones](#). Additional Lifecycle Information for StoreFront is provided in [CTX200356](#).

What's new

March 19, 2024

The 2402 LTSR includes the following releases.

- [2402 initial release](#)

What's new in 2402 (initial release)

April 23, 2024

StoreFront 2402 LTSR includes the following new features and enhancements since StoreFront 2203 LTSR:

Prevent .ica file downloads during Hybrid launch

To minimize security risks that might arise with the download of `.ica` files on local systems, the following settings have been introduced. Admins can configure these settings from the StoreFront admin console as a preventive measure against the misuse of downloaded `.ica` files.

These settings include:

- [Show **Already installed** link on client detection page](#)
- [Prevent ICA downloads on all platforms](#)

Edit Receiver for Web site - /Citrix/StoreWeb

StoreFront

- UI Experience
- Category Settings
- Customize Appearance
- Featured App Groups
- Authentication Methods
- Website Shortcuts
- Deploy Citrix Receiver/Workspace app**
- Session Settings
- Workspace Control
- Client Interface Settings
- Advanced Settings

Deploy Citrix Receiver/Workspace app

For the best user experience, Receiver for Web sites detect Windows and Mac OS X devices and offer users the opportunity to download and install Citrix Receiver/Workspace app. If users cannot install Citrix Receiver/Workspace app, enable Receiver for HTML5.

Deployment option: Use Receiver for HTML5 if local Citrix Receiver/Workspace a...

☐ Launch applications in the same tab as Receiver for Web

☐ Show 'Already Installed' link on client detection page ⓘ

☐ Prevent ICA downloads on all platforms ⓘ

☒ Allow users to download HDX engine (plug in) ⓘ

☐ Upgrade plug-in at logon ⓘ

Source for Receivers/Workspace app

Windows source: Local files on the StoreFront server

Windows Installer: ⓘ No file available in the directory. Browse...

Mac source: Local files on the StoreFront server

Mac Installer: ⓘ No file available in the directory. Browse...

OK Cancel Apply

For more information, see [Prevent ICA file download](#).

Enable advanced health check for all stores

Advanced health check is enabled for all existing stores on upgrade to 2402 to improve resiliency. With advanced health checks, StoreFront can more reliably check for any issues in the delivery controller. When used with Citrix Desktops as a Service, the advanced health checks provide additional information about the connectors present at the resource locations. This is useful in the event of an outage. When a user launches a resource, an appropriate connector to launch the resource is selected automatically using Local Host Cache.

If you want to disable advanced health check for all stores, you can use the following PowerShell script:

```
1 foreach ($store in Get-STFStoreService)
2 {
3
4     Set-STFStoreFarmConfiguration -StoreService $store -
        AdvancedHealthCheck $False
5 }
6
7 <!--NeedCopy-->
```

Deprecation announcement for Windows server 2016

Support for installing StoreFront on Windows server 2016 will be removed in a future release. It is recommended that you upgrade to a newer version of Windows server for continued support. For more information on deprecated items, see [Deprecation notices](#).

Citrix Secure Private Access on StoreFront

You can now connect to the Citrix Secure Private Access on-premises server using new PowerShell commands or StoreFront admin UI controls. It allows users to securely access web and SaaS apps through StoreFront. For more information, see [Manage the resources made available in stores](#).

Uninterrupted VDA launch in case of FAS server unavailability

You can now configure StoreFront so that a VDA launch is successful even if the FAS server is unavailable. In such cases, the end users can sign in using their username and password. Previously, the VDA launch would fail if the FAS servers were unreachable.

This feature is disabled by default and can be enabled using the following Powershell command.

`Set-STFStoreLaunchOptions` with parameter `FederatedAuthenticationServiceFailover`

You can use the same command to disable this feature, if required.

For more information, see [FAS](#).

Improved user-journey logs

Previously by default only errors were logged. The default logging level has now been changed to include warnings and tracing information. In addition the log messages have been improved. This ensures that by default, all the events that are part of the main user journeys are now logged. The default log file size is increased to 1GB (5*200MB) for each service. Typically this will require 1GB (for the roaming service) + 3GB per store (as each store service typically has a corresponding authentication service and receiver for web service). Ensure you have sufficient disk space available. For more information, see [Diagnostics logging](#).

Citrix Workspace web extensions - General Availability

Citrix Workspace web extensions are now generally available for use with StoreFront. These web extensions help you launch resources in your locally installed Citrix Workspace app without prompts

to open Workspace launcher or downloading an `.ica` file, making your experience safer and more reliable. For more information, see [Citrix Web Extensions](#).

The use of Citrix Workspace web extensions is enabled by default for every new installation of StoreFront. However, end users still need to download the extensions to use this feature.

Note:

Citrix Workspace web extension is not enabled automatically during a StoreFront version upgrade. If this feature was turned-off before the upgrade, it remains in the same state after the version update. It will be enabled for all deployments in a future release.

When upgrading an existing deployment you can enable this feature using the following command:

```
Add-STFFeatureState -Name "Citrix.StoreFront.EnableBrowserExtension" -IsEnabled $True
```

New UI for on-premises stores (Technical Preview)

The new UI, is now available for on-premises stores. This UI, previously available only for cloud stores, ensures a consistent look and feel across cloud and on-prem stores.

The new UI brings the following key improvements:

- **User friendly UI:** Reduces visual complexity and provides easy access to essential features. For more information, see [Workspace visual and layout improvements](#).
- **Activity Manager:** Facilitates quick actions on active virtual apps and desktops, saving resources and optimizing performance. For more information, see [Activity Manager](#).
- **Enhanced categorization of apps:** Multi-level folder structure that is responsive to your end user's screen size. For more information, see [categorization of apps](#).
- **Improved Search capabilities:** New search capabilities provide for better and faster results. For more information, see [Search options](#).

For detailed information on this preview, see [New UI \(Tech Preview\)](#).

Note:

You can provide feedback for this feature using this [Podio form](#).

Citrix Workspace app for HTML5

This release includes [Citrix Workspace app for HTML5 2402](#).

App Protection for hybrid launches

App Protection provides an additional level of security by blocking keyloggers and screen capture. Previously, this functionality was only available when accessing a store through Citrix Workspace apps for Windows, Mac and Linux. When viewing a store through a web browser, protected apps were not displayed. With this release it is now possible to configure a store website to display apps requiring App Protection when viewed through a browser, as long as StoreFront has detected that the user has a sufficiently new version of Citrix Workspace app for Windows, Mac or Linux installed that will be used to launch the app.

For more information see [App Protection](#).

Advanced Health Check enabled by default

From this release onward, the advance health check feature is enabled by default for new stores. Previously it had to be enabled manually.

When used with Citrix DaaS, Advance health check makes StoreFront aware of the connectors present at the resource locations. In the event of an outage, when a user launches a resource, StoreFront chooses an appropriate connector to launch the resource using Local Host Cache.

Deprecation of XenApp Services

From this release onward, support for XenApp Services URLs (also known as PNAgent) for connecting to stores is deprecated. It will be removed in a future release. Use Citrix Workspace app to connect to stores using the store URL.

Removal of ability to add XenApp 6.5 delivery controllers

It is no longer possible to add new XenApp 6.5 resource feeds using the StoreFront management console. It is still possible to add them using PowerShell [Add-STFStoreFarm](#) specifying the FarmType as [XenApp](#). For Example:

```
1 $store = Get-STFStoreService
2 Add-STFStoreFarm -StoreService $store -FarmName "XenApp" -FarmType
  XenApp -Port 80 -TransportType HTTP -Servers Xen1
3 <!--NeedCopy-->
```

Existing XenApp 6.5 resource feeds can be modified using the management console.

Note:

XenApp 6.5 is not supported by Citrix. The ability to use XenApp 6.5 delivery controllers will be

removed in a future release.

Removal of ability to open resources within Internet Explorer 11

It is no longer possible to open resources within the Internet Explorer 11 web browser. It is still possible to access your store from Internet Explorer 11 but you must install Citrix Workspace app for Windows to be able to launch resources.

Fixed Issues

Following is a list of issues that are fixed since version 2203 CU4:

- App enumeration on StoreFront servers might fail intermittently. [CVADHELP-23196]
- Names containing special characters might appear corrupted in the Home tab and Settings dropdown menu. [CVADHELP-24499]
- The first time a user opens a store website in their browser on ChromeOS, it prompts the user to perform client detection but Citrix Workspace app for ChromeOS does not support client detection. As a result, the client detection fails and the users would need to click “already installed” to continue. With this fix, the website skips client detection on ChromeOS. [WSP-22390]
- Citrix Workspace app for Mac might freeze after waking up from Sleep mode when connected to a StoreFront Store. [CVADHELP-23217]
- A race condition can cause the Citrix Subscriptions Store service to exit unexpectedly on the StoreFront server with warning messages. [CVADHELP-23326]
- [CVADHELP-22435] A year after detecting that the user has Citrix Workspace app installed, apps are launched in a browser rather than Citrix Workspace app.
- [CVADHELP-21886] When using the StoreFront Store Service API to launch an app, overriding settings such as audio quality and disabling printers, the settings may affect all subsequent requests rather than just the current request.

Known issues in 2402

March 8, 2024

2402 initial release

There are no new known issues.

New UI for on-premises stores (Technical Preview)

April 26, 2024

The new UI is now available for on-premises stores. This UI which was previously available only for cloud stores, ensures a consistent look and feel across cloud and on-prem stores.

The new user interface is designed to enhance and simplify the end-user experience to access Citrix apps and desktops. It reduces visual complexity, provides easy access to essential features, and refines the StoreFront app experience. It supports new features, such as Activity Manager that facilitates effective management of your virtual apps and desktop resources.

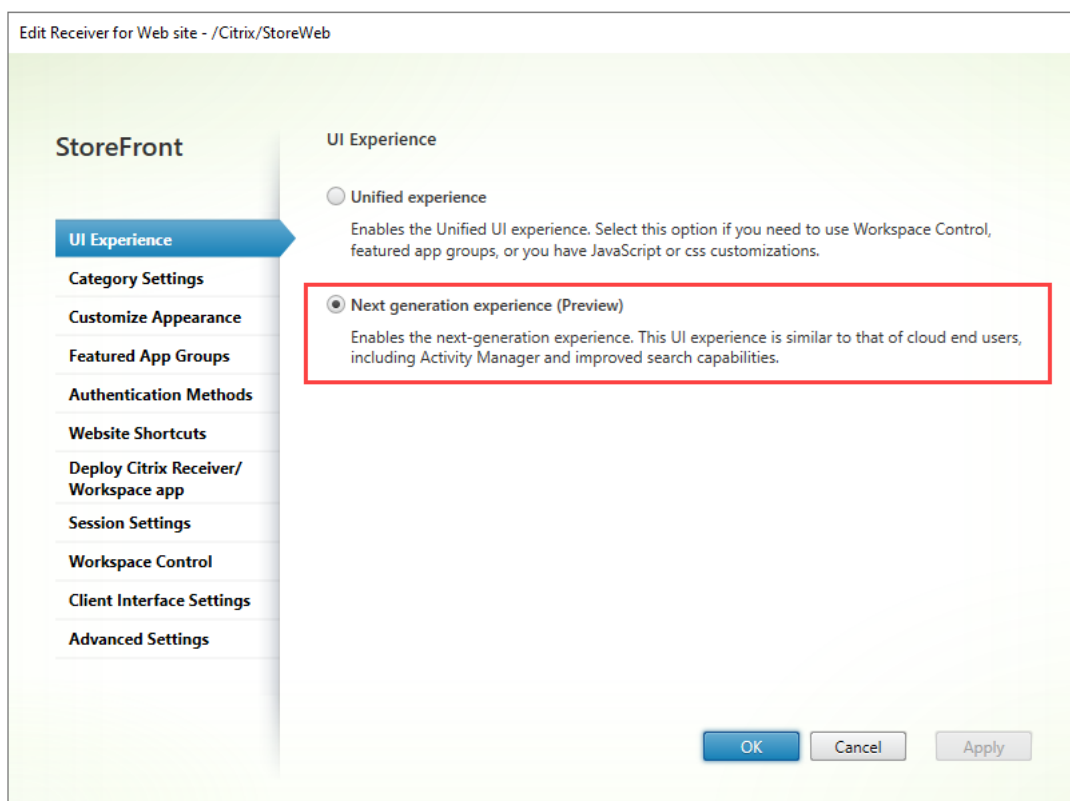
Note:

In this article the current UI experience has been referred to as the Unified UI experience.

Enable the new UI experience for on-prem stores

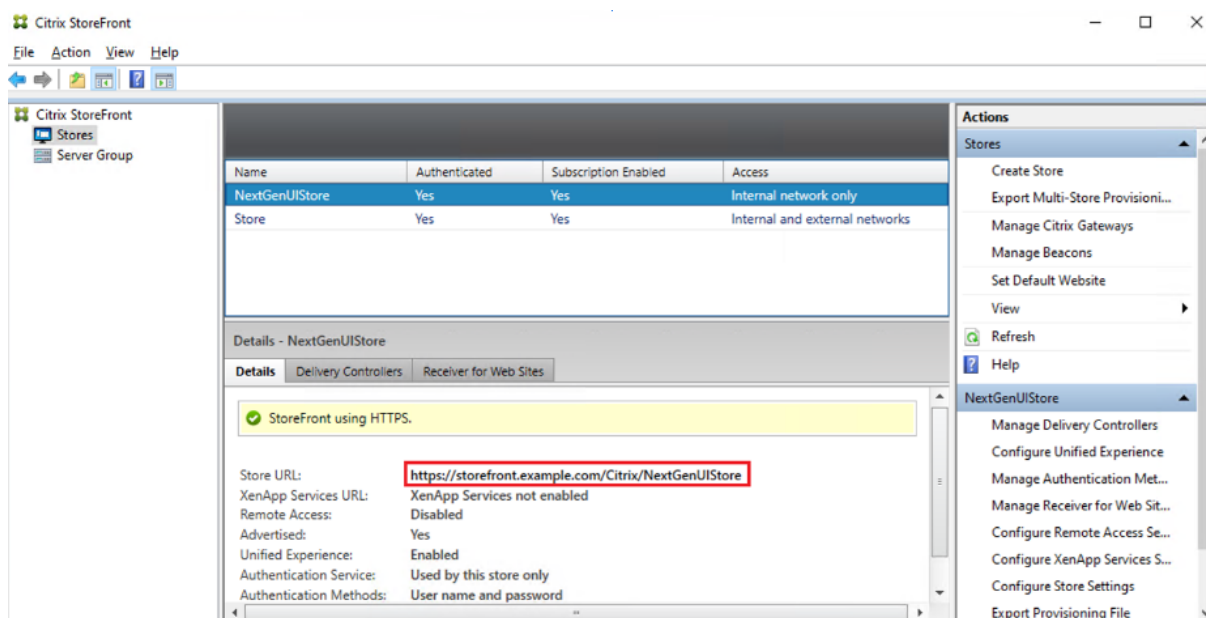
Since this feature is currently in preview, it's recommended that you create a new store and then enable the new UI experience for that particular store.

Once you've created the store, you need to enable the new UI by selecting **Next generation experience** on the Website Configuration page. Enabling the new UI for a new store helps you test the UI with a limited number of users.



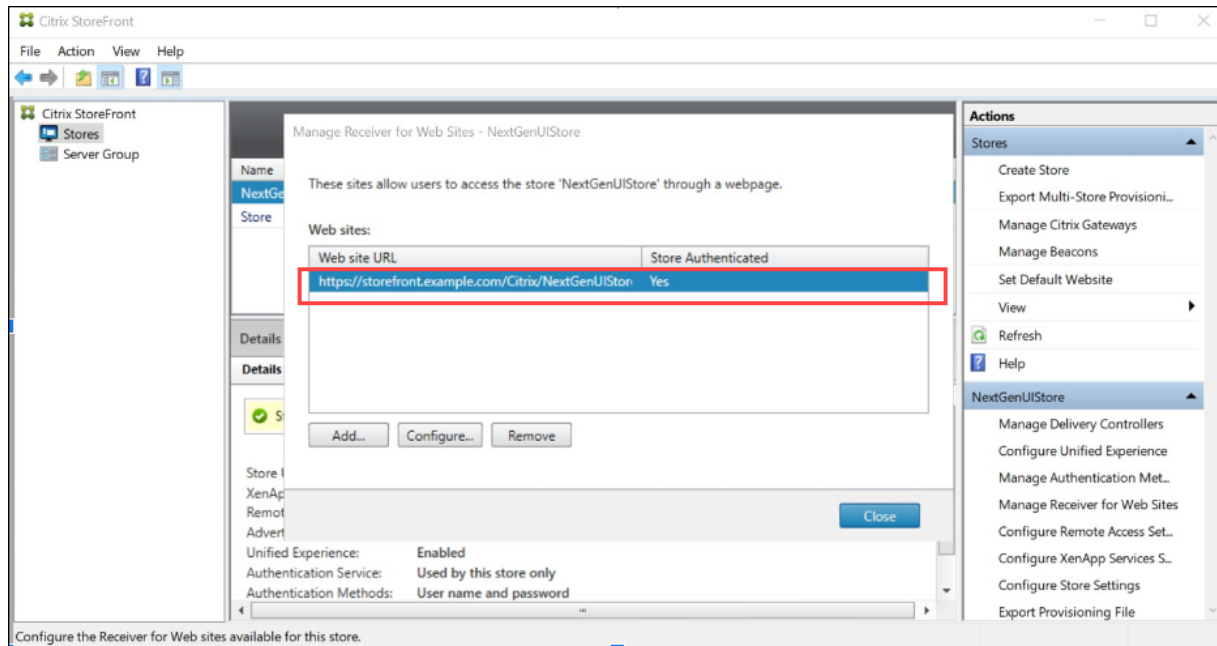
Once you've created a new store with the new-UI-enabled, you need to share the website or the store link with your end users.

- If your end users are using the native application, you must share the new store link with them.



- If your end users are signed in through a browser, you must share the new website link with

them.



Enable the new UI using PowerShell command

Admins can enable the new UI for their end users using the following PowerShell command `Set-STFWebReceiverService`.

For example:

```
1 $rfw=Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"
2 Set-STFWebReceiverService -WebReceiverService $rfw -WebUIExperience
  Workspace
3
4 <!--NeedCopy-->
```

Customize theme and logo

You can customize the theme and logo for your new-UI-enabled store. You can manage these settings from the **Customize Appearance** tab under **Manage your Website**. For detailed information on configuring a theme and logo, see [Customize appearance](#).

Key Benefits

The new UI brings the following key improvements:

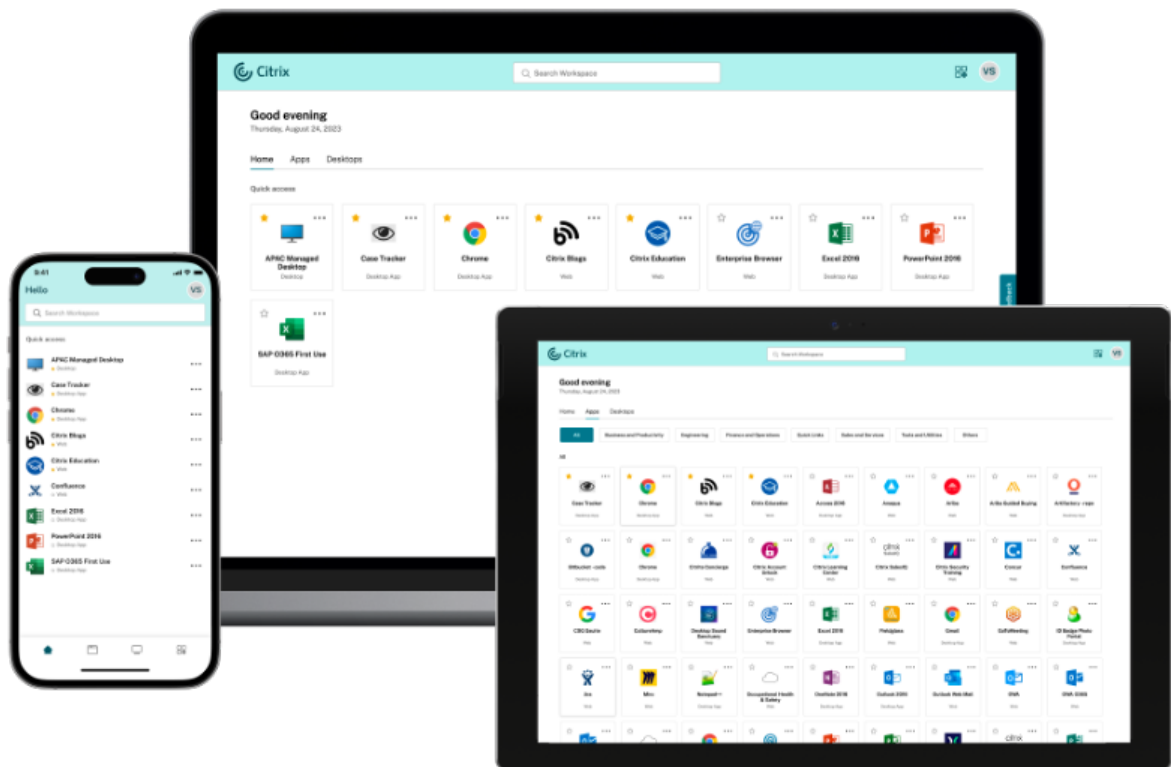
- **User friendly UI:** Reduces visual complexity and provides easy access to essential features. For more information, see Workspace visual and layout improvements.
- **Activity Manager:** Enables quick actions on active virtual apps and desktops, saving resources and optimizing performance. For more information, see Activity Manager.
- **Enhanced categorization of apps:** Multi-level folder structures that are responsive to the user's screen size. For more information, see categorization of apps.
- **Improved Search capabilities:** New search capabilities provide for better and faster results. For more information, see Search options.

Workspace visual and layout improvements

The new user experience is designed to provide an intuitive and simplified experience. The apps and desktops have been organized on the **Home**, **Apps**, and **Desktops** pages to provide easy navigation. Apps and desktops marked as favorites are placed at the beginning of the list for ease-of-access.

If your users have fewer than 20 apps, they're presented with a simple view that doesn't have any tabs or categories. All the apps and desktops appear on the same page. Apps marked as favorites are placed at the beginning of the list, followed by the other apps in an alphabetical order.

End users can mark any app or desktop as a Favorite by clicking the respective star icon. Similarly, they can remove an app or desktop from the list of Favorites by clicking the respective star icon.



If your users have more than 20 apps, they land on the **Home** page after sign-in. Favorite and up to five most recently used apps and desktops can be accessed from the **Home** page. Apps and desktops that have been mandated by the admins are indicated with a star icon. End users can't remove such apps and desktops from the list of Favorites.

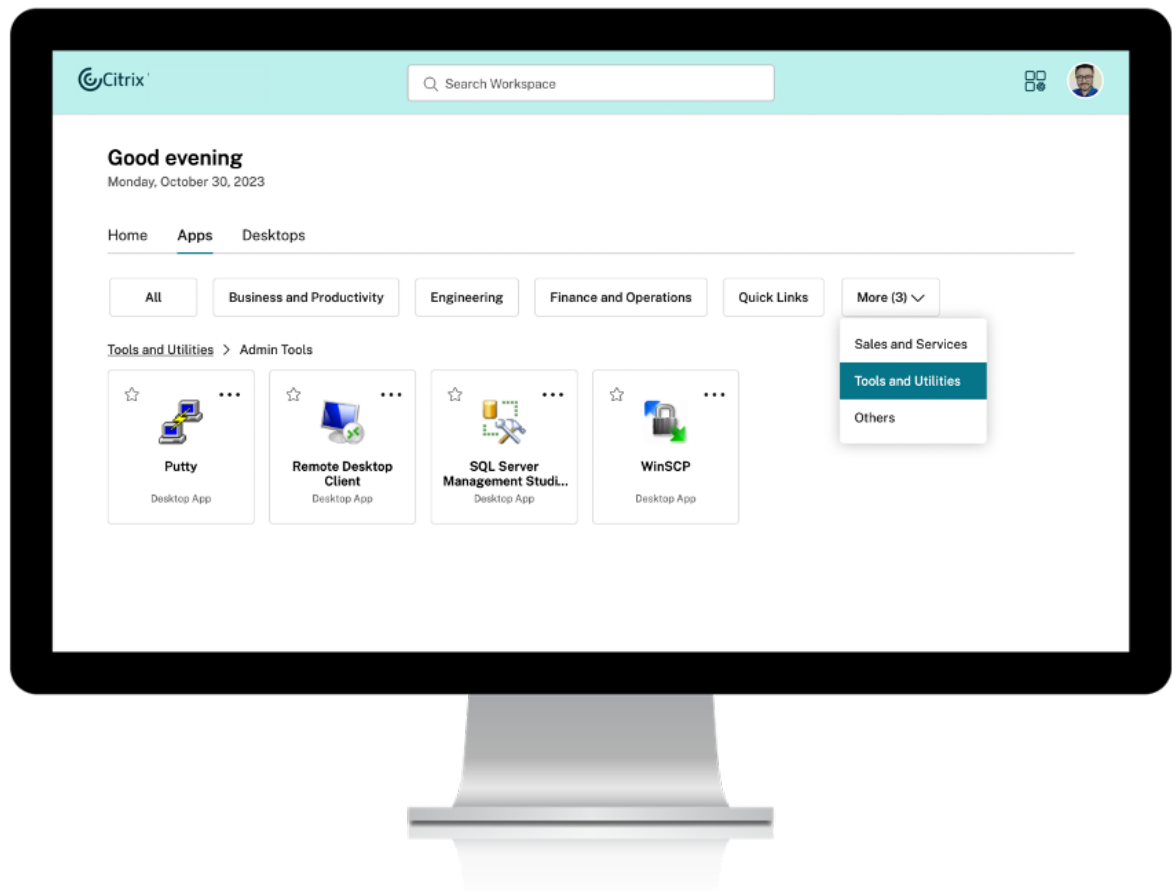
If the admin hasn't enabled the home page yet, users land on the **Apps** page. On this page too, Favorite apps are listed first, followed by all the other apps in an alphabetical order. If the admin has created app categories, users can click the categories to locate their apps.

Categorization of apps on the new UI

On the new UI, end users can view their apps organized into categories and sub-categories. The sub-categories appear in a folder structure. The organized multi-level structure makes for a clutter-free, optimized experience that helps enhance the overall user satisfaction. For more information on creating folders and sub-folders, see [Category settings](#).

When the number of primary categories created by the admins exceeds the available space on the user's screen, the user interface adjusts based on the screen size, and dynamically moves categories under the ***More dropdown**. The navigation breadcrumbs are also visible to the users.

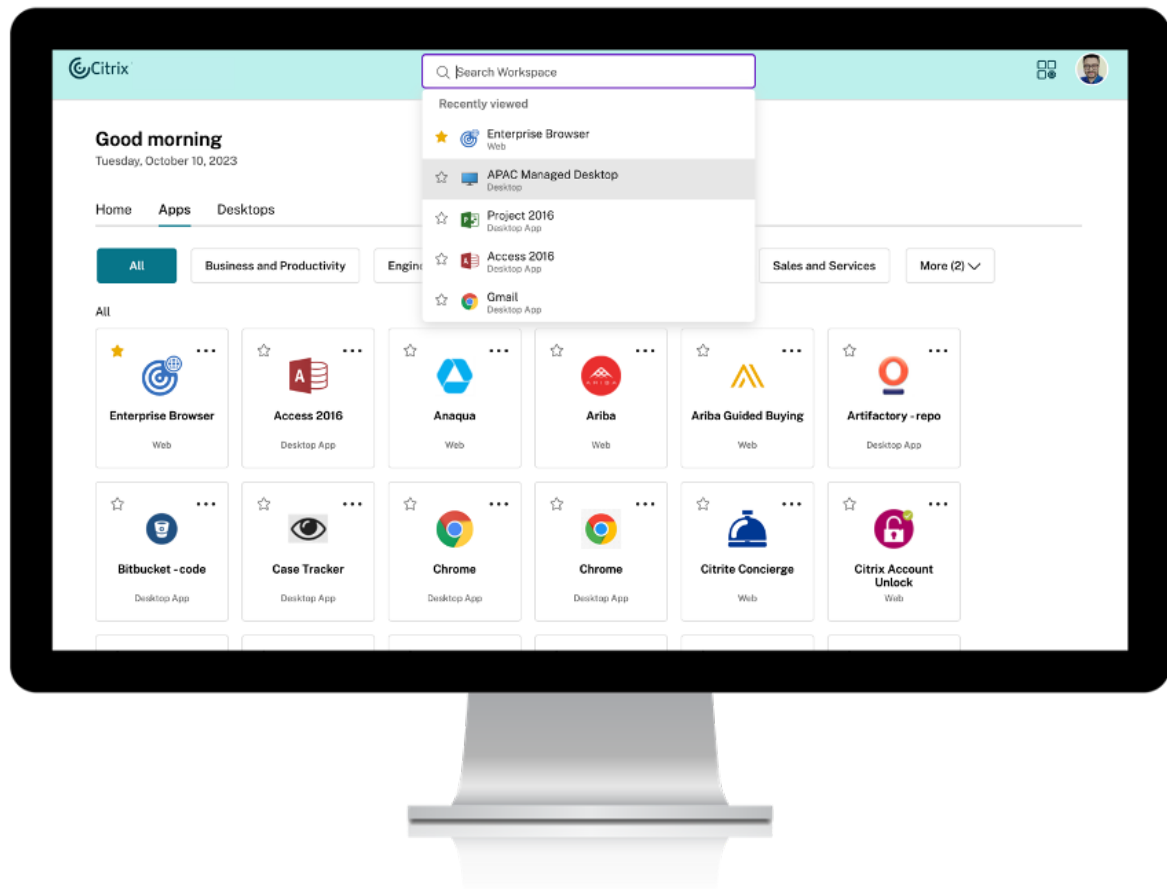
On mobile platforms, navigate to the **Apps** tab and click the **Categories** dropdown to view a list of available categories. Sub-categories appear as folders. The sub-folders might contain further sub-folders or apps as per the admin configuration.

**Note:**

On the Unified UI experience, apps are categorized into folders. The folder hierarchy is visible as breadcrumbs while you browse through apps or desktops. For more information, see [Category settings](#).

Search options

The search capability in the new UI is an improvement over the Unified UI. The enhanced Search feature on the new UI gives you better results from the search engines using fuzzy search mechanisms. The search option appears within the tool bar for ease of use, and allows you to do a quick and intuitive search.



It includes the following improvements:

- Default search displays the five most recently used apps or desktops
- Searches are enabled with spell check and display auto-complete results
- Perform a search by admin created categories
- Search result lists Favorites at the top

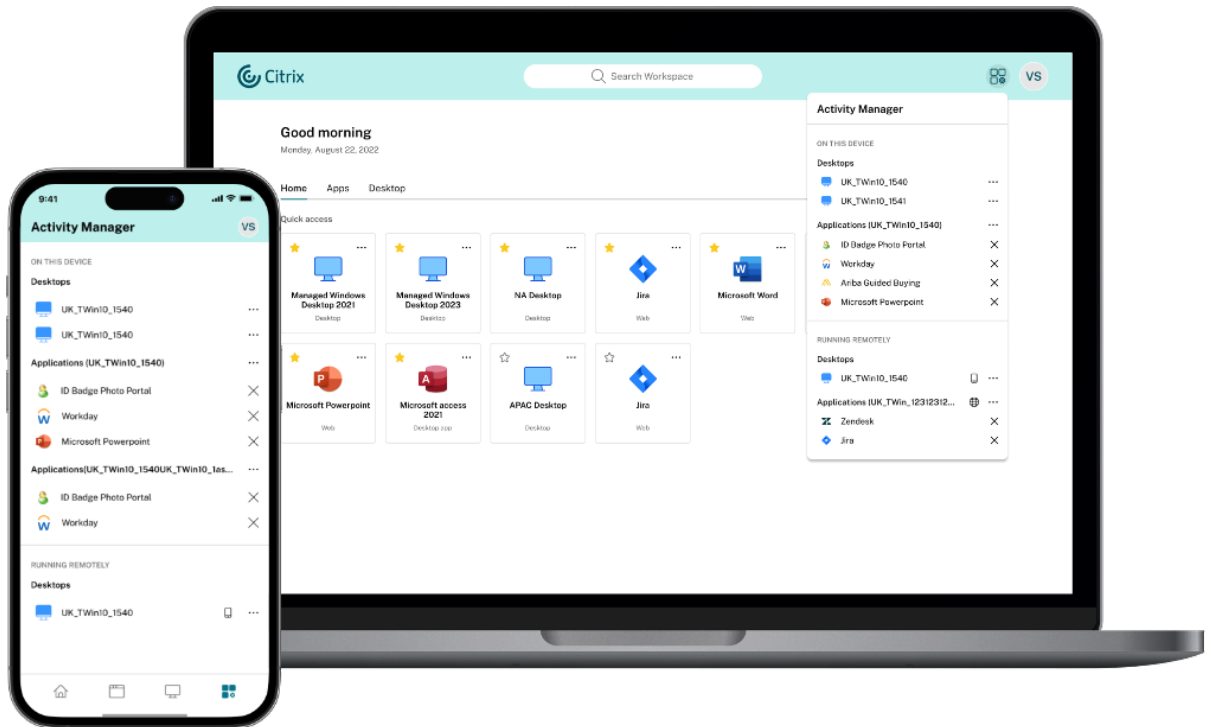
The Unified UI deploys basic search mechanisms that might not be as effective as the search capabilities on the new UI.

Activity Manager

Activity Manager is a simple yet powerful feature in Citrix Workspace that empowers users to effectively manage their resources. It enhances productivity by facilitating quick actions on active apps and desktops from any device. Users can seamlessly interact with their sessions, ending or disconnecting sessions that are no longer required, freeing up resources and optimizing performance.

The Activity Manager panel displays a consolidated list of apps and desktops that are active not only

on the current device but also on any remote device that has active sessions. Users can view this list by clicking the Activity Manager icon located next to the profile icon on the desktop and at the bottom of their screen on mobile devices.



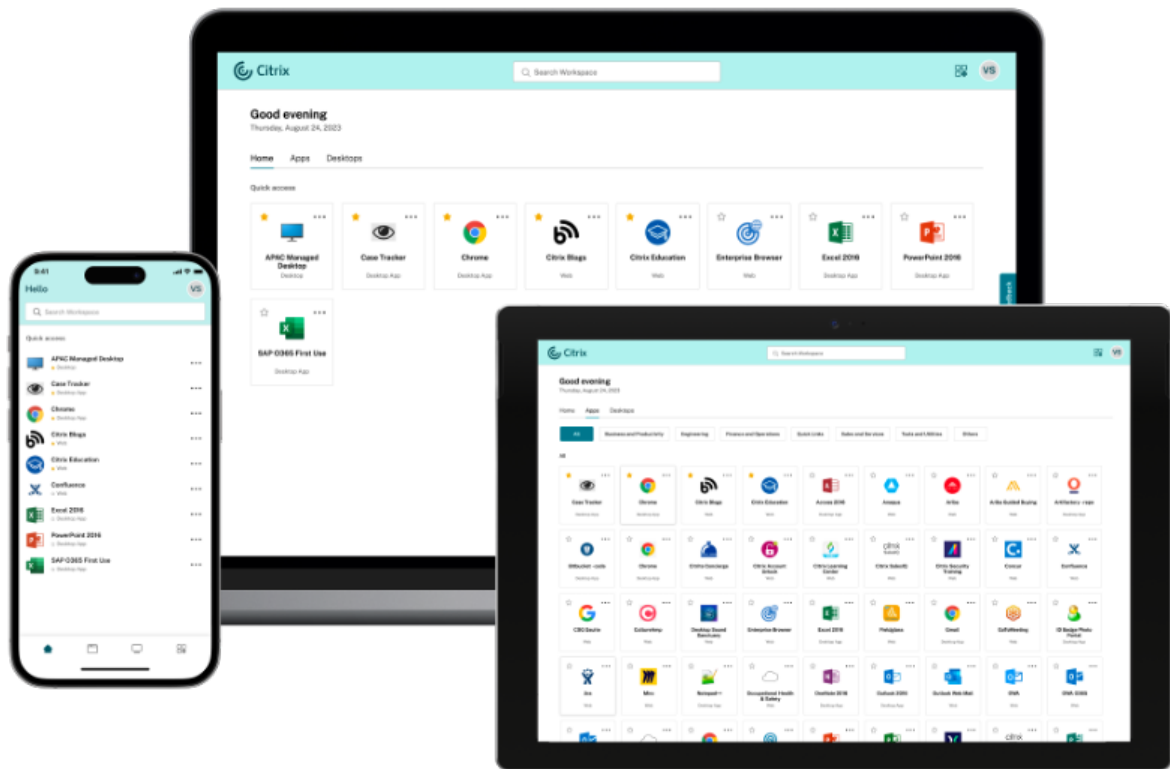
Important:

The Activity Manager feature is available only for stores that have the new UI enabled. It isn't available on the Unified UI experience.

Using Activity Manager

Active apps and desktops are grouped as follows in the Activity Manager panel.

- Apps and desktops that are active on the current device are grouped under **On this device**.
- Apps and desktops that are active on other devices are grouped under **Running Remotely**.

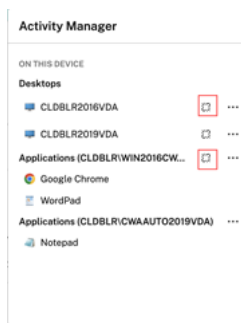


Users can perform the following actions on an app or desktop by clicking the respective ellipsis(...) button.

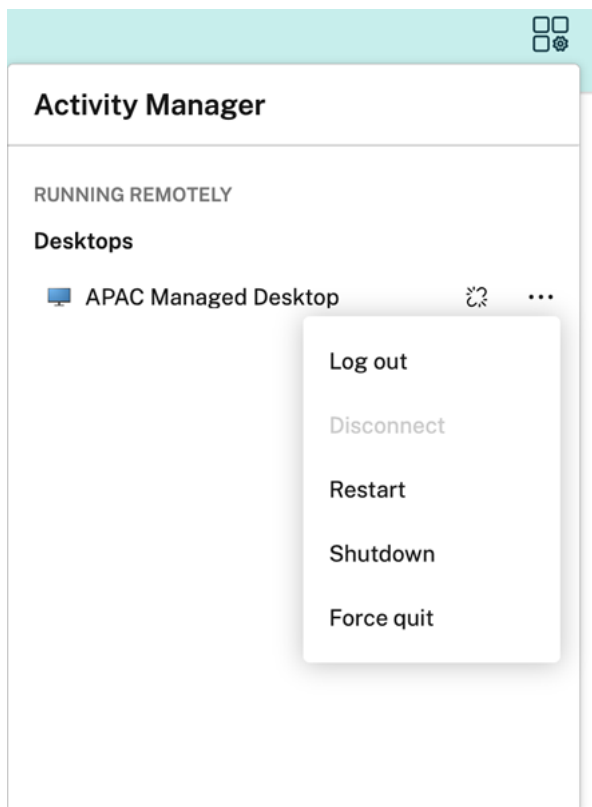
- **Disconnect:** The remote session is disconnected but the apps and desktops are active in the background.
- **Log out:** Logs out from the current session. All the apps in the session are closed, and any unsaved files are lost.
- **Shut Down:** Closes your disconnected desktops.
- **Force Quit:** Powers-off your desktop in case of a technical issue.
- **Restart:** Shuts down your desktop and start it again.

Disconnected apps and desktops

Activity Manager now enables end users to view and take actions on apps and desktops that are running in disconnected mode, locally or remotely. Sessions can be managed from mobile or desktop devices, enabling end users to take action on the go. Taking action on disconnected sessions such as log out or shut down promotes optimized use of resources and reduces energy consumption.



- The disconnected apps and desktops appear on the Activity Manager panel and are indicated by a disconnected icon.
- The disconnected apps are grouped under the respective sessions and the sessions are indicated by a disconnected icon.



End users can take the following actions on their disconnected desktops by clicking the ellipses button:

- **Log out:** use this option to log out from your disconnected desktop. All the apps in the session are closed, and any unsaved files are lost.
- **Shut Down:** use this option to close your disconnected desktops.

- **Power off:** use this option to forcefully power off your disconnected desktops if there's a technical issue.
- **Restart:** use this option to shut down and start the disconnected desktop again.

The behavior of disconnected sessions on Activity Manager differs as follows.

- If you're signed in through a browser, and disconnect from a local session, the session appears first under **On this device**. However, once you close and reopen Activity Manager, the disconnected session is moved under **Running Remotely**.
- If you're signed into a native device, and disconnect from a local session, the disconnected session disappears from the list. However, once you close and reopen Activity Manager again, the disconnected session is moved under **Running Remotely**.

Known Limitations

The new UI has the following limitations. These features are only available in the Unified UI experience.

- The new UI does not support deep customization using the JavaScript and CSS API.
- The new UI does not support embedded URL shortcuts that lead you directly to your app or desktop.
- The Workspace Control feature that lets end users connect back to their sessions from a remote device, is currently not available on the new UI experience.
- The password change functionality is not available on the new UI.
- [Citrix workspace web extensions](#) are not supported. [WSUI-8503]
- Direct SAML authentication is not available by enable when connecting using a web browser. You can use SAML authentication with a Citrix Gateway.

Known issues

- When you change the UI experience for an existing store, users connecting through locally installed Citrix Workspace app aren't updated. They must remove the store and add it back to their app. [WSP-21493]
- Activity Manager operations such as Logout, Disconnect, and more aren't supported for applications that have App Protection policies enabled. [WSP-21324]
- On Citrix Workspace app for iOS, the user's initials aren't displayed on the avatar. [WSUI-8482]
- On Citrix Workspace app for Mac Netscaler stores, the **Back to sign in** option might not work. [RFMAC-15496]
- Citrix Workspace app for iOS Netscaler store, users might be unable to sign in to the new UI if Secure Private Access is enabled with clientless VPN (cVPN) policies. [RFIOS-13733]

Install, set up, upgrade, and uninstall

March 11, 2024

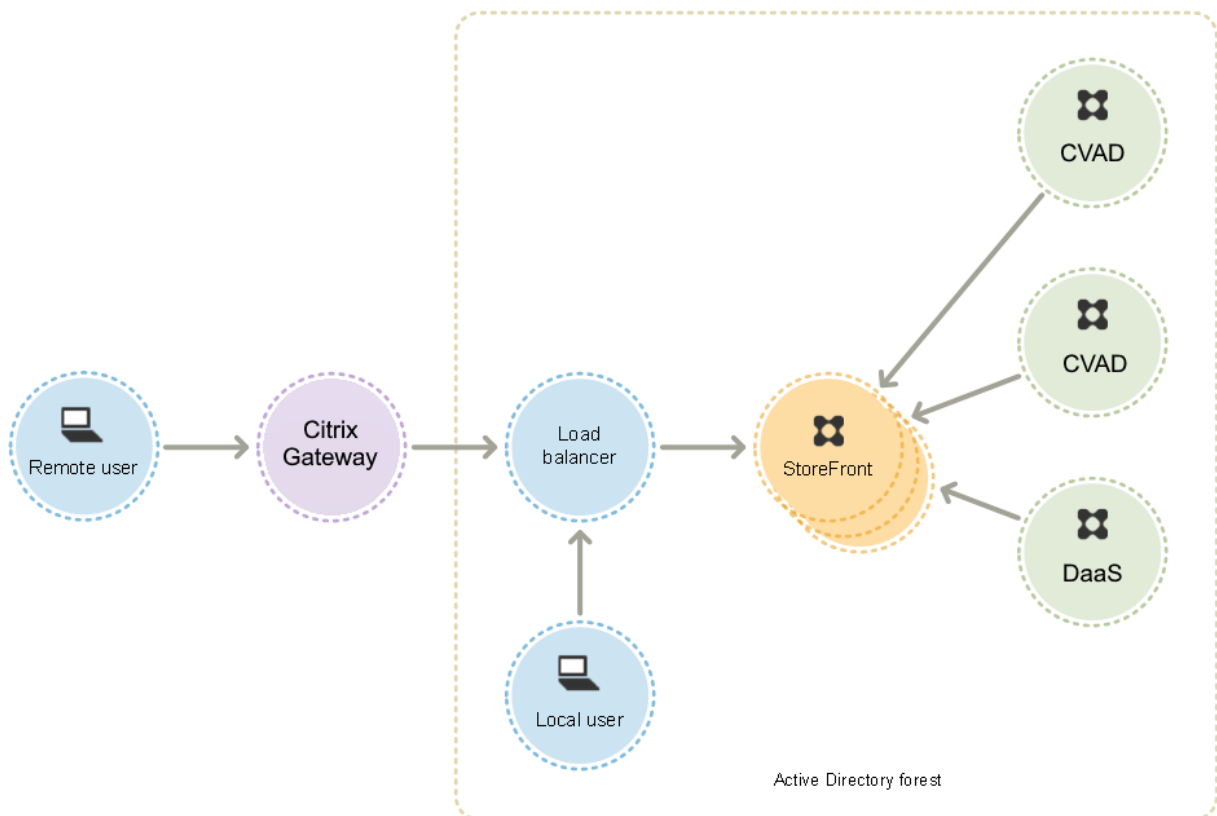
Task	Detail
Plan your StoreFront deployment	An overview of the components involved in a StoreFront deployment
User access options	An overview of the ways users can access your stores
System Requirements	Ensure that you have the pre-requisites to install StoreFront
Install StoreFront	Install StoreFront onto a new server
Secure StoreFront with HTTPS	Encrypt client access to StoreFront using HTTPS
Secure your StoreFront deployment	Configure StoreFront for increased security
Create a new deployment	Configure a new StoreFront server with a new store.
Join an existing server group	Configure a new StoreFront server to join an existing Server Group.
Upgrade StoreFront	Upgrade an StoreFront server running an older version
CEIP	Opt in or out of the Citrix Customer Experience Improvement Program (CEIP)
Citrix Analytics service	Configure StoreFront to send data to the Citrix Analytics Service
Uninstall StoreFront	Remove StoreFront from your server
Reset a server to factory defaults	Clear all StoreFront settings so that it can be re-configured.

Plan your StoreFront deployment

April 9, 2024

StoreFront integrates with your Citrix Virtual Apps and Desktops deployments, providing users with a single, self-service access point for their desktops and applications.

The figure shows a typical StoreFront deployment.



Active Directory

StoreFront uses Active Directory for authenticating users and looking up group membership and other details and for synchronizing data between StoreFront servers.

For single server deployments you can install StoreFront on a non-domain-joined server but certain functionality will be unavailable; otherwise, StoreFront servers must reside either within the Active Directory domain containing your users' accounts or within a domain that has a trust relationship with the user accounts domain unless you enable delegation of authentication to the Citrix Virtual Apps and Desktops sites or farms. All the StoreFront servers in a group must reside within the same domain.

StoreFront Server groups

StoreFront can be configured either on a single server or as a multiple server deployment called a StoreFront server group. Server groups not only provide additional capacity, but also greater availability. StoreFront ensures that configuration information and details of users' application subscriptions are stored on and replicated between all the servers in a server group. This means that if a

StoreFront server becomes unavailable for any reason, users can continue to access their stores using the remaining servers. Meanwhile, the configuration and subscription data on the failed server are automatically updated when it reconnects to the server group. Subscription data is updated when the server comes back online but you must propagate configuration changes if any were missed by the server while offline. In the event of a hardware failure that requires replacement of the server, you can install StoreFront on a new server and add it to the existing server group. The new server is automatically configured and updated with users' application subscriptions when it joins the server group.

Citrix recommends a maximum of six servers in a server group. In case of more than six servers, the overhead of synchronizing data outweighs the benefit of the additional servers, and the performance is degraded.

StoreFront server group deployments are only supported where links between servers in a server group have latency of less than 40 ms (with subscriptions disabled) or less than 3 ms (with subscriptions enabled). Ideally, all servers in a server group should reside in the same location (data center, availability zone), but server groups can span locations within the same region provided that links between servers in the group meet these latency criteria. Examples include server groups spanning availability zones within a cloud region, or between metropolitan area data centers. Note that latency between zones varies by cloud provider. Citrix do not recommend spanning locations as a disaster recovery configuration, but it may be suitable for high availability.

Load balancing

For multiple servers in a StoreFront server group, you must configure external load balancing. Use a load balancer with built-in monitors and session persistency, such as NetScaler ADC. For more information about load balancing with NetScaler ADC, see [Load Balancing](#).

Citrix Gateway for remote access

If you plan to enable access to StoreFront from outside the corporate network, a Citrix Gateway is required to provide secure connections for remote users. Deploy Citrix Gateway outside the corporate network, with firewalls separating Citrix Gateway from both the public and internal networks. Ensure that Citrix Gateway is able to access the Active Directory forest containing the StoreFront servers.

Global Server Load Balancer

In large Citrix deployments you may have StoreFront and NetScaler deployments in multiple data centers. Using a Global Server Load Balancer (GSLB) you can configure a single global URL which the GSLB

redirects to the specific URL of a gateway in one of the regions. Typically the GSLB chooses the closest gateway based on a load balancing algorithm such as round trip time (RTT) or Static Proximity.

For example you may have 3 regional gateways:

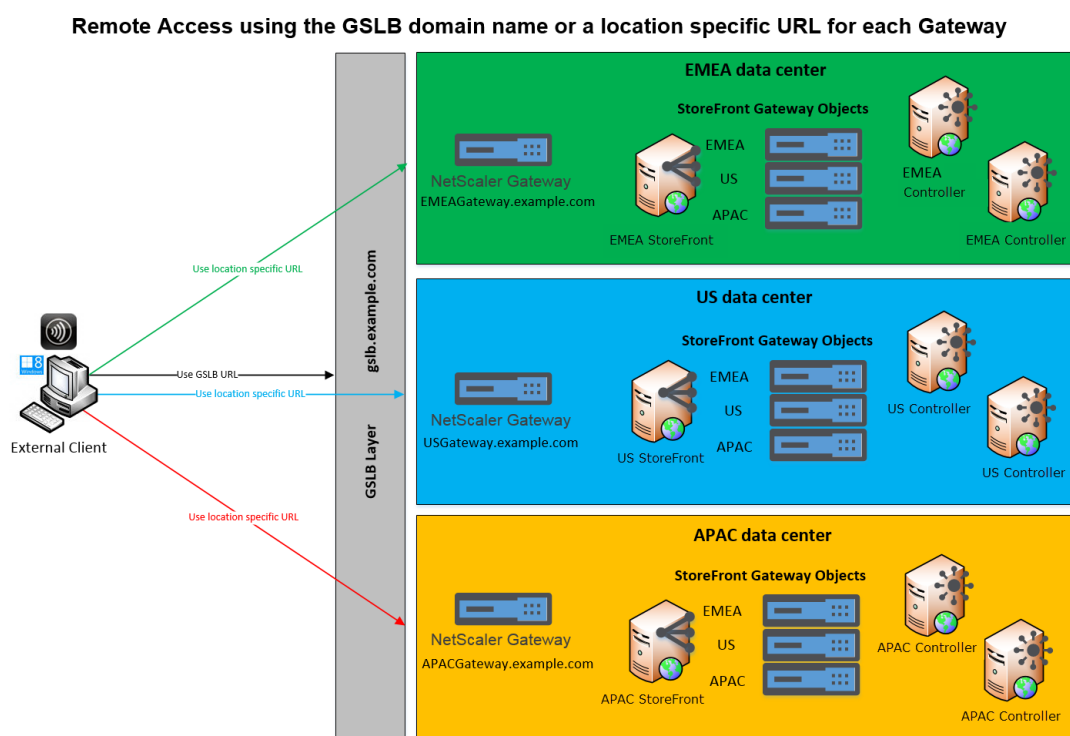
`emeagateway.example.com` - Europe gateway

`usgateway.example.com` - US gateway

`apacgateway.example.com` - Asia Pacific gateway

Along with a GSLB

`gslb.example.com`



Before configuring a GSLB, review what server certificates you have in place and how your organization performs DNS resolution. Any URLs that you want to use in your Citrix Gateway and StoreFront deployment must be present in your server certificates.

StoreFront does not have any built-in mechanism to synchronize configuration between server groups; instead it is up to the administrator to configure that each StoreFront Server Group is configured in the same way so the users get a consistent experience whichever server group they connect to.

StoreFront can periodically synchronize subscriptions (favorites) between server groups, see [Subscription synchronization](#).

User access

See [User access options](#).

User access options

April 26, 2024

Three different methods are available for users to access StoreFront stores.

- Citrix Workspace app installed locally - Users with compatible versions of Citrix Workspace app can access StoreFront stores within the Citrix Workspace app user interface. This provides the best user experience and the greatest functionality.
- Citrix Workspace app for HTML5 - Users with compatible web browsers can access StoreFront stores by browsing to the store's website. By default, users also require a compatible version of Citrix Workspace app to access their desktops and applications, known as hybrid launch. However, you can configure your website to enable users to access their resources through their browser without installing Citrix Workspace app.
- XenApp Services URLs - Users who have legacy Citrix clients that cannot be upgraded, can access stores using the XenApp Services URL for the store. When you create a new store, the XenApp Services URL is enabled by default.

Citrix Workspace app installed locally

Accessing stores from the locally installed [Citrix Workspace app](#) provides the best user experience. For the Citrix Workspace app versions that can be used to access stores in this way, see [System Requirements](#).

Citrix Workspace app uses internal and external URLs as beacon points. By attempting to contact these beacon points, Citrix Workspace app can determine whether users are connected to local or public networks. When a user accesses a desktop or application, the location information is passed to the server providing the resource so that appropriate connection details can be returned to Citrix Workspace app. This enables Citrix Workspace app to ensure that users are not prompted to log on again when they access a desktop or application. For more information, see [Configure beacon points](#).

Add Store to Workspace App

After installation, Citrix Workspace app must be configured with connection details for the stores providing users' desktops and applications. You can make the configuration process easier for your users

by providing them with the required information in one of the following ways.

Important:

By default, Citrix Workspace app requires HTTPS connections to stores. If StoreFront is not configured for HTTPS, users must carry out additional configuration steps to use HTTP connections. Citrix strongly recommends that you do not enable unsecured user connections to StoreFront in a production environment. For more information, see [Store configuration parameters](#) in the Citrix Workspace app for Windows documentation.

Manual configuration Users can connect Citrix Workspace app to their store by entering the store URLs into Citrix Workspace app. For more information, see the Citrix Workspace app documentation.

Provisioning files You can provide users with provisioning files containing connection details for their stores. After installing Citrix Workspace app, users open the .cr file to automatically configure accounts for the stores. By default, the website offers users a provisioning file for the single store for which the site is configured. You could instruct your users to visit the websites for the stores they want to access and download provisioning files from those sites. Alternatively, for a greater level of control, you can use the Citrix StoreFront management console to generate provisioning files containing connection details for one or more stores. You can then distribute these files to the appropriate users. For more information, see [Export store provisioning files for users](#).

Auto-generated setup URLs For users running macOS, you can use the Citrix Workspace app for Mac Setup URL Generator to create a URL containing connection details for a store. After installing Citrix Workspace app, users click on the URL to configure an account for the store automatically. Enter details of your deployment into the tool and generate a URL that you can distribute to your users.

Email-based account discovery With email-based account discovery, instead of needing to know the access details for their stores, users enter their email addresses during the Citrix Workspace app initial configuration process. For details of how to set this up see [Email based account discovery](#).

Global App Config Service

Use the Global App Config Service to configure Citrix Workspace app for your StoreFront stores. See [Configure settings for on-premises stores](#).

Citrix Workspace app for HTML5

As an alternative to using a locally installed Workspace app, users can access their store through a web browser with Workspace app for HTML5. When users come to launch their resources there are two possibilities.

1. Resources launch within locally installed Citrix Workspace app. This is known as a hybrid launch. This gives users the best experience as it can take advantage of full operating system integration. For more details see [Hybrid launch](#)
2. Resources launch within the browser. This makes it possible for users to access resources without needing to install any software locally.

The default configuration is to require that Citrix Workspace app is installed locally for a hybrid launch. You can change the configuration to either always launch resources in the browser or to give the user the choice. See [Deploy Workspace app](#).

If the admin selected **Use Receiver for HTML5 if local Receiver is unavailable** then when the user first opens the store website in their browser, the user has the option to click **Use Light Version** to launch resources within their web browser.

Requirements for opening resources in your browser

For users on the internal network, access through Citrix Workspace app for HTML5 to resources provided by Citrix Virtual Apps and Desktops is disabled by default. To enable local access to desktops and applications using Citrix Workspace app for HTML5, enable the ICA WebSockets connections policy on your Citrix Virtual Apps and Desktops servers. Citrix Virtual Apps and Desktops uses port 8008 for Citrix Workspace app for HTML5 connections. Ensure your firewalls and other network devices permit access to this port. For more information, see [WebSockets policy settings](#).

For Citrix Virtual Apps and Desktops resource launches to succeed, configure the TLS connections to the VDAs that host apps and desktops. Remote connections through a Citrix Gateway can launch resources using Citrix Workspace app for HTML5 without configuring TLS connections to the VDA.

Hybrid Launch

When users first open Citrix Workspace for HTML5 through their browser but launch apps within the locally installed Citrix Workspace app this is known as hybrid launch. There are a number of ways in which the web site can communicate with the locally installed Workspace app to launch resources.

Citrix Workspace launcher

When the user first goes to a StoreFront web site with a supported operating system and browser, Citrix Workspace app for HTML5 attempts to invoke the Citrix Workspace Launcher. If a supported version of Citrix Workspace app is installed then the app notifies StoreFront. Citrix Workspace app for HTML5 remembers this and when it launches an app it uses Citrix Workspace Launcher.

The store web site invokes Citrix Workspace Launcher on Windows, Mac and Linux with when using the following browsers:

- Firefox 52 or higher
- Chrome 42 or higher
- Safari 12 or higher
- Edge 25 or higher

Citrix Workspace Launcher requires the following minimum versions of Citrix Receiver or Citrix Workspace app.

- Receiver for Windows 4.3 or higher
- Receiver for Mac 12.0 or higher
- Workspace app for Linux 2003 or higher

If the Workspace app launcher is not available, or the user does not allow it to open, then it will not be able to detect the locally installed Citrix workspace app. The user has the option to try again, or to click **Already Installed**, in which case it falls back to launching apps using .ica files. The user can later try again by going to the Settings screen and clicking **Change Citrix Workspace app**.

If you are using multiple active StoreFront server groups behind a global server load balancer then Citrix Workspace launcher may fail intermittently. To avoid this you must configure your global server load balancer to force the user web session to be persistent to one StoreFront server group for the lifetime of the client detection process, see [CTX460312](#). Alternatively deploy Citrix Workspace web extensions.

When connecting to the website via a Citrix Gateway The Citrix Workspace launcher uses the gateway's HDX routing to proxy requests from Citrix Workspace app back to the StoreFront server. If the gateway is configured for **Authentication only** (not HDX routing) then Citrix Workspace Launcher does not work. Either enable HDX routing or deploy Citrix Workspace web extensions.

Citrix Workspace web extensions

The [Citrix Workspace web extensions](#) are extensions for commonly used web browsers that improve the user experience for detecting the locally installed Citrix Workspace app and launching virtual apps and desktops. Compared to Citrix Workspace launcher, this provides a better user experience and avoids issues with global server load balancers.

To enable the browser extension-based client detection:

- Enable the feature on the StoreFront server.
- Deploy the browser extension on the client devices.
- Deploy Citrix Workspace app for Windows 2303, Mac 2304 or Linux 2302 or higher.

The first time a user goes to a store website on a supported platform, it prompts the user to detect the locally installed Workspace app. It first tries to use the web extension and if this fails then it tries Citrix Workspace Launcher. Existing users who have already completed Workspace app detection can go to **Account Settings**, click **Change Citrix Workspace app** to re-detect workspace app.

Important

This feature is enabled by default for new installations. However, if you are upgrading from a previous version, you need to enable this feature manually. Administrators can enable this feature using the following PowerShell script on a StoreFront server: `Add-STFFeatureState -Name "Citrix.StoreFront.EnableBrowserExtension"-IsEnabled $True`.

Internet Explorer

The first time the user opens the store web site in Internet Explorer, it prompts the user to install Citrix Workspace app which includes the Citrix ICA Client Add-on for Internet Explorer. Once the plugin is installed, this is used to launch apps and desktops through the locally installed Citrix Workspace app.

ICA file downloads

If Citrix Workspace app for HTML5 is unable to detect a locally installed Citrix Workspace app by any other means then when a user launches an app or desktop then it downloads a .ica file. The user can open this file with the locally installed Citrix Workspace app.

Resource shortcuts

You can generate URLs that provide access to desktops and applications available in your store. Embed these links on websites hosted on the internal network to provide users with rapid access to resources. Users click on a link and are redirected to the store website, where they log on if they have not already done so. The store website automatically starts the resource. For more information about generating resource shortcuts, see [Website shortcuts](#).

When you create an application shortcut, ensure that no other applications available from the store have the same name. Shortcuts cannot distinguish between multiple instances of an application with

the same name. Similarly, if you make multiple instances of a desktop from a single desktop group available from the store, you cannot create separate shortcuts for each instance. Shortcuts cannot pass command-line parameters to applications.

To create application shortcuts, you configure StoreFront with the URLs of the internal websites that will host the shortcuts. When a user clicks on an application shortcut on a website, StoreFront checks that website against the list of URLs you entered to ensure that the request originates from a trusted website.

Customize the user interface

Citrix StoreFront provides a mechanism for customizing the user interface. These apply whether accessing a store through Citrix Workspace app or a web browser. You can customize strings, the cascading style sheet, and the JavaScript files. You can also add a custom pre-logout or post-logout screen, and add language packs. For more information see [Customize Appearance](#).

XenApp Services URLs

Note:

XenApp Services (also known as PNAgent) is deprecated. It is recommended that you use Citrix Workspace app to connect to StoreFront using a Store URL.

Users with older Citrix clients that cannot be upgraded can access stores by configuring their clients with the XenApp Services URL for a store. You can also enable access to your stores through XenApp Services URLs from domain-joined desktop appliances and repurposed PCs running the Citrix Desktop Lock. Domain-joined in this context means devices that are joined to a domain within the Microsoft Active Directory forest containing the StoreFront servers.

StoreFront supports pass-through authentication with proximity cards through Citrix Workspace app to XenApp Services URLs. Citrix Ready partner products use the Citrix Fast Connect API to streamline user logons through Citrix Receiver for Windows or Citrix Workspace app for Windows to connect to stores using the XenApp Services URL. Users authenticate to workstations using proximity cards and are rapidly connected to desktops and applications provided by Citrix Virtual Apps and Desktops. For more information, see the most recent [Citrix Workspace for Windows](#) documentation.

When you create a new store, the XenApp Services URL for the store is enabled by default. The XenApp Services URL for a store has the form `http[s]://serveraddress/Citrix/storename/PNAgent/config.xml`, where `serveraddress` is the fully qualified domain name of the server or load balancing environment for your StoreFront deployment and `storename` is the name specified for the store when it was created. This allows Citrix Workspace apps that can only use the PNAgent protocol to connect to StoreFront. For the clients that can be used to access stores through XenApp Services URLs, see [User device requirements](#).

Important considerations

XenApp Services URLs are intended to support users who cannot upgrade to Citrix Workspace app and for scenarios where alternative access methods are not available. When you decide whether to use XenApp Services URLs to provide users with access to your stores, consider the following restrictions.

- You cannot modify the XenApp Services URL for a store.
- You cannot modify XenApp Services URL settings by editing the configuration file, config.xml.
- XenApp Services URLs support explicit, domain pass-through, smart card authentication, and pass-through with smart card authentication. Explicit authentication is enabled by default. Only one authentication method can be configured for each XenApp Services URL and only one URL is available per store. If you need to enable multiple authentication methods, you must create separate stores, each with a XenApp Services URL, for each authentication method. Your users must then connect to the appropriate store for their method of authentication. For more information, see [XML-based authentication](#).
- Workspace control is enabled by default for XenApp Services URLs and cannot be configured or disabled.
- User requests to change their passwords are routed to the domain controller directly through the Citrix Virtual Apps and Desktops servers providing desktops and applications for the store, bypassing the StoreFront authentication service.

System requirements

April 11, 2024

Before you install StoreFront, review [Plan your StoreFront deployment](#).

StoreFront server requirements

Software

Citrix has tested and provides support for StoreFront installations on the following platforms:

- Windows Server 2022 Datacenter and Standard editions
- Windows Server 2019 Datacenter and Standard editions
- Windows Server 2016 Datacenter and Standard editions

Note:

StoreFront requires the Windows desktop experience so cannot be installed on Windows Server

Core.

All StoreFront servers in a server group must use the same operating system version, language and locale.

Upgrading the operating system version on a server running StoreFront is not supported. Citrix recommends that you install StoreFront on a new installation of the operating system.

Before you can install StoreFront, the following Windows features must be enabled on the web server. These components are enabled by default on a new Windows installation so no action is required unless they have been explicitly uninstalled.

- NET-Framework-45-Features
 - NET-Framework-45-Core
- PowerShellRoot
 - PowerShell

If the version of .NET Framework installed is older than 4.7.2 then the installer automatically installs .NET Framework 4.7.2. Note this requires that the NET-Framework-45-Core Windows feature is already installed.

If the StoreFront installer detects that any of the following Windows features are missing, they are automatically installed:

- Web-Server
 - Web-WebServer
 - ★ Web-Common-Http
 - Web-Default-Doc
 - Web-Http-Errors
 - Web-Static-Content
 - Web-Http-Redirect
 - ★ Web-Health
 - Web-Http-Logging
 - ★ Web-Security
 - Web-Filtering
 - Web-Basic-Auth
 - Web-Windows-Auth
 - ★ Web-App-Dev
 - Web-Net-Ext45
 - Web-AppInit

- Web-Asp-Net45
 - Web-ISAPI-Ext
 - Web-ISAPI-Filter
 - ★ Web-Mgmt-Tools
 - Web-Mgmt-Console
 - ★ Web-Scripting-Tools
- NET-Framework-45-Features
 - NET-Framework-45-ASPNET
 - NET-WCF-Services45
 - ★ NET-WCF-TCP-PortSharing45

It is possible to move the IIS website to a different directory or drive before installing StoreFront. The relative path to StoreFront in IIS must be the same on all the servers in a server group.

Hardware

Storefront servers must meet the following requirements:

- Processor: Minimum 2 virtual CPUs, recommended 4 virtual CPUs
- RAM: 4GB, plus 700 bytes per resource available, per user.
- Storage:
 - 250MB for StoreFront itself.
 - 30MB for each store, assuming one website per store.
 - For each store with favorites enabled, 5MB plus 8MB for each 1000 favorites.
 - Sufficient space for IIS log files according to your requirements, see [Microsoft documentation on Managing IIS Log File Storage](#).
 - Sufficient space for StoreFront diagnostics logs. By default StoreFront keeps 1GB of logs per service. A StoreFront deployment typically has 1 roaming service plus 3 services per store (store service, auth service and receiver for web service). See [Troubleshoot storefront](#).

Network

StoreFront uses the following ports for communication. Ensure your firewalls and other network devices permit access to these ports.

- TCP ports 80 and 443 are used by clients to connect to StoreFront using HTTP and HTTPS communications, respectively.

- TCP port 808 is used for communications between StoreFront servers within a server group.
- A TCP port randomly selected from all unreserved ports is used for communications between the StoreFront servers in a server group. When you install StoreFront, a Windows Firewall rule is configured enabling access to the StoreFront executable. However, since the port is assigned randomly, you must ensure that any firewalls or other devices on your internal network do not block traffic to any of the unassigned TCP ports.
- TCP port 8008 is used by Citrix Workspace app for HTML5, or supported versions of Citrix Workspace app, where enabled, for communications from local users on the internal network to the servers providing their desktops and applications.

StoreFront supports both pure IPv6 networks and dual-stack IPv4/IPv6 environments.

Active directory

Many StoreFront features require the Windows server on which StoreFront is installed to be joined to an Active Directory domain.

If you install StoreFront on a non-domain-joined server then the following features are not available:

- Server groups
- Favorites
- Authentication methods other than explicit username and password, either directly to StoreFront or via a Gateway. You must configure StoreFront to delegate authentication to the delivery controller.

Storing subscription data using Microsoft SQL Server

You can optionally [Store subscription data using Microsoft SQL Server](#). StoreFront supports same Microsoft SQL Server versions for this as Citrix Virtual Apps and Desktops does for databases. In Citrix Virtual Apps and Desktops system requirements, see [Databases](#).

Infrastructure requirements

Citrix has tested and provides support for StoreFront when used with the following Citrix product versions.

Citrix Virtual Apps and Desktops

StoreFront supports the following versions of Citrix Virtual Apps and Desktops:

- Citrix Virtual Apps and Desktops 2402 LTSR
- Citrix Virtual Apps and Desktops 2311
- Citrix Virtual Apps and Desktops 2308
- Citrix Virtual Apps and Desktops 2305
- Citrix Virtual Apps and Desktops 2203 LTSR
- Citrix Virtual Apps and Desktops 1912 LTSR

Citrix Gateway

The following versions of Citrix Gateway can be used to provide access to StoreFront for users on public networks.

- Citrix Gateway 14.1
- Citrix Gateway 13.1
- Citrix Gateway 13.0

Connections through Citrix Gateway can be made using the ICA proxy, Citrix Gateway plug-in, or clientless VPN (cVPN).

User device requirements

StoreFront provides various options for users to access their desktops and applications. Citrix users can either access stores through locally installed Citrix Workspace app, or use Citrix Workspace app for HTML5 within their browser.

Locally installed Citrix Workspace app

You can use all currently supported versions of Citrix Workspace app to access StoreFront stores from both internal network connections and through a Citrix Gateway. For Citrix Workspace app lifecycle dates, see <https://www.citrix.com/support/product-lifecycle/workspace-app.html>.

Citrix Workspace app for HTML5 in a web browser

You can use Citrix Workspace app for HTML5 to access your store using a web browser. Apps and desktops can be launched either via a natively installed Citrix Workspace app (known as hybrid launch), or within the web browser. Depending on your website configuration, it is possible for end users to switch between the two launch methods.

Use latest versions of the following browsers.

On Windows:

- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Internet Explorer 11 - only for browsing the store, not for connecting to resources.

On Mac:

- Safari
- Google Chrome
- Mozilla Firefox

On Linux:

- Google Chrome
- Mozilla Firefox

For further information on requirements for using Citrix Workspace app for HTML5 to connect to resources through a web browser see [Citrix Workspace app for HTML5 documentation](#).

Legacy devices

Legacy Citrix clients can use XenApp Services URLs to access StoreFront stores with reduced functionality. XenApp Services URLs provide backward compatible legacy support for connections made by Citrix Receiver 3.4 Enterprise and older clients. This functionality is deprecated and will be removed from a future release.

Smart card requirements

Using Citrix Workspace app with smart cards

Citrix tests for compatibility with the U.S. Government Dept. Of Defense Common Access Card (CAC), U.S. National Institute of Standards and Technology Personal Identity Verification (NIST PIV) cards, and some USB smart card tokens. You can use contact card readers that comply with the USB Chip/Smart Card Interface Devices (CCID) specification and are classified by the German Zentraler Kreditausschuss (ZKA) as Class 1 smart card readers. ZKA Class 1 contact card readers require that users insert their smart cards into the reader. Other types of smart card readers, including Class 2 readers (which have keypads for entering PINs), contactless readers, and virtual smart cards based on Trusted Platform Module (TPM) chips, are not supported.

For Windows devices, smart card support is based on Microsoft Personal Computer/Smart Card (PC/SC) standard specifications. As a minimum requirement, smart cards and card readers must be supported by the operating system and have received Windows Hardware Certification.

For more information about Citrix-compatible smart cards and middleware, see [Smart cards](#) in the Citrix Virtual Apps and Desktops documentation, and <http://www.citrix.com/ready>.

Citrix Analytics service requirements

You can configure Citrix StoreFront so that Citrix Workspace app can send data to the Citrix Analytics service. Configuration details are described in [Citrix Analytics service](#). This functionality is supported for the following scenarios:

- Stores which are accessed by web browsers.
- Stores which are accessed from Citrix Workspace app 1903 for Windows or later.
- Stores which are accessed from Citrix Workspace app 1901 for Linux or later.

Install StoreFront

March 11, 2024

Before installing and configuring

To install and configure StoreFront, complete the following steps in order:

1. Review the [System Requirements](#).
2. If you plan to use StoreFront to deliver Citrix Virtual Apps and Desktops resources to users, ensure that the StoreFront server is joined to either the Microsoft Active Directory domain containing your users' accounts or a domain that has a trust relationship with the user accounts domain.

Important:

- For single server deployments you can install StoreFront on a non-domain-joined server.
- StoreFront cannot be installed on a domain controller.

3. Optionally, if you plan to configure a multiple server StoreFront deployment, set up a load balancing environment for your StoreFront servers.

To use NetScaler ADC for load balancing, you define a virtual server to proxy your StoreFront servers. For more information on configuring NetScaler ADC for load balancing, see [Load balancing with NetScaler ADC](#).

4. Ensure your firewalls and other network devices permit access to TCP port 80 or 443, as appropriate, from both inside and outside the corporate network. In addition, ensure that any firewalls or other devices on your internal network do not block traffic to any of the unassigned TCP ports.

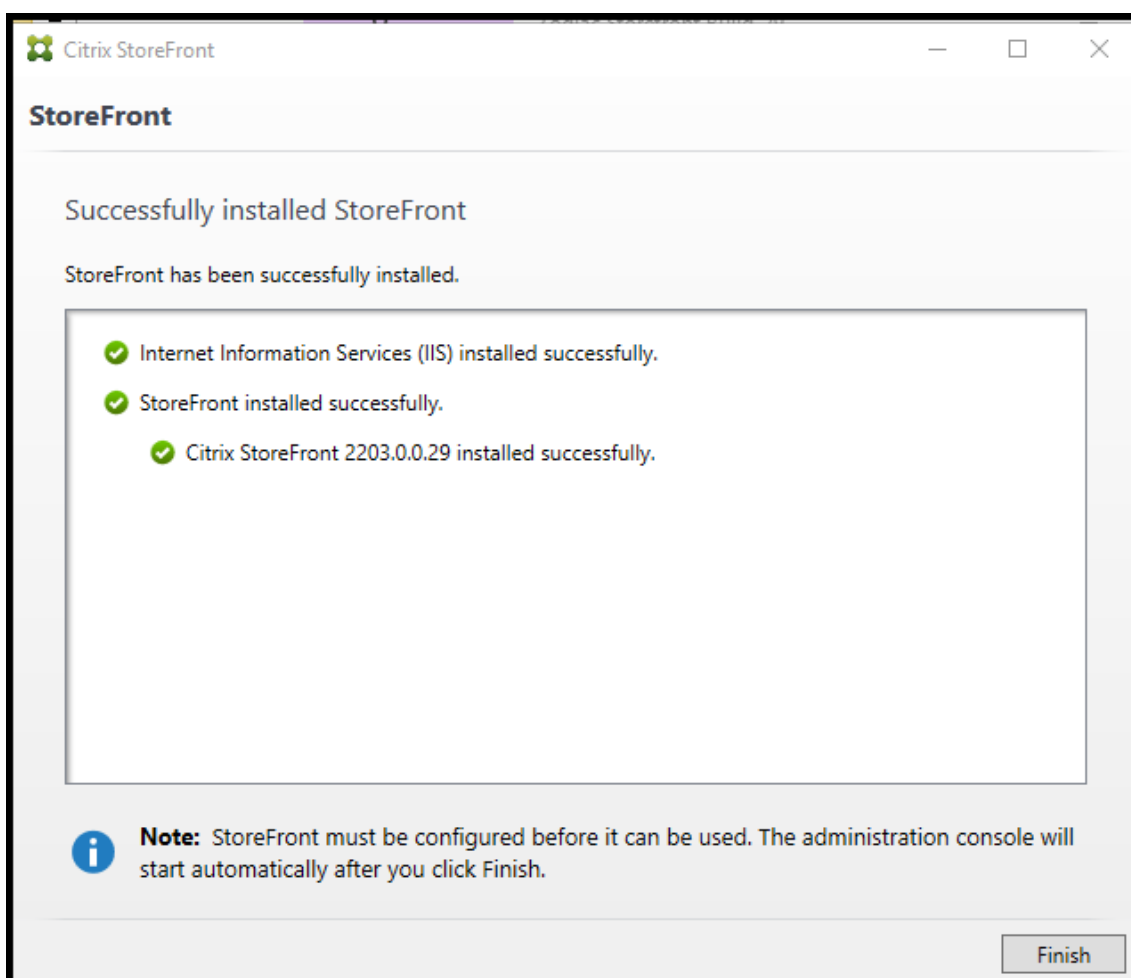
When you install StoreFront, a Windows Firewall rule is configured enabling access to the StoreFront executable through a TCP port randomly selected from all unreserved ports. This port is used for communications between the StoreFront servers in a server group.

Install StoreFront

Important

To avoid potential errors and data loss when installing StoreFront, ensure all applications are closed and no other tasks or operations are running on the target system.

1. Download the installer from the download page.
2. Log on to the StoreFront server using an account with local administrator permissions.
3. Locate CitrixStoreFront-x64.exe, and run the file as an administrator.
4. Read and accept the license agreement, and click **Next**.
5. If the Review prerequisites page appears, click **Next**.
6. On the Ready to install page, check the prerequisites and StoreFront components that are listed for installation and click **Install**.
7. When the installation is complete, click **Finish**.



8. StoreFront may ask to reboot to complete the installation. Click **Yes** to reboot now.
9. Configure Microsoft Internet Information Services (IIS) for HTTPS. For steps see [Securing StoreFront with HTTPS](#).

To install StoreFront at a command prompt

1. Log on to the StoreFront server using an account with local administrator permissions.
2. Ensure that the requirements for installation of StoreFront are met before installing StoreFront. Refer to [Before installing and configuring](#) for details.
3. Browse your installation media or download package, locate CitrixStoreFront-x64.exe, and copy the file to a temporary location on the server.
4. At a command prompt, navigate to the folder containing the installation file and type the following command.

```
1 CitrixStoreFront-x64.exe [-silent] [-INSTALLDIR  
    installationlocation] [-WINDOWS_CLIENT filelocation\filename.  
    exe] [-MAC_CLIENT filelocation\filename.dmg]  
2 <!--NeedCopy-->
```

Use the **-silent** argument to silently install StoreFront and its prerequisites. By default, StoreFront is installed at C:\Program Files\Citrix\Receiver StoreFront. However, you can specify a different installation location using the **-INSTALLDIR** argument, where *installationlocation* is the directory in which to install StoreFront. If you intend the server to be part of a server group, both the StoreFront installation location and IIS website settings, physical path and site IDs must be consistent across them.

When a user opens a store in a web browser on Windows or macOS, by default, if it cannot detect Citrix Workspace app, it prompts the user to download and install the appropriate Citrix Workspace app for their platform from the Citrix website. You can modify this behavior so that users download the Citrix Workspace app installation files from the StoreFront server instead. For more information, see [Configure how resources are displayed for users](#).

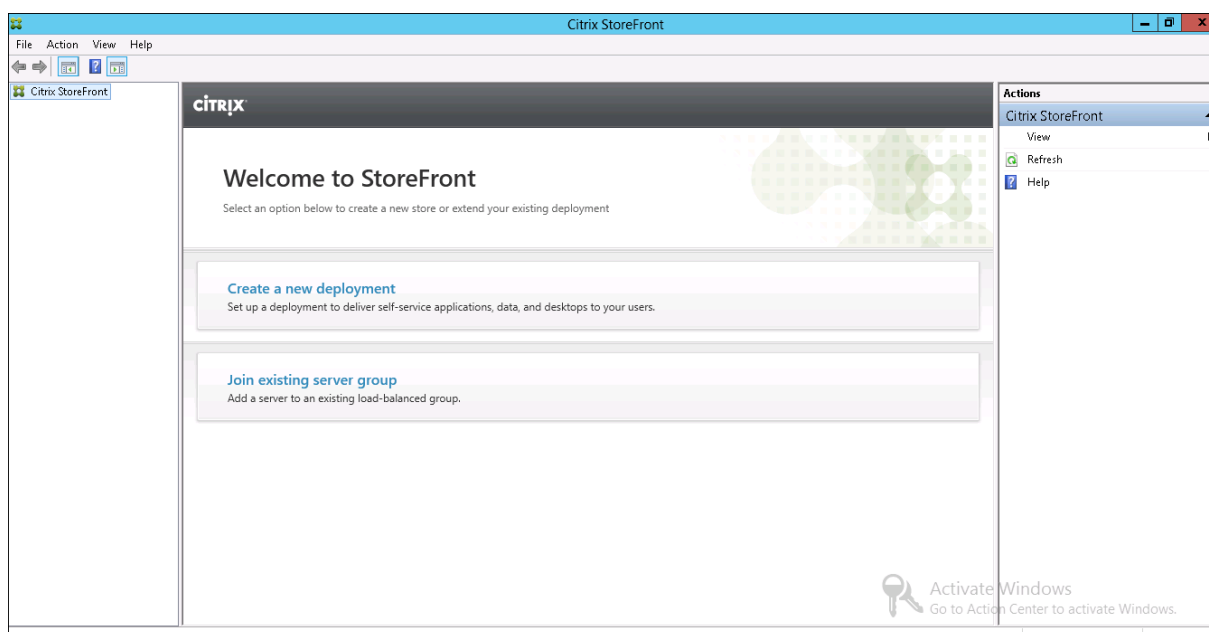
If you plan to make this configuration change, specify the **-WINDOWS_CLIENT** and **-MAC_CLIENT** arguments to copy Citrix Receiver for Windows or Citrix Workspace app for Windows, and Citrix Receiver for Mac or Citrix Workspace app for Mac installation files, respectively, to the appropriate location in your StoreFront deployment. Replace *filelocation* with the directory containing the installation file that you want to copy, and *filename* with the name of the installation file. Citrix Workspace app for Windows, and Citrix Receiver for Mac or Citrix Workspace app for Mac installation files are included on your Citrix Virtual Apps and Desktops installation media.

Installation logs

For more details of logs files, see [Installation Logs](#).

Configure StoreFront

When you complete installation, the Citrix StoreFront management console starts automatically. You can also open StoreFront from the Start menu. When the Citrix StoreFront management console first starts, two options are available.



- [Create a deployment](#). Configure the first server in a new StoreFront deployment. Single-server deployments are ideal for evaluating StoreFront or for small production deployments. Once you have configured your first StoreFront server, you can add more servers to the group at any time to increase the capacity of your deployment.
- [Join existing server group](#). Add another server to an existing StoreFront deployment. Select this option to rapidly increase the capacity of your StoreFront deployment. External load balancing is required for multiple server deployments. To add a server, you need access to an existing server in the deployment.

Your store is now available for users to access through a browser or Citrix Workspace app. See the [User guide](#).

Citrix Customer Experience Improvement Program

February 27, 2024

If you participate in the Citrix Customer Experience Improvement Program (CEIP), anonymous statistics and usage information are sent to Citrix to improve the quality and performance of Citrix products.

By default, you are automatically enrolled in CEIP when you install StoreFront. The first upload of data occurs approximately seven days after you install StoreFront. You can change this default in a registry setting. If you change the registry setting before installing StoreFront, that value is used. If you change the registry setting before upgrading StoreFront, that value is used.

Warning:

Editing the registry incorrectly can cause serious problems that may require you to reinstall your operating system. Citrix cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Use Registry Editor at your own risk. Be sure to back up the registry before you edit it.

Registry setting that controls automatic upload of analytics (default = 1):

```
1 Location: HKLM:\Software\Citrix\Telemetry\CEIP
2 Name: Enabled
3 Type: REG_DWORD
4 Value: 0 = disabled, 1 = enabled
5 <!--NeedCopy-->
```

By default, the **Enabled** property is hidden in the registry. When it remains unspecified, the automatic upload feature is enabled.

Using PowerShell, the following cmdlet disables enrollment in CEIP:

```
New-ItemProperty -Path HKLM:\SOFTWARE\Citrix\Telemetry\CEIP -Name
Enabled -PropertyType DWORD -Value 0
```

Note:

The registry setting controls the automatic upload of anonymous statistics and usage information for all components on the same server. For example, if you have installed StoreFront on the same server as the Delivery Controller and decide to opt-out of CEIP using the registry setting, the opt-out applies to both components.

CEIP data collected from StoreFront

The following table gives examples of the type of anonymous information collected. The data does not contain any details that identify you as a customer.

Data	Description
StoreFront version	String denoting the installed version of StoreFront. For example, “3.8.0.0”
Stores count	A counter for the number of stores in the deployment.
Server Count in server group	A counter for the number of Servers in the Server group.

Data	Description
Delivery Controller Count per store	List of numeric values indicating the number of Delivery Controllers available for each store in the Deployment.
HTTPS enabled	String denoting whether HTTPS is enabled (“True” or “False”) for the deployment.
HTML5 setting for Citrix Receiver for Web	List of Strings denoting the HTML5 Receiver setting (“Always”, “Fallback”, or “Off”) for each Receiver for Web site.
Workspace control enabled for Citrix Receiver/Workspace app	List of Booleans denoting whether “Workspace Control” is enabled (“True” or “False”) for each Receiver for Web site.
Remote Access enabled for store	List of Strings denoting whether “Remote Access” is enabled (“ENABLED” or “DISABLED”) for each store in the Deployment.
Gateways count	A counter for the number of Citrix Gateways configured in the deployment.

Citrix Analytics service

March 11, 2024

If you are a Monitor customer and you have an on-premises StoreFront deployment, you can configure StoreFront so that data is sent to the Citrix Analytics service in Monitor. When configured, Citrix Workspace app and web browsers send user events to Citrix Analytics for processing. Citrix Analytics aggregates metrics on users, applications, endpoints, networks, and data to provide comprehensive insights into user behavior. To read about this feature in the Citrix Analytics documentation, see [On-board Virtual Apps and Desktops Sites using StoreFront](#).

To configure this behavior:

- Download a configuration file from Citrix Analytics.
- Import Citrix Analytics data into your on-premises StoreFront deployment using PowerShell.

After StoreFront is configured, Citrix Workspace app can send data from StoreFront stores when the Citrix Analytics service requests it.

Important:

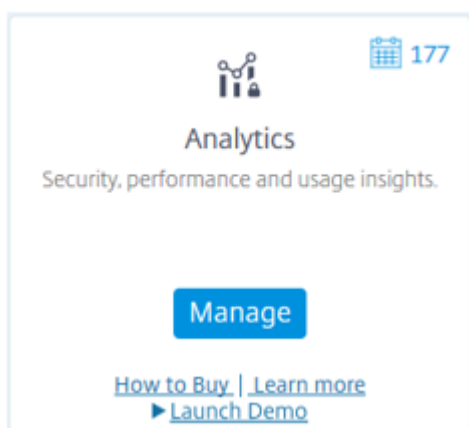
Your StoreFront deployment must be able to contact the following addresses at port 443 for this feature to work properly and consume the Monitor services:

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

Download the configuration file from Citrix Analytics**Important:**

A configuration file containing sensitive information is required for initial configuration. Keep the file safe after downloading. Do not share this file with anyone outside of your organization. After configuration you can delete this file. If you need to reapply the configuration again on another machine, you can download the file again from the Citrix Analytics service management console.

1. Log on to Monitor (<https://citrix.cloud.com/>) using an administrator account.
2. Select a Monitor customer.
3. Open the Citrix Analytics service management console by clicking **Manage**.



4. In the Citrix Analytics service management console, select **Settings > Data Sources**.
5. In the Virtual App and Desktops card, select the (⌵) menu icon then select **Connect StoreFront deployment**.
6. On the Connect StoreFront Deployment page, select **Download File** to download the *StoreFront-ConfigurationFile.json* file.

Example configuration file

```
1 {
2
3   "customerId": "<yourcloudcustomer>",
4   "enablementService": " https://api.analytics.cloud.com /casvc/<
      yourcloudcustomer>/ctxana/v1/cas/<yourcloudcustomer>/XenDesktop/<
      deviceid>/dsconfigdata",
5   "cwsServiceKey": "PFJTPn..... T4=",
6   "enablementServiceStatus": " https://api.analytics.cloud.com /casvc/<
      yourcloudcustomer>/ctxana/v1/cas/storefront/config",
7   "instanceId": "d98f21d0-56e0-11e9-ba52-5136d90862fe",
8   "name": "CASSingleTenant"
9 }
10
11 <!--NeedCopy-->
```

where

customerId is the unique ID for the current Monitor customer.

cwsServiceKey is a unique key identifying the current Monitor customer account.

instanceId is a generated ID used to sign (secure) requests made from Citrix Workspace app to Citrix Analytics. If you register multiple StoreFront servers or server groups with Monitor, then each one has a unique instanceId.

Import Citrix Analytics data into your StoreFront deployment

1. Copy the *StoreFrontConfigurationFile.json* file to a suitable folder on the on-premises StoreFront server (or one server in a StoreFront server group). The following commands assume that the file is saved to the Desktop.
2. Open PowerShell ISE and select **Run as Administrator**.
3. Run the following commands:

```
1 Import-STFCasConfiguration -Path "$Env:UserProfile\Desktop\
   StoreFrontConfigurationFile.json"
2 Get-STFCasConfiguration
3 <!--NeedCopy-->
```

4. This command returns a copy of the imported data and displays it in the PowerShell console.

```
CustomerId      : [REDACTED]
EnablementService : https://[REDACTED]
CwsServiceKey    : [REDACTED]

EnablementServiceStatus : https://[REDACTED]
InstanceId         : [REDACTED]
Name              : CASSingleTenant
```

Note:

On-premises StoreFront servers, which are installed on Windows Server 2012 R2, may require the C++ run time software components to be manually installed, so that they can register with CAS. If StoreFront is installed during Citrix Virtual Apps and Desktops installation, this step is not required, because the CVAD metainstaller already installs the C++ run time components. If StoreFront is installed using just the CitrixStoreFront-x64.exe metainstaller without the C++ runtime, it may fail to register with Monitor after you have imported the CAS configuration file.

Propagate Citrix Analytics data to a StoreFront server group

If you are performing these actions on a StoreFront server group, you must propagate the imported Citrix Analytics data to all members of the server group. This step is not necessary in a single StoreFront server deployment.

To propagate the data, use one of the following approaches:

- Use the StoreFront management console.
- Use the PowerShell cmdlet **Publish-STFServerGroupConfiguration**.

Check StoreFront server group ID

To check whether your deployment has successfully registered with the Citrix Analytics service, you can use PowerShell to discover the ServerGroupID for your deployment.

1. Log on to your StoreFront server, or to one StoreFront server in the server group.
2. Open PowerShell ISE and select **Run as Administrator**.
3. Run the following commands:

```
1 $WebConfigPath = "C:\Program Files\Citrix\Receiver StoreFront\
   Framework\FrameworkData\Framework.xml"
2 $XMLObject = (Get-Content $WebConfigPath) -as [Xml]
3 $XMLObject.framework.properties.property
4 <!--NeedCopy-->
```

For example, these commands generate output like the following:

```
1 name value
2 ----
3 ClusterId 8b8ff5c8-44ba-46e4-87f0-2df8cff31432
4 HostBaseUrl https://storefront.example.com/
5 SelectedIISWebSiteId 1
6 AdminConsoleOperationMode Full
7 <!--NeedCopy-->
```

Stop sending data to Citrix Analytics from StoreFront

1. Open PowerShell ISE and select **Run as Administrator**.
2. Run the following commands:

```
Remove-STFCasConfiguration
```

```
Get-STFCasConfiguration
```

Get-STFCasConfiguration returns nothing if the previously imported Citrix Analytics data has been successfully removed.

3. If you are performing these actions on a StoreFront server group, propagate the change and remove the imported Citrix Analytics data from all members of the server group. On one server in the server group, run the following command:

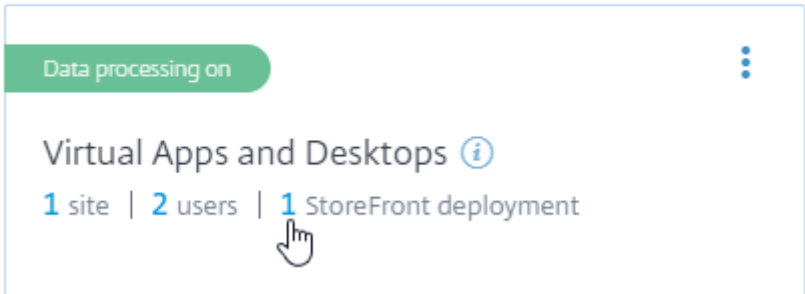
```
Publish-STFServerGroupConfiguration
```

4. On any other server group members, run the following command to confirm that Citrix Analytics configuration has been successfully removed from all servers in the group:

```
Get-STFCasConfiguration
```

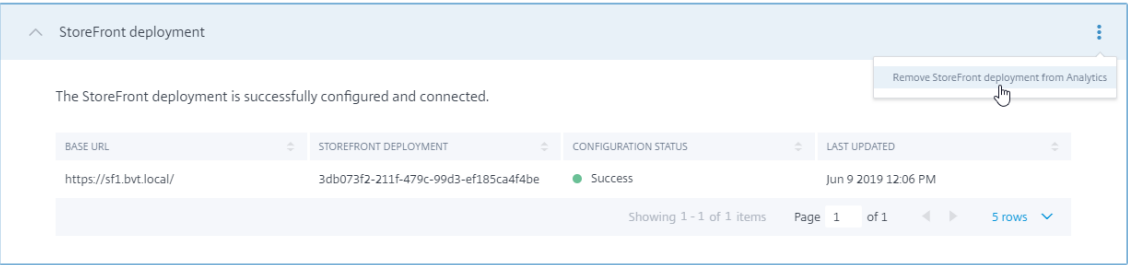
5. Log on to Monitor (<https://citrix.cloud.com/>) using an administrator account.
6. Select a Monitor customer.
7. Open the Citrix Analytics service management console by clicking **Manage**.
8. In the Citrix Analytics service management console, select **Settings > Data Sources**.
9. In the Virtual App and Desktops card, select the StoreFront deployment count:

CITRIX DATA SOURCES



10. Identify the StoreFront deployment you want to remove by referring to its host base URL and ServerGroupID.
11. In the (⋮) menu, select **Remove StoreFront deployment from Analytics**.

StoreFront deployments



Note:

If you remove the configuration from the server side, but not from Citrix Analytics, the StoreFront deployment entry remains in Citrix Analytics but receives no data from StoreFront. If you remove the configuration only from Citrix Analytics, the StoreFront deployment entry is re-added at the next App pool recycle (done on an IIS reset or automatically every 24 hours).

Configure StoreFront to use a web proxy to contact Monitor and register with Citrix Analytics

If StoreFront is placed on a host webserver behind a web proxy, registration with Citrix Analytics will fail. If StoreFront administrators use an HTTP proxy in their Citrix deployment, StoreFront traffic bound for the Internet must pass through the web proxy before it reaches Citrix Analytics in the cloud. StoreFront does not automatically use the hosting OS's proxy settings; additional configuration is required to instruct the store to send outbound traffic through the web proxy. You can configure a `<system.net>` proxy configuration by adding a new section to the store web.config file. Do this for every store on the StoreFront server that will be used to send data to Citrix Analytics.

Method 1: Set the store proxy configuration via Powershell for one or more stores (recommended)

Running the Powershell script Config-StoreProxy.ps1 automates this process for one or more stores and automatically inserts valid XML to configure <system.net>. The script also backs up the store web.config file to the current user's desktop, allowing the unmodified web.config file to be restored if necessary.

Note:

Running the script more than once may result in multiple copies of the <system.net> XML being added. Each store should only have a single entry for <system.net>. Adding multiple copies prevents the Store proxy configuration from working correctly.

1. Open up the Powershell ISE and select **Run as Admin**.
2. Set `$Stores = @("Store", "Store2")` to include the stores you wish to configure with a web proxy.
3. Specify either:
 - an IP address, OR
 - an FQDN for the web proxy
4. Run the following Powershell:

```
1 $Stores = @("Store", "Store2")
2 $ProxyIP = "10.0.0.1"
3 $ProxyFQDN = "proxyserver.example.com"
4 $ProxyPort = 8888
5
6 # Set this for every Store using Stores array
7 function Set-StoreProxyServer() # Tested with both IP and FQDN
8 {
9
10     [CmdletBinding()]
11     param([Parameter(Mandatory=$true, ParameterSetName="ProxyIP")] [
12         Parameter(Mandatory=$true, ParameterSetName="ProxyFQDN")] [
13             array]$Stores,
14             [Parameter(Mandatory=$true, ParameterSetName="ProxyIP")] [
15                 string]$ProxyIP,
16             [Parameter(Mandatory=$true, ParameterSetName="ProxyFQDN")] [
17                 string]$ProxyFQDN,
18             [Parameter(Mandatory=$true, ParameterSetName="ProxyIP")] [
19                 Parameter(Mandatory=$true, ParameterSetName="ProxyFQDN")
20                 ] [int]$ProxyPort)
21
22     foreach($Store in $Stores)
23     {
```



```
19 Write-Host "Backing up the Store web.config file for store
   $Store before making changes..." -ForegroundColor "
   Yellow"
20 Write-Host "`n"
21
22 if(!(Test-Path "$env:UserProfile\desktop\$Store\"))
23 {
24
25     Write-Host "Creating $env:UserProfile\desktop\$Store\
       directory for backup..." -ForegroundColor "Yellow"
26     New-Item -Path "$env:UserProfile\desktop\$Store\" -
       ItemType "Directory" | Out-Null
27     Write-Host "`n"
28 }
29
30
31 Write-Host "Copying c:\inetpub\wwwroot\Citrix\$Store\web.
   config to $env:UserProfile\desktop\$Store\..." -
   ForegroundColor "Yellow"
32 Copy-Item -Path "c:\inetpub\wwwroot\Citrix\$Store\web.
   config" -Destination "$env:UserProfile\desktop\$Store\"
   -Force | Out-Null
33
34 if(Test-Path "$env:UserProfile\desktop\$Store\web.config")
35 {
36
37     Write-Host "$env:UserProfile\desktop\$Store\web.config
       file backed up" -ForegroundColor "Green"
38 }
39
40 else
41 {
42
43     Write-Host "$env:UserProfile\desktop\$Store\web.config
       file NOT found!" -ForegroundColor "Red"
44 }
45
46 Write-Host "`n"
47
48 Write-Host "Setting the proxy server to $ProxyAddress for
   Store $Store..." -ForegroundColor "Yellow"
49 Write-Host "`n"
50
51 $StoreConfigPath = "c:\inetpub\wwwroot\Citrix\$Store\web.
   config"
52 $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
53
54 if([string]::IsNullOrEmpty($ProxyFQDN))
55 {
56
57     $ProxyServer = ("HTTP://$ProxyIP"+":"+$ProxyPort)
58 }
59
```

```

60     else
61     {
62
63         $ProxyServer = ("HTTP://$ProxyFQDN"+":"+$ProxyPort)
64     }
65
66
67     $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
68
69     # Create 3 elements
70     $SystemNet = $XMLObject.CreateNode("element","system.net",
        "")
71     $DefaultProxy = $XMLObject.CreateNode("element",
        "defaultProxy","")
72     $Proxy = $XMLObject.CreateNode("element","proxy","")
73     $Proxy.SetAttribute("proxyaddress",$ProxyServer)
74     $Proxy.SetAttribute("bypassonlocal","true")
75
76     # Move back up the XML tree appending new child items in
        reverse order
77     $DefaultProxy.AppendChild($Proxy)
78     $SystemNet.AppendChild($DefaultProxy)
79     $XMLObject.configuration.AppendChild($SystemNet)
80
81     # Save the modified XML document to disk
82     $XMLObject.Save($StoreConfigPath)
83
84     Write-Host "Getting the proxy configuration for c:\inetpub
        \wwwroot\Citrix\$Store..." -ForegroundColor "Yellow"
85     $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]
86     $ConfiguredProxyServer = $XMLObject.configuration.'system.
        net'.defaultProxy.proxy.proxyaddress | Out-Null
87     Write-Host ("Configured proxy server for Store $Store"+":
        "+ $ConfiguredProxyServer) -ForegroundColor "Green"
88     Write-Host "`n"
89 }
90
91 Write-Host "Restarting IIS..." -ForegroundColor "Yellow"
92 IISReset /RESTART
93 }
94
95
96 Set-StoreProxyServer -Stores $Stores -ProxyFQDN $ProxyFQDN -
    ProxyPort $ProxyPort
97 # OR
98 Set-StoreProxyServer -Stores $Stores -ProxyIP $ProxyIP -ProxyPort
    $ProxyPort
99 <!--NeedCopy-->

```

5. Check that the C:\inetpub\wwwroot\Citrix< Store>\web.config now contains a new <system.net> section at the end of the web.config file.

```
1 </dependentAssembly>
```

```
2     </assemblyBinding>
3 </runtime>
4 <system.net>
5     <defaultProxy>
6         <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
7             bypassonlocal="true" />
8     </defaultProxy>
9 </system.net>
10 </configuration>
11 <!--NeedCopy-->
```

6. Import the Citrix Analytics data as described in Import Citrix Analytics data into your StoreFront deployment.

Method 2: Manually add a `<system.net>` section to the store web.config file

This must be done for every store on the StoreFront server that will be used to send data to Citrix Analytics.

1. Back up the web.config file for the store and copy it to another location outside of C:\inetpub\wwwroot\Citrix<Store>\web.config.
2. Modify the following XML with your proxy settings using either an FQDN-and-port combination, or using an IP-and-port combination.

For example, using an FQDN-and-port combination, use the following `<system.net>` element:

```
1 <system.net>
2     <defaultProxy>
3         <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
4             bypassonlocal="true" />
5     </defaultProxy>
6 </system.net>
7 <!--NeedCopy-->
```

For example, using an IP-and-port combination, use the following `<system.net>` element:

```
1 <system.net>
2     <defaultProxy>
3         <proxy proxyaddress="HTTP://10.0.0.1:8888" bypassonlocal="true"
4             />
5     </defaultProxy>
6 </system.net>
7 <!--NeedCopy-->
```

3. At the end of the store web.config file, insert the appropriate `<system.net>` element where indicated here:

```

1 <runtime>
2 <gcServer enabled="true" />
3 <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
4   <dependentAssembly>
5     <assemblyIdentity name="System.Web.Mvc" publicKeyToken="31
      BF3856AD364E35" culture="neutral" />
6     <bindingRedirect oldVersion="0.0.0.0-5.0.0.0" newVersion="
      5.0.0.0" />
7   </dependentAssembly>
8   <dependentAssembly>
9     <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30
      ad4fe6b2a6aeed" culture="neutral" />
10    <bindingRedirect oldVersion="0.0.0.0-9.0.0.0" newVersion="
      9.0.0.0" />
11  </dependentAssembly>
12 </assemblyBinding>
13 </runtime>
14
15 Insert the <system.net> element here
16
17 </configuration>
18 <!--NeedCopy-->

```

4. Import the Citrix Analytics data as described in Import Citrix Analytics data into your StoreFront deployment.


Securing StoreFront with HTTPS

March 11, 2024

Citrix strongly recommends securing communications between StoreFront and users' devices using HTTPS. This ensures that passwords and other data sent between the client and StoreFront are encrypted. Furthermore, plain HTTP connections can be compromised by various attacks, such as man-in-the-middle attacks, particularly when connections are made from insecure locations such as public Wi-Fi hotspots. In the absence of the appropriate IIS configuration, StoreFront uses HTTP for communications.

Depending on your configuration, users may access StoreFront via a gateway or load balancer. You can terminate the HTTPS connection at the gateway or load balancer. However in this case Citrix still recommends that you secure connections between the gateway and StoreFront using HTTPS.

If StoreFront is not configured for HTTPS it displays the following warning:

 StoreFront using HTTP not HTTPS.

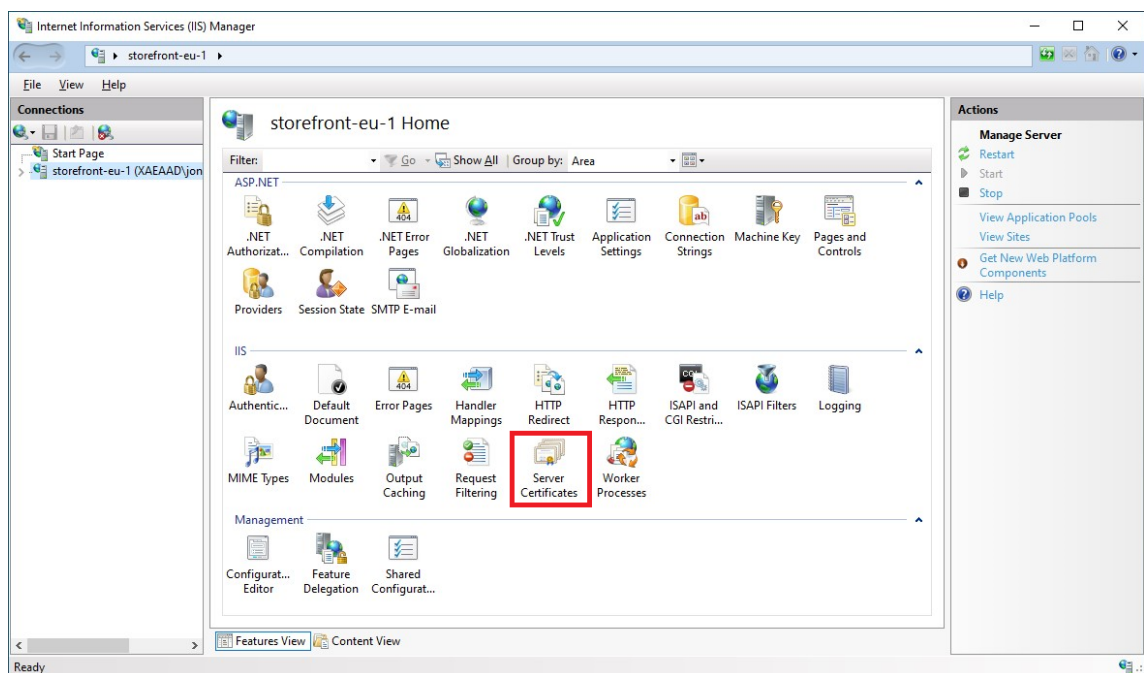
Creating Certificates

- Ensure that the FQDN(s) used to access StoreFront are included in the DNS field as Subject Alternative Name (SANs). If you are using a load balancer then include both the individual server's FQDN and the load balancer FQDN
- Sign the certificate using a third party CA such as Verisign or an enterprise root CA for your organization.
- Export the certificate in PFX format including the private key.

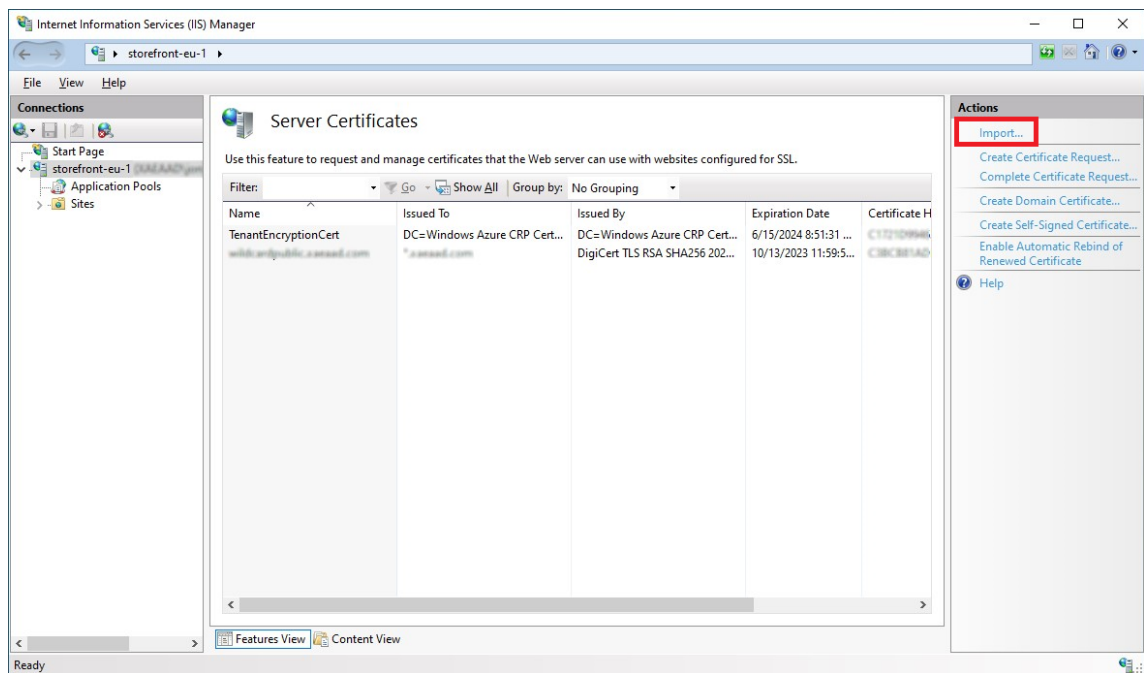
Configure IIS for HTTPS

To configure Microsoft Internet Information Services (IIS) for HTTPS on the StoreFront server:

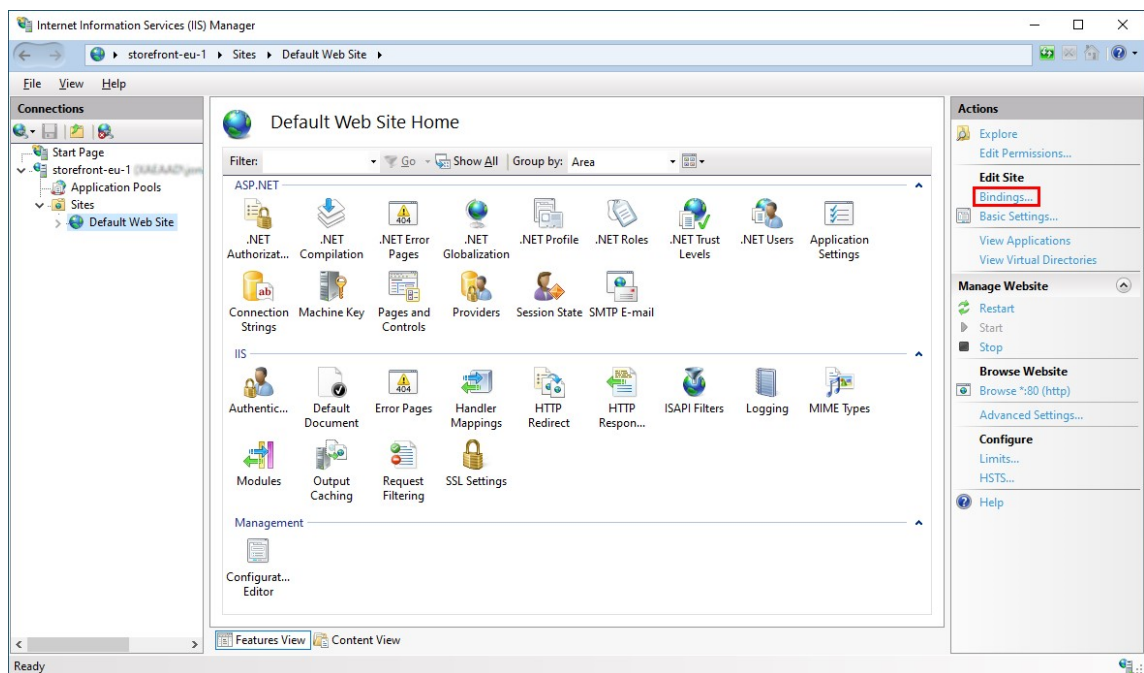
1. Open Internet Information Services (IIS) Manager console
2. In the tree view on the left select the server.
3. In the right hand pane double click **Server Certificates**



4. From the Server Certificates screen you can import an existing certificate or create a new certificate.



5. In the tree view on the left select **Default Web Site** (or the appropriate website)
6. In the Actions pane click **Bindings...**

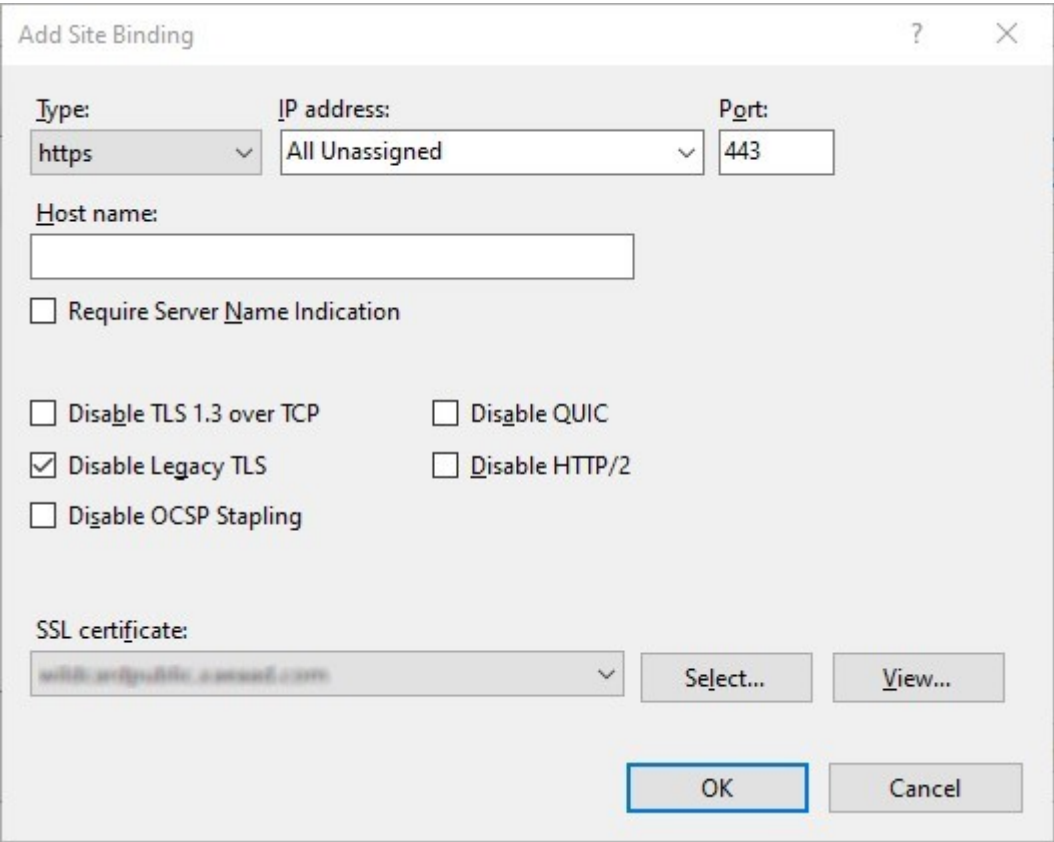


7. In the bindings window click **Add...**
8. In the **Type** drop down select **https**
9. On Windows Server 2022 or above, click **Disable Legacy TLS** to disable TLS older than 1.2.

On older Windows Server versions, you can disable legacy TLS versions using Windows registry

settings, see [Windows Server Documentation](#).

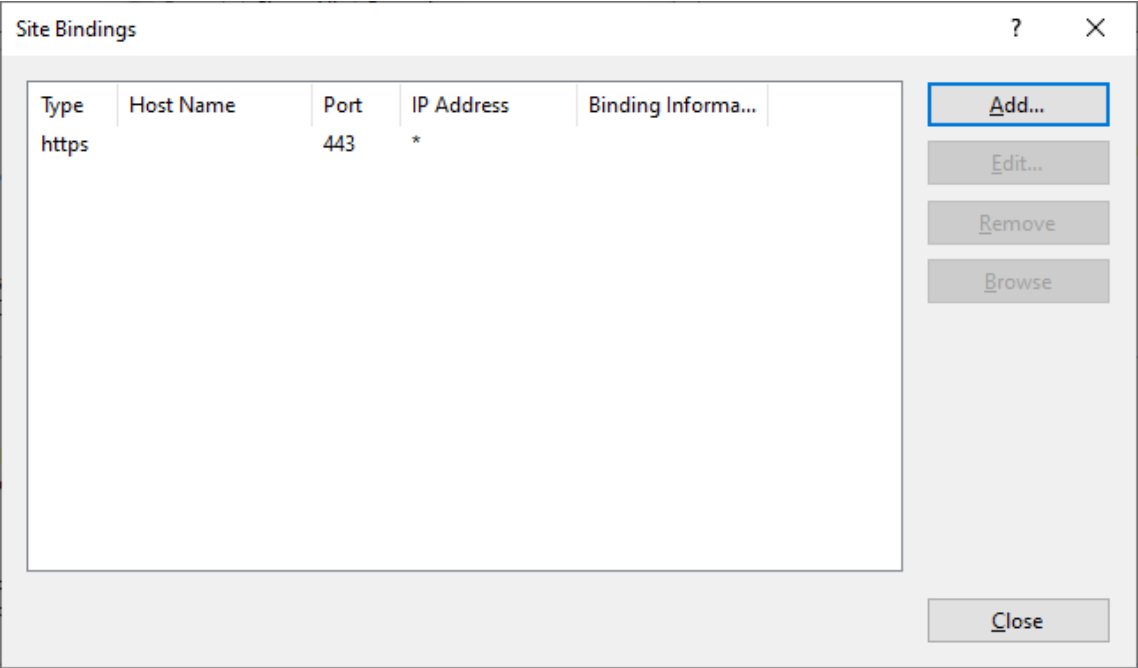
10. Select the certificate previously imported. Press OK



The 'Add Site Binding' dialog box is shown. It has a title bar with a question mark and a close button. The dialog contains the following fields and controls:

- Type:** A dropdown menu set to 'https'.
- IP address:** A dropdown menu set to 'All Unassigned'.
- Port:** A text box containing '443'.
- Host name:** An empty text box.
- Require Server Name Indication:** An unchecked checkbox.
- Disable TLS 1.3 over TCP:** An unchecked checkbox.
- Disable QUIC:** An unchecked checkbox.
- Disable Legacy TLS:** A checked checkbox.
- Disable HTTP/2:** An unchecked checkbox.
- Disable OCSP Stapling:** An unchecked checkbox.
- SSL certificate:** A dropdown menu showing 'website.mydomain.com'. To its right are 'Select...' and 'View...' buttons.
- At the bottom right are 'OK' and 'Cancel' buttons.

11. To remove HTTP access, select HTTP and click **Remove**.



The 'Site Bindings' dialog box is shown. It has a title bar with a question mark and a close button. The dialog contains a table with the following data:

Type	Host Name	Port	IP Address	Binding Informa...
https		443	*	

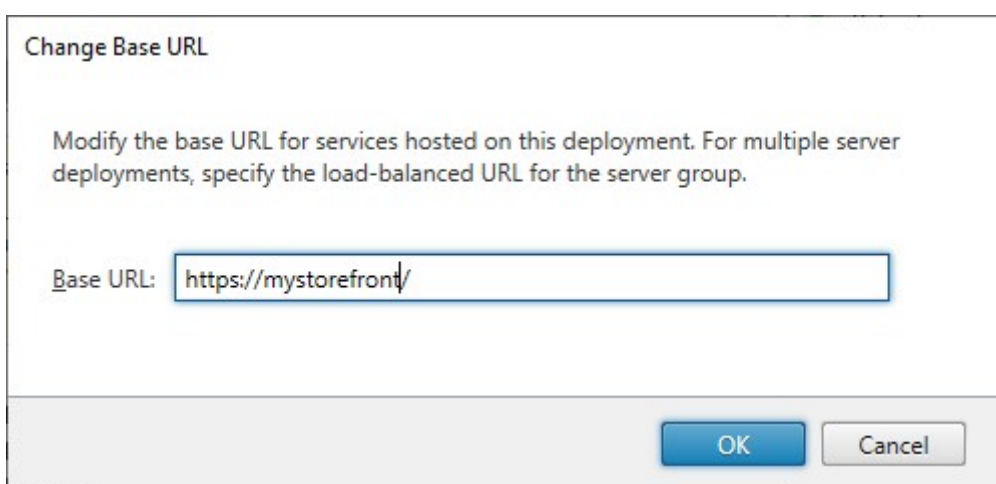
To the right of the table are four buttons: 'Add...', 'Edit...', 'Remove', and 'Browse'. At the bottom right is a 'Close' button.

Change StoreFront server base URL from HTTP to HTTPS

If you install and configure Citrix StoreFront without first installing and configuring an SSL certificate, StoreFront uses HTTP for communications.

If you install and configure an SSL certificate at some time later, use the following procedure to ensure StoreFront and its services use HTTPS connections.

1. In the Citrix StoreFront management console, in the left pane select **Server Group**.
2. In the Actions pane, select **Change Base URL**.
3. Update the base URL to start [https:](#) and click **OK**.



HSTS

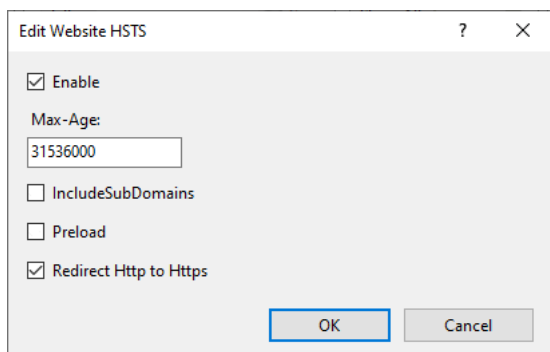
The user's client device is vulnerable even after you enable HTTPS on the server side. For example, a man-in-the-middle attacker could spoof the StoreFront server and trick the user into connecting to the spoof server over plain HTTP. They could then get access to sensitive information such as the user's credentials. The solution is to ensure that the user's browser doesn't attempt to access the RfWeb server over HTTP. You can achieve this with the [HTTP Strict Transport Security \(HSTS\)](#).

When HSTS is enabled, the server indicates to web browsers that requests to the web site should only ever be made over HTTPS. If a user attempts to access the URL using HTTP, the browser will automatically switch to using HTTPS instead. This ensures client-side validation of a secure connection as well as the server-side validation in IIS. The web browser maintains this validation for a configured period.

On Windows Server 2019 and above:

1. Open **Internet Information Services (IIS) Manager**.
2. Select **Default Web Site** (or the appropriate website).

3. In the Actions pane on the right hand side, click **HSTS...**
4. Tick **Enable**, enter a max age, e.g. 31536000 for one year and tick **Redirect HTTP to HTTPS**.
5. Press **OK**



Max-Age:
31536000

Note:

Enabling HSTS affects all web sites on the same domain. For example, if the website is accessible at <https://www.company.com/Citrix/StoreWeb>, then the HSTS policy will apply to all web sites under <https://www.company.com>, which may not be desired.

Secure your StoreFront deployment

April 26, 2024

This article highlights areas that may have an impact on system security when deploying and configuring StoreFront.

Communication between end users and StoreFront

Citrix recommends securing communications between users' devices and StoreFront using HTTPS. This ensures that passwords and other data sent between the client and StoreFront are encrypted. Furthermore, plain HTTP connections can be compromised by various attacks, such as man-in-the-middle attacks, particularly when connections are made from insecure locations such as public Wi-Fi hotspots. In the absence of the appropriate IIS configuration, StoreFront uses HTTP for communications.

Depending on your configuration, users may access StoreFront via a gateway or load balancer. You can terminate the HTTPS connection at the gateway or load balancer. However in this case Citrix still recommends that you secure connections between the gateway or load-balancer and StoreFront using HTTPS.

To enable HTTPS, disable HTTP and enable HSTS, see [Securing StoreFront with HTTPS](#).

StoreFront communications with Citrix Virtual Apps and Desktops servers

Citrix recommends using the HTTPS protocol to secure data passing between StoreFront and your Citrix Virtual Apps and Desktops delivery controllers. See [Install TLS server certificates on Controllers](#). StoreFront does not support TLS 1.0 or TLS 1.1 protocols between StoreFront and the delivery controller. Alternatively you can configure Windows to secure communication between the servers using IPSec.

You can configure the delivery controller and StoreFront to ensure that only trusted StoreFront servers can communicate with the delivery controller, see [Manage security keys](#).

StoreFront communications with Cloud Connectors

Citrix recommends using the HTTPS protocol to secure data passing between StoreFront and your Cloud Connectors. See [How to Enable SSL on Cloud Connectors to Secure XML Traffic](#). StoreFront does not support TLS 1.0 or TLS 1.1 protocols between StoreFront and the cloud connectors. Alternatively you can configure Windows to secure communication between the servers using IPSec.

Remote access

Citrix does not recommend exposing your StoreFront server directly to the internet. Citrix recommends using a Citrix Gateway to provide authentication and access for remote users.

Microsoft Internet Information Services (IIS) hardening

You can configure StoreFront with a restricted IIS configuration. Note that this is not the default IIS configuration.

Filename extensions

You can use request filtering to configure a lists of allowed file extensions and disallow unlisted file name extensions. See [IIS documentation](#).

StoreFront requires the following file name extensions:

- . (blank extension)
- .appcache
- .aspx
- .cr
- .css

- .dtd
- .png
- .htm
- .html
- .ica
- .ico
- .jpg
- .js
- .png
- .svg
- .txt
- .xml

If download or upgrade of Citrix Workspace app is enabled for a store website, StoreFront also requires these file name extensions:

- .dmg
- .exe

If Citrix Workspace app for HTML5 is enabled, StoreFront also requires these file name extensions:

- .eot
- .ttf
- .woff
- .wasm

Verbs

You can use request filtering to configure a list of allowed verbs and disallow unlisted verbs. See [IIS documentation](#).

- GET
- POST
- HEAD

Non-Ascii characters in URLs

If you ensure that the store name and website name only use ascii characters then StoreFront URLs do not contain ascii characters. You can use request filtering to disallow non-ascii characters. See [IIS documentation](#).

MIME Types

You can remove OS shell MIME Types corresponding to the following file extensions:

- .exe
- .dll
- .com
- .bat
- .csh

See [IIS documentation](#).

Remove X-Powered-By Header

By default IIS reports that it is using ASP.NET by adding a **X-Powered-By** header with value **ASP .NET**. You can configure IIS to remove this header. See [IIS Custom Headers documentation](#).

Remove Server header with IIS version

By default IIS reports the IIS version by adding a **Server** header. You can configure IIS to remove this header. See [IIS request filtering documentation](#).

Move the StoreFront website to a separate partition

You can host the StoreFront web sites on a separate partition from the system files. Within IIS you must move the **Default Web Site**, or create a separate site, on the appropriate partition prior to creating your StoreFront deployment.

IIS features

For the list of IIS features installed and used by StoreFront, see [System Requirements](#). You can remove other IIS features.

Although StoreFront does not use ISAPI filters directly, the feature is required by ASP.NET so cannot be uninstalled.

Handler Mappings

StoreFront requires the following Handler Mappings. You can remove other handler mappings.

- ExtensionlessUrlHandler-Integrated-4.0

- PageHandlerFactory-Integrated-4.0
- StaticFile

See [IIS Handlers Documentation](#).

ISAPI filters

StoreFront does not require any ISAPI filters. You can remove all ISAPI filters. See [IIS ISAPI Filters documentation](#).

.NET Authorization Rules

By default IIS servers have the “.NET Authorization Rule” set to Allow All Users. By default, the web site used by StoreFront inherits this configuration.

If you remove or change the .NET Authorization rule at the server level then you must override the rules on the web site used by StoreFront to add an allow rule for “All Users” and remove any other rules.

Retail mode

You can enable Retail mode, see [IIS documentation](#).

Application Pools

StoreFront creates the following application pools:

- Citrix Configuration Api
- Citrix Delivery Services Authentication
- Citrix Delivery Services Resources
- and Citrix Receiver for Web

Do not change the application pools used by each IIS application or the identity of each pool. If you are using multiple sites, it is not possible to configure each site to use separate application pools.

Under the Recycling settings, you can set the application pool idle time-out and Virtual Memory Limit. Note that when the “Citrix Receiver for Web” application pool recycles it causes users logged in through a web browser to be logged out, therefore it is set by default to recycle at 02:00 each day to minimize disruption. If you change any of the recycling settings this may result in users being logged off at other times of the day.

Required settings

- Do not change the IIS Authentication settings. StoreFront manages authentication and configures directories of the StoreFront site with the appropriate authentication settings.
- For the StoreFront server under **SSL Settings**, do not select **Client certificates: Require**. StoreFront installation configures the appropriate pages of the StoreFront site with this setting.
- StoreFront requires cookies for session state and other functionality. On certain directories, under **Session State, Cookie Settings, Mode** must be set to **Use Cookies**.
- StoreFront requires **.NET Trust Level** to be set to **Full Trust**. Do not set the .NET trust level to any other value.

Services

StoreFront installation creates the following Windows services:

- Citrix Configuration Replication (NT SERVICE\CitrixConfigurationReplication)
- Citrix Cluster Join (NT SERVICE\CitrixClusterService)
- Citrix Peer Resolution (NT SERVICE\Citrix Peer Resolution Service)
- Citrix Credential Wallet (NT SERVICE\CitrixCredentialWallet)
- Citrix Subscriptions Store (NT SERVICE\CitrixSubscriptionsStore)
- Citrix Default Domain Services (NT SERVICE\CitrixDefaultDomainService)

These accounts log on as **Network Service**. Do not change this configuration.

If you configure StoreFront Kerberos constrained delegation for XenApp 6.5, this in addition creates the Citrix StoreFront Protocol Transition service (NT SERVICE\CitrixStoreFrontProtocolTransition). This service runs as **NT AUTHORITY\SYSTEM**. Do not change this configuration.

User rights assignment

Modifying User Rights Assignment from the defaults may cause issues with StoreFront. In particular:

- Microsoft IIS is enabled as part of StoreFront installation. Microsoft IIS grants the logon right **Log on as a batch job**, and the privilege **Impersonate a client after authentication** to the built-in group IIS_IUSRS. This is normal Microsoft IIS installation behavior. Do not change these user rights. Refer to Microsoft documentation for details.
- When you install StoreFront, it creates Application Pools which IIS grants user rights **Log on as a service**, **Adjust memory quotas for a process**, **Generate security audits**, and **Replace a process level token**.
- To create or change a deployment, the admin must have rights **Restore files and directories**.

- For a server to join a server group, the Administrators group must have rights **Restore files and directories**, **Access this computer from the network** and **Manage auditing and security log**.
- For users to log on with a username and password authentication (directly or via a gateway), they must have rights to “Allow log on locally”, unless you have configured StoreFront to validate passwords via the delivery controller.

This is not a comprehensive list and other user access rights may be required.

Configure group memberships

When you configure a StoreFront server group, the following services are added to the Administrators security group:

- Citrix Configuration Replication (NT SERVICE\CitrixConfigurationReplication)
- Citrix Cluster Join (NT SERVICE\CitrixClusterService). This service is only seen on servers which are part of a group, and only runs while the join is in progress.

These group memberships are required for StoreFront to operate correctly, to:

- Create, export, import and delete certificates, and set access permissions on them
- Read and write the Windows registry
- Add and remove Microsoft .NET Framework assemblies in the Global Assembly Cache (GAC)
- Access the folder **Program Files\Citrix\<StoreFrontLocation>**
- Add, modify, and remove IIS app pool identities and IIS web applications
- Add, modify, and remove local security groups and firewall rules
- Add and remove Windows services and PowerShell snap-ins
- Register Microsoft Windows Communication Framework (WCF) endpoints

In updates to StoreFront, this list of operations might change without notice.

StoreFront installation also creates the following local security groups:

- CitrixClusterMembers
- CitrixCWServiceReadUsers
- CitrixCWServiceWriteUsers
- CitrixDelegatedAuthenticatorUsers
- CitrixDelegatedDirectoryClaimFactoryUsers
- CitrixPNRSReplicators
- CitrixPNRSUsers
- CitrixStoreFrontAdministrators
- CitrixSubscriptionServerUsers
- CitrixSubscriptionsStoreServiceUsers

- CitrixSubscriptionsSyncUsers

StoreFront maintains the membership of these security groups. They are used for access control within StoreFront, and are not applied to Windows resources such as files and folders. Do not modify these group memberships.

NTLM

StoreFront uses NTLM to authenticate between servers in a server group. If you disable NTLM then StoreFront is unable to synchronize data between StoreFront servers in a server group.

You can configure the server to only use NTLMv2 and reject NTLMv1, see [Microsoft documentation](#).

Certificates in StoreFront

Server certificates

Server certificates are used for machine identification and Transport Layer Security (TLS) transport security in StoreFront. If you decide to enable ICA file signing, StoreFront can also use certificates to digitally sign ICA files.

For more information see Communication between end users and StoreFront and [Ica file signing](#).

Token management certificates

Authentication services and stores each require certificates for token management. StoreFront generates a self-signed certificate when an authentication service or store is created. Self-signed certificates generated by StoreFront should not be used for any other purpose.

Citrix Delivery Services certificates

StoreFront holds a number of certificates in a custom Windows certificate store (Citrix Delivery Services). The Citrix Configuration Replication service, Citrix Credential Wallet service, and Citrix Subscriptions Store service use these certificates. Each StoreFront server in a cluster has a copy of these certificates. These services do not rely on TLS for secure communications, and these certificates are not used as TLS server certificates. These certificates are created when a StoreFront store is created or StoreFront is installed. Do not modify the contents of this Windows certificate store.

Code signing certificates

StoreFront includes a number of PowerShell scripts (.ps1) in the folder in *<InstallDirectory>\Scripts*. The default StoreFront installation does not use these scripts. They simplify the configuration steps for specific and infrequent tasks. These scripts are signed, allowing StoreFront to support PowerShell execution policy. We recommend the **AllSigned** policy. (The **Restricted** policy is not supported, as this prevents PowerShell scripts from executing.) StoreFront does not alter the PowerShell execution policy.

Although StoreFront does not install a code signing certificate in the Trusted Publishers store, Windows can automatically add the code signing certificate there. This happens when the PowerShell script is executed with the **Always run** option. (If you select the **Never run** option, the certificate is added to the Untrusted Certificates store, and StoreFront PowerShell scripts will not execute.) Once the code signing certificate has been added to the Trusted Publishers store, its expiration is no longer checked by Windows. You can remove this certificate from the Trusted Publishers store after the StoreFront tasks have been completed.

Disabling legacy TLS versions

Citrix recommends that you disable TLS 1.0 and 1.1 for both client and server communication on the Windows server. You can do this via Group Policy or alternatively via Windows registry settings. See [Microsoft documentation](#).

StoreFront security separation

If you deploy any web applications in the same web domain (domain name and port) as StoreFront, then any security risks in those web applications could potentially reduce the security of your StoreFront deployment. Where a greater degree of security separation is required, Citrix recommends that you deploy StoreFront in a separate web domain.

ICA file signing

StoreFront provides the option to digitally sign ICA files using a specified certificate on the server so that versions of Citrix Workspace app that support this feature can verify that the file originates from a trusted source. ICA files can be signed using any hash algorithm supported by the operating system running on the StoreFront server, including SHA-1 and SHA-256. For more information, see [Enable ICA file signing](#).

User change password

You can enable users logging on through a web browser with Active Directory domain credentials to change their passwords, either at any time or only when they have expired. However, this exposes sensitive security functions to anyone who can access any of the stores that use the authentication service. If your organization has a security policy that reserves user password change functions for internal use only, ensure that none of the stores are accessible from outside your corporate network. When you create the authentication service, the default configuration prevents users from changing their passwords, even if they have expired. For more information, see [Enable users to change their passwords](#).

Customizations

To strengthen security, do not write customizations that load content or scripts from servers not under your control. Copy the content or script into the website custom folder where you are making the customizations. If StoreFront is configured for HTTPS connections, ensure that any links to custom content or scripts also use HTTPS.

Security Headers

When viewing a store website through a web browser, StoreFront returns the following security related headers that place restrictions on the web browser.

Header name	Value	Description
<code>content-security-policy</code>	<code>frame-ancestors 'none'</code>	This prevents other sites from embedding a StoreFront websites within a frame which avoids click-jacking attacks. StoreFront uses inline scripts and styles so it is not possible to use a content-security-policy that blocks these. StoreFront websites only display content configured by administrators and do not display any user-entered content, therefore there is no need to block inline scripts.

Header name	Value	Description
X-Content-Type-Options	nosniff	This avoid MIME type sniffing.
X-Frame-Options	deny	This prevents other sites from embedding StoreFront websites within a frame which avoids click-jacking attacks. It is obsoleted by <code>content-security-policy</code> to <code>frame-ancestors 'none'</code> but is understood by some older browsers that do not support <code>content-security-policy</code>
X-XSS-Protection	1; mode=block	Used by some browsers to mitigate against XSS (cross-site-scripting) attacks

Cookies

StoreFront uses several cookies. Some of the cookies used in the operation of the website are as follows:

Cookie	Description
ASP.NET_SessionId	Tracks the user's session including authentication status. Has <code>HttpOnly</code> set.
CtxsAuthId	To prevent session fixation attacks, StoreFront in addition tracks whether the user is authenticated using this cookie. It has <code>HttpOnly</code> set.

Cookie	Description
CsrfToken	Used to prevent cross-site request forgery via the standard Cookie-to-header token pattern. The server sets a token in the cookie. The client reads the token from the cookie and includes the token in the query string or a header in subsequent requests. This cookie is required to have HttpOnly not set so the client JavaScript can read it.
CtxsDeviceId	Identifies the device. Has HttpOnly set.

StoreFront sets a number of other cookies to track user state, some of which need to be read by JavaScript so do not have [HttpOnly](#) set. These cookies do not contain any information relating to authentication or other confidential information.

Additional security information

Note:

This information may change at any time, without notice.

Your organization may want to perform security scans of StoreFront for regulatory reasons. The preceding configuration options can help to eliminate some findings in security scan reports.

If there is a gateway between the security scanner and StoreFront, particular findings may relate to the gateway rather than to StoreFront itself. Security scan reports usually do not distinguish these findings (for example, TLS configuration). Because of this, technical descriptions in security scan reports can be misleading.

Email-based account discovery

February 27, 2024

Configure email-based account discovery to enable users who install Citrix Workspace app on a device for the first time to set up their accounts without needing to know the store URL by entering their email addresses.

During the initial configuration process, Citrix Workspace app prompts users to enter either an email address or a store URL. If the user enters an email address, Citrix Workspace app looks up the email

domain in a number of locations to determine the StoreFront server. It then lists all visible stores for the user to choose from.

Citrix recommends using the Global App Config Service to configure email discovery. As an alternative you can configure email discovery using either DNS SVR records or a DNS alias.

Global App Config Service

To configure email discovery using the Global App Config Service, see [Setup email based discovery](#).

DNS SVR records records

As an alternative to Global App Config Service, you can use DNS SVR records to configure which StoreFront server Citrix Workspace app should use for an email domain.

On your DNS server for your email domain add a **SRV** record with the following properties:

Property	Value
Service	_citrixreceiver
Proto	TCP
Target	The fully qualified domain name (FQDN) and port for your Citrix Gateway appliance (to support both local and remote users) or StoreFront server (to support local users only) in the form <i>servername.domain:port</i> .

If your environment includes both internal and external DNS servers, you can add a SRV record specifying the StoreFront server FQDN on your internal DNS server and another record on your external server specifying the Citrix Gateway FQDN. With this configuration, local users are provided with the StoreFront details, while remote users receive Citrix Gateway connection information.

DNS discoverReceiver record

As a fallback to the other methods, you can create a DNS alias to the StoreFront server `discoverReceiver` on the email domain. For example if your email domain is `example.com`, create a DNS alias called `discoverReceiver.example.com`. If no SRV record is found in the specified domain, Citrix Workspace app searches for a machine named “discoverReceiver” to identify a StoreFront server.

If you use this mechanism, ensure that [discoverReceiver](#) is included as a subject alternate name in the HTTPS certificate for your StoreFront server.

Create a new deployment

March 19, 2024

1. If the Citrix StoreFront management console is not already open after installation of StoreFront, on the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. In the results pane of the Citrix StoreFront management console, click **Create a new deployment**.
3. If there are multiple IIS sites, choose from the **IIS site** drop down which site you would like to use.
4. If using a single StoreFront server, enter the server URL **Base URL**. If you will be configuring multiple StoreFront servers behind a load balancer, enter the load balancing url as the **Base URL**.

If you have not yet set up your load balancing environment, enter the server URL. You can modify the base URL for your deployment at any time.

5. Click **Next** and configure your first store as described in [Create Store](#).
6. Once you have completed all of the configuration steps, Click **Create** to create the deployment and the store.
7. StoreFront displays a summary of the store that it created. Click **Finish**.

Create a new deployment using the PowerShell SDK

To create a deployment using the [PowerShell SDK](#), call cmdlet [Add-STFDeployment](#).

Multiple Internet Information Services (IIS) websites

StoreFront allows you to deploy different Stores in different IIS websites per Windows server so that each store can have a different host name and certificate binding.

To create multiple web sites see [Microsoft IIS documentation](#).

It is not possible to create multiple StoreFront deployments using the management console; you must use the PowerShell SDK. For example to create two IIS website deployments, one for applications and one for desktop use the following commands:

```
1 Add-STFDeployment -SiteID 1 -HostBaseURL "https://apps.example.com"
2 Add-STFDeployment -SiteID 2 -HostBaseURL "https://desktops.example.com"
3 <!--NeedCopy-->
```

Once you have enabled multiple sites, StoreFront disables the management console and it is not possible to return StoreFront to single site mode. You must configure the sites using the StoreFront SDK and include the [SiteID](#) in each command.

Join an existing server group

March 11, 2024

Before installing StoreFront on a server you are adding to the group, ensure that:

- The server you are adding is running the same operating system version with the same locale settings as the other servers in the group. StoreFront server groups containing mixtures of operating system versions and locales are not supported.
- The relative path to StoreFront in IIS on the server you are adding is the same as on the other servers in the group.

Note:

For recommendation on server group size, see [StoreFront Server groups](#).

If the StoreFront server you are adding previously belonged to a server group and has been removed, before it can be added again, to the same or a different server group, you must reset the StoreFront server to a factory default state. See [Reset a server to factory defaults](#)

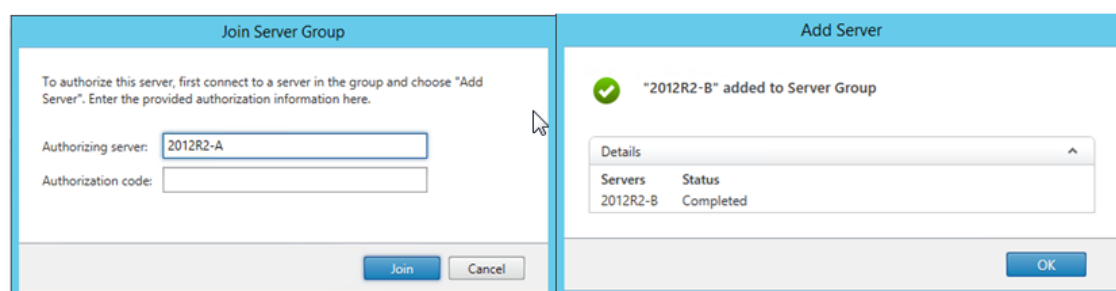
Important:

When you add a new server to a server group, StoreFront service accounts are added as members of the local administrators group on the new server. These services require local administrator permissions to join and synchronize with the server group. If you use Group Policy to prevent addition of new members to the local administrator group or if you restrict the permissions of the local administrator group on your servers, StoreFront cannot join a server group.

1. If the Citrix StoreFront management console is not already open after installation of StoreFront, on the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. In the results pane of the Citrix StoreFront management console, click **Join existing server group**.

3. Log on to a server in the StoreFront deployment that you wish to join and open the Citrix StoreFront management console. Select the Server Group node in the left pane of the console and, in the Actions pane, click **Add Server**. Make a note of the authorization code that is displayed.
4. Return to the new server and, in the Join Server Group dialog box, specify the name of the existing server in the Authorizing server box. Enter the authorization code obtained from that server and click **Join**.

Once joined to the group, the configuration of the new server is updated to match the configuration of the existing server. All the other servers in the group are updated with details of the new server.



To manage a multiple server deployment, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Any configuration changes you make must be propagated to the other servers in the group to ensure a consistent configuration across the deployment.

Upgrade StoreFront

April 9, 2024

Upgrading preserves your StoreFront configuration and leaves users' favorites intact. By contrast, [uninstalling StoreFront](#) removes StoreFront and associated services, sites, favorites (on stand-alone servers), and associated configuration.

Support upgrade paths

You can upgrade to StoreFront 2402 from:

- StoreFront 2311
- StoreFront 2308
- StoreFront 2203 LTSR (any CU)
- StoreFront 1912 LTSR (any CU)

- StoreFront 3.12 LTSR CU9

To upgrade from versions prior to 3.12 CU9 you must first upgrade to StoreFront 3.12 CU9.

Warning:

When you upgrade from versions prior to 3.12, any Desktop Appliance sites in your deployment are automatically removed. As an alternative, Citrix recommend using [Citrix Workspace app Desktop Lock](#) for all non-domain-joined use cases.

Good to know

- Upgrading to the latest StoreFront release from an older that is End of Life is not supported. For more information see [CTX200356](#).
- StoreFront does not support multiple server deployments containing different product versions, so all servers in a server group must be upgraded to the same version before you grant access to the deployment.
- Concurrent upgrade is not supported for multiple server deployments, servers must be upgraded sequentially.
- Before the StoreFront upgrade runs it performs some pre-upgrade checks. If any pre-upgrade check fails, the upgrade does not start and you are notified of the failures. Your StoreFront installation remains unchanged. After fixing the cause of the failures, rerun the upgrade.
- If the StoreFront upgrade itself fails, your existing StoreFront installation may lose its initial configuration. Restore your StoreFront installation to a functional state then rerun the upgrade. To restore StoreFront to a functional state consider the following approaches:
 - restoring the VM snapshot you created before the upgrade,
 - importing the StoreFront configuration you exported before the upgrade, see [Export and import the StoreFront configuration](#),
 - performing the troubleshooting advice in [Troubleshoot StoreFront upgrade issues](#).
- Any StoreFront upgrade failures which occur from the Citrix Virtual Apps and Desktops metainstaller are reported in a dialog, with a link to the relevant failure log.

Get ready to upgrade

Before you start the upgrade, we recommend that you perform the following steps which can prevent upgrade failure:

- Plan your backup strategy before upgrading.
- Verify that you are not attempting to upgrade from an End of Life StoreFront version. For more information see [CTX200356](#).

- Verify that you are upgrading from a supported version of StoreFront to the current version only.
- Download the StoreFront installer from the Citrix website.

Upgrade a single StoreFront server

1. Back up the server by creating a VM snapshot.
2. [Export the existing StoreFront configuration](#). If you have multiple servers in a server group then only export the server group configuration from one server. Provided you have propagated all changes between them, all servers in a server group maintain identical copies of the configuration. This backup allows you to easily build a new server group so that you can easily restore the configuration in case of issues. Note that you will only be able to restore this backup into a server running the same version it was exported from.
3. If you have made modifications to files in `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`, such as `default.ica` and `usernamepassword.tfrm`, back them up for each store. After the upgrade you can restore them to reinstate your modifications.
4. Prevent users from connecting by removing the server from any load balancer or otherwise blocking connections.
5. Restart the server.
6. Ensure that there are no applications running including StoreFront management console, Command line and PowerShell windows or any other applications that could have a lock on StoreFront files. This ensures that all StoreFront files are accessible by the installer during the upgrade. If the installer cannot access any files, they are not replaced and the upgrade fails, resulting in the removal of the existing StoreFront configuration.
7. Ensure you do not have any Windows explorer or command prompts open on directories that contain StoreFront files.
8. Disable any anti-virus applications.
9. Run the installation file for the required version of StoreFront.

To upgrade a StoreFront server group

Upgrading StoreFront server groups involves using one of the servers to remove the other servers from the group. The removed servers retain configuration related to the group, which can prevent them being joined to a new server group. Before they can be reused to build new server groups, or as standalone StoreFront servers, they must be reset to factory defaults, or have StoreFront reinstalled on them. Simultaneously upgrading the servers in a StoreFront server group is not supported.

Example 1: Upgrade a three-node StoreFront server group during scheduled maintenance downtime

This describes upgrading a StoreFront server group of three servers A, B, and C, during scheduled downtime.

1. Disable user access to the server group by disabling the load balancing URL. This prevents users from connecting to the deployment during the upgrade process.
2. Use server A to remove servers B and C from the group.
Servers B and C are now ‘orphaned’ from the server group.
3. Upgrade server A by following the instructions in Upgrade a single StoreFront server.
4. Ensure that server A has been successfully upgraded.
5. On servers B and C, uninstall the currently installed version of StoreFront, then install the new version of StoreFront.
6. Join servers B and C to the upgraded server A to create an upgraded server group. This server group consists of one upgraded server (A) and two freshly installed servers (B and C).
The [Join existing server group](#) process automatically propagates all configuration data and subscription data to new servers B and C.
7. Check all servers are functioning correctly.
8. Enable user access to the upgraded server group by enabling the load balancing URL.

Example 2: Upgrade a three-node StoreFront server group without scheduled downtime

This describes upgrading a StoreFront server group of three servers A, B, and C, without scheduled downtime.

Before upgrading a server group:

1. [Export the StoreFront configuration](#) using **Export-STFConfiguration**. This backup is necessary because servers are factory reset later in the process, which deletes configuration data.
2. Export subscription data from server A using **Export-STFStoreSubscriptions**. This backup is necessary because servers are factory reset later in the process, which deletes subscription data. See [Manage subscription data for a store](#).
3. Disable user access to server C by removing it from the load balancer. This prevents users from connecting to server C during the upgrade process. The load balancer continues to send requests to servers A and B.

4. Use server A to remove server C from the group.
Servers A and B continue to provide access to your users' resources. Server C is now orphaned from the server group, and is factory reset.
5. [Reset the orphaned server C to factory defaults](#) using **Clear-STFDeployment**.
6. [Import the StoreFront configuration](#) you previously exported into server C using **Import-STFConfiguration**. Server C now has an identical configuration to the old server group. It is *not* necessary to repeat this step again later. Only one server needs a copy of the configuration data to propagate it to any other servers that join the group.
7. Upgrade server C by following the instructions in [Upgrade a single StoreFront server](#). Server C now has an identical configuration to the old server group, and is upgraded to a new version of StoreFront.
8. [Import the subscription data](#) which you exported previously into server C. It is *not* necessary to repeat this step again later. Only one server needs a copy of the subscription data to propagate it to any other servers that join the group.
9. Repeat steps 3, 4, 5, and 7 using server B (do not repeat step 6). During this time, only server A is providing users with access to resources. It is therefore recommended to do this step during quiet working periods, where load on the StoreFront server group is expected to be minimal.
10. Join server B to server C using the [Join existing server group](#) process. This gives a single server deployment on the current version of StoreFront (server A), and a new two-node server group on the new StoreFront version (servers B and C).
11. Add servers B and C to the load balancing service so they can take over from server A.
12. Remove server A from the load balancer so that users are directed to the newly upgraded servers B and C.
13. Repeat steps 3, 4, 5, and 7 using server A (do not repeat step 6). The server group upgrade process is now complete. Servers A, B, and C have identical configuration and subscription data from the original group.

Note:

During the brief period when server A is the only accessible server, subscriptions can be lost (step 9). This can cause the new server group to have a slightly outdated copy of the subscription database after upgrade, and any new subscription records to be lost.

This has no functional impact because subscription data is not essential for users to be able to log on and launch resources. Users would, however, need to subscribe to a resource again after server A is factory reset and joined to the newly upgraded group. Although it is unlikely that more than a few subscription records would ever be lost, it is a possible consequence of upgrading a live StoreFront production environment with no downtime.

If the upgrade fails

1. In `C:\Windows\Temp\StoreFront`, open the latest `CitrixMsi*.log` and search for any exception errors.

Thumbs.db Access exceptions: caused by `thumbs.db` files inside `C:\inetpub\wwwroot\citrix` or in its subdirectories. Delete any `thumbs.db` files found.

Cannot get exclusive file access \in use exceptions: restore the snapshot/backup if available, or restart the server, and manually stop any StoreFront services.

Service cannot be started exceptions: restore the snapshot/backup if available, or install the full version of .NET framework 4.5 (not client profile).

2. If there are no exception errors in `CitrixMsi*.log`, check the server's **Event Viewer > Delivery Services** for any errors containing the preceding exception error messages. Follow the corresponding advice.
3. If there are no exception errors in the Event Viewer, check the Admin logs in `C:\Program Files\Citrix\Receiver StoreFront\logs` for any errors containing the preceding exception error messages. Follow the corresponding advice.

For more details of logs files, see [Installation Logs](#).

Reset a server to factory defaults

March 11, 2024

In some situations, there is a need to reset a StoreFront installation to its initial installation state. This is necessary, for example, before you can re-add a StoreFront server to a server group.

A manual uninstall and reinstall can be performed, but this is more time consuming and may cause other unforeseen issues. Instead you can run the **Clear-STFDeployment** PowerShell cmdlet to reset a StoreFront server to a factory default state.

1. Ensure that the StoreFront management console is closed.
2. Open the PowerShell ISE and select **Run as Administrator**.
3. Set the PowerShell path:

```
1 $env:PSModulePath = [Environment]::GetEnvironmentVariable('
   PSModulePath', 'Machine')
2 <!--NeedCopy-->
```

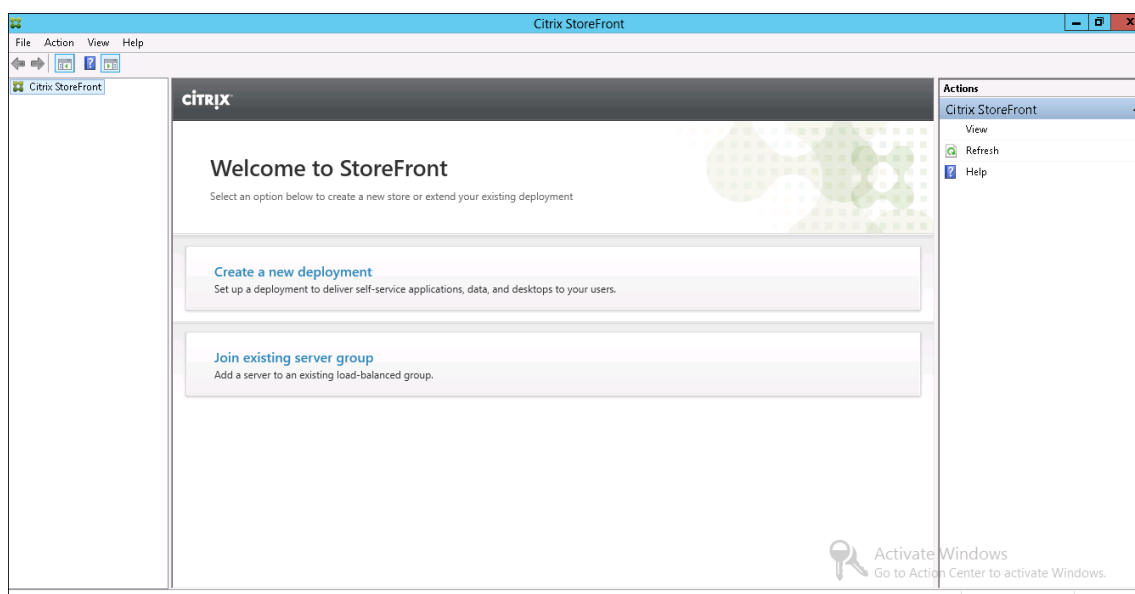
4. Import the Citrix StoreFront module.

```
1 Import-Module citrix.storefront -verbose
2 <!--NeedCopy-->
```

5. After the module is imported, run the **Clear-STFDeployment** command to reset the StoreFront server to the default settings:

```
1 Clear-STFDeployment -Confirm $False
2 <!--NeedCopy-->
```

6. When the command has completed successfully, open the StoreFront management console and confirm that all settings are reset. The options to **Create a new deployment** or **Join existing server group** are available.



Uninstall StoreFront

March 11, 2024

In addition to the product itself, uninstalling StoreFront removes the authentication service, stores, Citrix Receiver for Web sites, XenApp Services URLs, and their associated configurations. The subscription store service containing users' application subscription data is also deleted. In single-server deployments, details of users' application subscriptions are therefore lost. However, in multiple server deployments these data are retained on other servers in the group. Prerequisites enabled by the StoreFront installer, such as the .NET Framework features and the Web Server (IIS) role services, are not removed from the server when StoreFront is uninstalled.

1. Log on to the StoreFront server using an account with local administrator permissions.

2. Close the StoreFront management console if it is open.
3. Close any PowerShell sessions that may have been used to manage StoreFront via its PowerShell SDK.
4. Open the **Start** menu, press **Settings** (cog icon) then go to **Apps**.
5. In the **Programs and Features** windows, select **Citrix StoreFront** and click **Uninstall** to remove all StoreFront components from the server.
6. In the **Uninstall Citrix StoreFront** dialog box, click **Yes**. When the uninstallation is complete, click **OK**.

To manually remove StoreFront

After uninstalling StoreFront, to ensure that StoreFront is completely removed:

1. Remove Web Server Role.
2. Delete the folder *C:\Program Files\Citrix\Receiver StoreFront*.
3. Delete any subdirectories under *C:\Program Files\Citrix\StoreFront Install*.
4. Delete the folder *C:\Inetpub*.

You can now [reinstall StoreFront](#).

Installation logs

For more details of logs files, see [Installation Logs](#).

Configure authentication and delegation

March 11, 2024

Depending on your requirements, there are several authentication and delegations methods.

Method	Detail
Configure authentication	Configure which methods users can use to log into StoreFront through Citrix Workspace app.
Smart card authentication	Set up smart card authentication.
User name and password authentication	Allow users to authenticate using their Active Directory username and password and configure options for changing passwords and password expiry notifications.

Method	Detail
Domain pass-through authentication	Allow Windows devices to single sign on using their Windows credentials.
SAML authentication	Delegate authentication to third party identity providers using SAML.
Federated Authentication Service configuration	Configure StoreFront to integrate with Federated Authentication Service for single sign-on to VDAs

Configure authentication

March 19, 2024




Manage authentication methods

For each store you can choose one or more authentication methods that are available when logging in to the store through Citrix Workspace app.

1. Select the **Store** node in the left pane of the Citrix StoreFront management console and, in the **Actions** pane, click **Manage Authentication Methods**.
2. Specify the access methods that you want to enable for your users.

Manage Authentication Methods - Store

Select the methods which users will use to authenticate and access resources. i

Method	Settings
<input checked="" type="checkbox"/> User name and password	 ▼
<input type="checkbox"/> SAML Authentication	 ▼
<input checked="" type="checkbox"/> Domain pass-through Can be enabled / disabled separately on Receiver for Web sites	
<input type="checkbox"/> Smart card Can be enabled / disabled separately on Receiver for Web sites	
<input type="checkbox"/> HTTP Basic	
<input checked="" type="checkbox"/> Pass-through from Citrix Gateway	 ▼

Installing and uninstalling the authentication methods and the authentication service settings are included in the advanced options. Advanced ▼

- Select the **Username and password** check box to enable explicit active directory username and password authentication. For more information, see [User name and password authentication](#).
- Select the **SAML Authentication** check box to enable integration with a SAML Identity Provider. For more information, see [SAML authentication](#).
- Select **Domain pass-through** to enable pass-through of Active Directory domain credentials from users' devices. For more information, see [Domain pass-through authentication](#).
- Select **Smart card** to enable smart card authentication. For more information, see [Smart card authentication](#).
- Select **HTTP Basic** to enable HTTP Basic authentication. Users authenticate with the StoreFront server's IIS web server.
- Select **Pass-through from Citrix Gateway** to enable pass-through authentication from Citrix Gateway. Enable this if users connect to StoreFront through a Citrix Gateway with authentication enabled. For more information, see [Pass-through from Citrix Gateway](#).

Modifying the authentication methods for a store also updates the authentication methods used when accessing the store through a web browser. To change authentication methods when logging on through a web browser see [Authentication Methods](#).

Manage authentication methods using PowerShell SDK

To configure authentication using the [PowerShell SDK](#):

1. Call [Get-STFAuthenticationService](#) to get the authentication service for a store or a virtual directory and to view its current configuration.
2. On the authentication service, enable or disable the required authentication protocols. To get a list of available protocols, run [Get-STFAuthenticationServiceProtocol](#). To enable the protocols, run [Enable-STFAuthenticationServiceProtocol](#) with a list of protocols to enable. To disable the protocols, run [Disable-STFAuthenticationServiceProtocol](#) with the list of protocols to disable.
3. Configure the authentication protocols you have enabled. For details, see the documentation for each protocol.

Shared authentication service settings

Use the Shared Authentication Service Settings task to specify stores that share the authentication service enabling single sign-on between them.

1. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the **Actions** pane, click **Manage Authentication Methods**.
2. From the **Advanced** drop-down menu, select **Shared authentication service settings**.
3. Click the **Use shared authentication service** check box and select a store from the **Store** name drop-down menu.

Note:

There is no functional difference between a shared and dedicated authentication service. An authentication service shared by more than two stores is treated as a shared authentication service and any configuration changes affect the access to all the stores using the shared authentication service.

Smart card authentication

April 9, 2024

Users authenticate using smart cards and PINs when they access their stores. When you install StoreFront, smart card authentication is disabled by default. Smart card authentication can be enabled for users connecting to stores through Citrix Workspace app, web browsers, and XenApp Services URLs.

Use smart card authentication to streamline the logon process for your users while also enhancing the security of user access to your infrastructure. Access to the internal corporate network is protected by certificate-based two-factor authentication using the public key infrastructure. Private keys are protected by hardware controls and never leave the smart card. Your users get the convenience of accessing their desktops and applications from a range of corporate devices using their smart cards and PINs.

You can use smart cards for user authentication through StoreFront to desktops and applications provided by Citrix Virtual Apps and Desktops. Smart card users logging on to StoreFront can also access applications provided by the Endpoint Management. However, users must authenticate again to access Endpoint Management web applications that use client certificate authentication.

To enable smart card authentication, users' accounts must be configured either within the Microsoft Active Directory domain containing the StoreFront servers or within a domain that has a direct two-way trust relationship with the StoreFront server domain. Multi-forest deployments involving two-way trusts are supported.

The configuration of smart card authentication with StoreFront depends on the user devices, the clients installed, and whether the devices are domain-joined. In this context, domain-joined means devices that are joined to a domain within the Active Directory forest containing the StoreFront servers.

The document [Smart card configuration for Citrix environments](#) describes how to configure a Citrix deployment for smart cards uses a specific smart card type. Similar steps apply to smart cards from other vendors.

Prerequisites

- Ensure that accounts for all users are configured either within the Microsoft Active Directory domain in which you plan to deploy your StoreFront servers or within a domain that has a direct two-way trust relationship with the StoreFront server domain.
- If you plan to enable pass-through with smart card authentication, ensure that your smart card reader types, middleware type and configuration, and middleware PIN caching policy permit this.
- Install your vendor's smart card middleware on the virtual or physical machines running the Virtual Delivery Agent that provide users' desktops and applications. For more information about using smart cards with Citrix Virtual Desktops, see [Smart cards](#).
- Ensure that your public-key infrastructure is configured appropriately. Check that certificate to account mapping is configured correctly for your Active Directory environment and that user certificate validation can be performed successfully.

Configure StoreFront

- You must use HTTPS for communications between StoreFront and users' devices to enable smart card authentication. See [Secure StoreFront using HTTPS](#).
- To enable smart card authentication when connecting to a store through Citrix Workspace Apps, in the [Authentication Methods](#) tick or untick **Smart card**.
- Enabling smart card authentication for a store by default also enables it for all websites for that store. You can independently enable or disable smart card authentication for a specific website on the [Manage Receiver for Web Sites Authentication methods tab](#).
- If you configure both smart card and username and password authentication, users are initially prompted to log on using their smart cards and PINs but have the option to select explicit authentication if they experience any issues with their smart cards.

Configure Delivery Controller to trust StoreFront

When using smart card authentication, StoreFront does not have access to the user's credentials so is unable to authenticate to Citrix Virtual Apps and Desktops. You must therefore configure the Delivery Controller to trust requests from StoreFront, see [Citrix Virtual Apps and Desktops Security considerations and best practices](#).

Remote access via Citrix Gateway

For remote access, you can enable smart card on the Citrix Gateway and then enable pass-through authentication to StoreFront with Delegated authentication. For more details see [Gateway pass-through](#).

To ensure that users do not receive an additional prompt for their credentials at the virtual server when connections to their resources are established, create a second gateway and disable client authentication in the Secure Sockets Layer (SSL) parameters. For more information, see [Configuring smart card authentication](#). When accessing StoreFront via a gateway with Smartcard authentication. Configure optimal Citrix Gateway routing through this virtual server for connections to the deployments providing the desktops and applications for the store. For more information, see [Configure optimal HDX routing for a store](#).

Single sign-on to VDAs

You can enable single sign-on to the VDAs by passing-through users' smart card credentials. The store can be accessed through a web browser or Citrix Workspace app for Windows but the resource must

be opened in Citrix Workspace app for Windows. On other operating systems or when accessing the resources through a browser, users must re-enter their credentials when connecting to a VDA.

1. Include the Single Sign on component when installing Citrix Workspace for Windows and configure it for Single sign on. See [Configure domain pass-through authentication](#).
2. Use a text editor to open the default.ica file for the store. See [Default ica](#).
3. To enable pass-through of smart card credentials for users who access stores without Citrix Gateway, add the following setting in the [Application] section.

`DisableCtrlAltDel=Off`

This setting applies to all users of the store. To enable both domain pass-through and pass-through with smart card authentication to desktops and applications, you must create separate stores for each authentication method. Then, direct your users to the appropriate store for their method of authentication.

4. To enable pass-through of smart card credentials for users accessing stores through Citrix Gateway, add the following setting in the [Application] section.

`UseLocalUserAndPassword=On`

This setting applies to all users of the store. To enable pass-through authentication for some users and require others to log on to access their desktops and applications, you must create separate stores for each group of users. Then, direct your users to the appropriate store for their method of authentication.

Single sign-on to VDAs using FAS

Alternatively you can configure [Federated Authentication Service](#) to single sign-on to VDAs when using locally installed Citrix Workspace app but not Citrix Workspace app for HTML5.

Important considerations

Use of smart cards for user authentication with StoreFront is subject to the following requirements and restrictions.

- To use virtual private network (VPN) tunnels with smart card authentication, users must install the Citrix Gateway plug-in and log on through a webpage, using their smart cards and PINs to authenticate at each step. Pass-through authentication to StoreFront with the Citrix Gateway plug-in isn't available for smart card users.
- Multiple smart cards and multiple readers can be used on the same user device, but if you enable pass-through with smart card authentication, users must ensure that only one smart card is inserted when accessing a desktop or application.

- When a smart card is used within an application, such as for digital signing or encryption, users might see extra prompts to insert a smart card or enter a PIN. This can occur if more than one smart card has been inserted at the same time. It can also occur due to configuration settings - such as middleware settings like PIN caching that are typically configured using group policy. Users who are prompted to insert a smart card when the smart card is already in the reader must click Cancel. If users are prompted for a PIN, they must enter their PINs again.
- If you enable pass-through with smart card authentication to Citrix Virtual Apps and Desktops for Citrix Workspace app for Windows users with domain-joined devices who do not access stores through Citrix Gateway, this setting applies to all users of the store. To enable both domain pass-through and pass-through with smart card authentication to desktops and applications, you must create separate stores for each authentication method. Your users must then connect to the appropriate store for their method of authentication.
- If you enable pass-through with smart card authentication to Citrix Virtual Apps and Desktops for Citrix Workspace app for Windows users with domain-joined devices accessing stores through Citrix Gateway, this setting applies to all users of the store. To enable pass-through authentication for some users and require others to log on to their desktops and applications, you must create separate stores for each group of users. Then, direct your users to the appropriate store for their method of authentication.
- Only one authentication method can be configured for each XenApp Services URL and only one URL is available per store. If you need to enable other types of authentication in addition to smart card authentication, you must create separate stores, each with a XenApp Services URL, for each authentication method. Then, direct your users to the appropriate store for their method of authentication.
- When StoreFront is installed, the default configuration in Microsoft Internet Information Services (IIS) only requires that client certificates are presented for HTTPS connections to the certificate authentication URL of the StoreFront authentication service. IIS does not request client certificates for any other StoreFront URLs. This configuration enables you to provide smart card users with the option to fall back to explicit authentication if they experience any issues with their smart cards. Subject to the appropriate Windows policy settings, users can also remove their smart cards without needing to reauthenticate.

If you decide to configure IIS to require client certificates for HTTPS connections to all StoreFront URLs, the authentication service and stores must be colocated on the same server. You must use a client certificate that is valid for all the stores. With this IIS site configuration, smart card users can't connect through Citrix Gateway and can't fall back to explicit authentication. Users must log on again if they remove their smart cards from their devices.

Domain pass-through authentication

April 9, 2024

Users authenticate to their domain-joined Windows computers, and their credentials are used to log them into Citrix Workspace app automatically. This is supported through Citrix Workspace app for Windows and from the following web browsers on Windows:

- Internet Explorer
- Microsoft Edge
- Google Chrome
- Mozilla Firefox

StoreFront Configuration

To enable domain pass-through for Citrix Workspace Apps for Windows, in the [Authentication Methods](#) select **Domain pass-through**.

Enabling domain pass-through authentication for a store by default also enables it for Citrix Workspace app for HTML5 for all websites for that store. You can disable domain pass-through authentication for a specific website on the [Manage Receiver for Web Sites Authentication methods](#) tab.

Configure Delivery Controller to trust StoreFront

When using domain pass-through authentication, StoreFront does not have access to the user's credentials so is unable to authenticate to Citrix Virtual Apps and Desktops. You must therefore configure the Delivery Controller to trust requests from StoreFront, see [Citrix Virtual Apps and Desktops Security considerations and best practices](#).

Single sign-on to VDAs

To single sign-in to VDAs, you must use Citrix Workspace app for Windows with the **Enable single sign-on** component, see [Configure domain pass-through authentication](#). If using Citrix Workspace app for HTML5 then it must be configured to connect to resources in Citrix Workspace app for Windows rather than the browser.

Citrix Workspace app for Windows configuration

To enable domain pass-through to single sign-on to the store and VDAs using Citrix Workspace app for Windows, see [Citrix Workspace app for Windows documentation](#).

Citrix Workspace app for HTML5 configuration

You may need to update users' web browser configuration to allow domain pass-through authentication. You can use domain pass-through to sign into a store through a web browser. To single sign-on to the VDAs, users must open resources in Citrix Citrix Workspace app for Windows rather than the web browser.

Internet Explorer, Edge and Chrome Most web browsers use Windows Internet Explorer zones configuration to decide whether to enable single sign-on. By default it is only enabled for sites in the Local Intranet Zone. To add your site to the intranet zone:

1. Open Control Panel
2. Open Internet Options
3. Go to the **Security** tab.
4. Select **Local intranet**
5. Click **Sites**.
6. Click **Advanced**.
7. Add your StoreFront website.

These settings can be deployed using group policy.

Firefox Modify the browser advanced settings to trust the StoreFront website URI for single sign-on.

Warning:

Editing the advanced settings incorrectly can cause serious problems. Make edits at your own risk.

1. Open Firefox on the computer that will authenticate using domain pass-through.
2. In the address bar, type about:config.
3. Click "I accept the risk!".
4. In the Search bar, type negotiate.
5. Double-click network.negotiate-auth.delegation-uris.
6. Enter the name of your corporate Windows domain (for example, mydomain.com).
7. Click OK.
8. Double-click network.negotiate-auth.trusted-uris.
9. Enter the name of your corporate Windows domain (for example, mydomain.com).
10. Click OK.
11. Close and Restart Firefox.

Single sign-on to VDAs using FAS

Alternatively you can configure [Federated Authentication Service](#) to single sign-on to VDAs when using locally installed Citrix Workspace app but not Citrix Workspace app for HTML5.

Pass-through from Citrix Gateway

March 19, 2024

Users authenticate to Citrix Gateway and are automatically logged on when they access their stores. Pass-through from Citrix Gateway authentication is enabled by default when you first configure remote access to a store. Users can connect through Citrix Gateway to stores using Citrix Workspace app or a web browser. For more information about configuring StoreFront for Citrix Gateway, see [Configure a Citrix Gateway](#).

StoreFront supports pass-through with the following Citrix Gateway authentication methods.

- **Domain** Users log on using their Active Directory username nad password.
- **RSA** Users log on to Citrix Gateway using passcodes that are derived from tokencodes generated by security tokens combined, sometimes, with personal identification numbers. If you enable pass-through authentication by security token only, ensure that the resources you make available do not require extra or alternative forms of authentication, such as users' Microsoft Active Directory domain credentials.
- **Smart card** Users log on using smart cards
- **RSA + Domain** Users logging on to Citrix Gateway are required to enter both their domain credentials and security token passcodes.

If on the Citrix Gateway you have disabled authentication or you have disabled single-sign-on then pass-through is not used and you must configure one of the other authentication methods.

If you configure double-source authentication to Citrix Gateway for remote users accessing stores from within Citrix Workspace app, you must create two authentication policies on Citrix Gateway. Configure RADIUS (Remote Authentication Dial-In User Service) as the primary authentication method and LDAP (Lightweight Directory Access Protocol) as the secondary method. Modify the credential index to use the secondary authentication method in the session profile so that LDAP credentials are passed to StoreFront. When you add the Citrix Gateway appliance to your StoreFront configuration, set the Logon type to Domain and security token. For more information, see <http://support.citrix.com/article/CTX125364>

To enable multi domain authentication through Citrix Gateway to StoreFront, set SSO Name Attribute to userPrincipalName in the Citrix Gateway LDAP authentication policy for each domain. You can require users to specify a domain on the Citrix Gateway logon page so that the appropriate LDAP policy

to use can be determined. When you configure the Citrix Gateway session profiles for connections to StoreFront, do not specify a single sign-on domain. You must configure trust relationships between each of the domains. Ensure that you allow users to log on to StoreFront from any domain by not restricting access to explicitly trusted domains only.

Where supported by your Citrix Gateway deployment, you can use SmartAccess to control user access to Citrix Virtual Apps and Desktops resources based on Citrix Gateway session policies.

Enable Gateway pass-through

To enable or disable gateway pass-through authentication for a store when connecting through Workspace apps, in the [Authentication Methods](#) window tick or untick **Pass-through from Citrix Gateway**.

Enabling Citrix Gateway pass-through authentication for a store by default also enables it for all websites for that store. You can disable username and password authentication for a specific website on the [Authentication methods](#) tab.

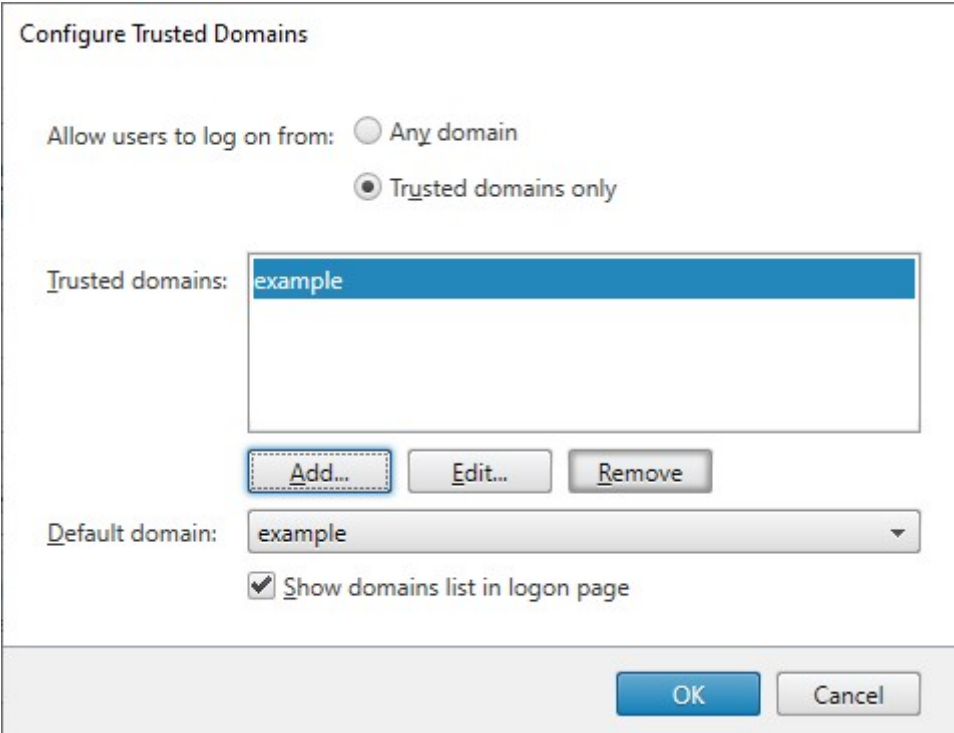
Configure trusted user domains

If your Citrix Gateway is configured to use LDAP authentication, you can restrict access to specific domains.

1. In the “Manage Authentication methods” window, from the **Pass-through from Citrix Gateway** > **Settings** drop-down menu, select **Configure Trusted Domains**.
2. Select **Trusted Domains only** and click **Add** to enter the name of a trusted domain. Users with accounts in that domain are able to log on to all stores that use the authentication service. To modify a domain name, select the entry in the Trusted domains list and click **Edit**. To discontinue access to stores for user accounts in a domain, select the domain in the list and click **Remove**.

The way in which you specify the domain name determines the format in which users must enter their credentials. If you want users to enter their credentials in domain user name format, add the NetBIOS name to the list. To require that users to enter their credentials in user principal name format, add the fully qualified domain name to the list. If you want to enable users to enter their credentials in both domain user name format and user principal name format, you must add both the NetBIOS name and the fully qualified domain name to the list.

3. If you configure multiple trusted domains, select from the Default domain list the domain that is selected by default when users log on.
4. If you want to list the trusted domains on the logon page, select the Show domains list in the logon page check box.



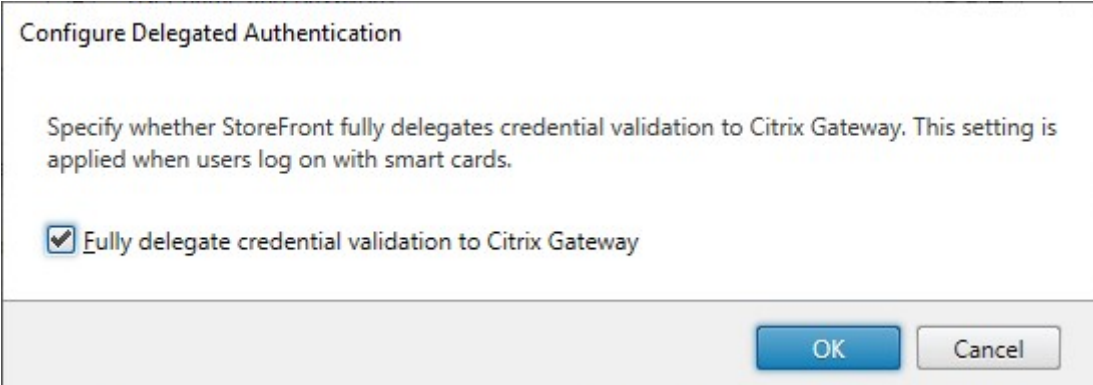
The 'Configure Trusted Domains' dialog box contains the following elements:

- Allow users to log on from:** Two radio buttons. 'Any domain' is unselected, and 'Trusted domains only' is selected.
- Trusted domains:** A list box containing the text 'example'.
- Buttons:** 'Add...', 'Edit...', and 'Remove' buttons are located below the list box.
- Default domain:** A dropdown menu with 'example' selected.
- Checkbox:** A checked checkbox labeled 'Show domains list in logon page'.
- Footer:** 'OK' and 'Cancel' buttons.

Delegate credential validation to Citrix Gateway

By default StoreFront validates the username and password it receives from the Gateway. If your Citrix Gateway is configured to use passwordless authentication methods such as smart card you must configure StoreFront so that it does not validate the credentials and so is reliant on the Gateway's authentication. In this case, it is recommended that you enter a callback URL when configuring the gateway so StoreFront can verify the request came from the gateway, see [Manage Citrix Gateways](#).

1. In the **Manage Authentication Methods** window, from the **Pass-through from Citrix Gateway** > **Settings** drop-down menu, select **Configure Delegated Authentication**.
2. Select **Fully delegate credential validation to citrix gateway**.



The 'Configure Delegated Authentication' dialog box contains the following elements:

- Text:** 'Specify whether StoreFront fully delegates credential validation to Citrix Gateway. This setting is applied when users log on with smart cards.'
- Checkbox:** A checked checkbox labeled 'Fully delegate credential validation to Citrix Gateway'.
- Footer:** 'OK' and 'Cancel' buttons.

PowerShell SDK

To configure the store to delegate authentication to the gateway using the PowerShell SDK, use cmdlet `Set-STFCitrixAGBasicOptions` to set `CredentialValidationMode` to `Auto`. To configure StoreFront to validate the credentials, set `CredentialValidationMode` to `Password`.

Allow users to change expired passwords at logon

If your Citrix Gateway is configured to use LDAP (username and password) authentication then you can configure NetScaler to allow changing expired passwords on log-in.

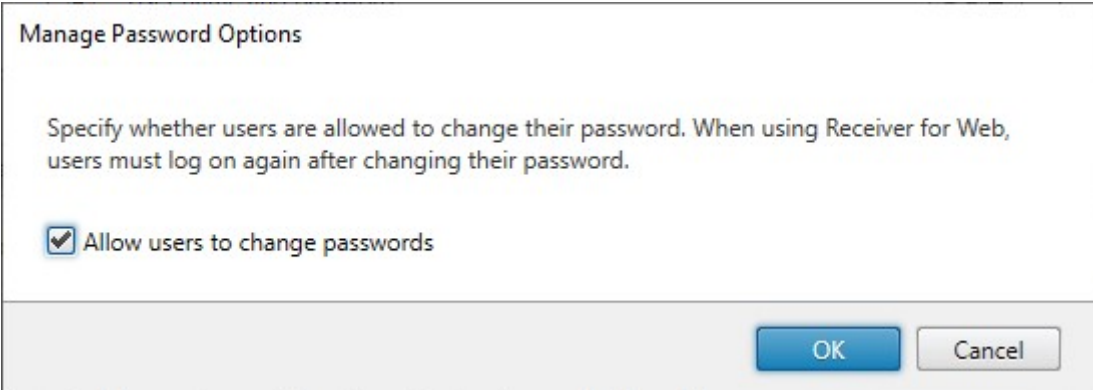
1. Log into the NetScaler administration website
2. On the side menu go to **Authentication > Dashboard**.
3. Click the authentication server.
4. Under **Other Settings** tick **Allow Password Change**.

Allow users to change passwords after logon

With **Pass-through from Citrix Gateway**, the Citrix Gateway is responsible for handling authentication. You can configure StoreFront to allow users to change their passwords after logging on. This functionality is only available when accessing StoreFront stores through Citrix Workspace app for HTML5, not locally installed Citrix Workspace apps.

The default StoreFront configuration prevents users from changing their passwords, even if the passwords have expired. If you decide to enable this feature, ensure that the policies for the domains containing your servers do not prevent users from changing their passwords. Enabling users to change their passwords exposes sensitive security functions to anyone who can access any of the stores that use the authentication service. If your organization has a security policy that reserves user password change functions for internal use only, ensure that none of the stores are accessible from outside your corporate network.

1. In the **Manage Authentication Methods** window, from the **Pass-through from Citrix Gateway > Settings** drop-down menu, select **Manage Password Options**
2. To allow users to change passwords, select **Allow users to change passwords** check box.



Manage Password Options

Specify whether users are allowed to change their password. When using Receiver for Web, users must log on again after changing their password.

☒ Allow users to change passwords

OK Cancel

Note:

If you select or clear **Allow users to change passwords**, this also affects settings under **Manage Password Options** for [Username and password](#) authentication.

PowerShell SDK

To modify change password options using the PowerShell SDK, use cmdlet [Set-STFExplicitCommonOptions](#).

Configure Delivery Controller to trust StoreFront

When the Citrix Gateway is configured with LDAP authentication, it passes the credentials through to StoreFront. For other authentication methods, StoreFront does not have access to the credentials so is unable to authenticate to Citrix Virtual Apps and Desktops. You must therefore configure the Delivery Controller to trust requests from StoreFront, see [Citrix Virtual Apps and Desktops Security considerations and best practices](#).

Single sign-on to VDAs using Federated Authentication Service

When the gateway is configured with LDAP authentication, it passes the credentials through to StoreFront so that it can single sign-on to VDAs. For other authentication methods, StoreFront does not have access to the credentials so single sign-on is not available by default. You can use [Federated Authentication Service](#) to provide single sign on.

SAML authentication

March 19, 2024

SAML (Security Assertion Markup Language) is an open standard used by identity and authentication products. Using SAML, you can configure StoreFront to redirect users to an external identity provider for authentication.

Note

Configure StoreFront with SAML authentication for internal access. For external access [configure Citrix Gateway with SAML authentication](#) then configure StoreFront with Gateway pass-through authentication.

StoreFront requires a SAML 2.0-compliant identity provider (IdP) such as:

- Microsoft AD Federation Services using SAML bindings (not WS-Federation bindings). For more information, see [AD FS Deployment](#) and [AD FS Operations](#).
- Citrix Gateway (configured as an IdP).
- Microsoft Entra ID. For more information, see [CTX237490](#).

The SAML assertion must contain a `saml:Subject` attribute containing the user's UPN.

To enable or disable SAML authentication for a store when connecting through Workspace apps, in the [Authentication Methods](#) window select **SAML Authentication**. Enabling SAML authentication for a store by default also enables it for all websites for that store. You can independently configure SAML for a particular website on the [Authentication methods](#) tab.

StoreFront SAML Endpoints

To configure SAML, your identity provider may require the following endpoints:

- The URL of the Entity ID. This is the path to the auth service of the store, normally `https://[storefront host]/Citrix/[StoreName]Auth`
- The URL of the Assertion Consumer Service, normally `https://[storefront host]/Citrix/[StoreName]Auth/Saml`
- The Metadata service, normally `https://[storefront host]/Citrix/[StoreName]Auth/SamlForms/ServiceProvider`

In addition there is a test endpoint, normally `https://[storefront host]/Citrix/[StoreName]Auth/SamlTest`

You can use the following PowerShell script to list out the endpoints for a specified store.

```
1 # Change this value for your Store
2 $storeVirtualPath = "/Citrix/Store"
3
4 $auth = Get-STFAuthenticationService -Store (Get-STFStoreService -
    VirtualPath $storeVirtualPath)
5 $spId = $auth.AuthenticationSettings["samlForms"].SamlSettings.
    ServiceProvider.Uri.AbsoluteUri
6 $acs = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.
    VirtualPath + "/SamlForms/AssertionConsumerService")
```

```
7 $md = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.  
    VirtualPath + "/SamlForms/ServiceProvider/Metadata")  
8 $samlTest = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.  
    VirtualPath + "/SamlTest")  
9 Write-Host "SAML Service Provider information:  
10 Entity ID: $spId  
11 Assertion Consumer Service: $acs  
12 Metadata: $md  
13 Test Page: $samlTest  
14 <!--NeedCopy-->
```

Example of the output:

```
1 SAML Service Provider information:  
2 Entity ID: https://storefront.example.com/Citrix/StoreAuth  
3 Assertion Consumer Service: https://storefront.example.com/Citrix/  
    StoreAuth/SamlForms/AssertionConsumerService  
4 Metadata: https://storefront.example.com/Citrix/StoreAuth/SamlForms/  
    ServiceProvider/Metadata  
5 Test Page: https://storefront.example.com/Citrix/StoreAuth/SamlTest  
6 <!--NeedCopy-->
```

Configure using Metadata exchange

To simplify configuration, you can exchange metadata (identifiers, certificates, endpoints and other configuration) between the Identity Provider and the Service Provider, which is StoreFront in this case.

If your Identity Provider supports metadata import, then you can point it at the StoreFront MetaData endpoint. **Note:** This must be done over HTTPS.

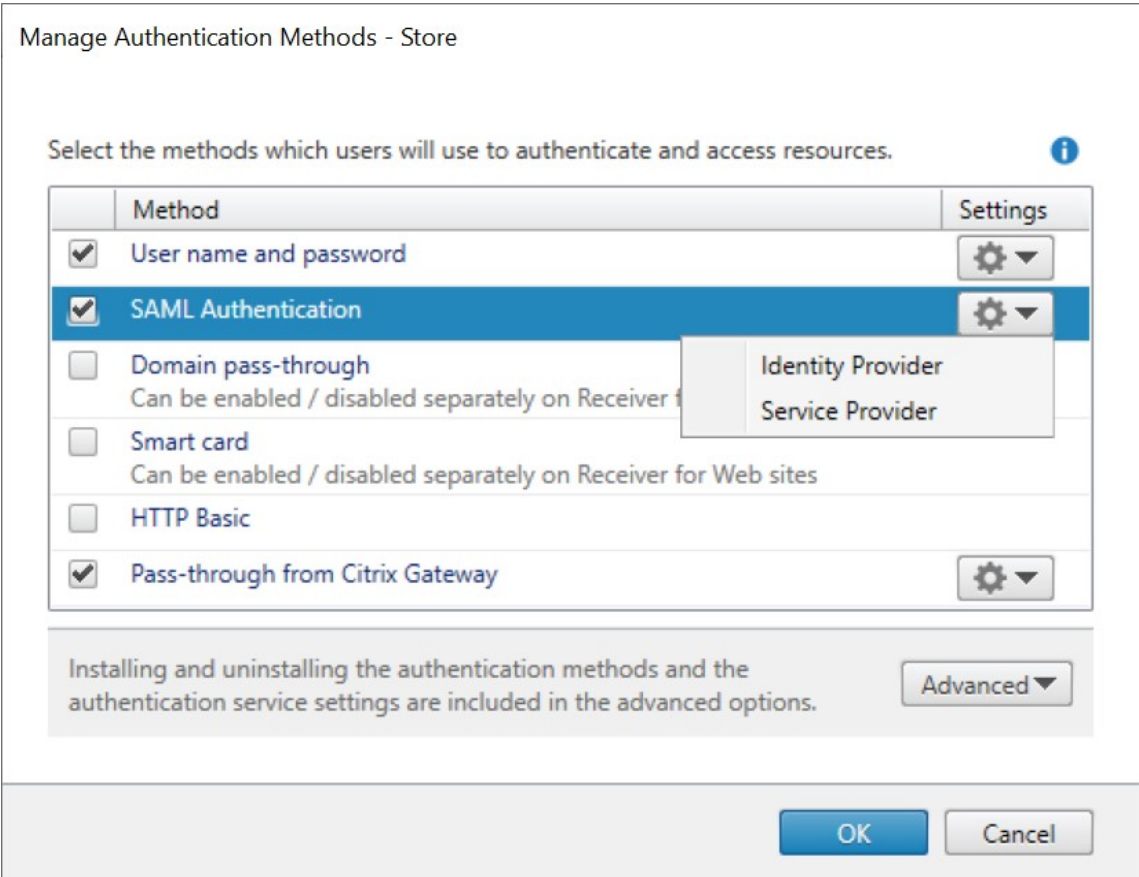
To configure StoreFront using the metadata from an Identity Provider, use the [Update-STFSamlIdPFromMetadata](#) cmdlet, for example:

```
1 Get-Module "Citrix.StoreFront*" -ListAvailable | Import-Module  
2  
3 # Remember to change this with the virtual path of your Store.  
4 $StoreVirtualPath = "/Citrix/Store"  
5  
6 $store = Get-STFStoreService -VirtualPath $StoreVirtualPath  
7 $auth = Get-STFAuthenticationService -StoreService $store  
8  
9 # To read the metadata directly from the Identity Provider, use the  
    following:  
10 # Note again this is only allowed for https endpoints  
11 Update-STFSamlIdPFromMetadata -AuthenticationService $auth -Url https:  
    //example.com/FederationMetadata/2007-06/FederationMetadata.xml  
12  
13 # If the metadata has already been download, use the following:  
14 # Note: Ensure that the file is encoded as UTF-8
```

```
15 Update-STFSamlIdPFromMetadata -AuthenticationService $auth -FilePath "C
16 :\\Users\\exampleusername\\Downloads\\FederationMetadata.xml"
16 <!--NeedCopy-->
```

Configure Identity Provider

- 1. Click the settings drop down in the **SAML Authentication** row and click **Identity Provider**.



Identity Provider

Identity Provider

StoreFront uses this information to configure the trust to the Identity Provider.

SAML Binding ⓘ Post

Address ⓘ

Signing Certificates

Subject Name	Thumbprint

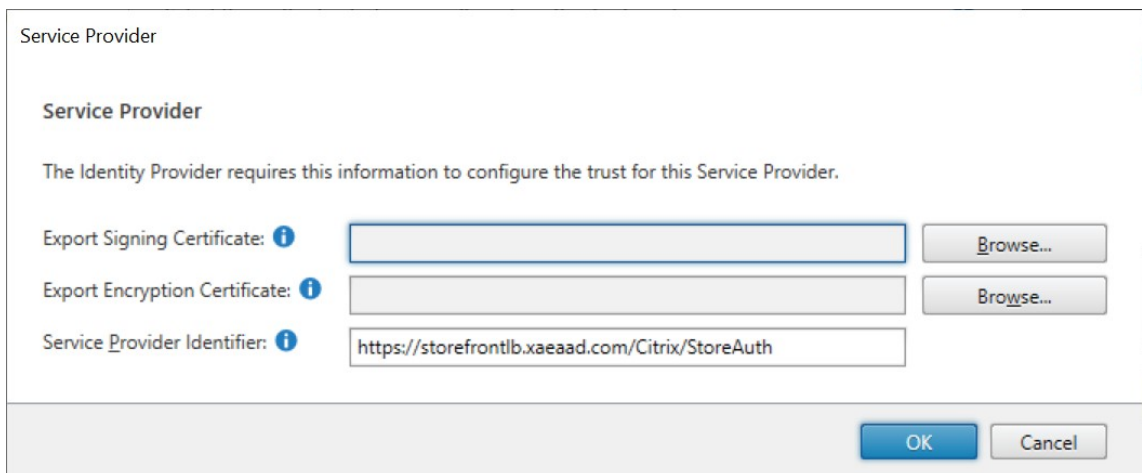
Add... Import... Edit... Remove

OK Cancel

2. Choose **SAML Binding** of **Post** or **Redirect**.
3. Enter the **Address** of the Identity Provider.
4. Import the certificate used to sign the SAML tokens.
5. Press **OK** to save changes.

Configure Service Provider


1. Click the settings drop down in the **SAML Authentication** row and click **Service Provider**.





Service Provider

Service Provider

The Identity Provider requires this information to configure the trust for this Service Provider.

Export Signing Certificate: 

Export Encryption Certificate: 

Service Provider Identifier: 

2. Optionally, choose an **Export Signing Certificate**, used to sign messages to the identity provider.
3. Optionally, choose an **Export Encryption Certificate**, used to decrypt messages received from the identity provider.
4. The **Service Provider Identifier** is pre-filled with the authentication service for the store.
5. Press **OK** to save changes.

PowerShell SDK

Using the PowerShell SDK:

- To import a signing certificate call cmdlet [Import-STFSamlSigningCertificate](#).
- To import an encryption certificate call cmdlet [Import-STFSamlEncryptionCertificate](#).

Testing

To test the SAML integration:

1. Go to the SAML test page, see StoreFront SAML Endpoints.
2. This redirects you to the identity provider. Enter your credentials.
3. You are redirected back to the test page that displays the identity claims and assertions.

Configure Delivery Controller to trust StoreFront

When using SAML authentication, StoreFront does not have access to the user's credentials so is unable to authenticate to Citrix Virtual Apps and Desktops. You must therefore configure the Delivery Controller to trust requests from StoreFront, see [Citrix Virtual Apps and Desktops Security considerations and best practices](#).

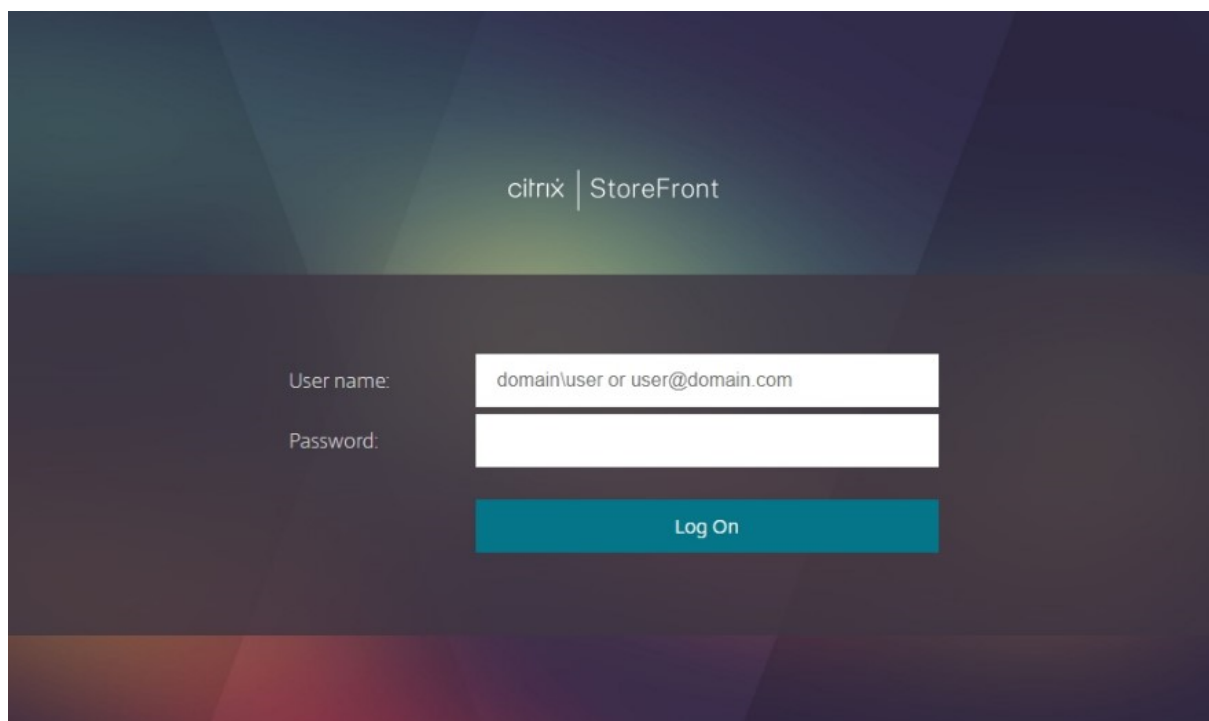
Single sign-on to VDAs using Federated Authentication Service

When using SAML authentication, StoreFront does not have access to the user's credentials so single sign-on to VDAs is not available by default. You can use [Federated Authentication Service](#) to provide single sign-on.

User name and password authentication

March 11, 2024

With username and password authentication, users enter their active directory credentials.



To enable or disable username and password authentication for a store when connecting through Workspace apps, in the [Authentication Methods](#) window tick or untick **User name and password**.

Enabling username and password authentication for a store by default also enables it for all websites for that store. You can disable username and password authentication for a specific website on the [Manage Receiver for Web Sites Authentication methods](#) tab.

Configure trusted user domains

You can restrict access to stores for users logging on with explicit domain credentials, either directly or using pass-through authentication from Citrix Gateway.

1. Select the Stores node in the left pane of the Citrix StoreFront management console and, in the results pane, select the appropriate authentication method. In the Actions pane, click **Manage Authentication Methods**.
2. From the **User name and password > Settings** list, select **Configure Trusted Domains**.
3. Select **Trusted Domains only** and click **Add** to enter the name of a trusted domain. Users with accounts in that domain are able to log on to all stores that use the authentication service. To modify a domain name, select the entry in the Trusted domains list and click **Edit**. To discontinue access to stores for user accounts in a domain, select the domain in the list and click **Remove**.

The way in which you specify the domain name determines the format in which users must enter their credentials. If you want users to enter their credentials in domain user name format, add the NetBIOS name to the list. To require that users to enter their credentials in user principal name format, add the fully qualified domain name to the list. If you want to enable users to enter their credentials in both domain user name format and user principal name format, you must add both the NetBIOS name and the fully qualified domain name to the list.

4. If you configure multiple trusted domains, select from the Default domain list the domain that is selected by default when users log on.
5. If you want to list the trusted domains on the logon page, select the Show domains list in the logon page check box.

Configure Trusted Domains

Allow users to log on from: ☐ Any domain ☒ Trusted domains only

Trusted domains:

Default domain:

☒ Show domains list in logon page

Enable users to change their passwords

You can allow users to change their passwords at any time. Alternatively, you can restrict password changes to users whose passwords have expired. This means you can ensure that users are never prevented from accessing their desktops and applications by an expired password.

Change password functionality is available in the following clients:

	User can change an expired password if enabled on StoreFront	User is notified that password will expire	User can change password before it expires if enabled on StoreFront
Citrix Workspace apps			
Windows	Yes		
Mac	Yes		
Android			
iOS			
Linux	Yes		
Web	Yes	Yes	Yes

The default configuration prevents Citrix Workspace app and web browser users from changing their passwords, even if the passwords have expired. If you decide to enable this feature, ensure that the policies for the domains containing your servers do not prevent users from changing their passwords. Enabling users to change their passwords exposes sensitive security functions to anyone who can access any of the stores that use the authentication service. If your organization has a security policy that reserves user password change functions for internal use only, ensure that none of the stores are accessible from outside your corporate network.

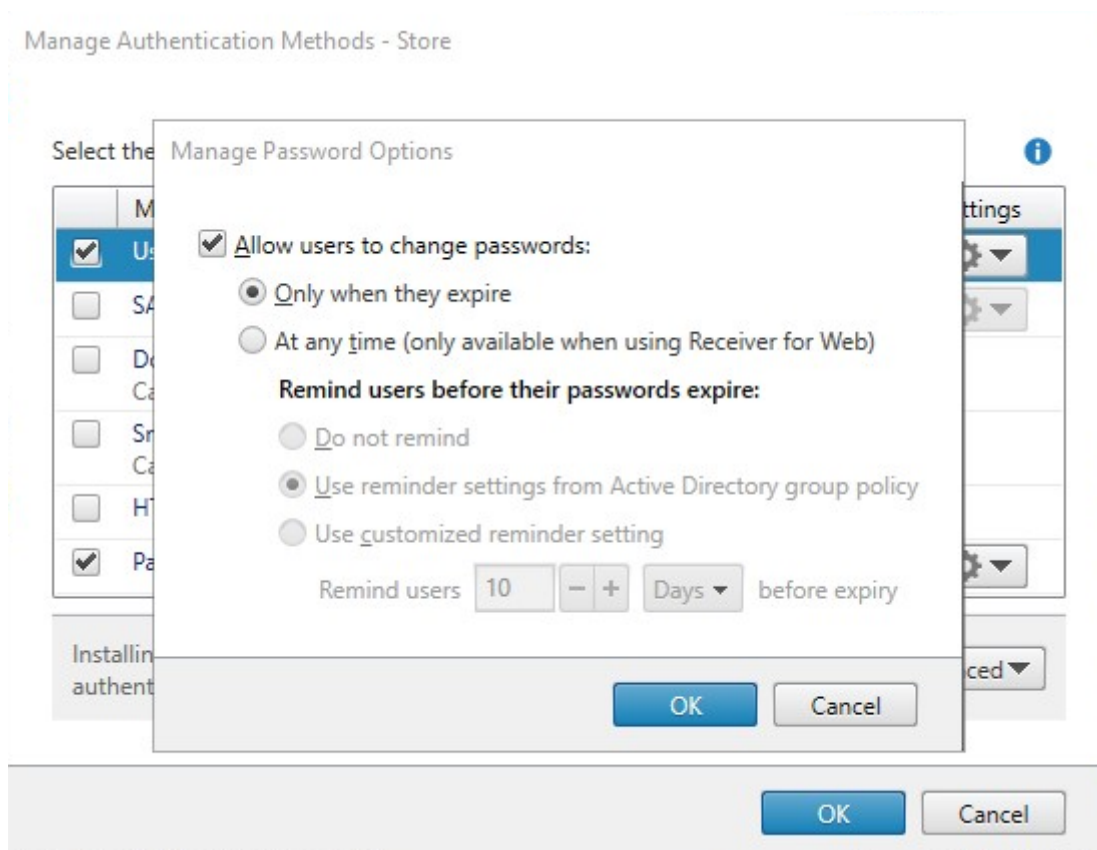
If you allow users to change their passwords at any time, local users whose passwords are about to expire are shown a warning when they log on. By default, the notification period for a user is determined by the applicable Windows policy setting. Alternatively you can configure a custom notification period.

1. In the **Manage Authentication Methods** window, from the **User name and password > Settings** drop-down menu, select **Manage Password Options**
2. To allow users to change passwords, check **Allow users to change passwords** check box.

Note:

If you do not select this option, you must make your own arrangements to support users who can't access their desktops and applications because their passwords have expired.

3. Choose whether to allow users to change passwords **Only when they expire** or **At any time**.
4. Choose whether to remind users before their passwords expire.

**Note 1:**

StoreFront does not support Fine-Grained Password Policies in Active Directory.

Note 2:

Ensure that there's sufficient disk space on your StoreFront servers to store profiles for all your users. To check whether a user's password is about to expire, StoreFront creates a local profile for that user on the server. StoreFront must be able to contact the domain controller to change users' passwords.

Note 3:

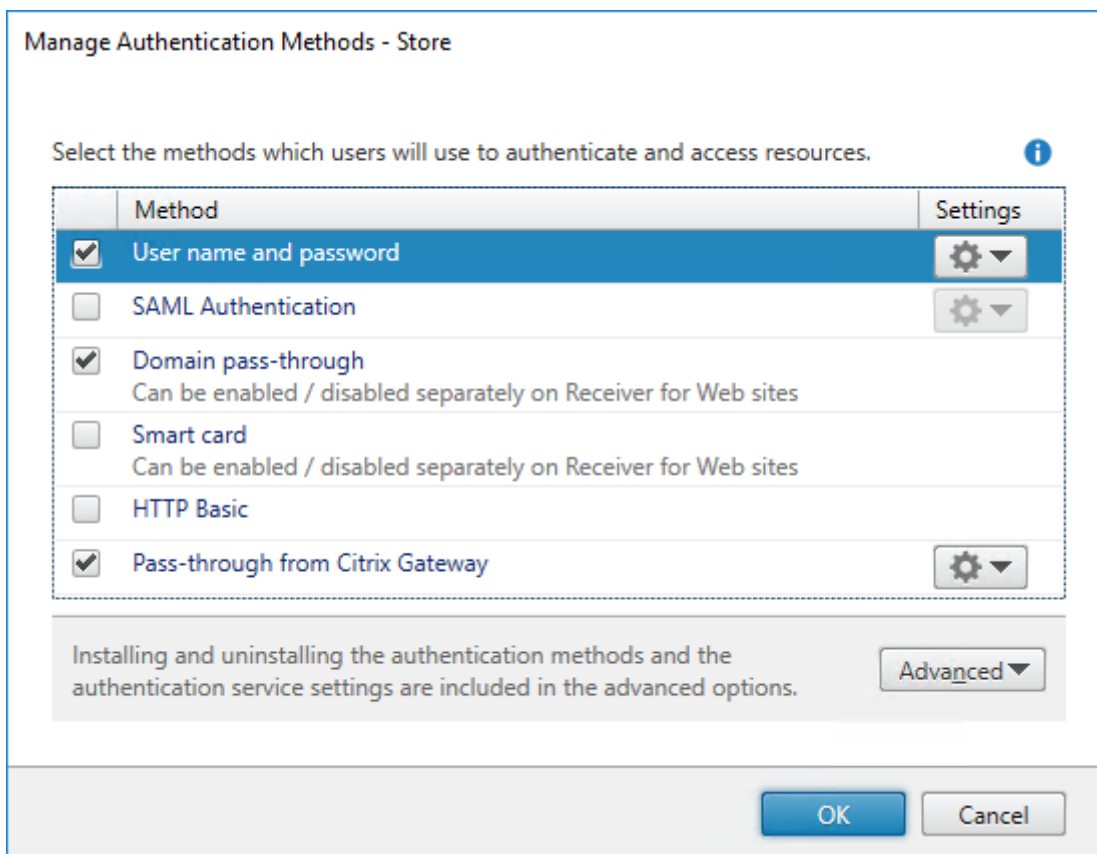
If you enable or disable changing passwords at any time, this also affects settings under **Manage Password Options** for [Pass-through from Citrix Gateway](#) authentication.

Credential password validation

Normally StoreFront communicates directly with Active Directory directly to validate the credentials.

When StoreFront is not in the same domain as Citrix Virtual Apps and Desktops, and it is not possible to put Active Directory trusts in place, you can configure StoreFront to use the Citrix Virtual Apps and Desktops delivery controllers to authenticate the user name and password credentials:

1. In the **Manage Authentication Methods** window, from the **User name and password > Settings** drop-down menu, select **Configure Password Validation**.



2. From the **Validation Password Via** list, select **Delivery Controllers**, and then click **Configure**.

Configure Password Validation

Use this setting to select how passwords are validated.

i Once configured, this setting applies to all password-based authentication methods: User name and password, pass-through from Citrix Gateway and HTTP Basic. You do not need to configure this setting again for these other authentication methods.

Validate Passwords Via Delivery Controllers ▾

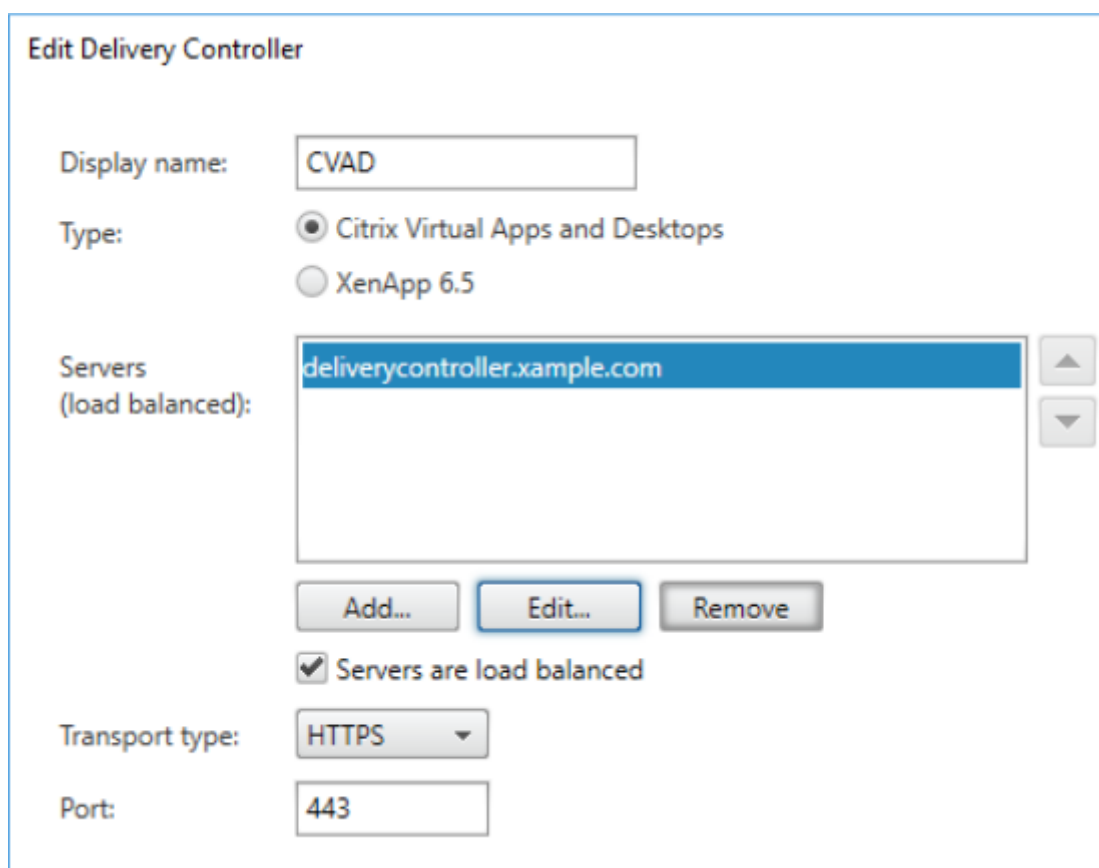
This method delegates end user authentication to Delivery Controllers. Click "Configure" and select one or more Delivery Controllers to validate user credentials.

[Configure...](#)

Configure Delivery Controllers

Delegate end user authentication to Delivery Controllers in Citrix Virtual A
Add one or more Delivery Controllers for validating user credentials.

3. Follow the **Configure Delivery Controllers** screens to add one or more **Delivery Controllers** for validating the user credentials and click **OK**.



Edit Delivery Controller

Display name:

Type: ☒ Citrix Virtual Apps and Desktops
☐ XenApp 6.5

Servers (load balanced):

deliverycontroller.xample.com

☒ Servers are load balanced

Transport type:

Port:

Use active directory

1. On the **Manage Authentication Methods** page, from the **User name and password > Settings** list, select **Configure Password Validation**.
2. From the **Validation Password Via** drop-down menu, select **Active Directory**, and then click **OK**.

Single sign-on to VDAs

When users launch a resource, StoreFront uses the credentials the user used to sign on to the store to single sign-on to the VDAs.

Customize the logon screen

The logon screen is generated from a template, typically located at C:\inetpub\wwwroot\Citrix\[Store name]\Auth\App_Data\Templates\UsernamePassword.tfrm. You can customize the screen.

Title Text

When users log on to a store, by default no title text is displayed on the logon dialog box. You can display the text “Please log on” or compose your own custom message:

1. Use a text editor to open the UsernamePassword.tfrm file for the authentication service.
2. Locate the following lines in the file.

```
1  @* @Heading("ExplicitAuth:AuthenticateHeadingText") *@
2  <!--NeedCopy-->
```

3. Uncomment the statement by removing the leading and trailing leading @* and trailing *@.

```
1  @Heading("ExplicitAuth:AuthenticateHeadingText")
2  <!--NeedCopy-->
```

Citrix Workspace app users see the default title text “Please log on”, or the appropriate localized version of this text, when they log on to stores that use this authentication service.

4. To modify the title text, use a text editor to open the *ExplicitFormsCommon.xx.resx* file for the authentication service, which is typically located in the C:\inetpub\wwwroot\Citrix\[Store name]\Auth\App_Data\resources\ directory.
5. Locate the following elements in the file. Edit the text enclosed within the <value> element to modify the title text that users see on the logon dialog box when they access stores that use this authentication service.

```
1  <data name="AuthenticateHeadingText" xml:space="preserve">
2    <value>My Company Name</value>
3  </data>
4  <!--NeedCopy-->
```

To modify the logon dialog box title text for users in other locales, edit the localized files *ExplicitAuth.languagecode.resx*, where **languagecode** is the locale identifier.

Prevent Citrix Workspace app for Windows from caching passwords and usernames

By default, Citrix Workspace app for Windows stores users’ passwords when they log on to StoreFront stores. To prevent Citrix Workspace app for Windows from caching users’ passwords, you edit the files for the authentication service.

1. Use a text editor to open the file inetpub\wwwroot\Citrix\[Store name]\Auth\App_Data\Templates\Username
2. Locate the following line in the file.

```
1  @SaveCredential(id: @GetTextValue("saveCredentialsId"), labelKey:
    "ExplicitFormsCommon:SaveCredentialsLabel", initiallyChecked:
    ControlValue("SaveCredentials"))
```

```
2 <!--NeedCopy-->
```

3. Comment the statement as shown below.

```
1 <!-- @SaveCredential(id: @GetTextValue("saveCredentialsId"),  
    labelKey: "ExplicitFormsCommon:SaveCredentialsLabel",  
    initiallyChecked: ControlValue("SaveCredentials")) -->  
2 <!--NeedCopy-->
```

Users must enter their passwords every time they log on to stores that use this authentication service.

By default, Citrix Workspace app for Windows automatically populates the last username entered. To suppress population of the username field, or for an alternative mechanism for suppressing caching passwords, see [Prevent Citrix Workspace app for Windows from caching passwords and usernames](#).

Remote access via Citrix Gateway

You can configure your Citrix Gateway so that users sign on to the gateway using their domain username and password. These credentials are passed through to StoreFront to sign on to the store. To configure your Citrix gateway for LDAP username and password authentication see [NetScaler documentation - LDAP authentication](#). To configure StoreFront see [Pass-through from Citrix Gateway](#).

Federated Authentication Service Configuration

May 7, 2024

When using authentication methods such as SAML, where the user does not enter their credentials directly into Citrix Workspace app, by default it is not possible to single sign-on into VDAs. In these cases, you can use [Federated Authentication Service](#) (FAS) to provide single sign-on to VDAs using certificate authentication.

To use FAS with StoreFront, you must configure StoreFront using the [PowerShell SDK](#). Use [Set-STFClaimsFactoryNames](#) to set the claims factory to [FASClaimsFactory](#) and use [Set-STFStoreLaunchOptions](#) to set the VDA logon data logon provider to [FASLogonDataProvider](#).

For example to enable FAS for a store:

```
1 $store = Get-STFStoreService -VirtualPath [VirtualPath]  
2 $auth = Get-STFAuthenticationService -StoreService $store  
3 Set-STFClaimsFactoryNames -AuthenticationService $auth -  
    ClaimsFactoryName "FASClaimsFactory"
```

```
4 Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider "  
  FASLogonDataProvider"  
5 <!--NeedCopy-->
```

To disable FAS for a store:

```
1 $store = Get-STFStoreService -VirtualPath [VirtualPath]  
2 $auth = Get-STFAuthenticationService -StoreService $store  
3 Set-STFClaimsFactoryNames -AuthenticationService $auth -  
  ClaimsFactoryName "standardClaimsFactory"  
4 Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""  
5 <!--NeedCopy-->
```

Substitute [VirtualPath] for the appropriate virtual path, e.g. /Citrix/Store.

To configure the list of FAS servers and other settings you must use Group policy. For more details see [FAS documentation](#).

FAS is not used when authenticating using domain pass-through or smart card through a browser.

FAS server unavailability

If the FAS server is unavailable the launch fails by default. However, you can configure StoreFront such that if the FAS server is unavailable, users can sign on to the VDA by entering their credentials. To change the configuration use Powershell cmdlet [Set-STFStoreLaunchOptions](#) with parameter [FederatedAuthenticationServiceFailover](#). For example to enable fail over for a store:

```
1 $storeService = Get-STFStoreService -VirtualPath [VirtualPath]  
2 Set-STFStoreLaunchOptions $storeService -  
  FederatedAuthenticationServiceFailover $True  
3 <!--NeedCopy-->
```

Configure and manage stores

March 11, 2024

In Citrix StoreFront, you can create and manage stores that aggregate applications and desktops from Citrix Virtual Apps and Desktops giving users on-demand, self-service access to resources.

Task	Detail
Create a store	Configure as many additional stores as you need.
Configure a store	Configure store settings

Task	Detail
Remove a store	Remove an unneeded store.
Export store provisioning files for users	Generate files containing connection details for stores, including any Citrix Gateway deployments and beacons configured for the stores.
Advertise and hide stores to users	Prevent stores being presented to users to add to their accounts when they configure Citrix Workspace app through email-based account discovery or FQDN.
Configure Kerberos Delegation	Configure whether StoreFront uses Kerberos Delegation to authenticate to delivery controllers.
Manage the resources made available in stores	Add and remove resources from stores.
Manage remote access to stores through Citrix Gateway	Configure access to stores through Citrix Gateway for users connecting from public networks.
Certificate Revocation List (CRL) checking	configure StoreFront to check the status of TLS certificates used by CVAD delivery controllers using a published certificate revocation list (CRL).
Configure two StoreFront stores to share a common subscription datastore	Configure two StoreFront stores to share a common subscription datastore.
Enable or disable favorites	Enable or disable favourites for the store.
Manage subscription data for a store	View, import, export and purge subscription data (favourites).
Configure two StoreFront stores to share a common subscription datastore	Configure two stores to share a common subscription database.
Store favorites data using Microsoft SQL Server	Use an external SQL server database for storing subscription (favourite) data.
Citrix Virtual Apps and Desktops configuration	Configure Citrix Virtual Apps and Desktops settings that affect how resources are displayed in store website
Advanced store settings	Configure advanced store settings.
Optimal HDX routing	Configure which gateway is used to connect to which resources.

Task	Detail
Default ica settings	Configure HDX settings by adding them to default.ica
ICA file signing	Configure ica file signing
Windows shortcuts	Configure how Citrix Workspace app for Windows creates Start menu and desktop shortcuts for favorite and mandatory apps.

Create store

March 19, 2024

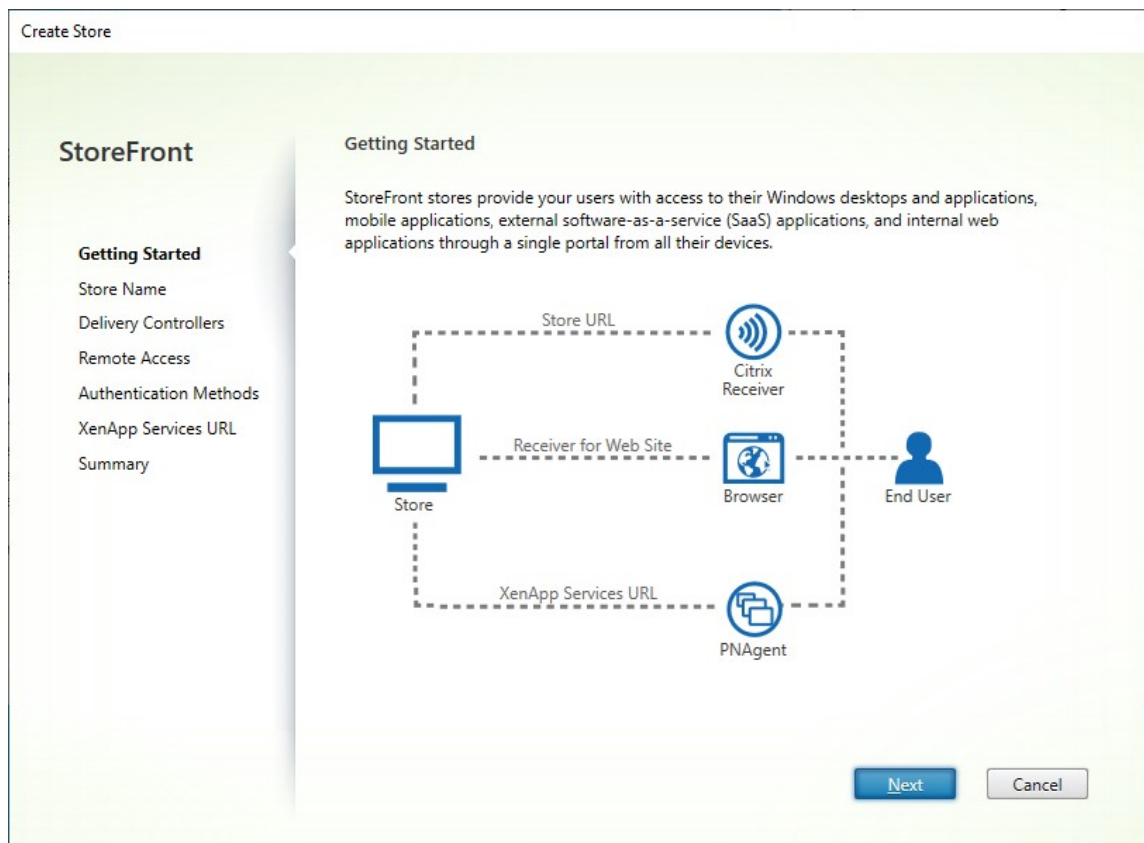
You can create as many stores as you need; for example, you can create a store for a particular group of users or to group together a specific set of resources.

Important:

In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, [propagate your configuration changes to the server group](#) so that the other servers in the deployment are updated.

To create a store, you identify and configure communications with the servers providing the resources that you want to make available in the store. Then, optionally, you configure remote access to the store through Citrix Gateway.

1. From the actions pane click **Create Store**.



Click **Next**

2. On the **Store Name** tab fill out the following:

- Enter a store name
- If you wish to allow users to access the store anonymously, or unauthenticated, tick **Allow only unauthenticated users to access this store**. When you create an unauthenticated store, **Authentication Methods** and **Remote Access** pages are not available, and **Server Group Node** in the left and Action panes are replaced by **Change Base URL**. (This is the only option available because server groups are not available in nondomain-joined servers.)

Create Store

StoreFront

- ✓ Getting Started
- Store Name**
- Delivery Controllers
- Remote Access
- Authentication Methods
- XenApp Services URL
- Summary

Store name and access

Enter a name that helps users identify the store. The store name appears in Citrix Receiver/Workspace app as part of the user's account.

i Store name and access type cannot be changed, once the store is created.

Store Name:

☐ Allow only unauthenticated (anonymous) users to access this store
Unauthenticated users can access the store without presenting credentials.

Receiver for Web Site Settings

☐ Set this Receiver for Web site as IIS default
When this is checked, the Receiver for Web site created with the store will be set as the default IIS website. This setting will override any previous defaults configured for the IIS sites.

Click **Next**

3. On the **Delivery Controllers** tab, add resource feeds for your virtual desktops and applications. For more details, see [Manage the resources made available in stores](#)

Create Store

StoreFront

✓ Getting Started

✓ Store Name

Delivery Controllers

Remote Access

Authentication Methods

XenApp Services URL

Summary

Delivery Controllers

Specify the Citrix Virtual Apps and Desktops delivery controllers or XenApp servers for this store.
Citrix recommends grouping delivery controllers based on deployments.

Name	Type	Servers
Controller	Citrix Virtual Apps and Desktops	cvad1.example.com

Add...

Edit...

Remove

Back

Next

Cancel

Click **Next**.

4. On the **Remote Access** tab choose whether you want make the store available via a Citrix Gateway. For more details see [Manage remote access to stores through Citrix Gateway](#).

The screenshot shows the 'Create Store' wizard in StoreFront 2402. The left sidebar lists the steps: 'Getting Started', 'Store Name', 'Delivery Controllers', 'Remote Access' (current step), 'Authentication Methods', 'XenApp Services URL', and 'Summary'. The main area is titled 'Remote Access' and contains the following text: 'Enabling remote access will allow users outside the firewall to access resources securely. You need to add a Citrix Gateway once remote access is enabled.' Below this, there is a checkbox labeled 'Enable Remote Access' which is checked. Underneath, it says 'Select the permitted level of access to internal resources'. There are two radio button options: 'Allow users to access only resources delivered through StoreFront (No VPN tunnel)' (selected) and 'Allow users to access all resources on the internal network (Full VPN tunnel)'. A note below the second option states 'Users may require the Citrix Gateway plug-in to establish a full VPN tunnel.' Below the radio buttons, there is a section for 'Citrix Gateway appliances:' with a text box containing 'Gateway' and an 'Add...' button. At the bottom, there is a 'Default appliance:' dropdown menu. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

5. On the **Authentication Methods** tab, select the methods your users will use to authenticate to the store and click **Next**.

For more details of the available authentication methods, see [Configure authentication](#).

Rather than configuring authentication methods separately for this store, it is possible to share the authentication configuration with another store. To do this, tick **Use a shared authentication service** then choose an existing store.

Create Store

StoreFront

- ✓ Getting Started
- ✓ Store Name
- ✓ Delivery Controllers
- ✓ Remote Access
- Authentication Methods**
- XenApp Services URL
- Summary

Configure Authentication Methods

Select the methods which users will use to authenticate and access resources. ?

Method
<input checked="" type="checkbox"/> User name and password
<input type="checkbox"/> SAML Authentication
<input type="checkbox"/> Domain pass-through Can be enabled / disabled separately on Receiver for Web sites
<input type="checkbox"/> Smart card Can be enabled / disabled separately on Receiver for Web sites
<input type="checkbox"/> HTTP Basic
<input type="checkbox"/> Pass-through from Citrix Gateway

☐ Use a shared Authentication Service

Using a shared authentication service for stores enables single sign on between them. Users do not have to logon when they are switching between stores.

Select the store with which this store will share an authentication service. The dialog will be refreshed and the methods will be updated based on the selected store.

Store name:

Click **Next**

6. On the **XenApp Services URL** tab, if you have legacy devices requiring PNAgent, leave **Enable XenApp Services URL** ticked, otherwise untick it.

Create Store

StoreFront

- ✓ Getting Started
- ✓ Store Name
- ✓ Delivery Controllers
- ✓ Remote Access
- ✓ Authentication Methods
- XenApp Services URL**
- Summary

Configure XenApp Services URL

URL for users who use PNAgent to access applications and desktops.

☒ **Enable XenApp Services URL**
URL: <https://storefrontlbeu.xaaad.com/Citrix/Store2/PNAgent/config.xml>

☐ **Make this the default Store for PNAgent**
PNAgent will use this store to deliver resources.

[Back](#) [Create](#) [Cancel](#)

Click **Create**

7. When the store has been created, click **Finish**.

When a new store is created it also creates a new website to allow users to access the store. You can [configure this website or create additional websites](#).

PowerShell SDK

To create a store using the [PowerShell SDK](#):

1. Create an authentication service using [Add-STFAuthenticationService](#). By convention, the virtual path is typically `/Citrix/[StoreName]Auth`. Alternatively you can get an existing authentication service using [Get-STFAuthenticationService](#). This step is not required for an anonymous store.
2. Configure the authentication service as required. See [Configure authentication](#).
3. Call [Add-STFStoreService](#).
 - Choose a virtual path for the store and set this as the `-VirtualPath` parameter. Typically this is `/Citrix/[StoreName]`.

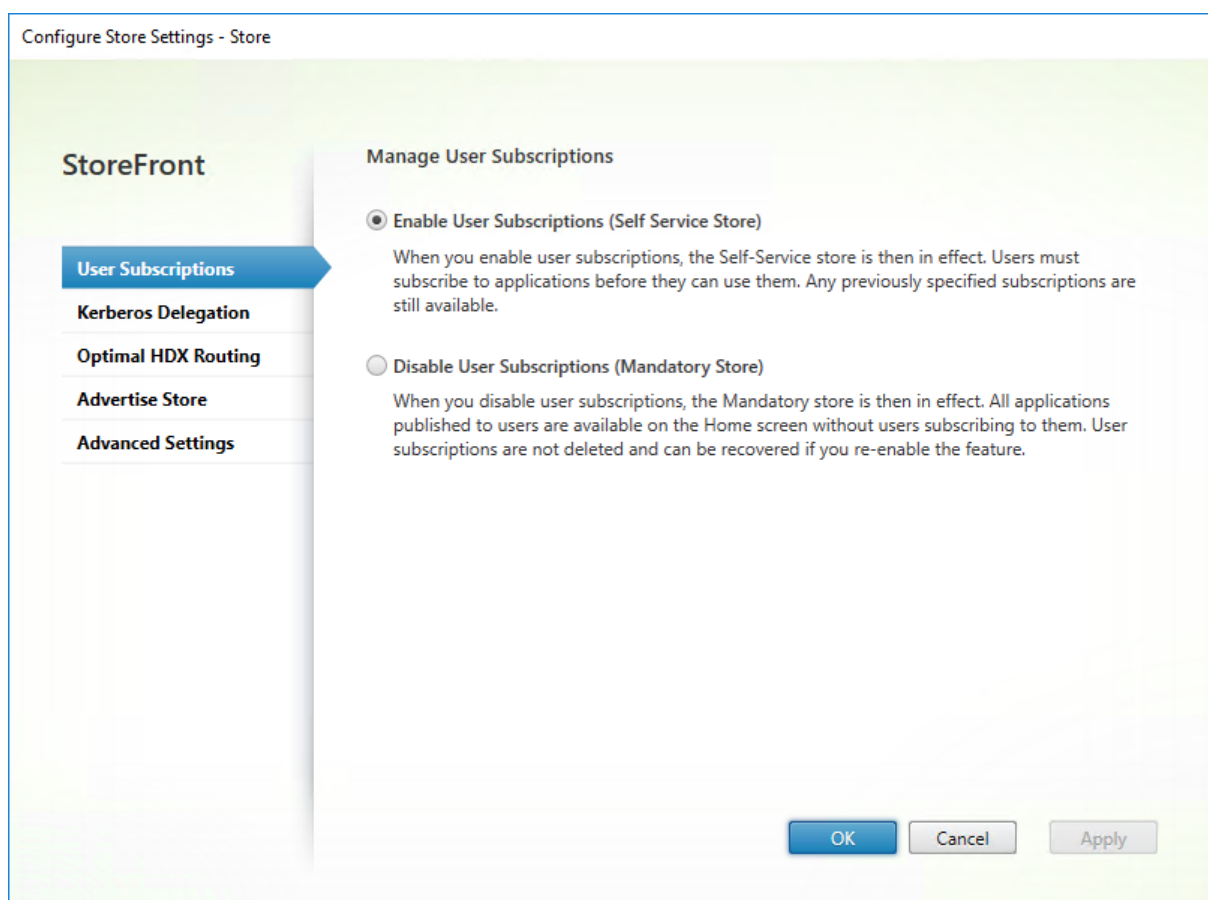
- Set `-AuthenticationService` to the authentication service created in step 1. Alternatively for an anonymous store set `-Anonymous $True`
- You can include the details of one resource feed. Further resource feeds must be configured separately.

Configure a Store

March 11, 2024

To modify a store:

1. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the **Actions** pane, click **Configure Store Settings**.
2. Go to the [User Subscriptions](#) tab to configure whether favourites are enabled.
3. Go to the [Kerberos Delegation](#) tab to configure whether the store uses Kerberos Delegation to authenticate to the delivery controller.
4. Go to the [Optimal HDX Routing](#) tab to configure which gateway is used for launching apps and desktops according to their location.
5. Go to the [Advertise Store](#) tab to configure whether Workspace app presents the store to the user when they enter the FQDN or email address.

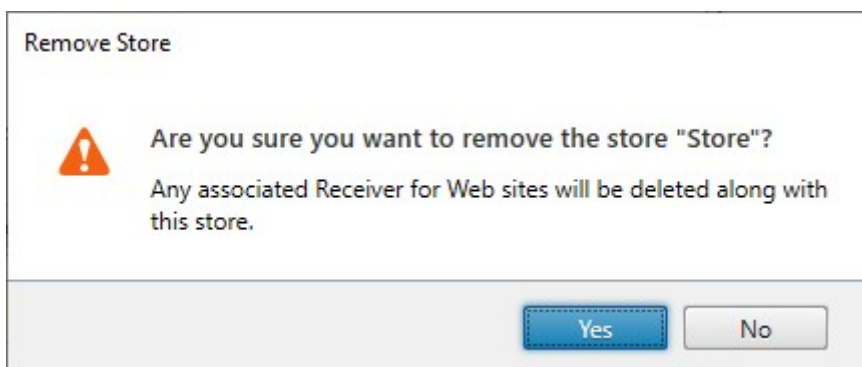


Remove a store

March 11, 2024

To remove a store:

1. Select the **Stores** node in the left pane of the Citrix StoreFront management console
2. In the **Actions** pane, click **Remove Store**
3. In the confirmation window Click **Yes**.



When you remove a store, any associated websites are also deleted.

Export store provisioning files for users

March 11, 2024

You can generate files containing connection details for stores, including any Citrix Gateway deployments and beacons configured for the stores. Make these files available to users to enable them to configure Citrix Workspace app automatically with details of the stores. Users can also download Citrix Workspace app provisioning files when accessing a store through a web browser.

Important:

In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, [propagate your configuration changes to the server group](#) so that the other servers in the deployment are updated.

1. To generate a provisioning file containing details for multiple stores, in the Actions pane, click **Export Multi-Store Provisioning File** and select the stores to include in the file.
2. Click **Export** and **Save** the provisioning file with a .cr extension to a suitable location on your network.

Advertise and hide stores to users

March 11, 2024

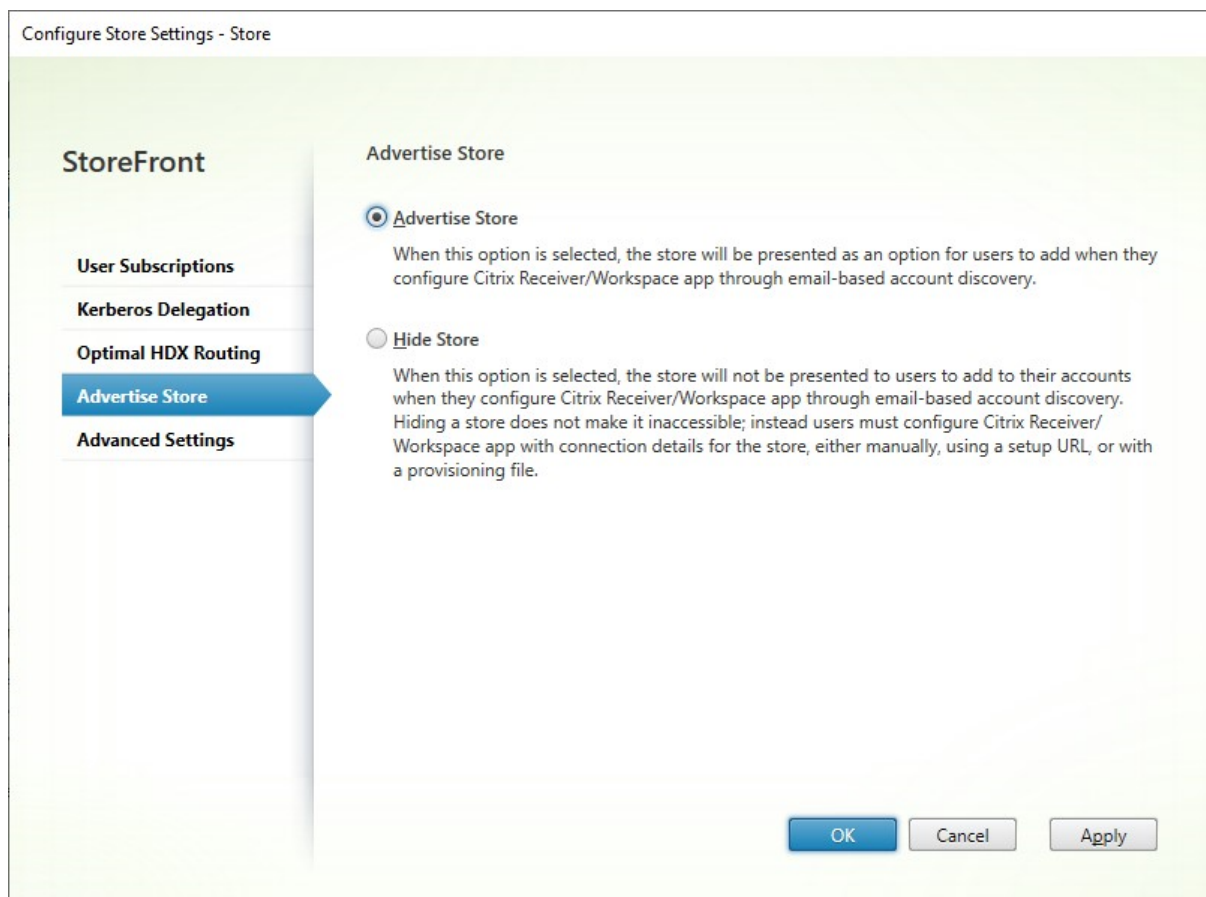
You can choose whether stores are presented to users to add to their accounts when they configure Citrix Workspace app through email-based account discovery or FQDN. By default, when you create a

store it is presented as an option for users to add in Citrix Receiver when they discover the StoreFront deployment hosting the store. Hiding a store does not make it inaccessible, instead users must configure Citrix Workspace app with connection details for the store, either manually, using a setup URL, or with a provisioning file.

Important:

In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, [propagate your configuration changes to the server group](#) so that the other servers in the deployment are updated.

1. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the **Actions** pane, click **Configure Store Settings > Advertise Store**.
2. On the **Advertise Store** page, select either **Advertise Store** or **Hide Store**.



Kerberos delegation

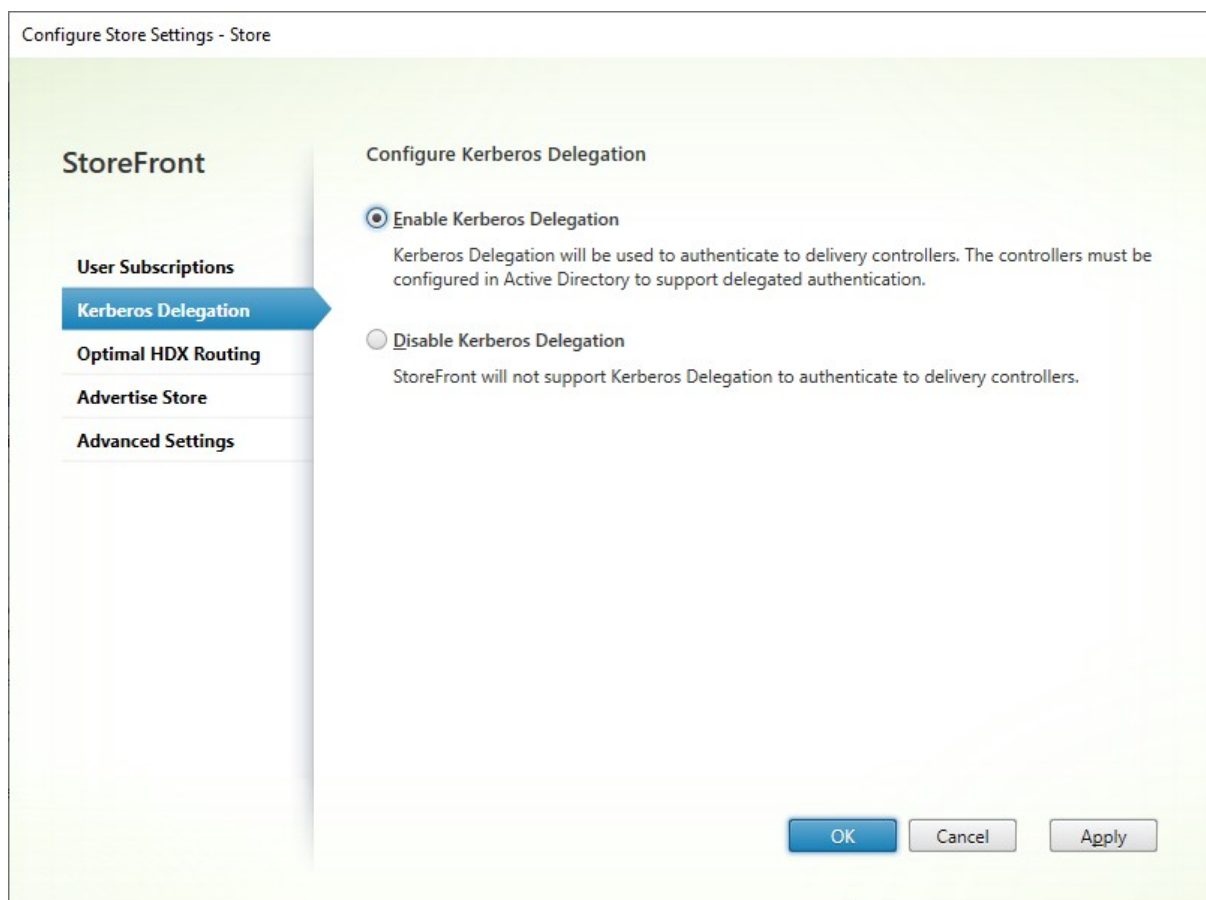
April 9, 2024

Note:

Kerberos delegation is deprecated and can only be used with XenApp 6.5 and earlier. It cannot be used with any supported version of Citrix Virtual Apps and Desktops.

When using domain pass-through or smart card authentication, either directly or via a Citrix Gateway, storeFront does not have the user's credentials so is unable to authenticate to the delivery controller with the user's credentials. When using XenApp 6.5 and earlier, you can enable Kerberos delegation to allow StoreFront to impersonate the user to authenticate to the delivery controller. This requires delegation to be configured within Active Directory.

1. Select a store and from the Actions pane and click **Configure store settings**.
2. Select the **Kerberos Delegation** tab.
3. Choose whether to **Enable Kerberos Delegation** or **Disable Kerberos Delegation**.
4. Press **Apply** or **OK** to save the changes.



PowerShell SDK

To configure Kerberos delegation, use cmdlet [Set-STFStoreService](#) with parameter `-KerberosDelegation`

Manage the resources made available in stores

April 9, 2024

Use the **Manage delivery controllers** screen to add, modify, and delete resource feeds provided by Citrix Virtual Apps and Desktops, Citrix Desktops as a Service, and Citrix Secure Private Access.

View resource feeds

1. From within the Citrix StoreFront management console, in the left pane select the **Stores** node.
2. Select a store in the results pane

3. In the **Actions** pane, click **Manage delivery controllers**.

View resource feeds using the PowerShell SDK

With the [PowerShell SDK](#), use the command [Get-STFStoreFarm](#) to list all resource feeds or a specific resource feed.

Add resource feeds

Add resource feeds for Citrix Virtual Apps and Desktops

1. In the **Manage delivery controllers** screen, click **Add**.
2. Enter a **Display name** that helps you to identify the feed.
3. Select the **Type** as **Citrix Virtual Apps and Desktops**.
4. Under **Servers** click **Add** and enter the name of the delivery controller. Repeat for each delivery controller. Citrix recommends that you have at least two servers for load balancing or failover.
5. Citrix recommends that you select the option **Servers are load balanced**. This causes StoreFront to distribute the load between all delivery controllers or connectors by selecting a server from the list at random during each launch. If this option is not selected, then the servers list is treated as a failover list in priority order. In this case 100% of launches occur on the first active Delivery Controller or connector in the list. If that server goes offline, 100% of launches occur using the second in the list, and so on.
6. From the **Transport type** list, select the type of connections for StoreFront to use for communications with the servers.
 - To send data over unencrypted connections, select **HTTP**. If you select this option, you must make your own arrangements to secure connections between StoreFront and your servers.
 - To send data over encrypted connections (recommended), select **HTTPS**. If you select this option for Citrix Virtual Apps and Desktops servers, ensure that the Citrix XML Service is set to share its port with Microsoft Internet Information Services (IIS) and that IIS is configured to support HTTPS.

Note:

If you're using HTTPS to secure connections between StoreFront and your servers, ensure that the names you specify in the servers list match exactly (including the case) the names on the certificates for those servers.

7. Specify the port for StoreFront to use for connections to the servers. The default port is 80 for HTTP connections and 443 for HTTPS connections. The specified port must be the port used by the Citrix XML Service.

Add Delivery Controller

Display name:

Type: ☒ Citrix Virtual Apps and Desktops
☐ XenApp 6.5

Servers (load balanced):

☒ Servers are load balanced

Transport type:

Port:

Advanced Settings
Configure delivery controller communication timeouts and other advanced settings using the 'Settings' dialog.

Add resource feeds for Citrix Desktops as a Service

1. In the **Manage delivery controllers** screen, click **Add**.
2. Enter a **Display name** that helps you to identify the feed.
3. Select the **Type** as **Citrix Virtual Apps and Desktops**.
4. Under **Servers** click **Add** and enter the name of a cloud connector. Repeat for each server or connector. Citrix recommends that you have at least two connectors for redundancy. If you have multiple resource locations, Citrix recommends that you add the cloud connectors from all resource locations so that in the event of an outage StoreFront can use the local host cache to launch VDAs at the appropriate location.

5. If you have connectors from multiple locations, Citrix recommends that you put the connectors with the lowest latency to the StoreFront server at the top of the list and clear the option **Servers are load balanced**. As the connectors are only proxying information to DaaS delivery controllers, there is limited benefit from using load balancing.
6. From the **Transport type** list, select the type of connections for StoreFront to use for communications with the servers.
 - To send data over unencrypted connections, select **HTTP**. If you select this option, you must make your own arrangements to secure connections between StoreFront and your cloud connectors.
 - To send data over encrypted connections (recommended), select **HTTPS**. If you select this option for you must ensure that the cloud connectors are configured for HTTPS.

Note:

If you're using HTTPS to secure connections between StoreFront and your servers, ensure that the names you specify in the servers list match exactly (including the case) the names on the certificates for those servers.

7. Specify the port for StoreFront to use for connections to the servers. The default port is 80 for HTTP connections and 443 for HTTPS connections.

Add Delivery Controller

Display name:

Type: ☒ Citrix Virtual Apps and Desktops
☐ XenApp 6.5

Servers (in failover order):

☐ Servers are load balanced

Transport type:

Port:

Advanced Settings
Configure delivery controller communication timeouts and other advanced settings using the 'Settings' dialog.

Add resource feeds for XenApp 6.5

XenApp 6.5 is not supported by Citrix. It is not possible to add a XenApp 6.5 resource feed using the management console. However, you can use PowerShell to continue.

Add resource feeds for Citrix Secure Private Access

If your StoreFront server is configured for Citrix Secure Private Access you can add Citrix Secure Private Access resource feeds.

1. Navigate to **Stores > Delivery Controllers** on StoreFront.
2. Click **Add**.
3. In the **Add Delivery Controller** window, provide a **Display name** to identify the feed.

4. Select the **Type** as **Citrix Secure Private Access**.
 5. Enter the Citrix Secure Private Access server name.
 6. From the **Transport type** dropdown, select the type of connection that can be used for communications with the servers.
 - **HTTP:** sends data over unencrypted connections
- Note:**

If you select **HTTP**, you must make your own arrangements to secure connections between StoreFront and your servers.
- **HTTPS:** sends data over secure HTTP connections using Secure Sockets Layer (SSL) or Transport Layer Security (TLS).
 7. Specify the port to be used for connections to the servers. The default port for **HTTP** is 80, and for **HTTPS** it is 443.
 8. Click **OK**.

Create a resource feed using the PowerShell SDK

To add a resource feed, use the command [Add-STFStoreFarm](#)

- For Citrix Virtual Apps and Desktops or Citrix Desktops as a Service, set [FarmType](#) to [XenDesktop](#).
- For XenApp 6.5, set [FarmType](#) to [XenApp](#).
- For Citrix Secure Private Access, set [FarmType](#) to [SPA](#).

Modify a resource feed

In the **Manage delivery controllers** screen, select a resource feed and click **Edit**.

Modify a resource feed using the PowerShell SDK

To modify a resource feed using PowerShell, use command [Set-STFStoreFarm](#)

Delete a resource feed

In the **Manage delivery controllers** screen, select a resource feed and click **Remove**.

Delete a resource feed using the PowerShell SDK

To delete a resource feed using PowerShell, use command [Remove-STFStoreFarm](#)

Configure server bypass behavior

To improve performance when some of the servers providing resources become unavailable, StoreFront temporarily bypasses servers that fail to respond. While a server is being bypassed, StoreFront ignores that server and does not use it to access resources. Use these parameters to specify the duration of the bypass behavior:

- **All failed bypass duration** specifies a reduced duration in minutes that StoreFront uses instead of **Bypass duration** if all servers for a particular Delivery Controller are being bypassed. The default is 0 minutes.
- **Bypass duration** specifies the time in minutes that StoreFront bypasses an individual server after a failed attempt to contact that server. The default bypass duration is 60 minutes.

Considerations when specifying All failed bypass duration

Setting a larger **All failed bypass duration** reduces the impact of unavailability of a particular Delivery Controller, however it has the negative affect that resources from this Delivery Controller are unavailable to users for the specified duration after a temporary network outage or server unavailability. Consider the use of larger **All failed bypass duration values** when many Delivery Controllers have been configured for a store, particularly for nonbusiness-critical Delivery Controllers.

Setting a smaller **All failed bypass duration** increases the availability of resources served by that Delivery Controller but increases the possibility of client-side timeouts if many Delivery Controllers are configured for a store and several of them become unavailable. It is worth keeping the default 0-minute value when not many farms are configured and for business-critical Delivery Controllers.

To change the bypass parameters

1. From within the Citrix StoreFront management console, in the left pane select the **Stores** node.
2. Select a store in the results pane.
3. In the **Actions** pane, click **Manage Delivery Controllers**.
4. Select a controller, click **Edit**, and then click **Settings** on the **Edit Delivery Controller** screen.
5. Under Advanced Settings click **Settings**.
6. In the Configure Advanced Settings dialog:

- a) On the **All failed bypass duration** row, click in the second column and enter a time, in minutes, for which a Delivery Controller is considered offline after all its servers fail to respond.
- b) On the **Bypass duration** row, click in the second column and enter a time, in minutes, for which a single server is considered offline after it fails to respond.

Map users to resource feeds

By default, users accessing a store see an aggregate of all the resources available to them from all the resource feeds configured for that store. To provide different resources for different users, you can configure separate stores or even separate StoreFront deployments. Alternatively, you can provide access to particular deployments on the basis of users' membership of Microsoft Active Directory groups. This enables you to configure different experiences for different user groups through a single store.

For example, you can group common resources for all users on one deployment and finance applications for the Accounts department on another deployment. In such a configuration, a user who is not a member of the Accounts user group sees only the common resources when accessing the store. A member of the Accounts user group is presented with both the common resources and the finance applications.

Alternatively, you can create a deployment for power users that provides the same resources as your other deployments, but with faster and more powerful hardware. This enables you to provide an enhanced experience for business-critical users, such as your executive team. All users see the same desktops and applications when they log on to the store, but members of the Executives user group are preferentially connected to resources provided by the power user deployment.

Note:

This filters entire resource feeds. In addition, within a resource feed, applications may be filtered by user group within Citrix Virtual Apps and Desktops Studio configuration.



To configure specific resource feeds for particular user groups:

1. From the **Manage delivery controllers** screen, under **User Mapping and Multi-Site Aggregation Configuration**, click **Configure**. This option is only available if two or more resource feeds are configured.

This opens the **Configure User Mapping and Multi-site** Aggregation screen.

Configure User Mapping and Multi-site Aggregation

Configure user mapping and performance optimization for large scale StoreFront installations that have multiple controllers. Use this feature to de-duplicate overlapping resources across multiple controllers and also provide access to particular controllers based on user's membership in Active Directory groups.

 Map users to controllers Use this setting to provide access to deployments based on user's membership of Active Directory groups.	No mappings
 Aggregate resources Use this optional setting to help de-duplicate overlapping resources across multiple controllers. At least one user mapping must be defined before aggregating resources.	No aggregation

OK **Cancel**

2. Click **Map users to controllers**. This opens the **Create User Mapping** screen to create your first mapping. You will be able to create further mappings later.

Create User Mapping

StoreFront

User Groups

Controllers

User Groups

Specify the user groups that will have access to the controllers.

☒ **Everyone**

☐ **Specific User Groups**

Add... **View** **Remove**

Next **Cancel**

3. Either choose **Everyone** or choose **Specific User Groups** and add one or more group.

Create User Mapping

StoreFront

User Groups
Controllers

User Groups
Specify the user groups that will have access to the controllers.

☐ Everyone
☒ Specific User Groups

XAEAAD\DesktopOnly Users

Add... View Remove

Next Cancel

4. Click **Next**. This takes you to the **Controllers** tab.

Create User Mapping

StoreFront

✓ User Groups

Controllers

Assign Controllers to the User Groups

During enumeration, StoreFront contacts the controllers and displays resources to the users. The resources from the controllers that are aggregated will be deduplicated.

When an aggregated resource is available from multiple controllers, StoreFront launches the resource from one of the controllers chosen at random in order to balance the load.

Controller	Aggregated	Type
------------	------------	------

Add...

Remove

Back

Create

Cancel

5. Click **Add** and add one ore more controller.

Create User Mapping

StoreFront

✓ User Groups

Controllers

Assign Controllers to the User Groups

During enumeration, StoreFront contacts the controllers and displays resources to the users. The resources from the controllers that are aggregated will be deduplicated.

When an aggregated resource is available from multiple controllers, StoreFront launches the resource from one of the controllers chosen at random in order to balance the load.

Controller	Aggregated	Type
CVAD site A	No	Citrix Virtual Apps and Desktops

Add...

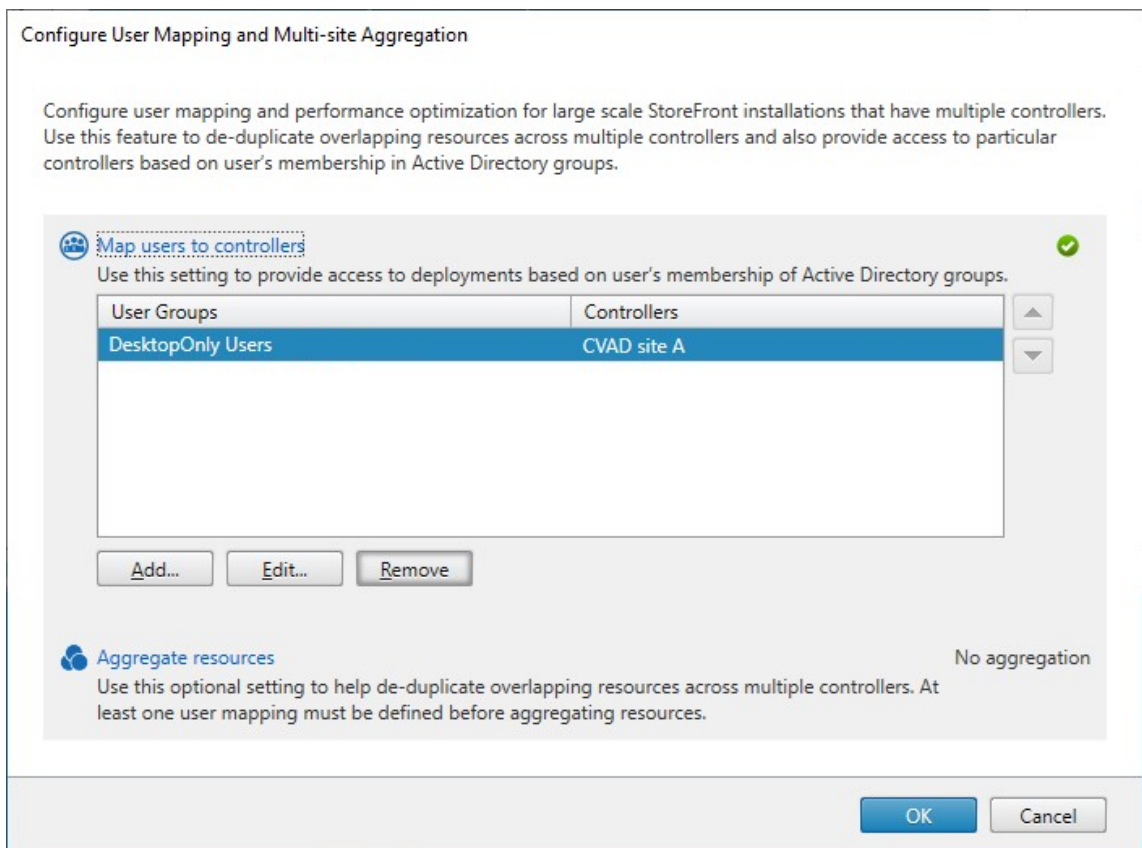
Remove

Back

Create

Cancel

6. Click **Create**.



7. Click **Add...** to create further mappings as required.

Map users to resources using PowerShell SDK

You can map users to resources using the [PowerShell SDK](#)

1. For each resource feed, create an EquivalentFarmset. All resource feeds must be part of a farm-set, otherwise they will not be available to any user. Call [New-STFEquivalentFarmset](#) with the following parameters:
 - **Name** - a unique name for the EquivalentFarmSet
 - **PrimaryFarms** - the name of non-aggregated resource feed (farm).
2. For each set of users who require access to a different set of resource feeds, create mappings between those users and each of the EquivalentFarmSets. To create the UserFarmMapping, call [Add-STFUserFarmMapping](#) with the following parameters:
 - **StoreService** - The Store service to add the UserFarmMapping to.
 - **Name** - A unique name for the mapping.
 - **GroupMembers** - A hashtable containing the names and SIDs of the user groups that are part of the mapping. The name is used for display only; the SID defines the group.

To add all users, create a single entry in the hashtable with name `Everyone` and value `Everyone`.

- `EquivalentFarmSet` - A `EquivalentFarmSet` created in the previous step.

You must ensure that every resource feed (farm) is included in at least one `UserFarmMapping`, otherwise no users will be able to access that resource.

Multi-Site Aggregation

By default, StoreFront enumerates all the deployments providing desktops and applications for a store and treats all those resources as distinct. This means that if the same resource is available from several deployments, users see an icon for each resource, which might be confusing if the resources have the same name. When you set up highly available multi-site configurations, you can group Citrix Virtual Apps and Desktops deployments that deliver the same desktop or application so that identical resources can be aggregated for users. Grouped deployments do not need to be identical, but resources must have the same name and path on each server to be aggregated.

With multi-site aggregation, when a desktop or application is available from multiple Citrix Virtual Apps and Desktops deployments configured for a particular store, StoreFront aggregates all instances of that resource and presents users with a single icon. When a user starts an aggregated resource, StoreFront determines the most appropriate instance of that resource for the user on the basis of server availability, whether the user already has an active session, and the ordering you specified in your configuration.

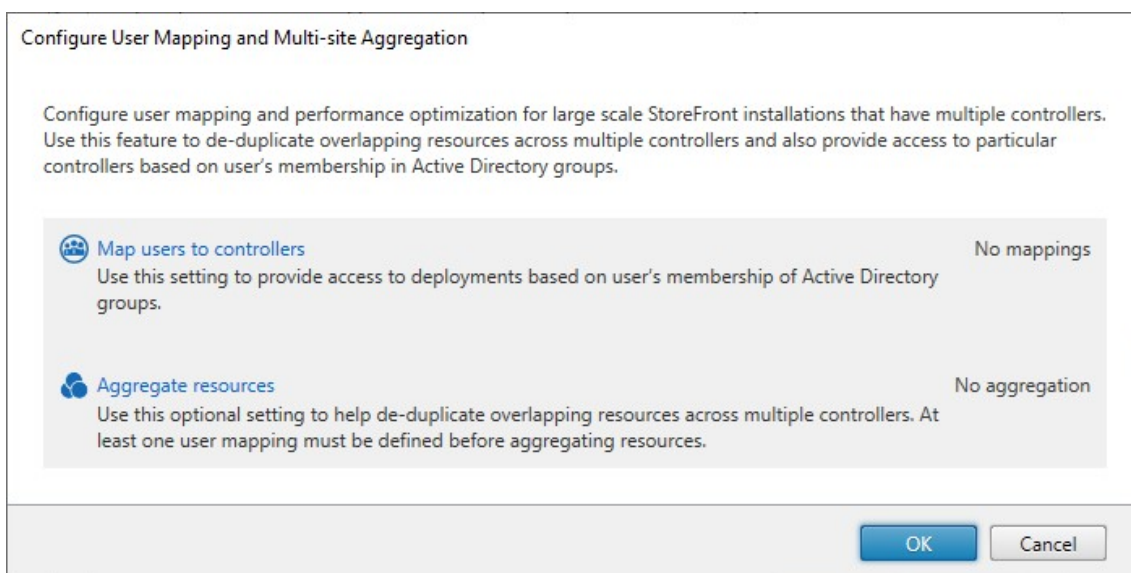
StoreFront dynamically monitors servers that fail to respond to requests on the basis that such servers are either overloaded or temporarily unavailable. Users are directed to resource instances on other servers until communications are re-established. Where supported by the servers providing the resources, StoreFront attempts to reuse existing sessions to deliver additional resources. If a user already has an active session on a deployment that also provides the requested resource, StoreFront reuses the session if it is compatible with that resource. Minimizing the number of sessions for each user reduces the time taken to start additional desktops or applications and can allow for more efficient use of product licenses.

After checking for availability and existing user sessions, StoreFront uses the ordering specified in your configuration to determine the deployment to which the user is connected. If multiple equivalent deployments are available to the user, you can specify that users are connected either to the first available deployment or randomly to any deployment in the list. Connecting users to the first available deployment enables you to minimize the number of deployments in use for the current number of users. Randomly connecting users provides a more even distribution of users across all the available deployments.

You can override the specified deployment ordering for individual Citrix Virtual Apps and Desktops resources to define preferred deployments to which users are connected when they access a particular

desktop or application. This enables you to, for example, specify that users are preferentially connected to a deployment specifically adapted to deliver a particular desktop or application, but use other deployments for other resources. To do this, append the string **KEYWORDS:Primary** to the description of the desktop or application on the preferred deployment and **KEYWORDS:Secondary** to the resource on other deployments. Where possible, users are connected to the deployment providing the primary resource, regardless of the deployment ordering specified in your configuration. Users are connected to deployments providing secondary resources when the preferred deployment is unavailable.

1. On the **Manage Delivery Controllers** screen, under **User Mapping and Multi-Site Aggregation Configuration** click **Configure**. This option is only available if two or more resource feeds are configured.



2. Click **Aggregate resources**. This shows the **Aggregate Resources** screen.

Aggregate Resources

StoreFront allows you to aggregate the resources from multiple deployments. Select the controllers that need to be aggregated.

	Controller	Type
Aggregated		
<i>None</i>		
Not Aggregated		
<input type="checkbox"/>	CVAD site A	Citrix Virtual Apps and Desktops
<input type="checkbox"/>	CVAD Site B	Citrix Virtual Apps and Desktops

Aggregated Controller Settings

These settings apply to all controllers marked as Aggregated

☐ Controllers publish identical resources

☒ Load balance resources across controllers

3. Choose the resource feeds that have the same resources and click **Aggregate**.

Aggregate Resources

StoreFront allows you to aggregate the resources from multiple deployments. Select the controllers that need to be aggregated.

	Controller	Type
Aggregated		
<input type="checkbox"/>	CVAD Site B	Citrix Virtual Apps and Desktops
<input type="checkbox"/>	CVAD site A	Citrix Virtual Apps and Desktops
Not Aggregated		
None		

Aggregated Controller Settings
These settings apply to all controllers marked as Aggregated

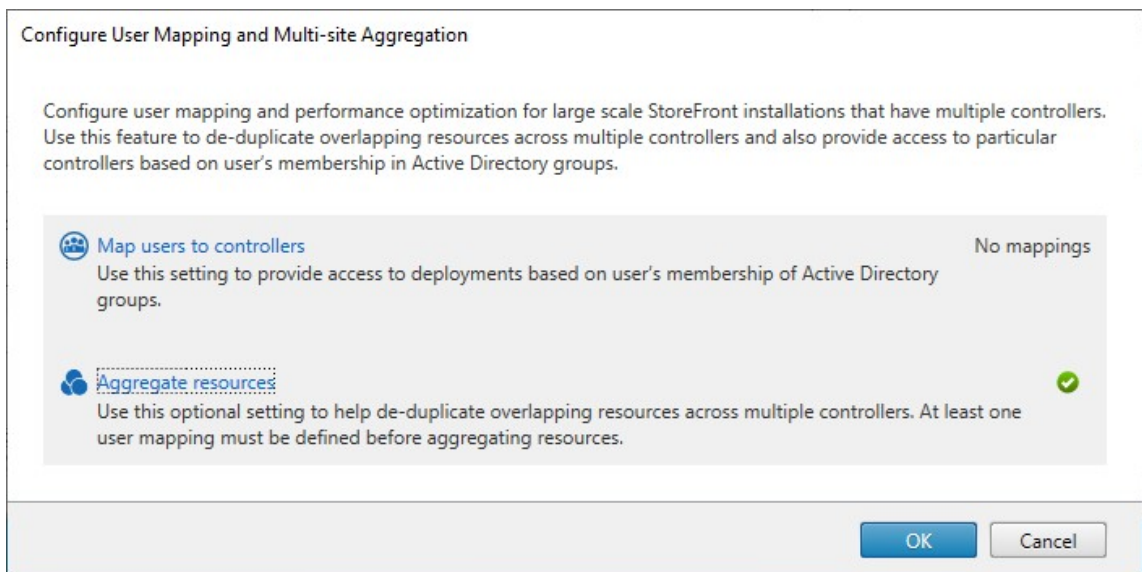
☐ Controllers publish identical resources

☒ Load balance resources across controllers

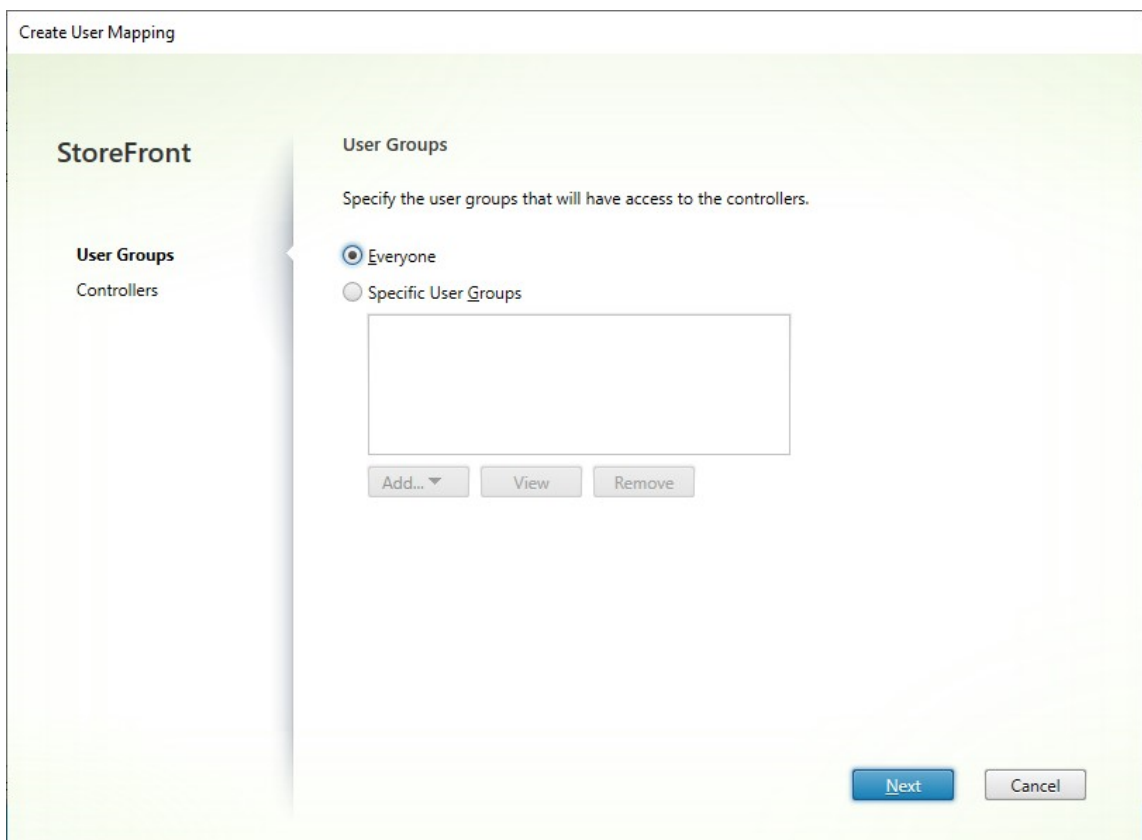
4. Select **Aggregated Controller Settings** options as required:

- **Controllers publish identical resources** - When selected, StoreFront enumerates resources from only one of the controllers in the aggregated set. When not selected, StoreFront enumerates resources from all controllers in the aggregated set (to accumulate the user's entire set of available resources). Selecting this option gives a performance improvement when enumerating resources, but we do not recommend it unless you are certain that the list of resources is identical across all aggregated feeds.
- **Load balance resources across controllers** - When selected, launches are distributed evenly among the available controllers. When not selected, launches are directed to the first controller specified in the user mapping dialog screen, failing over to subsequent controllers if the launch fails.

5. Click **OK** to take you back to the **Configure User Mapping and Multi-site Aggregation** screen. **Aggregate resources** is now ticked.



6. When resources are aggregated, by default, no users have access to the resources so you must add the user mappings. Click **Map users to controllers**. This opens the **Create user mapping** screen.



7. Either choose **Everyone** or choose **Specific User Groups** and add one or more group. For instance you may wish to choose a group representing users in a particular location.

8. Add the aggregated resource feeds. You must add all of the aggregated resource feeds, any not included become Not Aggregated. You may also include non-aggregated resources.
9. If you did not tick **Load balance resources across controllers** then you can choose the order in which StoreFront should prefer to launch resources.

Create User Mapping

StoreFront

✓ User Groups

Controllers

Assign Controllers to the User Groups

During enumeration, StoreFront contacts the controllers and displays resources to the users. The resources from the controllers that are aggregated will be deduplicated.

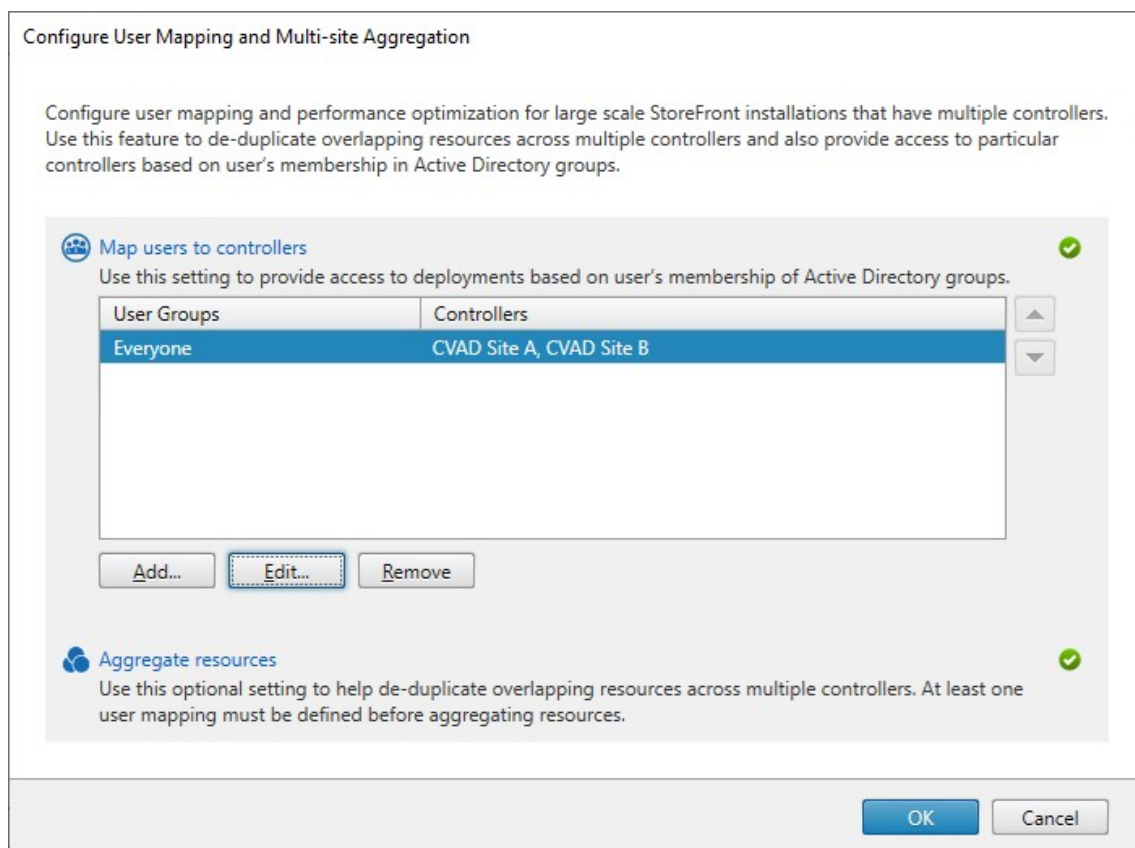
When an aggregated resource is available from multiple controllers, StoreFront launches the resource from the controller at the top of the list, in fail over order. The order of the list can be changed using the buttons provided.

Controller	Aggregated	Type
CVAD Site A	Yes	Citrix Virtual Apps and Desktops
CVAD Site B	Yes	Citrix Virtual Apps and Desktops

Add... Remove

Back Create Cancel

10. Press **Create** to return to **Configure User Mapping and multi-site Aggregation**.



11. Add further mappings as required. Ensure that every resource feed is mapped to a user group, otherwise those resources will not be usable by anyone.
12. Click **OK**.

Advanced configurations using PowerShell SDK

You can configure many common multi-site and high availability operations with the StoreFront management console. You can also configure StoreFront using the [PowerShell SDK](#), which provides the following extra functionality:

- Ability to specify multiple groupings of deployments for aggregation.
 - The management console allows only a single grouping of deployments, which is sufficient for most cases.
 - For stores with many deployments with disjointed sets of resources, multiple groupings might give performance improvements.
- Ability to specify complex preference orders for aggregated deployments. The management console allows aggregated deployments to be load balanced or to be used as a single failover list. Using PowerShell you can have multiple groups of feeds that are load balanced and fail over between different groups.

Warning:

After configuring advanced multi-site options by using PowerShell, it is no possible to modify the options using the management console.

1. Decide what aggregation groups you wish to use. Within an aggregation group, applications with the same display name are aggregated into a single icon. Each aggregation group needs a name. With the management console you can only create one aggregation group. Through PowerShell you can define multiple aggregation groups.
2. For each aggregation group, create one or more EquivalentFarmset listing the resource feeds (known in the SDK as farms) that you wish to aggregate. If different resource feeds within the aggregation group will be assigned to different users then you must create a separate EquivalentFarmSet for each set of users but sharing the same [AggregationGroupName](#). To create the EquivalentFarmSet, call [New-STFEquivalentFarmset](#) with the following parameters:
 - [Name](#) - a unique name for the EquivalentFarmset.
 - [AggregationGroupName](#) - the name of the aggregation group the farmset is part of.
 - [LoadBalanceMode](#) - either [LoadBalanced](#) or [Failover](#).
 - [PrimaryFarms](#) - The farms you wish to be aggregated. If [LoadBalanceMode](#) is [Failover](#) then ensure farms are listed in the required order. If there are multiple EquivalentFarmSets for an aggregation group then this order is combined with the [IndexNumber](#) defined in the [UserFarmMapping](#) when evaluating which resource feed to use to launch a resource.
 - [BackupFarms](#) - A list of farms to use in case none of the primary farms are available. This functionality is depreciated. Instead add additional EquivalentFarmSets with a higher [IndexNumber](#).
3. For each resource feed not part of an aggregation group, create an EquivalentFarmset without specifying an [AggregationGroupName](#). All resource feeds must be part of a farmset. Call [New-STFEquivalentFarmset](#) with the following parameters:
 - [Name](#) - a unique name for the EquivalentFarmSet
 - [PrimaryFarms](#) - the name of non-aggregated farm.
4. For each set of users who require access to a different set of resource feeds, create mappings between those users and each of the EquivalentFarmSets. To create the [UserFarmMapping](#), call [Add-STFUserFarmMapping](#) with the following parameters:
 - [StoreService](#) - The Store service to add the [UserFarmMapping](#) to.
 - [Name](#) - A unique name for the mapping.
 - [GroupMembers](#) - A hashtable containing the names and SIDs of the user groups that are part of the mapping. The name is used for display only; the SID defines the group.

To add all users, create a single entry in the hashtable with name [Everyone](#) and value [Everyone](#).

- [EquivalentFarmSet](#) - A EquivalentFarmSet created in the previous step.
- [IndexNumber](#) - Sets the order in which resource feeds are evaluated. This sets the order of preference of which resource feed to use to launch a resource.

You must ensure that every resource feed (farm) is included in at least one UserFarmMapping, otherwise no users would be able to access that resource.

Manage remote access to stores through Citrix Gateway

March 11, 2024

Use the Remote Access Settings task to configure access to stores through Citrix Gateway for users connecting from public networks. Remote access through a Citrix Gateway cannot be applied to unauthenticated stores.

Important:

In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, [propagate your configuration changes to the server group](#) so that the other servers in the deployment are updated.

1. Select the Stores node in the right pane of the Citrix StoreFront management console and, in the results pane, select a store. In the Actions pane, click **Configure Remote Access Settings**.

Configure Remote Access Settings - Store

Enabling remote access allows users outside the firewall to securely access resources. After you enable remote access, add a NetScaler Gateway appliance.

☒ Enable Remote Access

Select the permitted level of access to internal resources

☒ Allow users to access only resources delivered through StoreFront (No VPN tunnel) i

☐ Allow users to access all resources on the internal network (Full VPN tunnel) i

Users may require the NetScaler Gateway Plug-in to establish a full VPN tunnel.

NetScaler Gateway appliances:

☒ ProductionGateway i

Add...

Default appliance:

ProductionGateway

OK

Cancel

2. In the Configure Remote Access Settings dialog box, specify whether and how users connecting from public networks can access the store through Citrix Gateway.

- To make the store unavailable to users on public networks, do not check **Enable remote access**. Only local users on the internal network will be able to access the store.
- To enable remote access, check **Enable Remote Access**.
 - To make resources delivered through the store available through Citrix Gateway, select **No VPN tunnel**. Users log on using either ICAProxy or clientless VPN (cVPN) to Citrix Gateway and do not need to use the Citrix Gateway plug-in to establish a full VPN.
 - To make the store and other resources on the internal network available through a Secure Sockets Layer (SSL) virtual private network (VPN) tunnel, select **Full VPN tunnel**. Users require the Citrix Gateway plug-in to establish the VPN tunnel.

When you enable remote access to the store, the **Pass-through from Citrix Gateway** authentication method is automatically enabled. Users authenticate to Citrix Gateway and are automatically logged on when they access their stores.

3. If you enabled remote access, select from the **Citrix Gateway appliances** list the deployments through which users can access the store. Any deployments you configured previously for this and other stores are available for selection in the list. If you want to add a further deployment to the list, click **Add** and follow the steps in [Configure Citrix Gateway](#).
4. If you enable access through multiple appliances by selecting more than one entry in the list, specify the **Default appliance** to be used to access the store from Citrix Workspace app.
5. Click **OK** to save the configuration and close the Configure Remote Access dialog.

Citrix Workspace app uses beacon points to determine whether users are connected to local or public networks and then selects the appropriate access method. For more information about changing beacon points, see [Configure beacon points](#).

By default StoreFront uses the Gateway through which the user is connected to the store to launch resources. To configure StoreFront to launch resources using an alternative gateway or no gateway, see [Optimal HDX routing](#).

Certificate Revocation List (CRL) checking

March 19, 2024

Introduction

You can configure StoreFront to check the status of TLS certificates used by CVAD delivery controllers using a published certificate revocation list (CRL). You may need to revoke access to a certificate if:

- you believe the private key has been compromised
- the CA is compromised
- the affiliation has been changed
- the certificate has been superseded

Note:

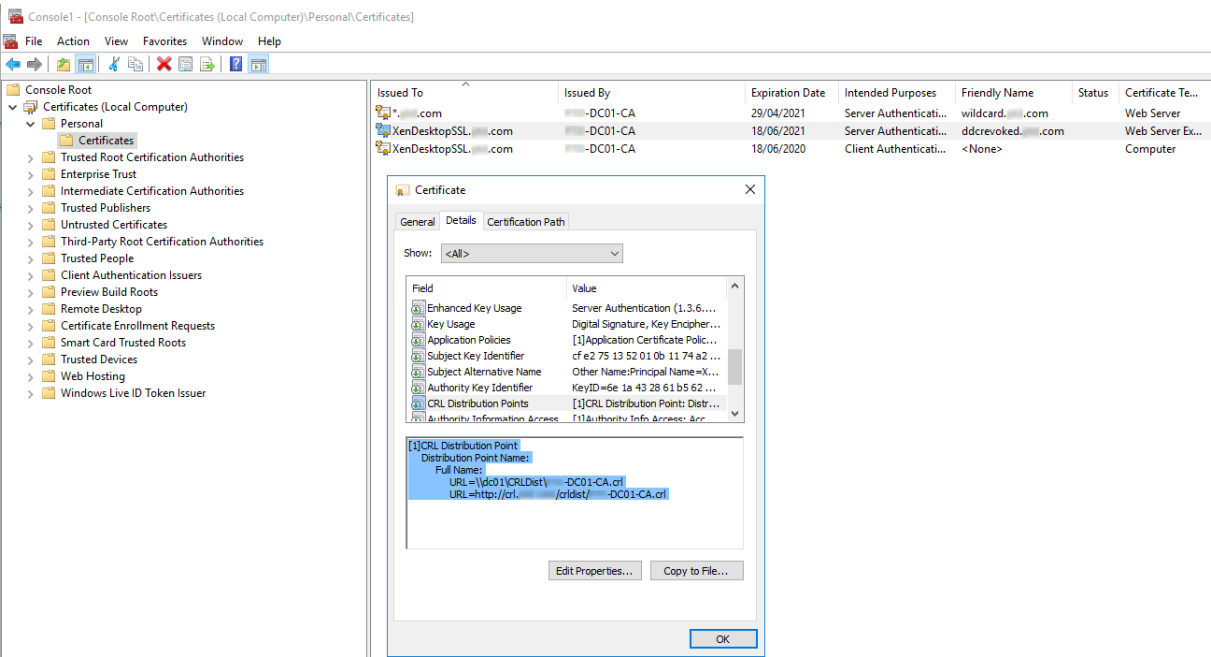
This topic is only relevant when HTTPS connections between StoreFront and Citrix Virtual Apps and Desktops delivery controllers are used. HTTP connections to delivery controllers do not require a certificate, so the `-CertRevocationPolicy` setting for the Store, described here, has no effect.

StoreFront supports certificate revocation checking using CRL Distribution

Point (CDP) certificate extensions and locally installed certificate revocation lists (CRLs). StoreFront supports full CRLs only; delta CLRs are not supported.

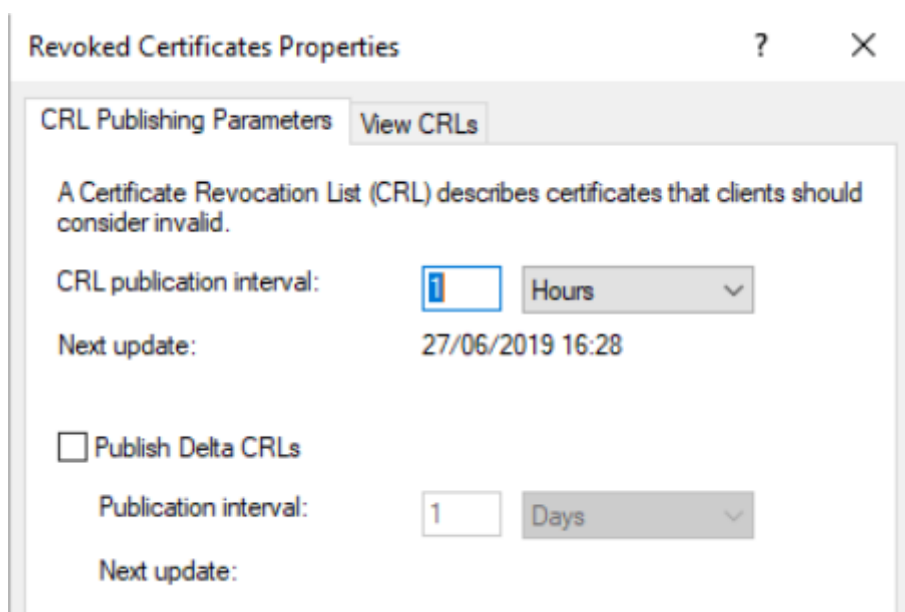
CRL Distribution Points (CDP) extensions

StoreFront does not enumerate resources from Citrix Virtual Apps and Desktops delivery controllers which are using revoked certificates whose serial numbers are listed in the published CRL. To detect which certificates have been revoked, StoreFront must be able to access the published CRL using one of the URLs defined in the CDP certificate extensions.



CRL publishing interval

To make StoreFront detect revoked certificates on the delivery controller more quickly, reduce the CRL publishing interval on the CA. Edit the properties of the CLR Distribution Points extension to set a lower CLR publishing interval value appropriate to your public key infrastructure.



Client CRL caching

The Windows public key infrastructure client caches CRLs locally. A more recent CRL is not downloaded until the locally cached CRL has expired.

StoreFront's access to certificate revocation lists (CRLs)

Certificate revocation checking relies on StoreFront's ability to access CRLs. Consider carefully how StoreFront contacts the webserver or the certificate authority (CA) that publishes the CRL, and how StoreFront receives CRL updates.

Internal enterprise CAs and private certificates on delivery controllers To use private CAs and certificates, StoreFront requires a correctly configured enterprise CA and a published CRL which it can access within your organization and internal network. Refer to Microsoft documentation for information on configuring the enterprise CA to publish CDP extensions. Any certificates on your delivery controllers, which existed before the CA was configured to include CDP extensions, may need to be reissued.

It is typical for StoreFront and Citrix Virtual Apps and Desktops servers to be in isolated private networks without access to the Internet. In this scenario, private CAs should be used.

External public CAs and public certificates on delivery controllers StoreFront servers and Citrix Virtual Apps and Desktops delivery controllers can use certificates issued by public CAs. StoreFront must be able to contact the public CA's webserver via the Internet, using the URL referenced in the CDP

extensions. If StoreFront cannot download a copy of the CRL using a CDP URL after a public certificate has been revoked, then StoreFront cannot perform the CRL check.

Certificate revocation policy settings

Use the Citrix StoreFront PowerShell cmdlets **Get-STFStoreFarmConfiguration** and **Set-STFStoreFarmConfiguration** to set the certificate revocation policy for a store. Running **Get-Help Set-STFStoreFarmConfiguration -detailed** displays the PowerShell help and examples containing the option `-CertRevocationPolicy`. For more information of these StoreFront PowerShell cmdlets, see [Citrix StoreFront SDK PowerShell Modules](#).

The **-CertRevocationPolicy** option can be set to the following values:

Setting	Description
NoCheck	StoreFront does not check the revocation state of the certificate on the delivery controller. StoreFront still enumerates resources from delivery controllers that use revoked certificates. This is the default setting.
MustCheck	This is the most secure option. StoreFront attempts to obtain a CRL by contacting the URLs referenced in the CDP extensions of the certificate on the delivery controller. StoreFront fails to enumerate from the delivery controller if the CRL is not available or if the certificate in use on the delivery controller has been revoked. The URL can point to an internal webserver if the certificate is private, or to a public internet webserver if the certificate is issued by a public CA.

Setting	Description
FullCheck	StoreFront attempts to contact the URLs published in the CDP extensions of the delivery controller certificate. If StoreFront fails to obtain a copy of the CRL from the URLs, then it still allows enumeration of resources from the delivery controller. If StoreFront successfully obtains the CRL and the delivery controller's certificate has been revoked, then StoreFront does not enumerate resources. The URL can point to an internal webserver if the certificate is private, or to a public internet webserver if the certificate is issued by a public CA.
NoNetworkAccess	Only CRLs, which have been imported locally into the Citrix Delivery Servers certificate store on the StoreFront server are checked. StoreFront does not attempt to contact any of the URLs specified in the CDP extensions. If StoreFront fails to obtain a local copy of the CRL, then it still allows enumeration of resources from the delivery controller. If StoreFront successfully obtains a local copy of the CRL from the Citrix Delivery Servers certificate store, and the delivery controller's certificate has been revoked, then StoreFront does not enumerate resources.

Configure a store for certificate revocation checking

To set the certificate revocation policy for a store, open the PowerShell ISE with **Run As Admin**, then run the following PowerShell cmdlets. If you have multiple stores, repeat this procedure on them all. -CertRevocationPolicy is a store-level setting which affects all delivery controllers configured for the store specified in \$StoreVirtualPath.

```
1 $SiteID = 1
2 $StoreVirtualPath = "/Citrix/Store"
3 $StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
4 $StoreVirtualPath
5 Set-STFStoreFarmConfiguration -StoreService $StoreObject -
  CertRevocationPolicy "MustCheck"
```

```
6 <!--NeedCopy-->
```

To check that the setting has been correctly applied, or to view the current -CertRevocationPolicy configuration, run the following:

```
1 (Get-STFStoreFarmConfiguration -StoreService $StoreObject).  
   CertRevocationPolicy  
2 <!--NeedCopy-->
```

Using locally imported CRLs on the StoreFront server

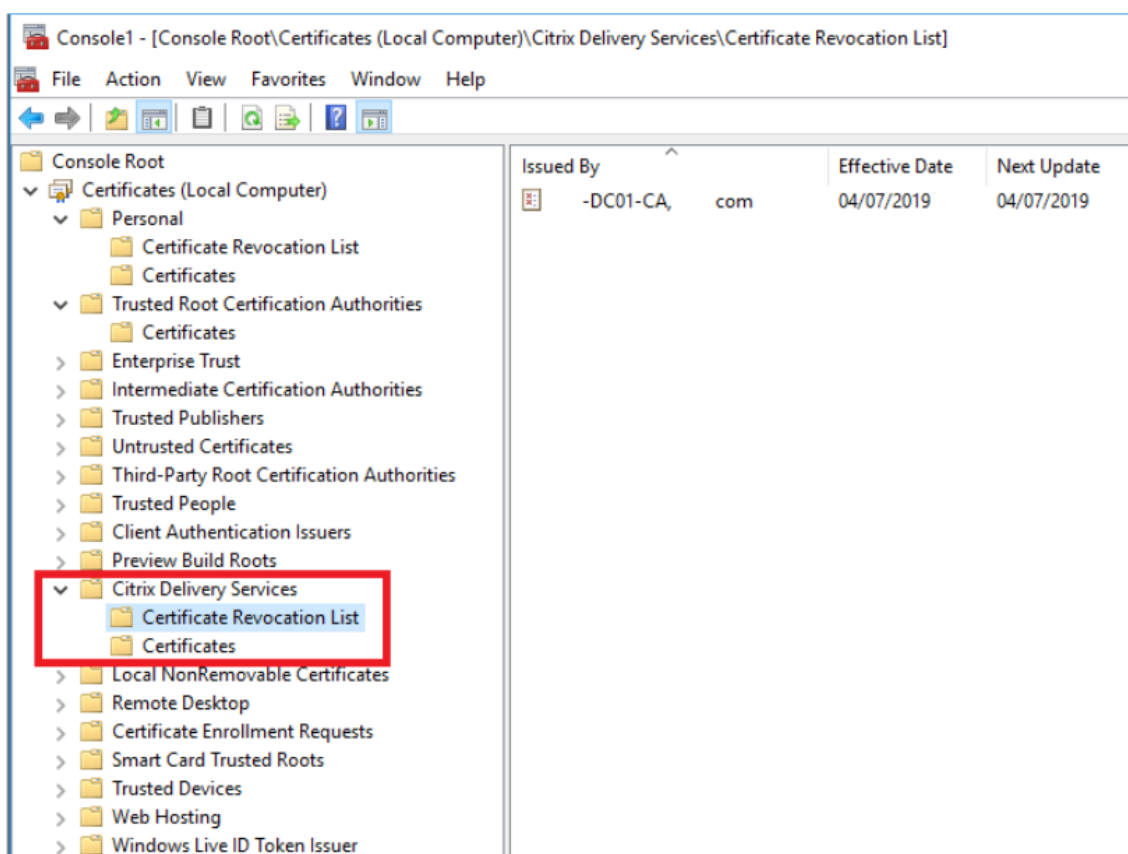
Using locally imported CRLs is supported, but Citrix does not recommend it because:

- They are difficult to manage and update in large enterprise deployments, where multiple StoreFront server groups may be involved.
- Manually updating CRLs on every StoreFront server, every time a certificate is revoked, is much less efficient than using CDP extensions and published CRLs on the entire active directory domain.

Using locally installed or updated CRLs can be used if -CertRevocationPolicy is set to “NoNetworkAccess”, and you have the means to distribute the CRL efficiently to all StoreFront servers.

To use locally imported CLR

1. Copy the CRL to the StoreFront server’s desktop. If the StoreFront server is part of a server group, copy it to all the StoreFront servers in the group.
2. Open the MMC snap-in and select **File > Add/remove Snapins > Certificates > Computer Account > Citrix Delivery Services certificate store**.
3. Right click and select **All Tasks > Import**, then browse to the .CRL file and choose **Select All Files > Open > Place all certificates in the following Store > Citrix Delivery Services**.



To add the CRL to the Citrix Delivery Services certificate store via PowerShell or the command line

1. Log into StoreFront and copy the .CRL file to the desktop of the current user.
2. Open the PowerShell ISE and select **Run as Admin**.
3. Run the following:

```
1 certutil -addstore "Citrix Delivery Services" "$env:UserProfile\Desktop\Example-DC01-CA.crl"
```

If successful, the following is returned:

```
1 Citrix Delivery Services
2 CRL "CN=Example-DC01-CA, DC=example, DC=com" added to store.
3 CertUtil: -addstore command completed successfully.
```

You can use this command as an example to distribute the CRL to all StoreFront servers in your deployment automatically via scripts.

XML authentication using delivery controllers

You can configure StoreFront to delegate user authentication to Citrix Virtual Apps and Desktops delivery controllers. Users are prevented from signing in to StoreFront if the certificate on the delivery controller has been revoked. This behaviour is desirable as active directory users should not be able to sign in to StoreFront if the certificate on the Citrix Virtual Apps and Desktops delivery controller, responsible for authenticating them, has been revoked.

To delegate user authentication to delivery controllers

1. Configure the store for certificate revocation as described in the previous section [Configure a store for certificate revocation checking](#).
2. Configure the delivery controller to use HTTPS, following the procedure described in [XML service-based authentication](#).

Configure an XML authentication service for certificate revocation checking

These steps are only required if you are using XML authentication in your deployment.

Note:

StoreFront supports two models for mapping stores to an authentication service. The recommended approach is a one-to-one mapping between store and Authentication Service. In this case you must perform the steps in this section on all stores and their respective authentication services.

Make sure that the certificate revocation mode is set to the same value for both the store and the authentication service. Alternatively, if the authentication configuration is identical for all stores, multiple stores can be configured to share a single authentication service.

The authentication service PowerShell cmdlets have no equivalent of **Set-STFStoreFarmConfiguration**, so a slightly different PowerShell approach is required. Use the same [Certificate revocation policy settings](#) describe in the earlier section.

1. Open the PowerShell ISE and select **Run As Admin**.

```
1 $SiteID = 1
2 $StoreVirtualPath = "/Citrix/Store"
3 $AuthVirtualPath = "/Citrix/StoreAuth"
4 <!--NeedCopy-->
```

2. Select the store service, authentication service, and delivery controller to be used for XML authentication. Ensure that the delivery controller is already configured for the Store.


```
1 $StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
   $StoreVirtualPath
2 $FarmObject = Get-STFStoreFarm -StoreService $StoreObject -
   FarmName "CVAD"
3 $AuthObject = Get-STFAuthenticationService -SiteID $SiteID -
   VirtualPath $AuthVirtualPath
4 <!--NeedCopy-->
```

3. Modify the CertRevocationPolicy property of the authentication service directly.

```
1 $AuthObject.FarmsConfiguration.CertRevocationPolicy = "FullCheck"
2 $AuthObject.Save()
3 Enable-STFXmlServiceAuthentication -AuthenticationService
   $AuthObject -Farm $FarmObject
4 <!--NeedCopy-->
```

4. Confirm that you have set the correct certificate revocation mode.

```
1 $AuthObject = Get-STFAuthenticationService -SiteID 1 -VirtualPath
   $AuthVirtualPath
2 $AuthObject.FarmsConfiguration.CertRevocationPolicy
3 <!--NeedCopy-->
```

Windows Event Viewer errors to expect

When CRL checking is enabled, errors are reported in the Windows Event Viewer on the StoreFront server.

To open the Event Viewer:

- On the StoreFront server type **Run**.
- Type **eventvwr** then press enter.
- In Applications and Services look for Citrix Delivery Services events.

Example Error: Store cannot contact a delivery controller with a revoked certificate

```
1 An SSL connection could not be established: An error occurred during
   SSL cryptography: Access is denied.
2
3 This message was reported from the Citrix XML Service at address https:
   //deliverycontrollerTLS.domain.com/scripts/wpnbr.dll.
4
5 The specified Citrix XML Service could not be contacted and has been
   temporarily removed from the list of active services.
6 <!--NeedCopy-->
```

Example Error: From Receiver for Web if user cannot log in due to failing XML authentication

```
1 An unexpected response was received during the authentication process.
2
3 Citrix.DeliveryServicesClients.Authentication.Exceptions.
   ExplicitAuthenticationFailure,
4 Citrix.DeliveryServicesClients.Authentication, Version=3.20.0.0,
5 Culture=neutral, PublicKeyToken=null
6
7 General Authentication Failure
8
9 ExplicitResult.State: 5
10
11 AuthenticationControllerRequestUrl:
12 https://storefront.example.com/Citrix/StoreWeb/ExplicitAuth/
   LoginAttempt
13
14 ActionType: LoginAttempt
15
16 at
17 Citrix.Web.AuthControllers.Controllers.ExplicitAuthController.
   GetExplicitAuthResult(ActionType
18 type, Dictionary`2 postParams)
19 <!--NeedCopy-->
```

Configure two StoreFront stores to share a common subscription datastore

February 27, 2024

The StoreFront installation process installs a Windows datastore locally on each StoreFront server to maintain its subscription data. In StoreFront server group environments, each server also maintains a copy of the subscription data used by its store. This data is propagated to other servers to maintain user subscriptions across the whole group. By default, StoreFront creates a single datastore for each store. Each subscription datastore is updated independently from each other store.

Where different configuration settings are required, it is common for administrators to configure StoreFront with two distinct stores; one for external access to resources using Citrix Gateway and another for internal access using the corporate LAN. You can configure both “external” and “internal” stores to share a common subscription datastore by making a simple change to the store web.config file.

In the default scenario involving two stores and their corresponding subscription datastores, a user must subscribe to the same resource twice. Configuring the two stores to share a common subscription database improves and simplifies the roaming experience when users access the same resource

from inside or outside the corporate network. With a shared subscription datastore it does not matter whether they use the “external” or “internal” store when they initially subscribe to a new resource.

- Each store has a web.config file located in C:\inetpub\wwwroot\citrix<storename>.
- Each store web.config contains a client endpoint for the Subscription Store Service.

```
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1__Citrix_<StoreName>" authenticationMode="windows" transferMode="Streamed">
```

The subscription data for each Store is located in:

```
C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>
```

For two stores to share a subscription datastore, you need only point one store to the subscription service end point of the other store. In the case of a server group deployment, all servers have identical pairs of stores defined and identical copies of the shared datastore they both share.

Note:

The Citrix Virtual Apps and Desktops controllers configured on each store must match exactly; otherwise, an inconsistent set of resource subscriptions on one store compared to another might occur. Sharing a datastore is supported only when the two stores reside on the same StoreFront server or server group deployment.

StoreFront subscription datastore endpoints

1. On a single StoreFront deployment, open the external store web.config file using Notepad and search for the clientEndpoint. For example:

```
1 <subscriptionsStoreClient enabled="true">
2 <clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1__Citrix_External" authenticationMode="windows" transferMode="Streamed">
3 <clientCertificate thumbprint="0" />
4 </clientEndpoint>
5 </subscriptionsStoreClient>
6 <!--NeedCopy-->
```

2. Change the external to match the internal store endpoint:

```
1 <subscriptionsStoreClient enabled="true">
2 <clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1__Citrix_Internal" authenticationMode="windows" transferMode="Streamed">
3 <clientCertificate thumbprint="0" />
4 </clientEndpoint>
```

```
5 </subscriptionsStoreClient>
6 <!--NeedCopy-->
```

3. If using StoreFront server group then propagate any changes made to the web.config file of the primary node to all other nodes.

Both stores are now set to share the internal store subscription datastore.

Manage favorites for a store

April 9, 2024

You can manage subscription data (favorites) for a store using PowerShell cmdlets.

Note:

Use either the StoreFront management console or PowerShell to manage StoreFront. Do not use both methods at the same time. Always close the StoreFront management console before using PowerShell to change your StoreFront configuration. Citrix also recommends that you take a backup of your existing subscription data before making changes so that rollback to a previous state is possible.

Purge subscription data

A folder and datastore containing subscription data exists for each store in your deployment.

1. Stop the Citrix Subscriptions Store service on the StoreFront server. If the Citrix Subscriptions Store service is running, it is not possible to delete subscription data for any of your stores.
2. Locate the subscription store folder on the StoreFront server: `C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>`
3. Delete the contents of the subscription store folder, but do not delete the folder itself.
4. Restart the Citrix Subscriptions Store service on the StoreFront server.

In StoreFront 3.5 or later, you can use the following PowerShell script to purge subscription data for a store. Run this PowerShell function as an administrator with rights to stop or start services and delete files. This PowerShell function achieves the same result as the manual steps described above.

To run the cmdlets successfully, the Citrix Subscriptions Store service must be running on the server.

```
1 function Remove-SubscriptionData
2 {
3
```

```
4      [CmdletBinding()]
5
6      [Parameter(Mandatory=$False)][String]$Store = "Store"
7
8      $SubsService = "Citrix Subscriptions Store"
9
10     # Path to Subscription Data in StoreFront version 2.6 or later
11
12     $SubsPath = "C:\Windows\ServiceProfiles\NetworkService\AppData\
        Roaming\Citrix\SubscriptionsStore\1__Citrix_$Store\*"
13
14     Stop-Service -displayname $SubsService
15
16     Remove-Item $SubsPath -Force -Verbose
17
18     Start-Service -displayname $SubsService
19
20     Get-Service -displayname $SubsService
21 }
22
23
24 Remove-SubscriptionData -Store "YourStore"
25 <!--NeedCopy-->
```

Export subscription data

You can obtain a backup of the Store subscription data in the form of a tab separated .txt file using the following PowerShell cmdlet.

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
    yourstore>"
2
3 Export-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env:
    :USERPROFILE\Desktop\Subscriptions.txt"
```

If you are managing a multiple-server deployment, you can run this PowerShell cmdlet on any server within the StoreFront server group. Each server in the server group maintains an identical synced copy of the subscription data from its peers. If you believe you are experiencing issues with subscription synchronization between the Storefront servers, then export the data from all servers in the group and compare them to see differences.

Restore subscription data

Use Restore-STFStoreSubscriptions to overwrite your existing subscription data. You can restore a Store's subscription data using the tab separated .txt file backup you created earlier using Export-STFStoreSubscriptions.

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
  yourstore>"
2 Restore-STFStoreSubscriptions -StoreService $StoreObject -FilePath "
  $env:USERPROFILE\Desktop\Subscriptions.txt"
3 <!--NeedCopy-->
```

For more information on Restore-STFStoreSubscriptions, see <https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/2402/Restore-STFStoreSubscriptions/>

Restoring Data on a Single StoreFront Server

In a single server deployment, there is no need to shut down the Subscriptions Store service. There is also no need to purge the existing subscription data before restoring the subscription data.

Restoring Data on a StoreFront Server Group

To restore subscription data to a server group, the following steps are required.

Example Server Group Deployment containing three StoreFront servers.

- StoreFrontA
 - StoreFrontB
 - StoreFrontC
1. Back up of the existing subscription data from any of the three servers.
 2. Stop the Subscriptions Store service on servers StoreFrontB and C. This action prevents the servers from sending or receiving subscription data during the update of StoreFrontA.
 3. Purge the subscription data from servers StoreFrontB and C. This prevents mismatch of the re-stored subscription data.
 4. Restore the data on StoreFrontA using the **Restore-STFStoreSubscriptions** cmdlet. It is not necessary to stop the Subscriptions Store service, or to purge the subscription data on StoreFrontA (it is overwritten during the restore operation).
 5. Restart the Subscriptions Store service on servers StoreFrontB and StoreFrontC. The servers can then receive a copy of the data from StoreFrontA.
 6. Wait for synchronization to occur between all servers. The time required depends on the number of records that exist on StoreFrontA. If all servers are on a local network connection, synchronization normally occurs quickly. Synchronization of subscriptions across a WAN connection may take longer.
 7. Export the data from StoreFrontB and C to confirm that the synchronization has completed, or view the Store Subscription counters.

Import subscription data

Use **Import-STFStoreSubscriptions** when there is no subscription data for the Store. This cmdlet also allows subscription data to be transferred from one Store to another or if subscription data is imported to newly provisioned StoreFront servers.

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
  yourstore>"
2 Import-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env
  :USERPROFILE\Desktop\Subscriptions.txt"
3 <!--NeedCopy-->
```

For more information on Import-STFStoreSubscriptions, see <https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/2402/Import-STFStoreSubscriptions/>

Subscription data file details

The subscription data file is a text file containing one line per user subscription. Each line is a tab-separated sequence of values:

```
<user-identifier> <resource-id> <subscription-id> <subscription-
status> <property-name> <property-value> <property-name> <property
-value> ...
```

where:

- **<user-identifier>** - Required. A sequence of characters identifying the user. This identifier is the user's Windows Security Identifier.
- **<resource-id>** - Required. A sequence of characters identifying the subscribed resource.
- **<subscription-id>** - Required. A sequence of characters uniquely identifying the subscription. This value is not used (although, a value must be present in the data file).
- **<subscription-status>** - Required. The status of the subscription: subscribed or unsubscribed.
- **<property-name>** and **<property-value>** - Optional. A sequence of zero or more pairs of property name/value pairs. These represent properties associated with the subscription by a StoreFront client (typically a Citrix Workspace app). A property with multiple values that is represented by multiple name/value pairs that have the same name (for example, "...MyProp A MyProp B ..." represents the property MyProp with values A, B).

Example

```
S-0-0-00-0000000000-0000000000-0000000000-0000    XenApp.Excel    21EC2020-3AEA-4069-A2DD-
08002B30309D Subscribed dazzle:position 1
```

Size of subscription data on the StoreFront server disk

No of Records	Size MB
0	6.02
1,000	7.02
10,000	40.00
100,000	219.00
200,000	358.00
500,000	784.00
800,000	1213.02
1,000,000	1597.15
1,300,000	1919.15
1,500,000	2205.15
2,000,000	2915.15

Size of import and export .txt files

No of Records	Size MB
0	0.00
1,000	0.13
10,000	1.30
100,000	12.80
200,000	25.60
500,000	64.10
800,000	102.00
1,000,000	128.00
1,300,000	166.00
1,500,000	192.00
1,700,000	218.00
2,000,000	256.00

Store Subscription Counters

You can use Microsoft Windows Performance Monitor counters (**Start > Run > perfmon**) to show, for example, the total numbers of subscription records on the server or number of records synchronized between StoreFront server groups.

View the Subscription Counters using PowerShell

```
1 Get-Counter -Counter "\Citrix Subscription Store(1__citrix_store)\
   Subscription Entries Count (including unpurged deleted records)"
2
3 Get-Counter -Counter "\Citrix Subscription Store Synchronization\
   Subscriptions Store Synchronizing"
4
5 Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number
   Subscriptions Synchronized"
6
7 Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number
   Subscriptions Transferred"
8 <!--NeedCopy-->
```

Store subscription data using Microsoft SQL Server

March 11, 2024

Note:

This document assumes basic knowledge of MS SQL server and T-SQL queries. Administrators must be comfortable configuring, using, and administering SQL server before attempting to follow this document.

Introduction

ESENT is an embeddable, transactional database engine which Windows can use. All versions of StoreFront support the use of a built in ESENT database by default. They can also connect to a Microsoft SQL server instance if the store is configured to use an SQL connection string.

The main advantage of switching StoreFront to using SQL instead of ESENT is that T-SQL update statements allow you to manage, modify, or delete subscription records. If you use SQL, you do not need to export, modify and re import the entire ESENT subscription data whenever minor changes to the subscription data are performed.

To migrate existing subscription data from ESENT to Microsoft SQL server, the flat ESENT data exported from StoreFront needs to be transformed into an SQL friendly format for bulk import. For new deployments without any new subscription data, this step is not required. The data transformation step is only needed once. This article describes the supported configuration which can be used in all StoreFront versions from version 3.5, which introduced the -STF PowerShell SDK referenced in the article.

Note:

Failures to connect to the SQL server instance used by StoreFront to store the subscription data due to network outages do not render the StoreFront deployment unusable. Outages only result in a temporarily degraded user experience; users cannot add, remove, or view favorite resources until the connection to SQL server is restored. Resources can still be enumerated and launched during the outage. The expected behavior is the same as if the Citrix Subscription Store service were to stop while using ESENT.

Tip:

Resources configured with KEYWORDS:Auto or KEYWORDS:Mandatory behave the same way when using both ESENT or SQL. New SQL subscription records are created automatically when a user first logs on if either KEYWORD is included in the user’s resources.

Advantages of ESENT and SQL server

ESENT	SQL
Default and requires no addition configuration to use StoreFront “out of the box”.	Much more manageable and subscription data can be manipulated or updated easily using T-SQL queries. Allows records per user to be deleted or updated Allows easy means to count records per application, delivery controller or user. Allows easy means to remove unnecessary user data for users who have left the company/organization. Allows easy means to update delivery controller references such as when the admin switches to using aggregation or new delivery controllers are provisioned.

ESENT	SQL
<p>Simpler to configure replication between different server groups using subscription syncing and pull schedules. See Configure subscription synchronization</p> <p>SQL unnecessary when subscription management is not needed. If the subscription data will never need updating, ESENT is likely to meet customer needs.</p>	<p>Decoupled from StoreFront so no need to back up the subscription data before StoreFront upgrade as the data is maintained on a separate SQL server. Subscription backup is independent of StoreFront and uses SQL backup strategies and mechanisms.</p> <p>Single copy of the subscription data shared by all members of the server group so less chance of data differences between servers or data syncing issues.</p>

Disadvantages of ESENT and SQL server

ESENT	SQL
<p>No easy means to manage subscription data easily and in a granular manner. Requires subscription manipulations to be done in exported .txt files. The whole subscription database must be exported and re imported. Potentially thousands of records may need to be changed using find and replace techniques, which is labor intensive and potentially error prone.</p> <p>A copy of the ESENT database must be maintained on each StoreFront server within a server group. On rare occasions this database can get out of sync within a server group or between different server groups.</p>	<p>Requires basic SQL expertise and infrastructure. Can require an SQL license to be purchased, which increases total cost of ownership of StoreFront deployment. Although a Citrix Virtual Apps and Desktops database instance can also be shared with StoreFront to reduce costs.</p> <p>Replicating subscription data between server groups is a non-trivial deployment task. It requires multiple SQL instances and transaction replication between each of them per data center. This requires specialized MS SQL expertise.</p> <p>Data migration from ESENT and transformation to SQL friendly format required. This process is only required once.</p> <p>Extra windows servers and licenses may be needed.</p> <p>Extra steps to deploy StoreFront.</p>

Deployment scenarios

Note:

Each store configured within StoreFront requires either an ESENT database or a Microsoft SQL database if you want to support user subscriptions. The method of storing the subscription data is set at the store level within StoreFront.

Citrix recommended all store databases reside on the same Microsoft SQL server instance to reduce management complexity and reduce the scope for misconfiguration.

Multiple stores can share the same database, provided they are all configured to use the same identical connection string. It does not matter if they use different delivery controllers. The disadvantage of multiple stores sharing a database is that there is no way to tell which store each subscription record corresponds to.

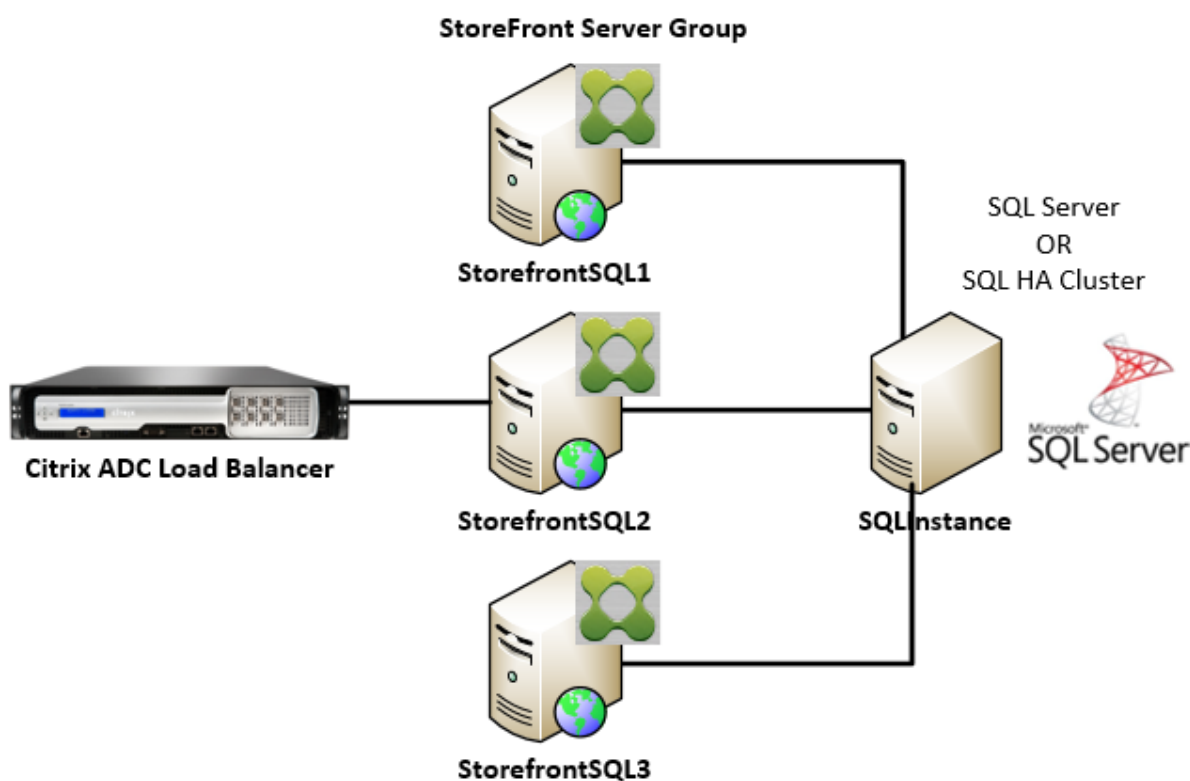
A combination of the two data storage methods is technically possible on a single StoreFront deployment with multiple stores. It is possible to configure one store to use ESENT and another to use SQL. This is not recommended due to increased management complexity and the scope for misconfiguration.

There are four scenarios you can use for storing subscription data in SQL Server:

Scenario 1: Single StoreFront Server or Server Group using ESENT (default) By default, all versions of StoreFront since version 2.0 use a flat ESENT database to store and replicate subscription data between members of a server group. Each member of the server group maintains an identical copy of the subscription database, which is synced with all other members of the server group. This scenario requires no additional steps to configure. This scenario is suitable for most customers who do not expect frequent changes to Delivery Controller names or do not need to perform frequent management tasks on their subscription data like removing or updating old user subscriptions.

Scenario 2: Single StoreFront Server and a local Microsoft SQL server instance installed StoreFront uses a locally installed SQL server instance and both components reside on the same server. This scenario is suitable for a simple single StoreFront deployment where customers might need to make frequent changes to Delivery Controller names, or they need to perform frequent management tasks on their subscription data like removing or updating old user subscriptions, but they do not require a high availability StoreFront deployment. Citrix do not recommend this scenario for server groups because it creates a single point of failure on the server group member that hosts the Microsoft SQL database instance. This scenario is not suitable for large enterprise deployments.

Scenario 3: StoreFront server group and a dedicated Microsoft SQL server instance configured for high availability (recommended) All StoreFront server group members connect to the same dedicated Microsoft SQL server instance or SQL failover cluster. This is the most suitable model for large enterprise deployments where Citrix administrators want to make frequent changes to delivery controller names or want to perform frequent management tasks on their subscription data like removing or updating old user subscriptions and require high availability.

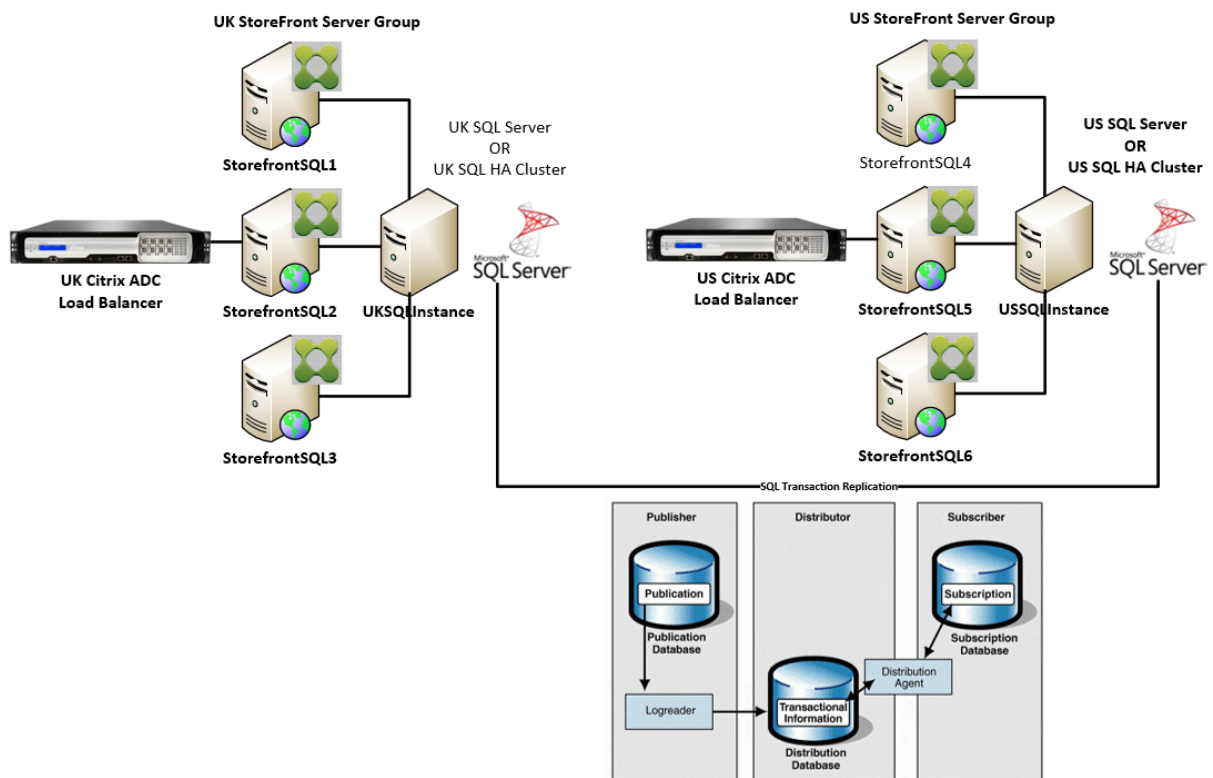


Scenario 4: Multiple StoreFront server groups and a dedicated Microsoft SQL server instance in each data center per server group

Note:

This is an advanced configuration. Only attempt it if you are an experienced SQL server administrator familiar with transaction replication, and you have the necessary skills to deploy it successfully.

This is the same as scenario 3, but extends it to situations where multiple StoreFront server groups are required in different remote data centers. Citrix Administrators may choose to synchronize subscription data between different server groups in the same or different data centers. Each server group in the data center connects to its own dedicated Microsoft SQL server instance for redundancy, failover, and performance. This scenario requires considerable extra Microsoft SQL server configuration and infrastructure. It relies entirely on Microsoft SQL technology to replicate the subscription data and its SQL transactions.



Resources

You can download the following scripts from <https://github.com/citrix/sample-scripts/tree/master/storefront> to help you:

Configuration scripts

- **Set-STFDatabase.ps1** –sets the MS SQL connection string for each Store. Run on the StoreFront server.
- **Add-LocalAppPoolAccounts.ps1** –grants the local StoreFront server’s app pools read and write access to the SQL database. Run for scenario 2 on the SQL server.
- **Add-RemoteSFAccounts.ps1** –grants the all StoreFront servers in a server group read and write access to the SQL database. Run for scenario 3 on the SQL server.
- **Create-StoreSubscriptionsDB-2016.sql** –creates the SQL database and schema. Run on the SQL server.

Data transformation and import scripts

- **Transform-SubscriptionDataForStore.ps1** –exports and transforms existing subscription data within ESENT into an SQL friendly format for import.

- **Create-ImportSubscriptionDataSP.sql** –creates a stored procedure to import the data transformed by Transform-SubscriptionDataForStore.ps1. Run this script once on the SQL server after you have created the database schema using Create-StoreSubscriptionsDB-2016.sql.

Configure the StoreFront server's local security group on the SQL Server

Scenario 2: Single StoreFront Server and a local Microsoft SQL server instance installed

Create a local security group called <SQLServer>\StoreFrontServers on the Microsoft SQL server, and add the virtual accounts for the IIS APPPOOL\DefaultAppPool and IIS APPPOOL\Citrix Receiver for Web to allow the locally installed StoreFront to read and write to SQL. This security group is referenced in the .SQL script that creates the store subscription database schema, so ensure that the group name matches.

You can download the script [Add-LocalAppPoolAccounts.ps1](#) to help you.

Install StoreFront before running the *Add-LocalAppPoolAccounts.ps1* script. The script depends on the ability to locate the IIS APPPOOL\Citrix Receiver for Web virtual IIS account, which does not exist until StoreFront has been installed and configured. IIS APPPOOL\DefaultAppPool is created automatically by installing the IIS webserver role.

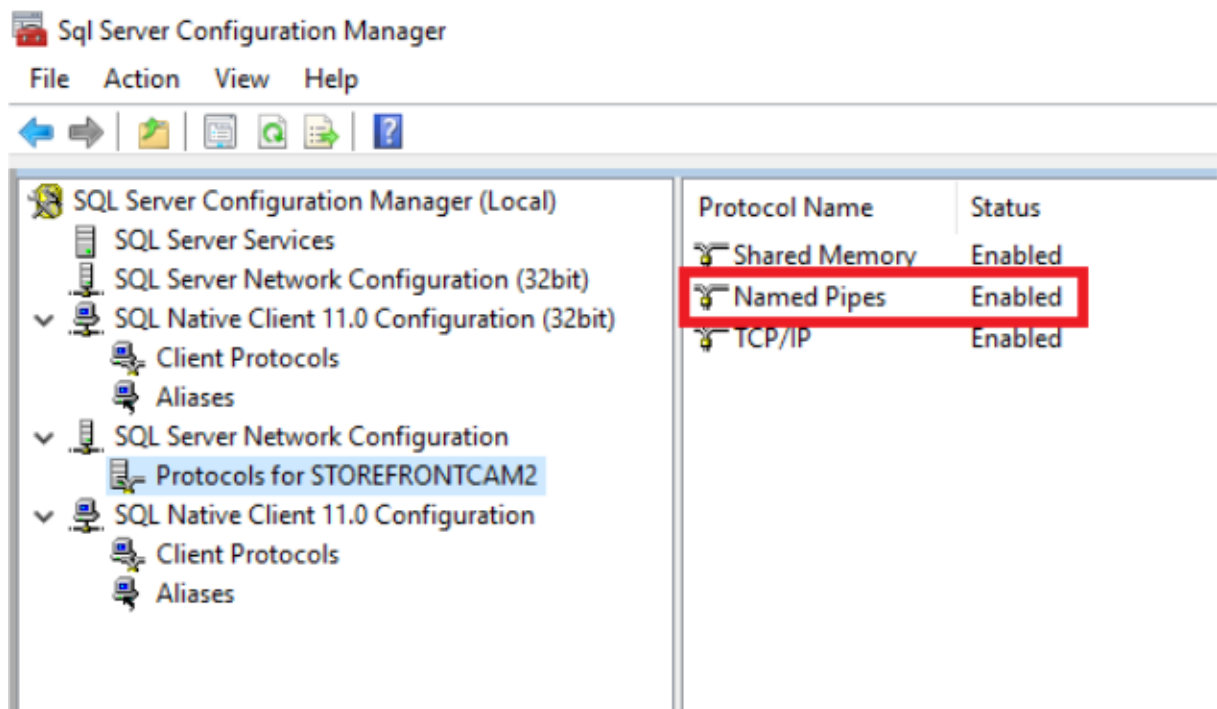
```
1 # Create Local Group for StoreFront servers on DB Server
2 $LocalGroupName = "StoreFrontServers"
3 $Description = "Contains StoreFront Server Machine Accounts or
   StoreFront AppPool Virtual Accounts"
4
5 # Check whether the Local Group Exists
6 if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))
7 {
8
9     Write-Host "$LocalGroupName already exists!" -ForegroundColor "
       Yellow"
10 }
11
12 else
13 {
14
15     Write-Host "Creating $LocalGroupName local security group" -
       ForegroundColor "Yellow"
16
17     # Create Local User Group
18     $Computer = [ADSI]"WinNT://$env:ComputerName,Computer"
19     $LocalGroup = $Computer.Create("group",$LocalGroupName)
20     $LocalGroup.setinfo()
21     $LocalGroup.description = $Description
22     $LocalGroup.SetInfo()
23     Write-Host "$LocalGroupName local security group created" -
       ForegroundColor "Green"
```

```

24 }
25
26 $Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"
27
28 # Add IIS APPPOOL\DefaultAppPool
29 $objAccount = New-Object System.Security.Principal.NTAccount("IIS
    APPPOOL\DefaultAppPool")
30 $StrSID = $objAccount.Translate([System.Security.Principal.
    SecurityIdentifier])
31 $DefaultSID = $StrSID.Value
32
33 $Account = [ADSI]"WinNT://$DefaultSID"
34 $Group.Add($Account.Path)
35
36 # Add IIS APPPOOL\Citrix Receiver for Web
37 $objAccount = New-Object System.Security.Principal.NTAccount("IIS
    APPPOOL\Citrix Receiver for Web")
38 $StrSID = $objAccount.Translate([System.Security.Principal.
    SecurityIdentifier])
39 $WebRSID = $StrSID.Value
40
41 $Account = [ADSI]"WinNT://$WebRSID"
42 $Group.Add($Account.Path)
43
44 Write-Host "AppPools added to $LocalGroupName local group" -
    ForegroundColor "Green"
45 <!--NeedCopy-->

```

Enable named pipes within your local SQL instance using SQL server configuration manager. Named pipes are required for interprocess communication between StoreFront and SQL server.



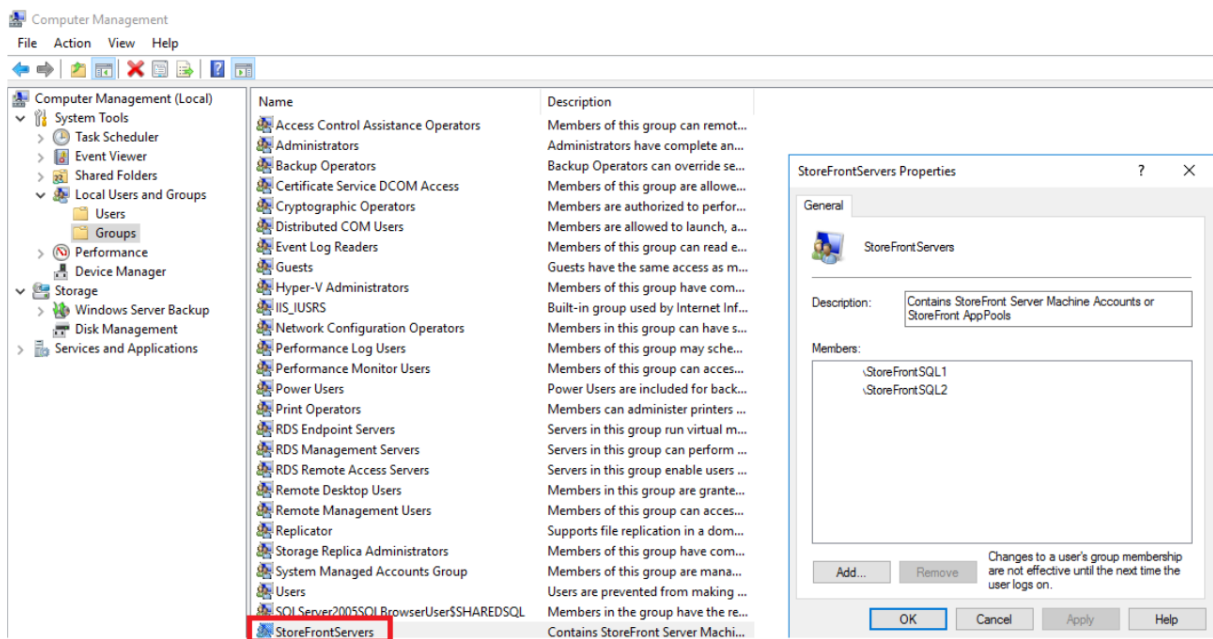
Ensure the Windows firewall rules are correctly configured to allow SQL server connections using either a specific port or dynamic ports. Refer to Microsoft documentation for how to do this in your environment.

Tip:

If connection to the local SQL instance fails, check that localhost or `<hostname>` used in the connection string resolves to the correct IPv4 address. Windows may attempt to use IPv6 instead of IPv4, and DNS resolution of localhost may return `::1` instead of the correct IPv4 address of the StoreFront and SQL server. Completely disabling the IPv6 network stack on the host server may be required to resolve this problem.

Scenario 3: StoreFront server group and a dedicated Microsoft SQL server instance

Create a local security group called `<SQLServer>\StoreFrontServers` on the Microsoft SQL server and add all members of the StoreFront server group. This security group is referenced later in the **Create-StoreSubscriptionsDB-2016.sql** script that creates the subscription database schema within SQL.



Add all StoreFront server group domain computer accounts to the `<SQLServer>\StoreFrontServers` group. Only StoreFront server domain computer accounts listed in the group will be able to read and write subscription records in SQL if Windows authentication is used by SQL server. The following PowerShell function, provided in script [Add-RemoteSFAccounts.ps1](#), creates the local security group and adds two StoreFront servers to it named StoreFrontSQL1 and StoreFrontSQL2.

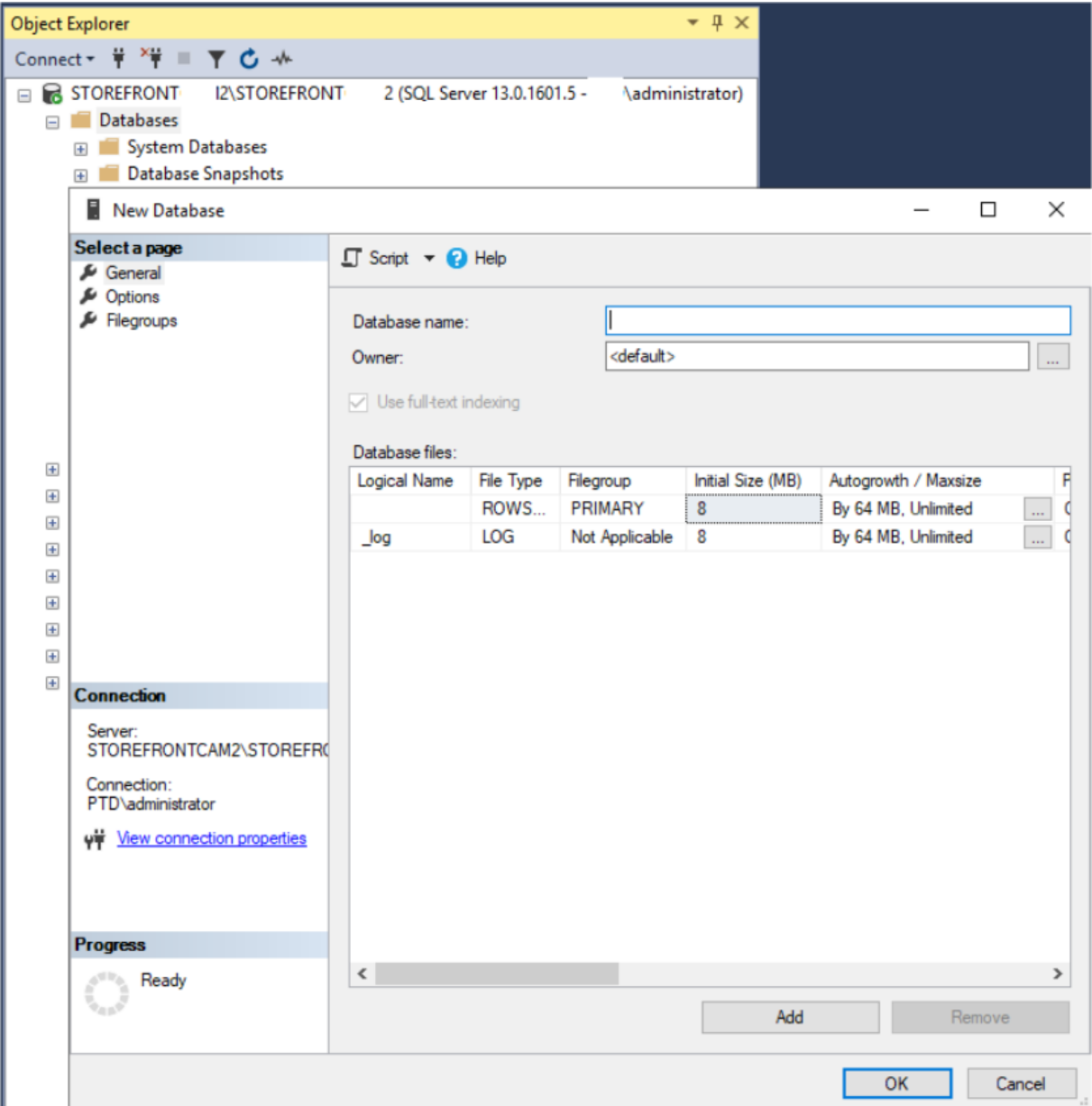
```
1 function Add-RemoteSTFMachineAccounts
2 {
```

```
3
4 [CmdletBinding()]
5 param([Parameter(Mandatory=$True)][string]$Domain,
6 [Parameter(Mandatory=$True)][array]$StoreFrontServers)
7
8 # Create Local Group for StoreFront servers on DB Server
9 $LocalGroupName = "StoreFrontServers"
10 $Description = "Contains StoreFront Server Machine Accounts or
    StoreFront AppPool virtual accounts"
11
12 # Check whether the Local Security Group already exists
13 if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))
14 {
15
16     Write-Host "$LocalGroupName already exists!" -ForegroundColor "
        Yellow"
17 }
18
19 else
20 {
21
22     Write-Host "Creating $LocalGroupName local group" -ForegroundColor
        "Yellow"
23
24     # Create Local Security Group
25     $Computer = [ADSI]"WinNT://$env:ComputerName,Computer"
26     $LocalGroup = $Computer.Create("group",$LocalGroupName)
27     $LocalGroup.setinfo()
28     $LocalGroup.description = $Description
29     $Localgroup.SetInfo()
30 Write-Host "$LocalGroupName local group created" -ForegroundColor "
    Green"
31 }
32
33 Write-Host "Adding $StoreFrontServers to $LocalGroupName local group" -
    ForegroundColor "Yellow"
34
35 foreach ($StoreFrontServer in $StoreFrontServers)
36 {
37
38     $Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"
39     $Computer = [ADSI]"WinNT://$Domain/$StoreFrontServer$"
40     $Group.Add($Computer.Path)
41 }
42
43 Write-Host "$StoreFrontServers added to $LocalGroupName" -
    ForegroundColor "Green"
44 }
45
46 Add-RemoteSTFMachineAccounts -Domain "example" -StoreFrontServers @"(
    StoreFrontSQL1","StoreFrontSQL2")
47 <!--NeedCopy-->
```

Configure the subscription database schema within Microsoft SQL Server for each store

Create a named instance on your Microsoft SQL server for use by StoreFront. Set the path within the .SQL script to correspond to where your version of SQL is installed, or its database files are stored. The example script [Create-StoreSubscriptionsDB-2016.sql](#) uses SQL Server 2016 Enterprise.

Create an empty database using SQL Server Management Studio (SSMS) by right clicking **Databases** then selecting **New Database**.



Type a **Database name** to match your store, or choose a different name such as *STFSubscriptions*.
Before running the script, for each store in your StoreFront deployment, modify the references in the

example script to match your StoreFront and SQL deployments. For example, modify:

- Name each database you create to match the store name in StoreFront in `USE [STFSubscriptions]`.
- Set the path to the database .mdf and .ldf files to where you want to store the database.

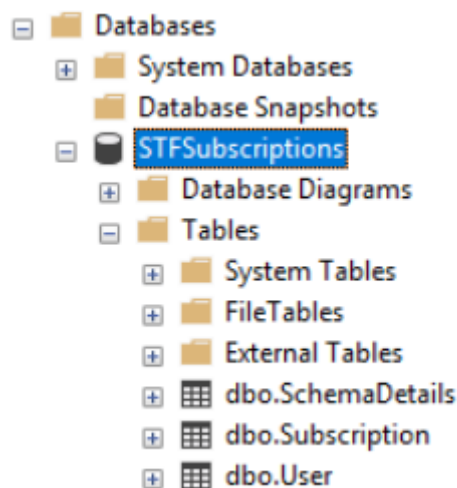
```
C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\STFSubscriptions.mdf
```

```
C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\STFSubscriptions.ldf
```

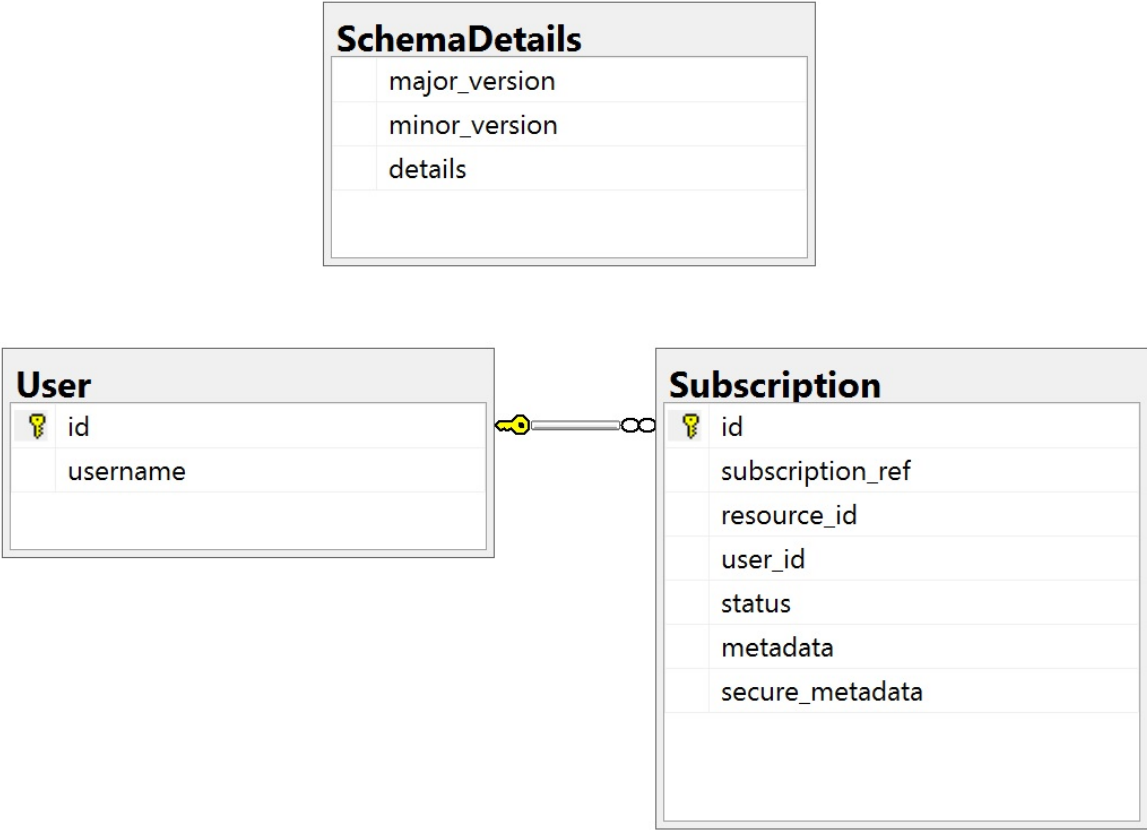
- Set the reference to your SQL server's name within the script:

```
CREATE LOGIN [SQL2016\StoreFrontServers] FROM WINDOWS;  
ALTER LOGIN [SQL2016\StoreFrontServers]
```

Run the script. After successful configuration of the schema, three database tables are created: *SchemaDetails*, *Subscription*, and *User*.



The following database diagram shows the subscriptions database schema that the *Create-StoreSubscriptionsDB-2016.sql* script creates:



Configure the SQL Server Connection String for each StoreFront store

Scenario 1

Tip:

The original subscription data stored on disk in the ESENT database is not destroyed or removed. If you decide to revert from Microsoft SQL server to using ESENT, it is possible to remove the store connection string and simply switch back to using the original data. Any additional subscriptions that were created while SQL was in use for the store will not exist in ESENT and users will not see these new subscription records. All original subscriptions records will still be present.

To re-enable ESENT subscriptions on a store Open the PowerShell ISE and select **Run as Administrator**.

Use the **-UseLocalStorage** option to specify the store you want to re-enable ESENT subscriptions on:

```
1 $SiteID = 1
2 $StoreVirtualPath = "/Citrix/Store1"
```

```
3
4 # Sets SQL DB Connection String
5 $StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath
   $StoreVirtualPath
6
7 # Removes the SQL DB Connection string and reverts back to using ESENT
8 Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
   UseLocalStorage
9 Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
10 <!--NeedCopy-->
```

Scenarios 2, 3 and 4

Open the PowerShell ISE and select **Run as Administrator**.

Specify the store you want to set a connection string for using **\$StoreVirtualPath**

```
1 $SiteID = 1
2 $VirtualPath= "/Citrix/Store1"
3 $DBName = "Store1"
4 $DBServer = "SQL2016Ent"
5 $DBLocalServer = "localhost"
6 $SQLInstance = "StoreFrontInstance"
7
8 # For a remote database instance
9 $ConnectionString = "Server=$DBServer\$SQLInstance;Database=$DBName;
   Trusted_Connection=True;"
10 <!--NeedCopy-->
```

OR

```
1 # For a locally installed database instance
2 $ConnectionString = "$DBLocalServer\$SQLInstance;Database=$DBName;
   Trusted_Connection=True;"
3
4 # Sets SQL DB Connection String
5 $StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath "/"
   Citrix/Store"
6 Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
   ConnectionString $ConnectionString
7 Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
8 <!--NeedCopy-->
```

Repeat the process for every store in your deployment if you want to configure them all to use an SQL connection string.

Migrate existing data from ESENT into Microsoft SQL Server

To migrate your existing ESENT data to SQL a two-step data transformation process is required. Two scripts are provided to assist you in performing this one-time operation. If the connection string in StoreFront and the SQL instance are correctly configured, then all new subscriptions are created automatically within SQL in the correct format. After migration, the historic ESENT subscription data is transformed into an SQL format and users can also see their previously subscribed resources.

Example: four SQL subscriptions for the same domain user

Results							Messages
id	subscription_id	resource_id	user_id	status	metadata	secure_metadata	
1	D002B848A9917585DC00F92A7005	XenDesktopSSL Notepad++ TLS	1	1	<SubscriptionProperties xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><property key="date:position"><value>1</value></property></SubscriptionProperties>	NULL	
2	2A3C23FE9145C74D9CF8B3C2118C27	XenDesktopSSL Windows Media Player TLS	1	1	<SubscriptionProperties xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><property key="date:position"><value>2</value></property></SubscriptionProperties>	NULL	
3	4206646F9102864200066E00F56A23	XenDesktopSSL Calculator TLS	1	1	<SubscriptionProperties xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><property key="date:position"><value>3</value></property></SubscriptionProperties>	NULL	
4	9632ACE317D0118E1F79C5A26929CA	XenDesktopSSL IE11 TLS	1	1	<SubscriptionProperties xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><property key="date:position"><value>4</value></property></SubscriptionProperties>	NULL	
id	username						
1	51525	6059					

Step 1 Use the Transform-SubscriptionDataForStore.ps1 script to convert the ESENT data into an SQL friendly format for bulk import Log into the StoreFront server that you want to transform ESENT data from.

Any member of a server group is suitable provided they all contain the same number of subscription records.

Open the PowerShell ISE and select **Run as Administrator**.

Run the script [Transform-SubscriptionDataForStore.ps1](#) which exports a <StoreName>.txt file from the ESENT database to the current user’s desktop.

The PowerShell script provides verbose feedback on each subscription row that is processed to aid debugging and help you assess the success of the operation. This may take a long time to process.

The transformed data is written out to <StoreName>SQL.txt on the current user’s desktop after the script has completed. The script summarizes the number of unique user records and the total number of subscriptions processed.

Repeat this process for every store you want to migrate to SQL server.

Step 2 Use a T-SQL stored procedure to bulk SQL import the transformed data Each store’s data must be imported one store at a time.

Copy the <StoreName>SQL.txt file created in Step 1 from the StoreFront server’s desktop to C : \ on the Microsoft SQL server and rename it to SubscriptionsSQL.txt.

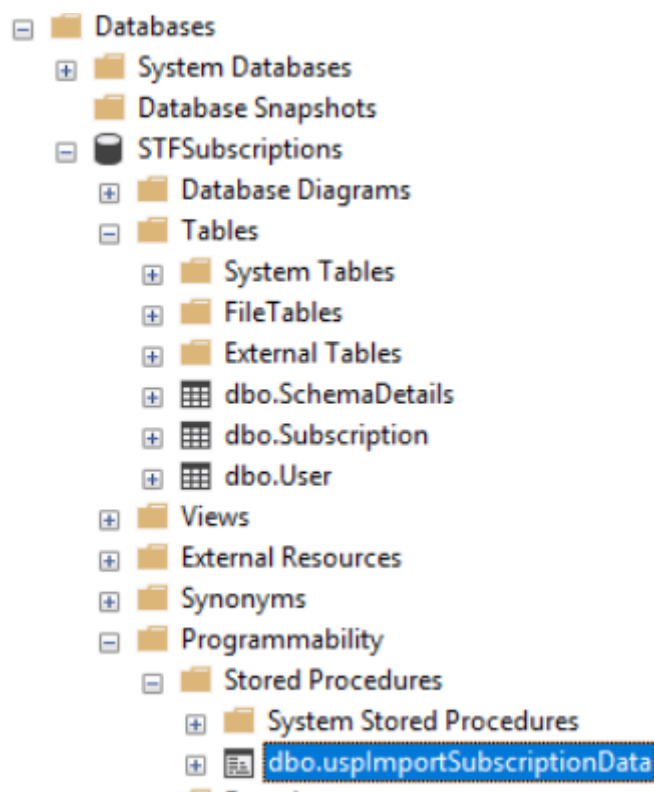
The [Create-ImportSubscriptionDataSP.sql](#) script creates a T-SQL stored procedure to bulk import the subscription data. It removes duplicate entries for each unique user so the resulting SQL data is correctly normalized and split into the correct tables.

Before executing *Create-ImportSubscriptionDataSP.sql*, change `USE [STFSubscriptions]` to match the database under which you want to create the Stored Procedure.

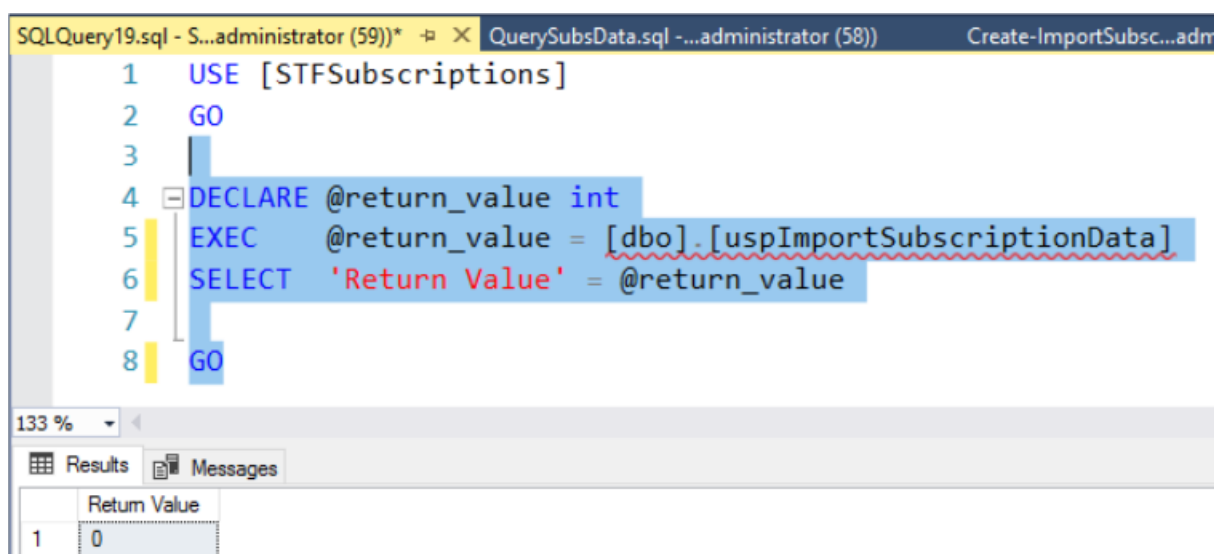
Open the *Create-ImportSubscriptionDataSP.sql* file using SQL Server Management Studio and execute the code within it. This script adds the *ImportSubscriptionDataSP* Stored Procedure to the database you created earlier.

After successful creation of the Stored Procedure the following message is shown in the SQL console, and the *ImportSubscriptionDataSP* Stored Procedure is added to the database:

Commands completed successfully.



Execute the Stored Procedure by right clicking it, then select **Execute Stored Procedure**, and click **OK**.



Return value 0 indicates all data imported successfully. Any problems on import are logged to the SQL console. After the stored procedure has run successfully, compare the total number of subscription records and unique users that [Transform-SubscriptionDataForStore.ps1](#) provides with the result of the two SQL queries below. The two totals should match.

The total number of subscriptions from the transformation script should match the total number reported from SQL by

```

1  SELECT COUNT(*) AS TotalSubscriptions
2  FROM [Subscription]
3  <!--NeedCopy-->

```

The number of unique uses from the transformation script should match the number of records in the User table reported from SQL by

```

1  SELECT COUNT(*) AS TotalUsers
2  FROM [User]
3  <!--NeedCopy-->

```

If the transformation script shows 100 unique users and 1000 total subscription records, then SQL should show the same two numbers after successful migration.

Log in to StoreFront to check whether existing users can see their subscription data. Existing subscription records are updated in SQL when users subscribe or unsubscribe their resources. New users and subscription records are also created in SQL.

Step 3 Run T-SQL queries on your imported data

Note:

All Delivery Controller names are case sensitive and must exactly match the case and name used within StoreFront.

```
1 -- Get all SQL subscription records
2 Use [STFSubscriptions]
3 SELECT * FROM [Subscription]
4 SELECT * FROM [User]
5 <!--NeedCopy-->
```

```
1 -- Get all subscription records for a particular user SID
2 Use [STFSubscriptions]
3 SELECT * FROM [Subscription]
4 INNER JOIN [User]
5 ON [Subscription].[user_id] = [User].[id]
6 WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
   xxxx'
7
8 -- Get total number of Subscription records for a particular user SID
9 Use [STFSubscriptions]
10 SELECT COUNT(Subscription.id)
11 FROM [Subscription]
12 INNER JOIN [User]
13 ON [Subscription].[user_id] = [User].[id]
14 WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
   xxxx'
15 <!--NeedCopy-->
```

```
1 -- Get all subscription records for a particular delivery controller
2 Use [STFSubscriptions]
3 SELECT * FROM [Subscription]
4 WHERE [resource_id] LIKE 'DeliveryController.%'
5
6 -- OR for aggregated resources use the name of the aggregation group
7 Use [STFSubscriptions]
8 SELECT * FROM [Subscription]
9 WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'
10
11 -- Get all subscription records for a particular application
12 Use [STFSubscriptions]
13 SELECT * FROM [Subscription]
14 WHERE [resource_id] = ' DeliveryController.Application'
15 <!--NeedCopy-->
```

Update or delete existing subscription records using T-SQL

DISCLAIMER:

All example SQL update and delete statements are used entirely at your own risk. Citrix is not responsible for any loss or accidental alteration of your subscription data by incorrect use of the provided examples. The following T-SQL statements are provided as a guide to enable simple updates to be performed. Back up all subscription data in SQL database full backups before

attempting to update your subscriptions or remove obsolete records. Failure to perform the necessary backups may result in data loss or corruption. Before executing your own T-SQL UPDATE or DELETE statements against the production database, test them on dummy data or on a redundant copy of the production data away from the live production database.

Note:

All Delivery Controller names are case sensitive and must exactly match the case and name used within StoreFront.

```
1 -- Update the delivery controller used in all subscriptions.
2 Use [STFSubscriptions]
3 UPDATE [Subscription]
4 SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
    NewDeliveryController.')
5 WHERE [resource_id] LIKE 'OldDeliveryController.%'
6 <!--NeedCopy-->
```

```
1 -- After enabling multi-site aggregation, update the resource_id
2 Use [STFSubscriptions]
3 UPDATE [Subscription]
4 SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
    DefaultAggregationGroup.')
5 WHERE [resource_id] LIKE 'OldDeliveryController.%'
6 <!--NeedCopy-->
```

```
1 -- Delete all subscription records for a particular Delivery Controller
2 Use [STFSubscriptions]
3 DELETE FROM [Subscription]
4 WHERE [resource_id] LIKE 'DeliveryController.%'
5 <!--NeedCopy-->
```

```
1 -- OR for aggregated resources use the name of the aggregation group
2 Use [STFSubscriptions]
3 DELETE FROM [Subscription]
4 FROM [Subscription]
5 WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'
6 <!--NeedCopy-->
```

```
1 -- Delete all subscription records for a particular application
2 Use [STFSubscriptions]
3 DELETE FROM [Subscription]
4 FROM [Subscription]
5 WHERE [resource_id] LIKE '%.Application'
6 <!--NeedCopy-->
```

```
1 -- Delete all subscription records for an application published via a
    specific delivery controller
2 Use [STFSubscriptions]
3 DELETE FROM [Subscription]
4 FROM [Subscription]
```

```
5 WHERE [resource_id] = 'DeliveryController.Application'
6 <!--NeedCopy-->
```

```
1 -- Delete all subscription records for a particular user SID
2 -- relies on cascade to delete records from [Subscription]
3 Use [STFSubscriptions]
4 DELETE FROM [User]
5 WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
   xxxx'
6 <!--NeedCopy-->
```

```
1 -- Delete ALL subscription data from a particular database and reset
   the primary key clustered index to start numbering from 0.
2 -- USE WITH EXTREME CARE AND NOT ON LIVE PRODUCTION DATABASES.
3 -- Can be useful whilst debugging data import issues to start with a
   clean database.
4
5 Use [STFSubscriptions]
6 DELETE FROM [Subscription]
7 DBCC CHECKIDENT ([Subscription], RESEED, 0)
8 DELETE FROM [User]
9 DBCC CHECKIDENT ([User], RESEED, 0)
10 <!--NeedCopy-->
```

Enable or disable favorites

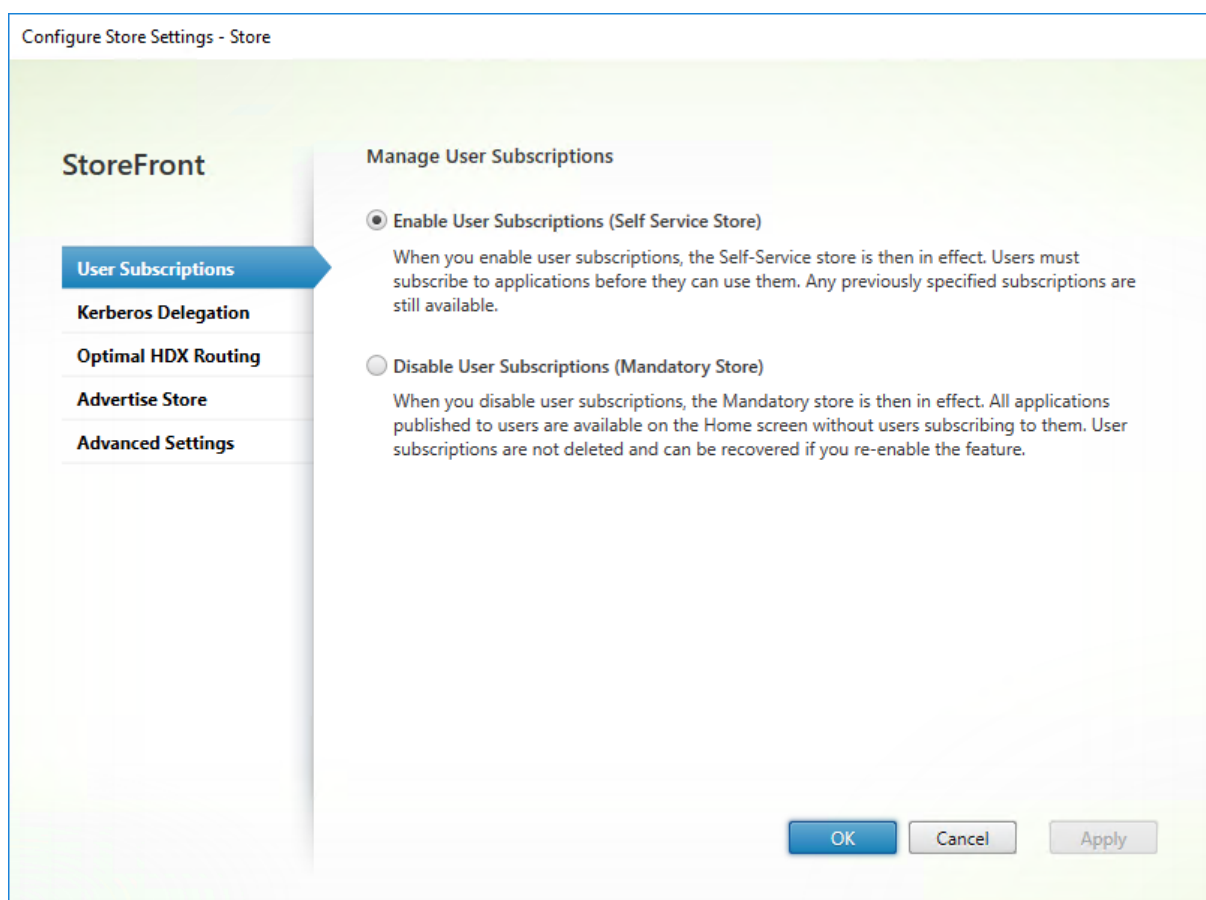
March 19, 2024

Use the User Subscriptions screen to do select one of the following options:

- Allow users to create and remove favorites (Self Service Store). Users can favorite an app by clicking the star on the app tile. Users can click the star again un-favorite an app. Favorite apps are displayed on the **Home** tab.
- Disable favorites (Mandatory Store). Users cannot favorite or un-favorite apps. The home tab is not displayed.

Disabling subscriptions does not delete the Store subscription data. Re-enabling subscriptions for the store will allow the user to see their favourites whenever they next log on.

1. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the **Actions** pane, click **Configure Store Settings**
2. Click on the **User Subscriptions** tab to toggle the user favorites feature off or on.
3. Choose **Enable user subscriptions (Self Service Store)** to enable favorites.
4. Choose **Disable user subscriptions (Mandatory Store)** to disable favorites.



Alternatively, you can use the PowerShell cmdlet [Get-STFStoreService](#) to configure user subscriptions for a store, for example:

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
   yourstore>"
2 Set-STFStoreService -StoreService $StoreObject -LockedDown $True -
   Confirm:$False
3 <!--NeedCopy-->
```

Citrix Virtual Apps and Desktops configuration

March 11, 2024

When delivering applications with Citrix Virtual Apps and Desktops or Citrix Desktops as a Service, consider the following options to enhance the experience for users when they access their applications through your stores. For more information about delivering applications, see [Applications](#).

- In the **Application name (for user)** field enter the application name as you wish it to appear within your store website.

- In the **Description and keywords** field enter the description that is displayed on the store website when you expand the app details, alongside any keywords.
- Choose the **Application icon** to help users visually identify an application on the StoreFront website.
- In the **Application category** field, optionally enter a category. Include \ in the category name to create a folder hierarchy. You could, for example, group applications according to type or, alternatively, create folders for different user roles in your organization. In the store website **Apps** tab, **Category** view displays a list of categories and the apps in each category.

Keywords

You can add keywords to an app or desktop by appending the string `KEYWORDS : [keywordname]` to the application description. Multiple keywords must be separated by spaces only; for example, `KEYWORDS :Accounts Featured`. Keywords can be used in a number of ways:

- Filter applications - see [Advanced store settings](#))
- Create [Featured app groups](#).
- Some keywords have special meanings.

Keyword name	Description
Mandatory	Adds an application to the Home tab. Unlike favourites, users cannot remove mandatory applications from the Home tab. Has no effect if favourites are disabled for the store.
Auto	When users log on to the store, the application or desktop is automatically favourited and added to their Home tab. Users can unfavourite such applications. Has no effect if favourites are disabled for the store.
TreatAsApp	Apply to desktops to force StoreFront to treat it as an app. The desktop is displayed on the Apps tab rather than the Desktops tab. In addition, the desktop is not automatically started when the user logs on to the store website and is not accessed with the Desktop Viewer, even if the site is configured to do this for other desktops.

Keyword name	Description
prefer="application"	Where <i>application</i> identifies a locally installed application. Applies only on Citrix Workspace app on Windows. This indicates that the locally installed version of an application should be used in preference to the equivalent delivered instance if both are available. For more information, see Configuring Local App Access applications .
Primary and Secondary	When using Multi-Site Aggregation , the one with the keyword primary specified always preferred over the one with the keyword secondary .

Advanced store settings

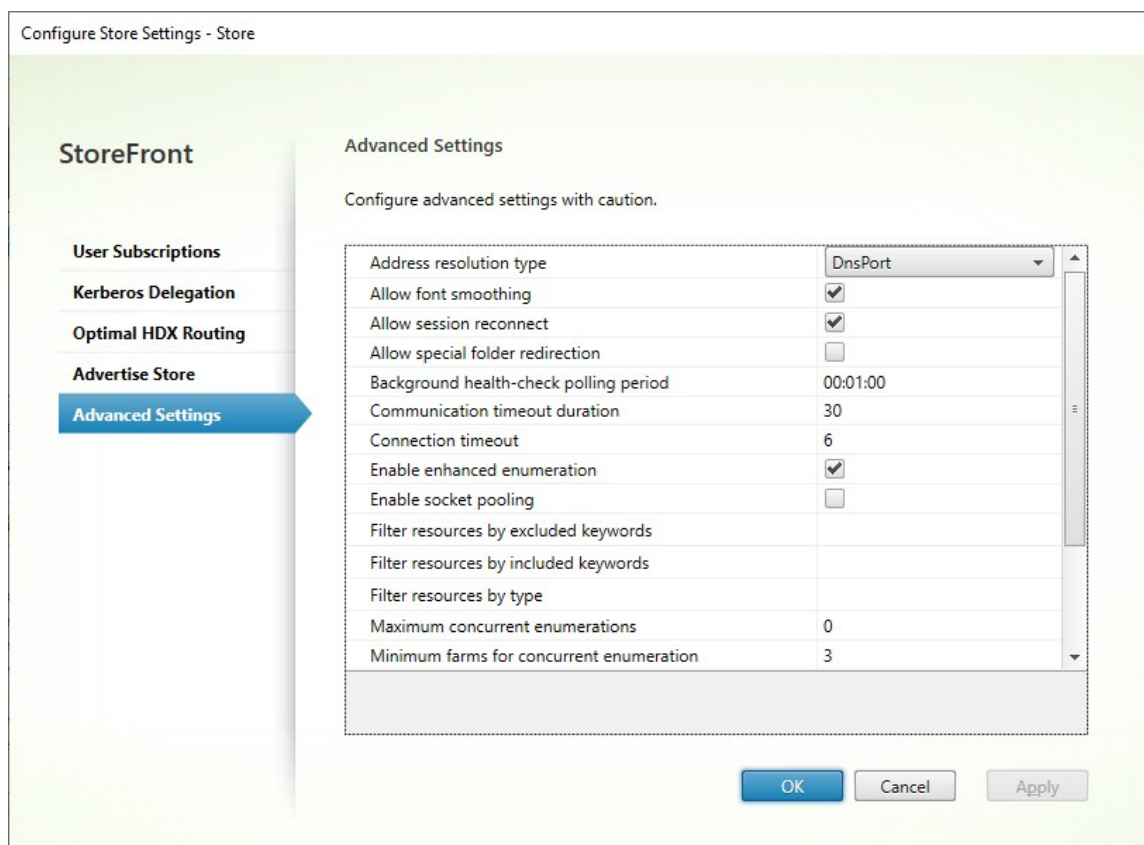
April 9, 2024

You can configure most advanced store properties by using the Advanced Settings page in the Configure Store Settings. Some settings can only be modified using PowerShell.

Important:

In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, [propagate your configuration changes to the server group](#) so that the other servers in the deployment are updated.

1. Select the Stores node in the left pane of the Citrix StoreFront management console, select a store in the center pane, and in the Action pane, select **Configure Store Settings**.
2. On the **Configure Store Settings** page, select **Advanced Settings** and make the required changes.



3. Click **OK** to save your changes.

Address resolution type

You can specify the type of address to request from the server. The default is DnsPort.

From the **Advanced Settings** window, choose a value from the **Address resolution type** drop down list.

- Dns
- DnsPort
- IPV4
- IPV4Port
- Dot
- DotPort
- Uri
- NoChange

Allow font smoothing

You can specify if you want font smoothing for HDX sessions. The default is On.

From the **Advanced Settings** window, select the **Allow font smoothing** option, and click **OK**.

Allow session reconnect

You can specify if you want HDX sessions to be reconnected. The default is On.

From the **Advanced Settings** window, select the **Allow session reconnect** option.

Allow special folder redirection

With special folder redirection configured, users can map Windows special folders for the server to those on their local computers. Special folders refer to standard Windows folders, such as *\Documents* and *\Desktop*, which are always presented in the same way regardless of the operating system.

From the **Advanced Settings** window, select or clear the **Allow special folder redirection** option to enable or disable special folder redirection, and click **OK**.

Advanced health check

StoreFront runs periodic health checks on each Citrix Virtual Apps and Desktops delivery controller, Cloud Connector and Secure Private Access server to reduce the impact of intermittent server availability. With Advanced health check StoreFront performs a more in-depth check that is more likely to detect any issues.

When connecting to Citrix Desktops as a Service via a Cloud connector, advanced health check has the added benefit that it retrieves additional information about what VDAs are in the same location as the cloud connector. In the event that the cloud connectors are unable to contact Citrix Desktops as a Service, cloud connectors use their local host cache to facilitate connections to VDAs that are co-located. StoreFront uses the additional information from the advanced health check results to contact the most appropriate online connector to launch apps and desktops.

To ensure resource availability during an outage, without having to publish resources in every zone (resource location), ensure that on all StoreFront servers you configure the resource feed to include all cloud connectors in all resource locations and enable the advanced health check feature.

Advanced health check is enabled by default for new stores. Citrix recommends that you leave it enabled for all StoreFront deployments. To enable or disable advanced health check, use the PowerShell cmdlet [Set-STFStoreFarmConfiguration](#) with parameter [AdvancedHealthCheck](#).

Background health check polling period

StoreFront runs periodic health checks on each Citrix Virtual Apps and Desktops delivery controller, Cloud Connector and Secure Private Access server to reduce the impact of intermittent server availability. The default is every minute (00:01:00). From the **Advanced Settings** window, specify a time for the **Background health-check Polling period**, and click **OK** to control the frequency of the health check. Setting the polling period to a low value is not recommended when the Advanced health check is enabled as it may have an impact on performance.

Communication time-out duration

By default, requests from StoreFront to a server providing resources for a store time out after 30 seconds. The server is considered unavailable after 1 unsuccessful communication attempt. From the **Advanced Settings** window, make your changes to the default time, and click **OK** to change these settings.

Connection timeout

You can specify the number of seconds to wait when establishing an initial connection with a Delivery Controller. The default is 6.

From the **Advanced Settings** window, specify the seconds to wait when establishing the initial connection, and click **OK**.

Enable enhanced enumeration

This option controls whether StoreFront queries Delivery Controllers concurrently or sequentially when enumerating apps and desktops across multiple Citrix Virtual Apps and Desktops Sites. Concurrent enumeration provides faster responses to user queries when aggregating resources across multiple Sites. When this option is selected (the default), StoreFront sends out enumeration requests to all Delivery Controllers at the same time and aggregates responses when they have all responded. You can use the options **Maximum concurrent enumerations** and **Minimum farms for concurrent enumeration** to tune this behavior.

From the **Advanced Settings** window, select (or clear) the **Enable enhanced enumeration** option, and click **OK**.

Enable socket pooling

Socket pooling is disabled by default in stores. When socket pooling is enabled, StoreFront maintains a pool of sockets, rather than creating a socket each time one is needed and returning it to the

operating system when the connection is closed. Enabling socket pooling enhances performance, particularly for Secure Sockets Layer (SSL) connections. To enable socket pooling, you edit the store configuration file. From the **Advanced Settings** window select the **Enable socket pooling** option, and click **OK** to enable socket pooling.

File type association

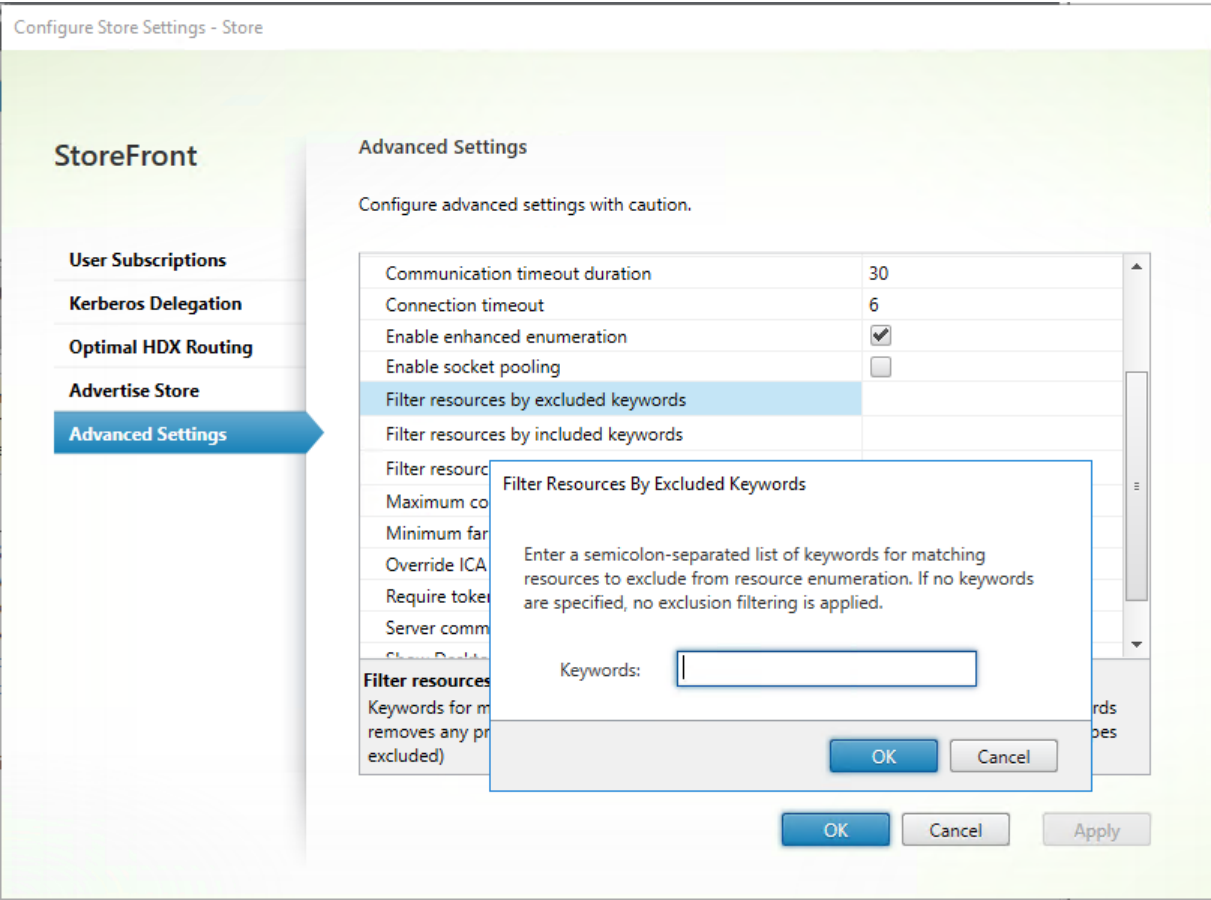
By default, file type association is enabled in stores so that content is seamlessly redirected to users' subscribed applications when they open local files of the appropriate types. To enable disable file type association, use the PowerShell command [Set-STFStoreFarmConfiguration](#). For example:

```
1 $storeService = Get-STFStoreService -VirtualPath '/Citrix/Store'  
2 Set-STFStoreFarmConfiguration $storeService -EnableFileTypeAssociation  
   $false  
3 <!--NeedCopy-->
```

Filter resources by excluded keywords

You can filter matching resources by excluded keywords. Specifying exclusion keywords removes any previously configured inclusion keywords. The default is no filtering (no resource types excluded).

1. From the **Advanced Settings** window, find the **Filter resources by excluded keywords** row.
2. Click in the right hand column to bring up the **Filter resources by excluded keywords** window.
3. Enter a semicolon-separated list of keywords in the enter keywords box
4. Click **OK**.



To change the setting using PowerShell, use cmdlet [Set-STFStoreEnumerationOptions](#) with parameter `-FilterByKeywordsExclude`.

The following keywords are reserved and must not be used for filtering:

- Auto
- Mandatory

Filter resources by included keywords

You can filter matching resources by inclusion keywords. Specifying inclusion keywords removes any previously configured exclusion keywords. The default is no filtering (no resource types excluded).

1. From the **Advanced Settings** window, find the **Filter resources by included keywords** row.
2. Click in the right hand column to bring up the **Filter resources by included keywords** window.
3. Enter a semicolon-separated list of keywords in the enter keywords box
4. Click **OK**.

To change the setting using PowerShell, use cmdlet [Set-STFStoreEnumerationOptions](#) with parameter `-FilterByKeywordsInclude`.

The following keywords are reserved and must not be used for filtering:

- Auto
- Mandatory

Filter resources by type

Choose the resource types to be included in resource enumeration. The default is No filtering (all resource types included).

From the **Advanced Settings** window, select **Filter resources by type**, click to the right of it, choose the resource types to include in the enumeration, and click **OK**.

To change the setting using PowerShell, use cmdlet [Set-STFStoreEnumerationOptions](#) with parameter `-FilterByTypesInclude`, specifying an array of resource types (Applications, Desktops or Documents).

Maximum concurrent enumerations

Specify the maximum number of concurrent requests to send to all Delivery Controllers. This option takes effect when the option **Enable enhanced enumeration** is enabled. The default is 0 (No Limit).

From the **Advanced Settings** window, select **Maximum concurrent enumerations**, enter a number, and click **OK**.

Minimum farms for concurrent enumeration

Specify the minimum number of Delivery Controllers required to trigger concurrent enumeration. This option takes effect when the option **Enable enhanced enumeration** is enabled. The default is 3.

From the **Advanced Settings** window, select **Minimum farms for concurrent enumerations**, enter a number, and click **OK**.

Override ICA client name

Overrides the client name setting in the .ica launch file with a unique ID generated by the web browser. When disabled, Citrix Workspace app specifies the client name. The default is Off.

From the **Advanced Settings** window, select the **Override the ICA client name** option, and click **OK**.

Require token consistency

When enabled, StoreFront enforces consistency between the gateway used to authenticate and the gateway used to access the store. When the values are inconsistent, users must reauthenticate. You must enable this for Smart Access. You must disable this if users access the store through a gateway with authentication disabled. The default is On.

From the **Advanced Settings** window, select the **Require token consistency** option, and click **OK**.

Server communication attempts

Specify the number of attempts to communicate with Delivery Controllers before marking them unavailable. The default is 1.

From the **Advanced Settings** window, select **Server communication attempts**, enter a number, and click **OK**.

Show Desktop Viewer for legacy clients

Specify whether to show the Citrix Desktop Viewer window and toolbar when users access their desktop from legacy clients. The default is Off.

From the **Advanced Settings** window, select the **Show Desktop Viewer for legacy clients** option, and click **OK**.

Treat desktops as apps

Specify whether, when the store is accessed, Desktops are displayed in the Apps view rather than in the Desktops view. The default is Off.

From the **Advanced Settings** window, select the **Treat desktops as apps** option, and click **OK**.

Configure optimal HDX routing for a store

March 19, 2024

Configure optimal Citrix Gateway routing to optimize the handling of ICA connection routing from the HDX engine to Citrix Virtual Apps and Desktops published applications using StoreFront. Typically, the optimal gateway for a site is colocated in the same geographical location.

You need only define optimal Citrix Gateway appliances for deployments where the appliance through which users access StoreFront is not the optimal gateway. If launches should be directed back through the gateway making the launch request, StoreFront does this automatically.

You can either map gateways to specific delivery controllers or to zones. A zone is a grouping of delivery controllers and usually represents a data center in a geographic location. Zones are defined in Citrix Virtual Apps and Desktops and any zones defined in StoreFront must exactly match the zone names defined in Citrix Virtual Apps and Desktops. You can map an optimal gateway to more than one zone, but typically you should use a single zone. A zone usually represents a data center in a geographic location. It is expected that each zone has at least one optimal Citrix Gateway that is used for HDX connections to resources within that zone.

For more information about zones, see [Zones](#).

Example scenario using farms

1 x UK Gateway -> 1 x UK StoreFront

- UK Apps and Desktops local
- US Apps and Desktops used only for UK failover

1 x US Gateway -> 1 x US StoreFront

- US Apps and Desktops local
- UK Apps and Desktops used only for US failover

A UK gateway provides remote access to UK hosted resources such as apps and desktops using a UK StoreFront.

The UK StoreFront has both a UK-based and US-based Citrix Gateway defined and UK and US controllers in its Delivery Controller list. UK users access remote resources through their geographically colocated gateway, StoreFront, and farms. If their UK resources become unavailable, they can connect to US resources as a temporary failover alternative.

Without optimal gateway routing all ICA launches would pass through the UK gateway that made the launch request regardless of where the resources are geographically located. By default, gateways used to make launch requests are identified dynamically by StoreFront when the request is made. Optimal gateway routing overrides this and forces US connections through the gateway closest to the US farms that provides apps and desktops.

Note:

You can map only one optimal gateway per site for each StoreFront store.

Example scenario using zones

1 x CAMZone -> 2 x UK StoreFronts

- Cambridge, UK: Apps and Desktops
- Fort Lauderdale, Eastern US: Apps and Desktops
- Bangalore, India: Apps and Desktops

1 x FTLZone -> 2 x US StoreFronts

- Fort Lauderdale, Eastern US: Apps and Desktops
- Cambridge, UK: Apps and Desktops
- Bangalore, India: Apps and Desktops

1 x BGLZone -> 2 x IN StoreFronts

- Bangalore, India: Apps and Desktops
- Cambridge, UK: Apps and Desktops
- Fort Lauderdale, Eastern US: Apps and Desktops

Figure 1. Suboptimal gateway routing

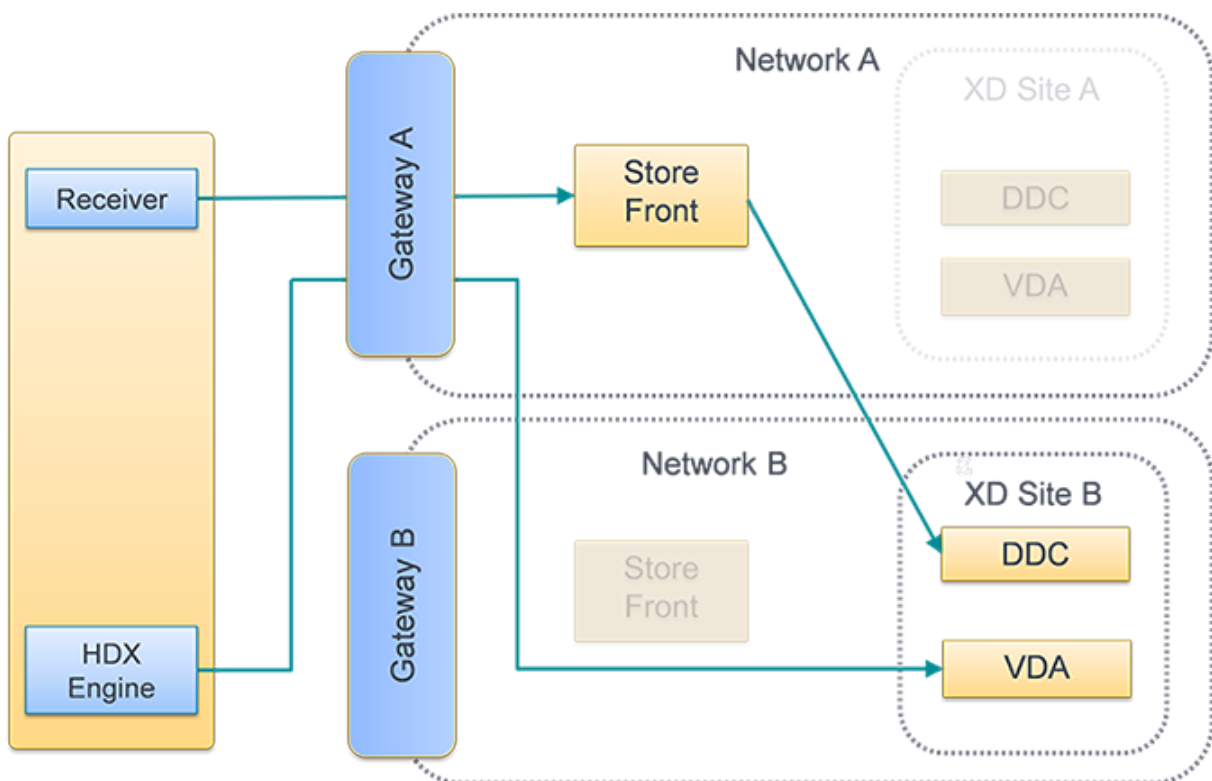
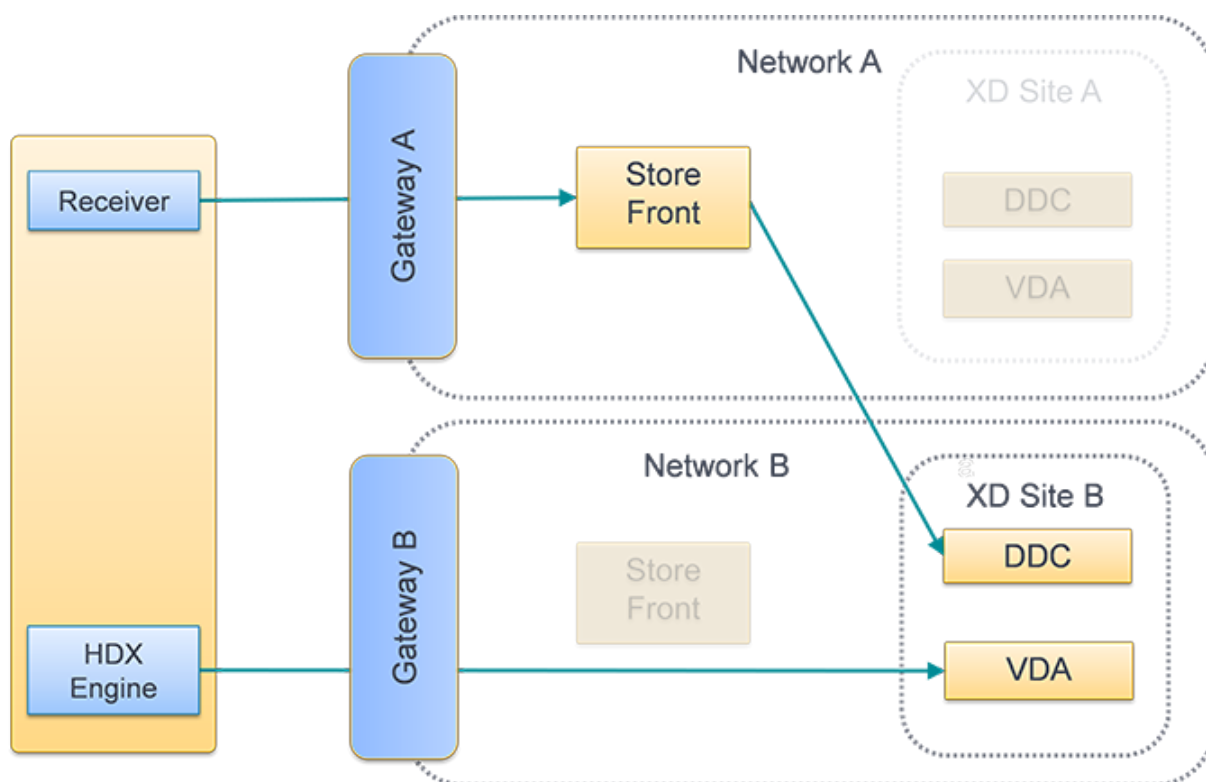


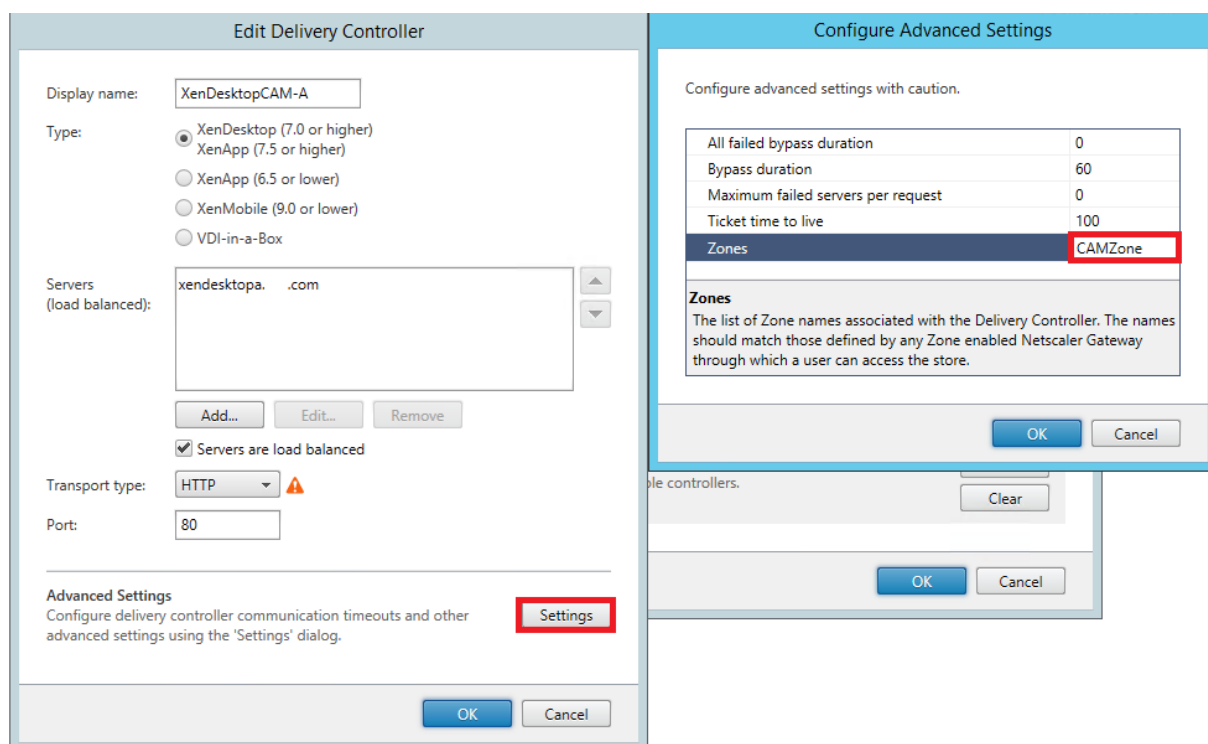
Figure 2. Optimal gateway routing



Place a Delivery Controller into a zone

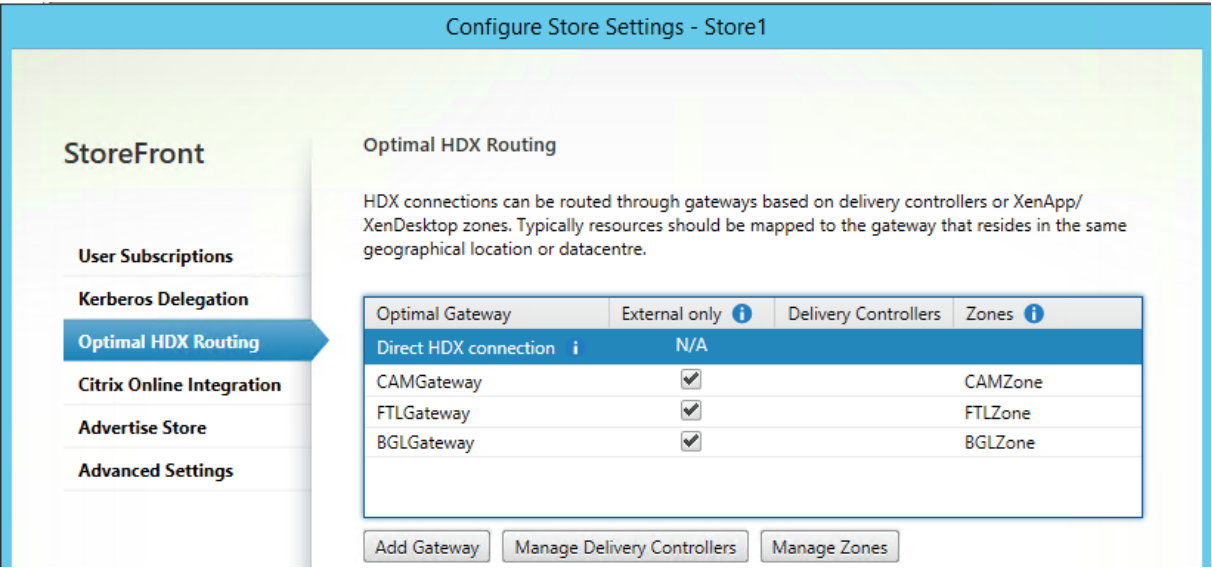
Set the zone attribute on every Delivery Controller you wish to place within a Zone.

1. Select the **Stores** node in the left pane of the Citrix StoreFront management console and click **Manage Delivery Controllers** in the **Actions** pane.
2. Select a controller, click **Edit**, and then click **Settings** on the **Edit Delivery Controller** screen.
3. On the **Zones** row, click in the second column.
4. Click **Add** on the **Delivery Controller Zone Names** screen and then add a zone name.



Configure Optimal HDX routing

1. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the **Actions** pane, click **Configure Store Settings**.
2. Select the **Optimal HDX Routing** tab.
3. Select a gateway.
 - a) To use the gateway when accessing resources from specific delivery controllers, click **Manage Delivery Controllers** and tick one or more delivery controllers
 - b) To use the gateway when accessing resources from a group of delivery controllers in a Zone, click **Manage Zones** and enter one or more zone.
 - c) By default once you add a delivery controller or zone, **External Only** is ticked, meaning StoreFront only uses the gateway to launch StoreFront for users connected to StoreFront via a gateway. If you wish to also use the gateway to launch resources for users who have connected directly to StoreFront without going via a gateway, untick **External Only**.
4. If you wish to always connect directly to certain resources without using a gateway, even for users accessing StoreFront remotely via a gateway, select **Direct HDX connection** and choose some delivery controllers or zones.



Use PowerShell to configure optimal Citrix Gateway routing for a store

- To configure optimal gateway routing for a store use [Register-STFStoreOptimalLaunchGateway](#).
- To remove optimal gateway routing for a store use [Unregister-STFStoreOptimalLaunchGateway](#).
- To view optimal routing for a store use [Get-STFStoreRegisteredOptimalLaunchGateway](#).

Subscription synchronization

March 19, 2024

StoreFront automatically synchronizes subscriptions between servers in a StoreFront server group. If you have multiple server groups (typically in different geographic location) then you can configure periodic pull synchronization of users’subscriptions from stores in different StoreFront deployments. This must be done using PowerShell.

Note:

The StoreFront and PowerShell consoles cannot be open at the same time. Always close the StoreFront management console before using the PowerShell console to administer your StoreFront configuration. Likewise, close all instances of PowerShell before opening the StoreFront console.

When establishing your subscription synchronization, note that the configured Delivery Controllers must be named identically between the synchronized Stores including the case. Failing to duplicate

the Delivery Controller names exactly may lead to users having different subscriptions across the synchronized Stores. If you synchronizing subscriptions from aggregated resources, the name of the aggregation groups used by both Stores must also match. Delivery Controller names and Aggregation Group names are case sensitive; for example, *CVAD_US* is different to *Cvad_Us*.

1. Use an account with local administrator permissions to start the Windows PowerShell ISE.
2. To configure synchronization, use the [Publish-STFServerGroupConfiguration](#) command. You can either specify a start time and recurring interval or a list of times. For example to start synchronizing at 08:00 then every 30 minutes:

```
1 Add-STFSubscriptionSynchronizationSchedule -RecurringStartTime
   08:00:00 -RecurringInterval 30
2 <!--NeedCopy-->
```

We recommend that you stagger pull schedules to avoid two server groups attempting to pull subscription data from each other at the same time. For example, a schedule to pull data from each server group every 60 mins would be configured as follows. Server group 1 pulls data from server group 2 at 01:00, 02:00, 03:00 and so on. Server group 2 pulls data from server group 1 at 01:30, 02:30, 03:30 and so on.

3. To specify the remote StoreFront deployment containing the store to be synchronized, type the following command. You must configure this for each data center where a StoreFront server group resides so it can pull subscription data from other remote datacenters. See the following US and UK datacenter examples:

- Run on US data center StoreFront servers to pull data from the UK datacenter servers:

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/
   Citrix/Store"
2 Add-STFSubscriptionSynchronizationSource -FriendlyName "
   SyncFromUKStore" -StoreService $StoreObject -
   RemoteStoreFrontAddress "UKloadbalancedStoreFront.example.
   com"
3 <!--NeedCopy-->
```

- Run on UK data center StoreFront servers to pull data from the US datacenter servers:

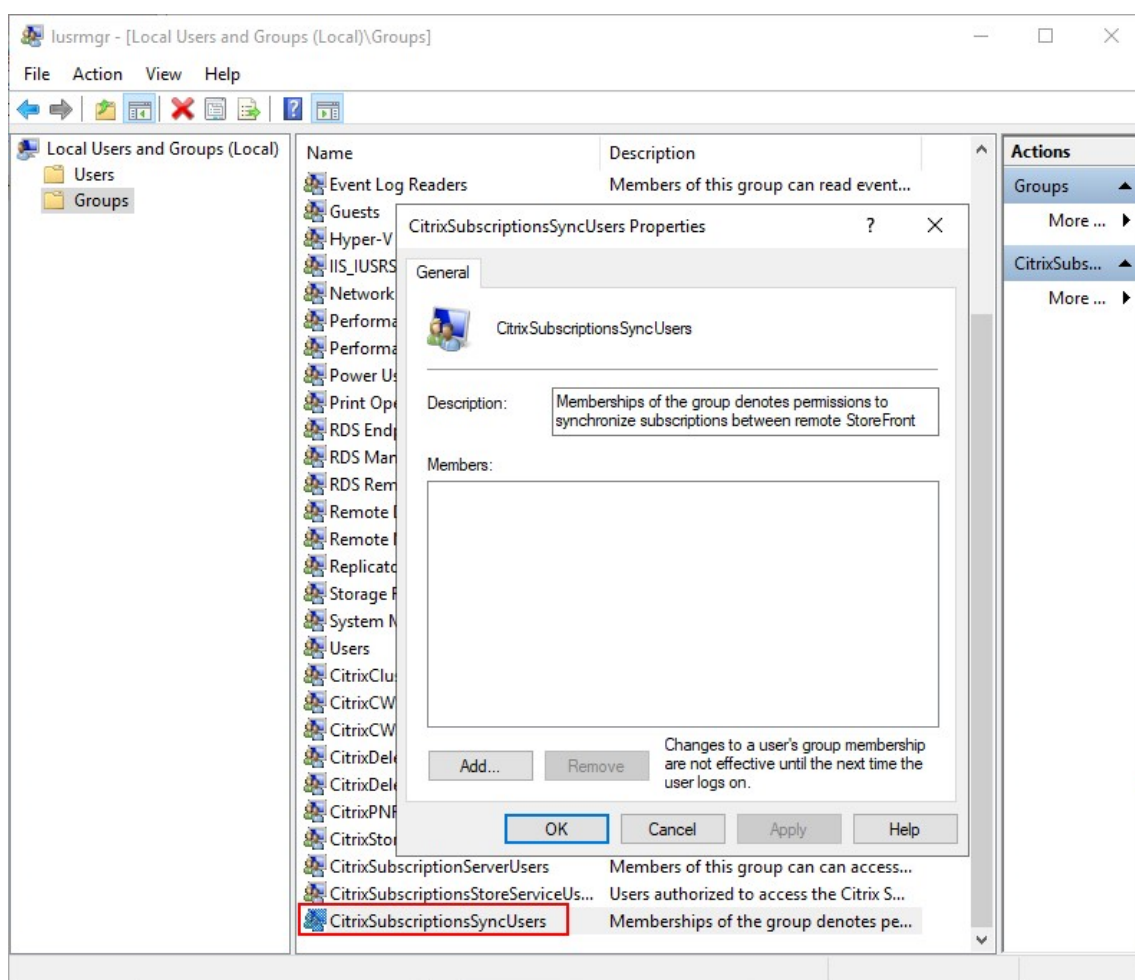
```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/
   Citrix/Store"
2 Add-STFSubscriptionSynchronizationSource -FriendlyName "
   SyncFromUSStore" -StoreService $StoreObject -
   RemoteStoreFrontAddress "USloadbalancedStoreFront.example.
   com"
3 <!--NeedCopy-->
```

where *FriendlyName* is a name that helps you identify the remote deployment and *RemoteStoreFrontAddress* is the FQDN of the StoreFront server or load-balanced server group for the remote

deployment. To synchronize application subscriptions between two or more stores, all stores which are to be synchronized must have the same name in their respective StoreFront deployments.

4. Add the Microsoft Active Directory domain machine accounts for each StoreFront server in the remote deployment to the local Windows user group CitrixSubscriptionSyncUsers on the current server.

This allows the current servers to pull new or updated subscription data from the remote servers listed in CitrixSubscriptionSyncUsers once you have configured a synchronization schedule. For more information about modifying local user groups, see [https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772524\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772524(v=ws.11)).



5. When you have configured the schedule as you intend, use the Citrix StoreFront management console, or the Powershell below, to propagate the subscription synchronization schedules and sources to the all other servers in the group.

```
1 Publish-STFServerGroupConfiguration
2 <!--NeedCopy-->
```

For more information about propagating changes in a multiple server StoreFront deployment, see [Configure server groups](#).

6. To remove an existing subscription synchronization schedule, run the following command, then propagate the configuration change to the other StoreFront servers in the deployment.

```
1 Clear-STFSubscriptionSynchronizationSchedule
2 Publish-STFServerGroupConfiguration
3 <!--NeedCopy-->
```

7. To remove a specific subscription synchronization source, run the following command, then propagate the configuration change to the other StoreFront servers in the deployment.

```
1 Remove-STFSubscriptionSynchronizationSource -FriendlyName "
   SyncFromUKStore"
2 Publish-STFServerGroupConfiguration
3 <!--NeedCopy-->
```

8. To remove all existing subscription synchronization sources, run the following command, then propagate the configuration change to the other StoreFront servers in the deployment.

```
1 Clear-STFSubscriptionSynchronizationSource
2 Publish-STFServerGroupConfiguration
3 <!--NeedCopy-->
```

9. To list the subscription synchronization schedules currently configured for your StoreFront deployment, run the following command.

```
1 Get-STFSubscriptionSynchronizationSchedule
2 <!--NeedCopy-->
```

10. To list the subscription synchronization sources currently configured for your StoreFront deployment, run following command.

```
1 Get-STFSubscriptionSynchronizationSource
2 <!--NeedCopy-->
```

Configure session settings

March 11, 2024

When a user launches an application, StoreFront generates a document (known as an ica file) that is contains all of the settings that Citrix Workspace app needs to launch and configure that session.

In most cases it is recommended to modify sessions settings using [Citrix Virtual Apps and Desktops Policies](#) or [Citrix DaaS Policies](#). However in some cases it useful to override these settings for a partic-

ular store. This can be useful if a store aggregates resources from multiple sites and you want to apply the same settings to all resources for that store.

To define session settings for a store, either:

- Use the Global App Config Service. This is a service on Citrix Cloud. For more details see [Configure Citrix Workspace app using Global App Configuration service](#).
- On the StoreFront server, add settings to the store's default.ica file.

You can find default.ica on the StoreFront server in the `\inetpub\wwwroot\Citrix\[StoreName]\App_Data` directory.

For a list of available settings see [ICA Settings Reference](#). Some settings apply globally. You can also add sections that apply to specific apps by adding a section whose name exactly matches the application name as configured in Studio.

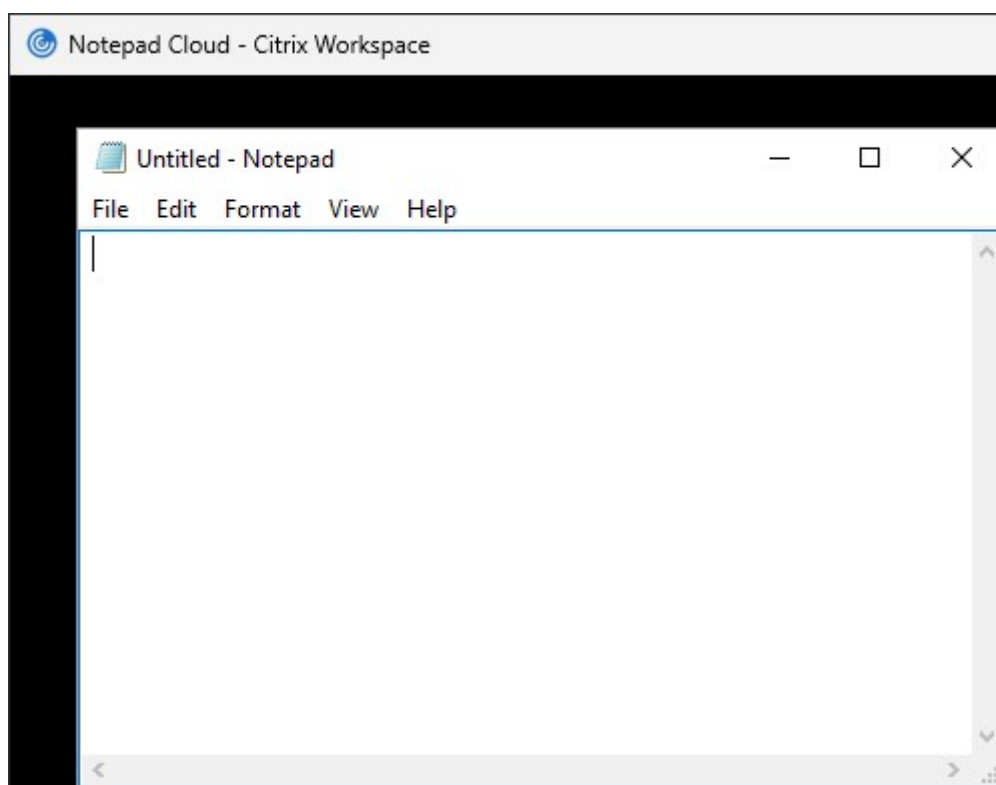
Example: Launch Notepad in windowed mode

To configure an application to launch in Windowed mode, in default.ica, add a section for the application with the settings:

- TWIMode - set to Off to enable windowed mode.
- DesiredHRES - optionally the horizontal number of pixels.
- DesiredVRES - optionally the vertical number of pixels.

For example:

```
1 [Notepad]
2 TWIMode=Off
3 DesiredHRES=1024
4 DesiredVRES=768
5 <!--NeedCopy-->
```



ICA file signing

February 27, 2024

StoreFront provides the option to digitally sign ICA files so that versions of Citrix Workspace app that support this feature can verify that the file originates from a trusted source. When file signing is enabled in StoreFront, the ICA file generated when a user starts an application is signed using a certificate from the personal certificate store of the StoreFront server. ICA files can be signed using any hash algorithm supported by the operating system running on the StoreFront server. The digital signature is ignored by clients that do not support the feature or are not configured for ICA file signing. If the signing process fails, the ICA file is generated without a digital signature and sent to Citrix Workspace app, the configuration of which determines whether the unsigned file is accepted.

To be used for ICA file signing with StoreFront, certificates must include the private key and be within the allowed validity period. If the certificate contains a key usage extension, this must allow the key to be used for digital signatures. Where an extended key usage extension is included, it must be set to code signing or server authentication.

For ICA file signing, Citrix recommends using a code signing or SSL signing certificate obtained from a public certification authority or from your organization's private certification authority. If you are

unable to obtain a suitable certificate from a certification authority, you can either use an existing SSL certificate, such as a server certificate, or create a new root certification authority certificate and distribute it to users' devices.

ICA file signing is disabled by default in stores. To enable ICA file signing, you edit the store configuration file and execute Windows PowerShell commands. For more information about enabling ICA file signing in Citrix Workspace app for Windows, see [ICA File Signing](#).

Note:

The StoreFront and PowerShell consoles cannot be open at the same time. Always close the StoreFront management console before using the PowerShell console to administer your StoreFront configuration. Likewise, close all instances of PowerShell before opening the StoreFront console.

1. Ensure that the certificate you want to use to sign ICA files is available in the Citrix Delivery Services certificate store on the StoreFront server and not the current user's certificate store.
2. Enable signing using the `Set-STFStoreService` PowerShell cmdlet:

```
1 $storeService = Get-STFStoreService
2 Set-STFStoreService $storeService -IcaFileSigning $true -
  IcaFileSigningCertificateThumbprint [certificatethumbprint]
3 <!--NeedCopy-->
```

Where **[certificatethumbprint]** is the digest (or thumbprint) of the certificate data produced by the hash algorithm.

If you want to use a hash algorithm other than SHA-1, add a parameter **-IcaFileSigningHashAlgorithm** set to sha256, sha384, or sha512, as required.

Citrix Workspace app configuration

March 11, 2024

Global App Config service

The Global App Config service is a cloud service for managing Citrix Workspace app configuration. Within your Citrix Cloud account you can claim your store URLs and define the configuration for each of your stores. For more details see [Configure settings for on-premises stores](#).

Store account settings

As an alternative to Global App Config service, you can configure Citrix Workspace app via the store account settings. When a user adds a store to a locally installed Citrix Workspace app, it retrieves the store account settings StoreFront. This can include configuration properties, for instance to tell Citrix Workspace app for Windows whether it should create start menu shortcuts for apps. See the Workspace app documentation for details of properties, for instance [Using StoreFront account settings to customize app shortcut locations](#).

To modify these settings:

1. Open web.config file in `C:\inetpub\wwwroot\Citrix\Roaming`.
2. In the `<Accounts>` section, find the element `<account ... name="Store" ... >` for the store you wish to change.
3. Under the `Account` section, find the `<annotatedServices>/<annotatedServiceRecord>/<metadata>/<properties>` section.
4. After the `<clear/>` element, add the properties in the form `<property name="[name]" value="[value]" />`. For example:

```
1 <properties>
2   <clear/>
3   <property name="PutShortcutsOnDesktop" value="true"/>
4   <property name="DesktopDir" value="Citrix Applications"/>
5 </properties>
6 <!--NeedCopy-->
```

Important

In multiple server deployments, use only one server at a time to change the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server group, so that the other servers in the deployment are updated.

Workspace app website

To configure which website configuration is used by locally installed Citrix Workspace app, see [Configure Workspace app website](#).

Manage a website

March 11, 2024

For each store you can configure one or more website which users can access through either through a browser or through Citrix Workspace app.

Use the StoreFront management console to perform the following tasks:

Task	Detail
Create a website	Create websites, which enable users to access stores through a web page or Workspace app.
Configure a website	Modify settings for your website.
Remove a website	Remove a Citrix Receiver for Web site.
Configure Workspace app website	Choose which website to use from within the Citrix Workspace app.

Create a website

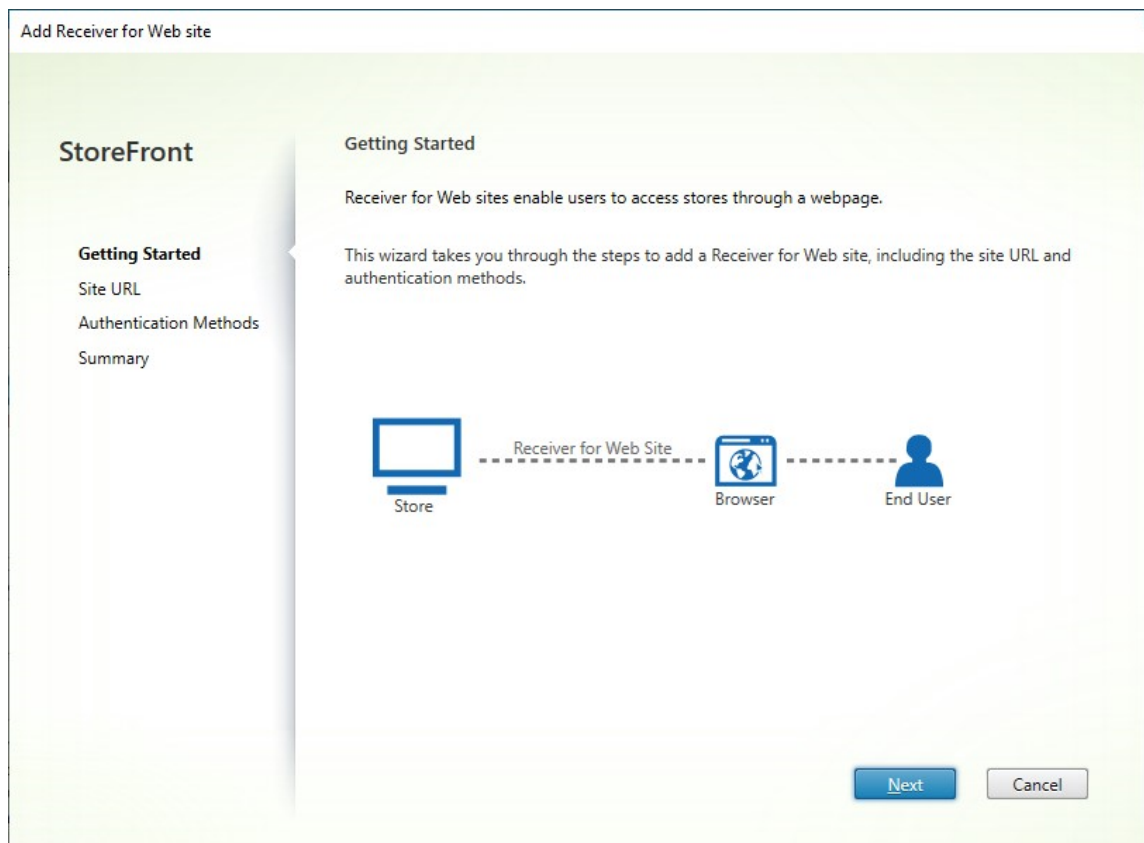
March 19, 2024

When you create a store, a website is created for it automatically. You can add additional websites to existing stores. This allows you to provide different URLs with different configurations to your users. However multiple websites can only be accessed through a web browser as Citrix Workspace Apps are configured to use one specific website for a store, see [Configure Workspace app website](#).

Important:

In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, [propagate your configuration changes to the server group](#) so that the other servers in the deployment are updated.

1. From the management console, select the store for which you want to create the website, and in the Actions pane, click **Manage Receiver for Web Sites**.
2. Click **Add** then click **Next**.



3. Type the desired **Web Site Path**, choose if you want to this to be the default website for the base URL and click **Next**.

Add Receiver for Web site

StoreFront

- ✓ Getting Started
- Site URL**
- Authentication Methods
- Summary

Site URL

Allow users to connect to a store through a webpage.

Base URL: https://storefrontlbeu.xaeaad.com/

Web Site Path: /Citrix/StoreWeb3

☐ Set this Receiver for Web site as IIS default

When this is checked, the Receiver for Web site created with the store will be set as the default IIS website. This setting will override any previous defaults configured for the IIS sites.

Back Next Cancel

4. Tick or untick the desired [authentication methods](#). Some methods are only available if they have been configured for the store. Press **Next**.

Add Receiver for Web site

StoreFront

- ✓ Getting Started
- ✓ Site URL
- Authentication Methods**
- Summary

Authentication Methods

Select the authentication methods which users will use to authenticate and access resources. The authentication methods will be specific to the website. ⓘ

Method
<input checked="" type="checkbox"/> User name and password
<input type="checkbox"/> SAML Authentication Method not available. Disabled for the store.
<input type="checkbox"/> Domain pass-through To provide good user experience, all Windows client devices need to be domain-joined and have single sign-on enabled for Citrix Receiver/Workspace app.
<input type="checkbox"/> Smart card
<input checked="" type="checkbox"/> Pass-through from Citrix Gateway

Back Create Cancel

5. When the site has been created, click **Finish**.
6. Select the newly created site and press **Edit** to configure your web site as required, see [Configure Websites](#).

Create a website using the PowerShell SDK

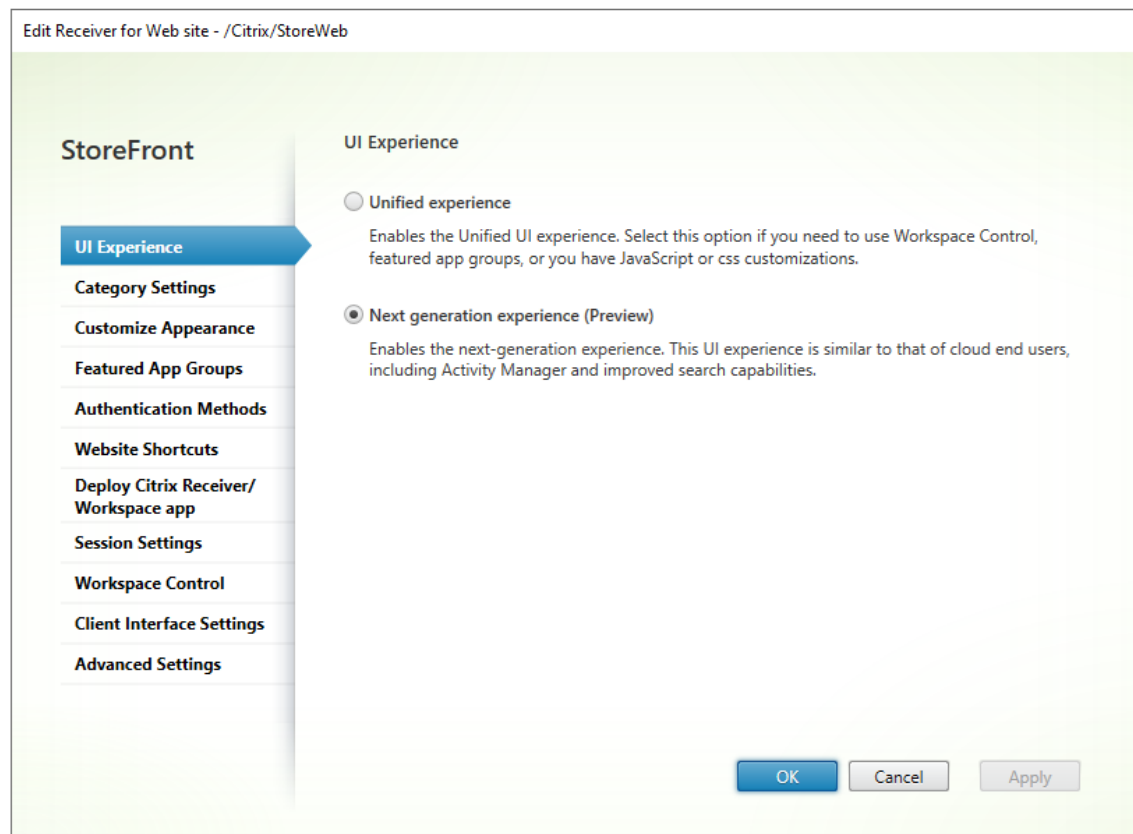
To create a website with the [PowerShell SDK](#), call the [Add-STFWebReceiverService](#) cmdlet.

Configure website

March 11, 2024

To configure a website:

1. Select the **Stores** node in the left pane and in the **Actions** pane, click **Manage Receiver for Web**
2. Select a web site and press **Configure...**



3. Modify the settings on the appropriate tabs.

- [UI Experience](#)
- [Category Settings](#)
- [Customize Appearance](#)
- [Featured App Groups](#)
- [Authentication Methods](#)
- [Website Shortcuts](#)
- [Deploy Citrix Receiver/Workspace app](#)
- [Session Settings](#)
- [Workspace Control](#)
- [Client Interface Settings](#)
- [Advanced Settings](#)

4. Once you have finished your changes, click **OK**.

5. To configure [App Protection](#) you must use PowerShell. Ensure you close StoreFront management console before running PowerShell commands.

Important:

In multiple server deployments, use only one server at a time to make changes to the configura-

tion of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, [propagate your configuration changes to the server group](#) so that the other servers in the deployment are updated.

Category Settings

March 19, 2024

Within Citrix Virtual Apps and Desktops, you can assign each application to a category as described in the [Applications](#) article. Use the \ symbol to create a folder hierarchy of categories. Within StoreFront, you can configure how this folder hierarchy is displayed.

Application Settings

IE11 Cloud

Identification

Delivery

Location

Groups

Limit Visibility


File Type Association

Zone

Delivery

Specify how this application will be delivered to users.

Application icon:

 Change...

Application category (optional):

Browsers\Legacy

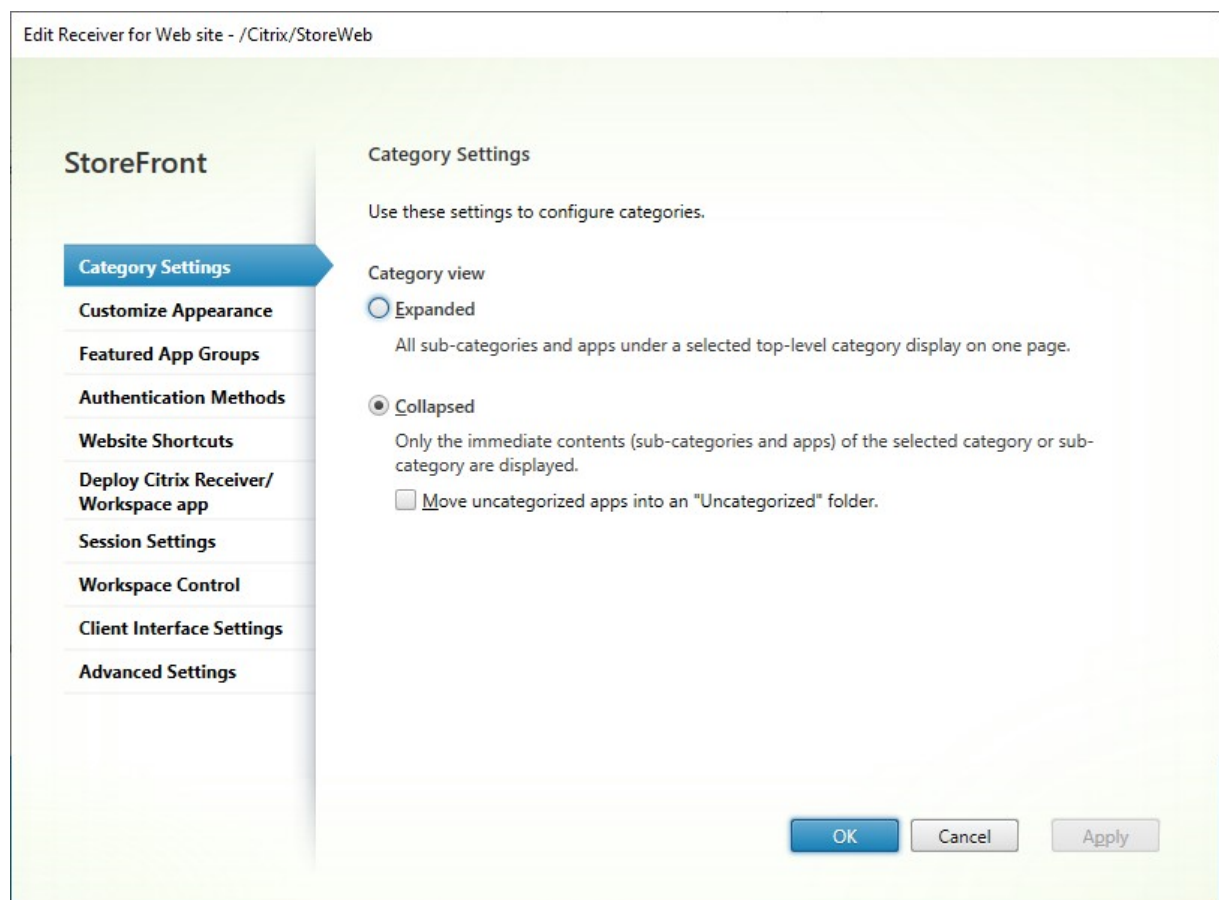
The Category in Citrix Workspace app where the application appears.

☐ Add shortcut to user's desktop

How do you want to control the use of this application?

☒ Allow unlimited use

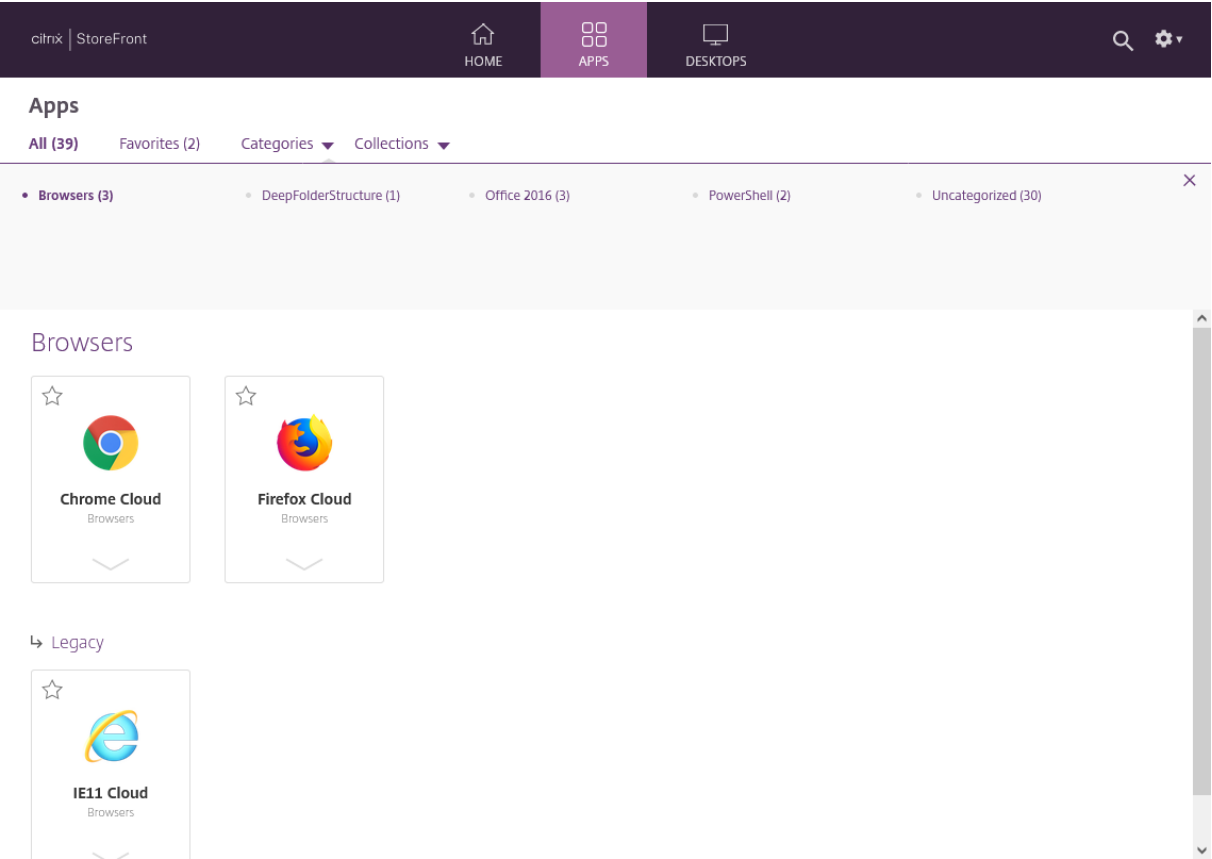
To modify category settings, go to [Edit Receiver for web site](#) and select the **Category Settings** tab.



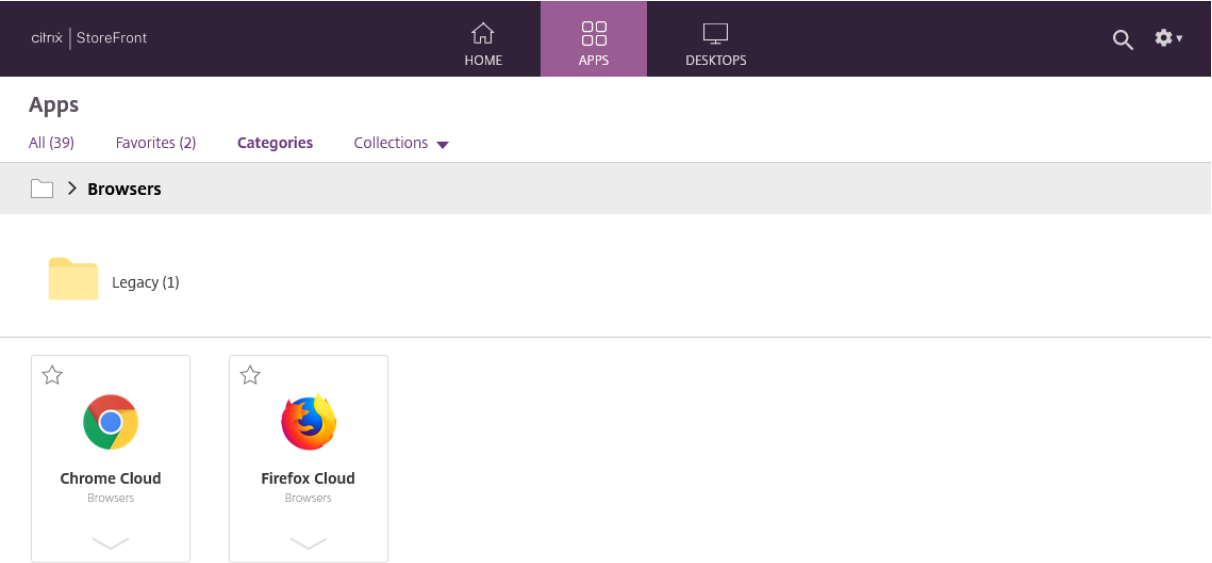
Category view

In the expanded view, StoreFront displays a list of top level categories. When the user clicks a top level category, StoreFront displays all apps in all subcategories on one page.

For example, if you have a category Browser with subcategory Legacy then it shows all browsers including those under legacy on one page:

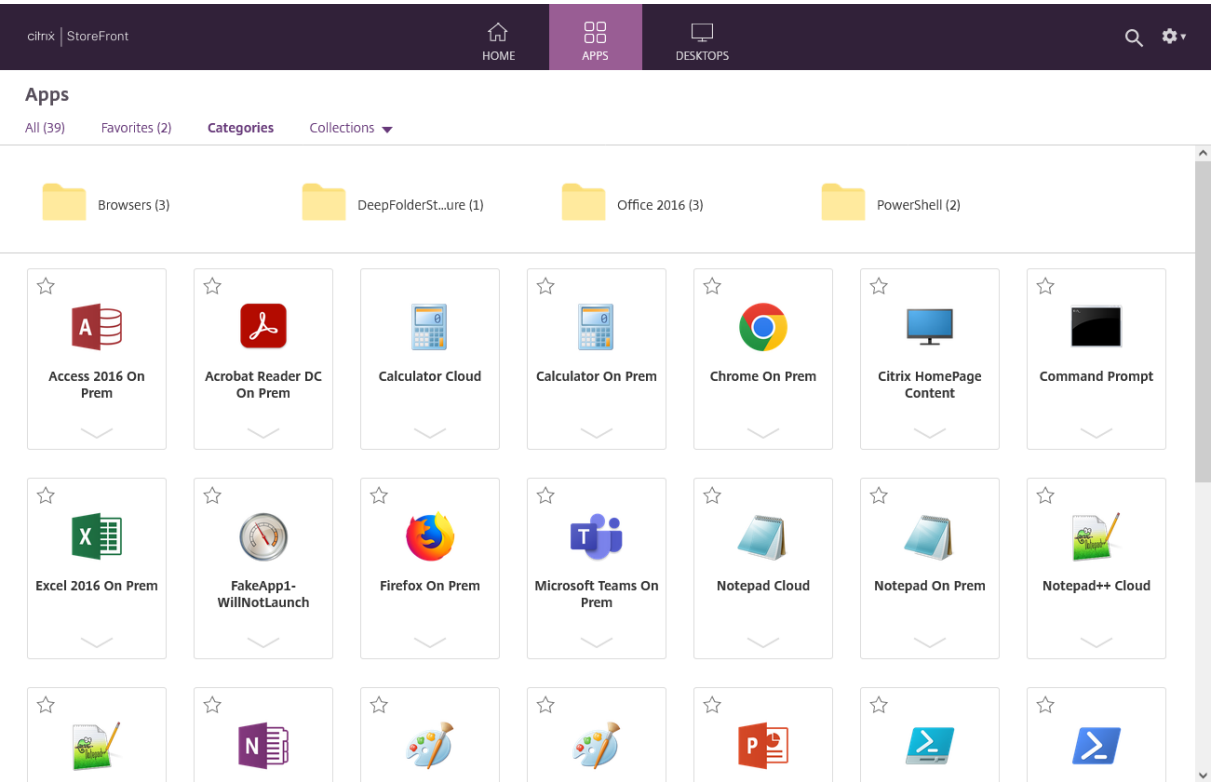


In the collapsed view, StoreFront initially displays a list of top level categories, and optionally all uncategorized apps. When the user clicks a category, StoreFront displays only the immediate contents (subcategories and apps) of the selected category. The user can click each subcategory to expand the contents.

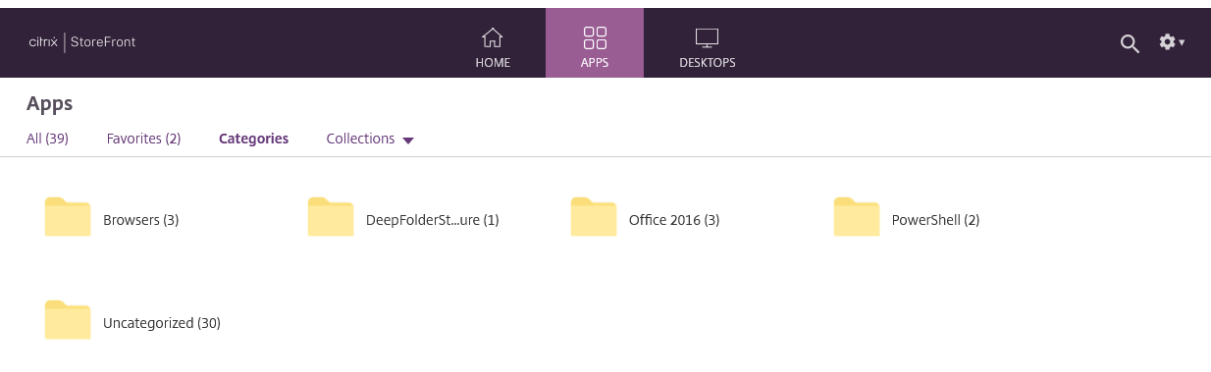


Uncategorized apps

In the collapsed view, clear the **Move uncategorized apps into an “Uncategorized” folder** option to display all apps and desktops without categories on the initial view. This behavior is similar to earlier versions of StoreFront.



In the collapsed view, check **Move uncategorized apps into an “Uncategorized” folder** to move all the apps and desktops without categories into a separate **Uncategorized** folder.



Configure category settings using PowerShell SDK

To use the PowerShell SDK to enable or disable category view call cmdlet [Set-STFWebReceiverUserInterface](#) with parameter [EnableAppsFolderView](#).

To use the PowerShell SDK to change the category view call cmdlet [Set-STFWebReceiverUserInterface](#) with parameter [CategoryViewCollapsed](#).

Customize appearance

March 19, 2024

You can modify the logo and colors used within your store website.

Edit logo and colors

To customize the appearance, go to [Edit Receiver for web site](#) and select the **Customize Appearance** tab. You can modify the following:

- **Logon branding logo** - The logo displayed on the logon screen. It is not displayed when logging on through a Citrix Gateway. Press **Browse...** and select a file of type .jpg, .jpeg, .png, .png or .bmp. It is recommend you use an image of size 350px x 120px.
- **Header branding logo**. The logo displayed in the top left corner after logging on. Press **Browse ...** and select a file of type .jpg, .jpeg, .png, .png or .bmp. It is recommend you use an image of size 340px x 80px.
- **Background color** - The background color of the navigation section at the top of the page.
- **Text and icon color** - The text and icon color in the navigation section at the top of the page.
- **Link color** - The color used to highlight the currently selected item.

Edit Receiver for Web site - /Citrix/StoreWeb

StoreFront

- Category Settings
- Customize Appearance**
- Featured App Groups
- Authentication Methods
- Website Shortcuts
- Deploy Citrix Receiver/Workspace app
- Session Settings
- Workspace Control
- Client Interface Settings
- Advanced Settings

Customize Receiver for Web Appearance

Use these settings to customize the Receiver for web pages.

Logon branding

Logo: (350 x 120 px)

This logo appears on the Receiver logon page.

Header branding (Post logon)

Logo: (340 x 80 px)

Preview (Post logon)

Background color:

Text and icon color:

Content branding (Post logon)

Link color:

citrix | StoreFront

Text and icon color

Link color

Edit logo and colors using PowerShell SDK

Using the [PowerShell SDK](#), call cmdlet `Set-STFWebReceiverSiteStyle`.

Reset appearance to default

Press **Reset to default style** to return the logos and colors to the default.

Reset appearance to default using PowerShell SDK

Using the [PowerShell SDK](#), call cmdlet `Clear-STFWebReceiverSiteStyle`.

Customization using Javascript and CSS

You can further customize the web site using the [StoreFront Client UI Customization API](#).

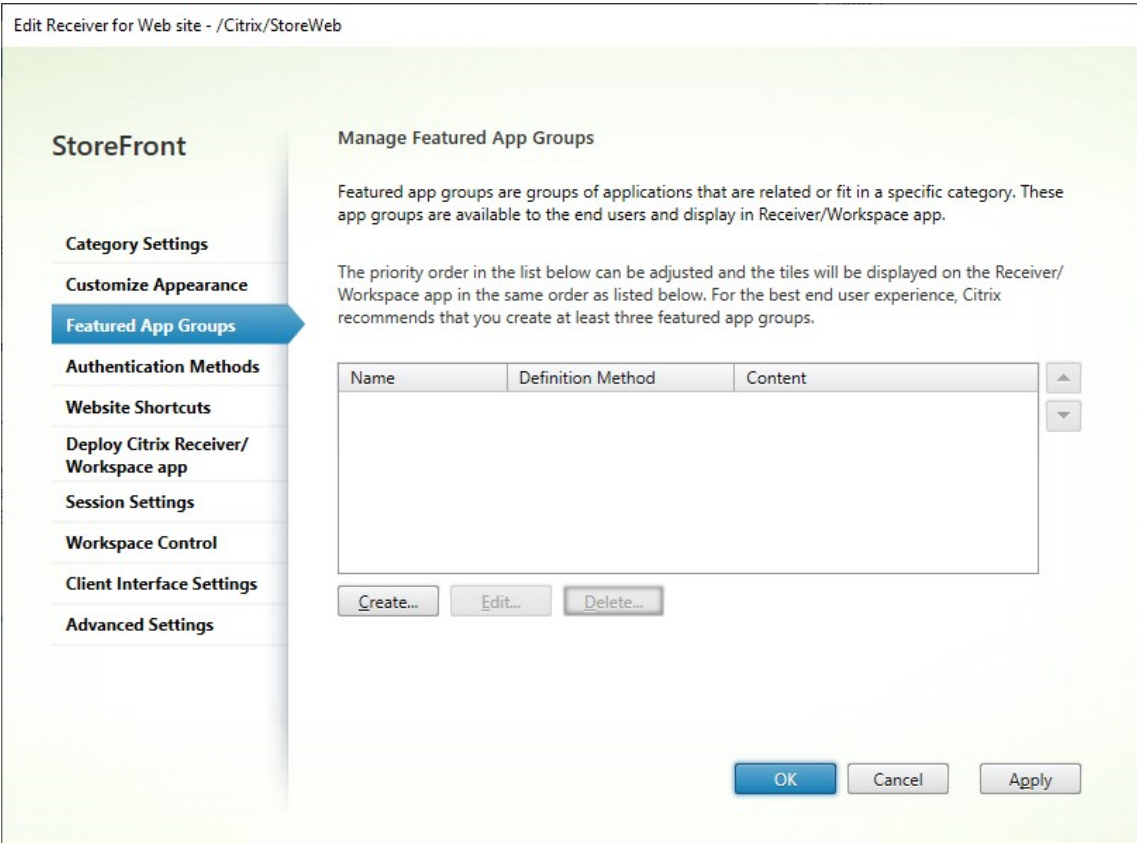
Featured app groups

March 19, 2024

You can create product featured app groups for your end users that are related to or fit in a specific category. For example, you can create a Sales Department featured app group containing applications that are used by that department. You can define featured apps in the StoreFront administration console by using application names or by using keywords or application categories that were defined in the Studio console.

Create featured app group

1. In the [Edit Receiver for web site](#) screen, select the **Featured App Groups** tab.



2. Click **Create** to define a new featured app group.
3. Specify a featured app group name, description (optional), background, and the method by which you define the featured app groups. You can choose keywords, application names, or application category.

Option	Description
Keywords	Matches apps based on the keyword, defined Studio by including keywords in the app’s description, for example “Use to send and receive emails KEYWORDS:collaboration”
Application category	Matches apps in a specific application category entered in Studio.
Application names	Use the application name to define the featured app group. All applications names matching the name included here in the Create a Featured App Group dialog screen are included in the featured app group. StoreFront does not support wildcards in application names. The match is not case sensitive, but it does match whole words. For example, if you type Excel, StoreFront matches a published app named Microsoft Excel 2013 but typing Exc does not match anything.

Create Featured App Group


Name:

i

Description:
(Optional)

i

Background style:



▼

Add applications to the featured app group

You can add applications to a featured app group using keywords, application names or application category.

Definition method:

Keyword

▼

i

Keyword:

Keywords should be defined in the application properties dialog of Studio console or the XenApp Delivery Services Console. Use the same keyword for each application to display in the same app group.

OK

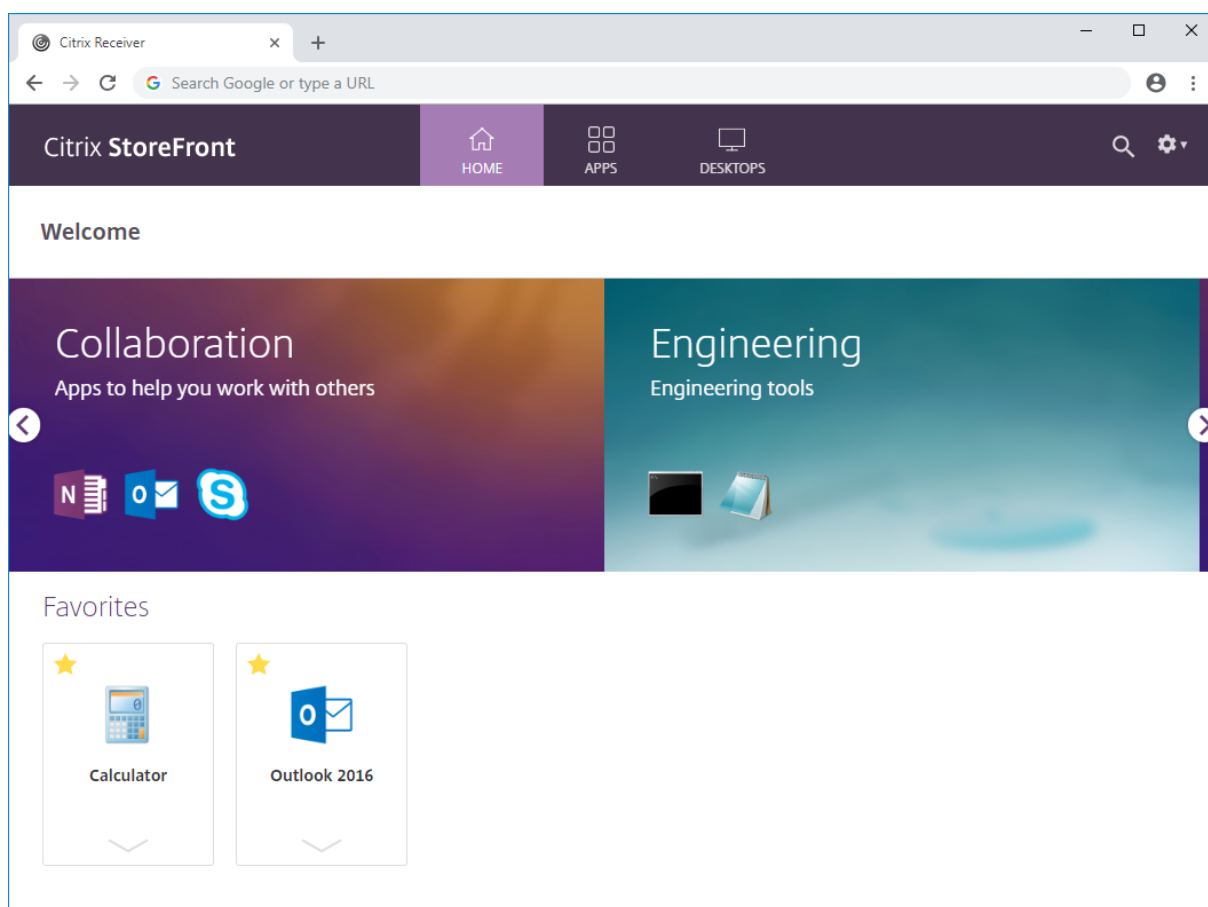
Cancel

4. Click **OK**

Example:

We created two featured app groups:

- Collaboration - Created by matching apps in the **Collaboration** category in Studio.
- Engineering - Created by naming the app group and specifying a collection of app names.



Create featured app group using the PowerShell SDK

To add a feature app group with the [PowerShell SDK](#), use the cmdlet [New-STFWebReceiverFeaturedAppGroup](#).

Edit featured app group

In the [Edit Receiver for web site](#) screen, select the **Featured App Groups** tab. Select the group that you want to edit and click **Edit...**

Edit featured app group using the PowerShell SDK

To modify a feature app group with the [PowerShell SDK](#), use the cmdlet [Set-STFWebReceiverFeaturedAppGroup](#).

Delete featured app group

In the [Edit Receiver for web site](#) screen, select the **Featured App Groups** tab. Select the group that you want to edit and click **Delete...**

Delete featured app group using the PowerShell SDK

Using the [PowerShell SDK](#) to delete a feature app group use the cmdlet [Remove-STFWebReceiverFeaturedAppGroup](#) and to delete all featured app groups use the cmdlet [Clear-STFWebReceiverFeaturedAppGroup](#).

Authentication methods

April 9, 2024

To configure the authentication methods available for a store, see [Configure Authentication](#). You can override some of these settings for a particular web site. These overrides only apply using Citrix Workspace app for HTML5 through a web browser. Locally installed Citrix Workspace app uses the settings from the store rather than the web site.

Warning:

Any time you change the authentication methods for a store, this overrides the settings for all websites for that store so any changes must be re-applied.

To modify authentication methods, go to [Edit Receiver for web site](#) and select the **Authentication Methods** tab.

Edit Receiver for Web site - /Citrix/StoreWeb

StoreFront

- Category Settings
- Customize Appearance
- Featured App Groups
- Authentication Methods**
- Website Shortcuts
- Deploy Citrix Receiver/Workspace app
- Session Settings
- Workspace Control
- Client Interface Settings
- Advanced Settings

Authentication Methods

Select the authentication methods which users will use to authenticate and access resources. The authentication methods will be specific to the website. i

Method
<input checked="" type="checkbox"/> User name and password
<input type="checkbox"/> SAML Authentication Method not available. Disabled for the store.
<input type="checkbox"/> Domain pass-through To provide good user experience, all Windows client devices need to be domain-joined and have single sign-on enabled for Citrix Receiver/Workspace app.
<input type="checkbox"/> Smart card
<input checked="" type="checkbox"/> Pass-through from Citrix Gateway

OK
Cancel
Apply

- Select the **Username and password** check box to enable explicit authentication. See [User name and password authentication](#). This option is only available if it's enabled for the store.
- Select the **SAML Authentication** check box to enable integration with a SAML Identity Provider. See [SAML authentication](#). This option is only available if it's been enabled for the store.
- Select **Domain pass-through** to enable pass-through of Active Directory domain credentials from users' devices. See [Domain pass-through authentication](#). This option is only available if it has been enabled for the store.
- Select **Smart card** to enable smart card authentication. See [Smart card authentication](#).
- Select **Pass-through from Citrix Gateway** to enable pass-through authentication from Citrix Gateway. Enable this if users connect to StoreFront through a Citrix Gateway with authentication enabled. See [Pass-through from Citrix Gateway](#).

Configure using PowerShell SDK

To configure the available authentication methods using the [PowerShell SDK](#), use the cmdlet [Set-STFWebReceiverAuthenticationMethods](#).

Website shortcuts

March 19, 2024

Use website shortcuts to provide users with rapid access to desktops and applications from trusted websites hosted on the internal network. You generate URLs for resources available through the Citrix Receiver for Web site and embed these links on your websites. Users click a link and are redirected to the Receiver for Web site, where they log on if they have not already done so. The Receiver for Web site automatically starts the resource. In the case of applications, users are also subscribed to the application if they haven't subscribed previously.

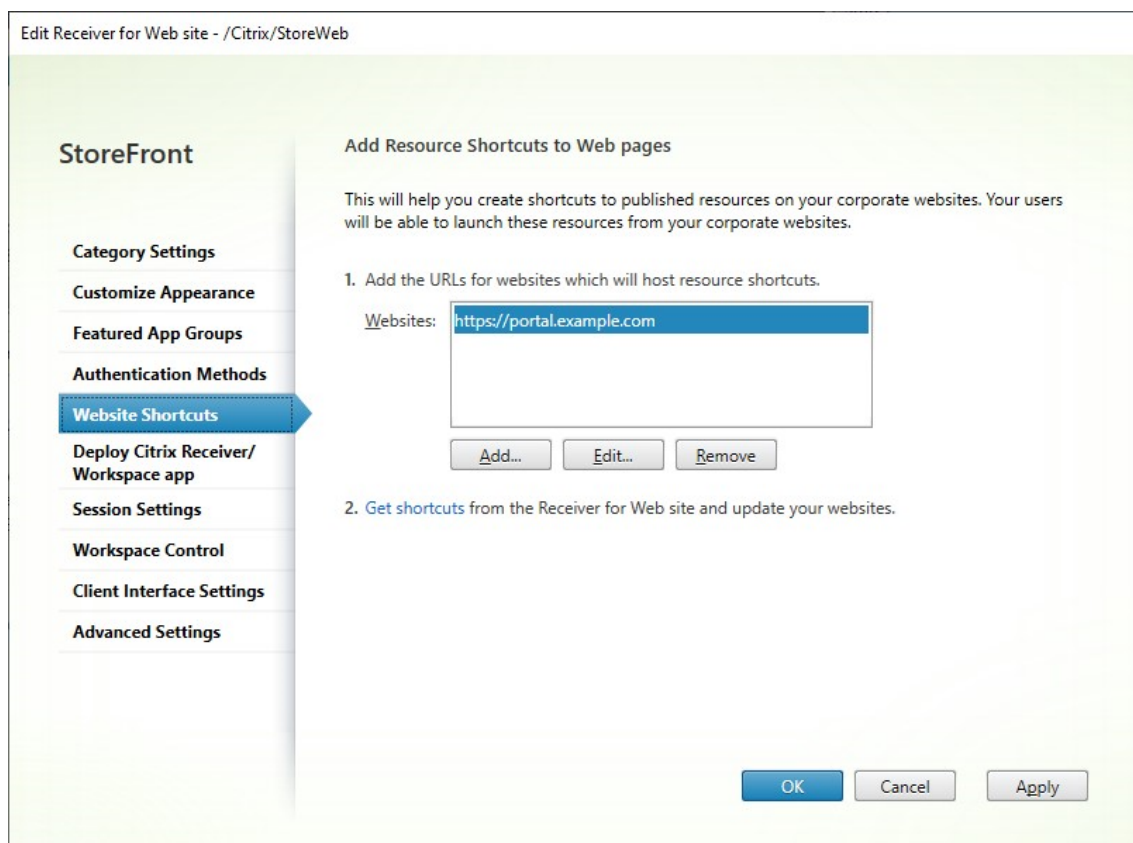
Before you can generate resource shortcuts, you must add the URLs of host websites to the *trusted URLs* list, using the Citrix StoreFront management console or using PowerShell.

By default, StoreFront warns users if they attempt to launch resource shortcuts from untrusted websites, but users can still choose to launch the resource. To stop these warnings from appearing, click **Manage Receiver for Web Sites** in the Stores pane > Click **Configure** > Choose **Advanced Settings** > Clear the **Prompt for untrusted shortcuts** option.

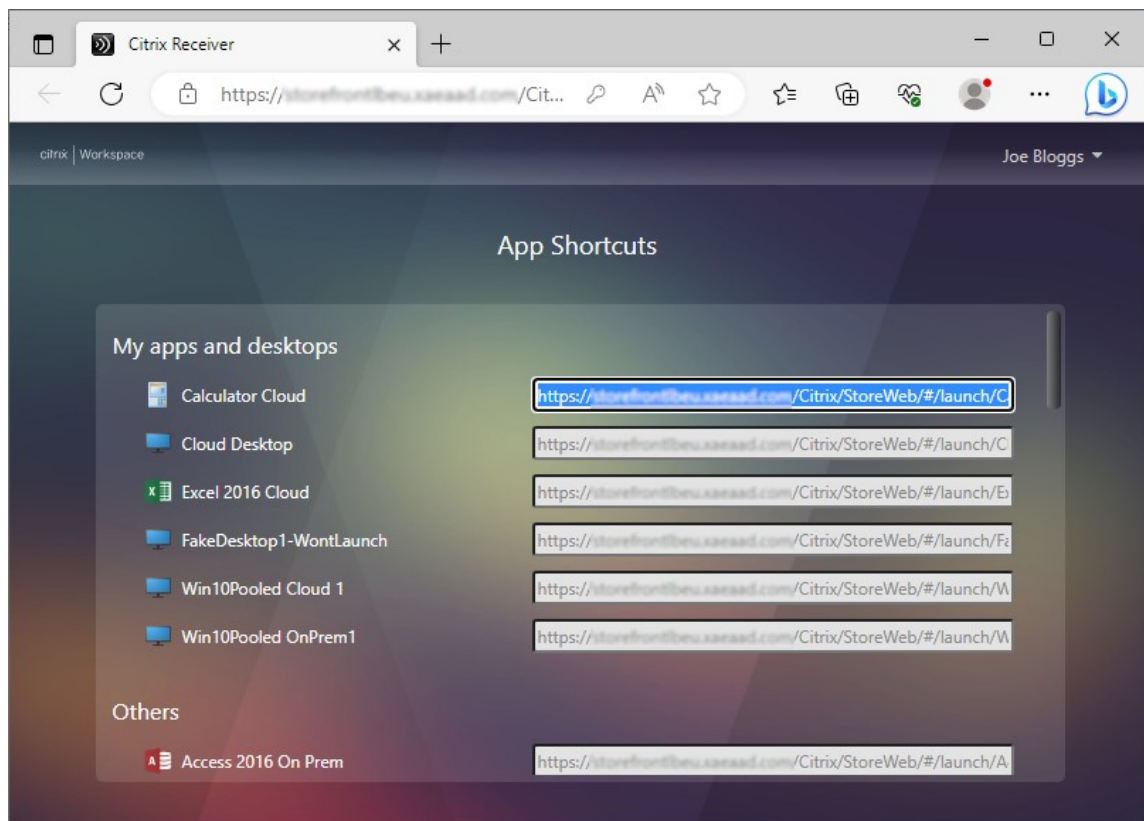
For security reasons, Internet Explorer users may be prompted to confirm that they want to start resources accessed through shortcuts. Instruct your users to add the StoreFront server FQDN the Local intranet or Trusted sites zones in Internet Explorer to avoid this extra step.

Add trusted websites using the management console

1. On the [Edit Receiver for web site](#) screen, select the **Website Shortcuts** tab.



2. Click **Add** to enter the URL for a website on which you plan to host shortcuts. URLs must be specified in the form `http[s]://hostname[:port]`, where host name is the fully qualified domain name of the website host, and port is the port used for communication with the host of the default port for the protocol unavailable. Paths to specific pages on the website are not required. To modify a URL, select the entry in the Websites list and click **Edit**. Select an entry in the list and click **Remove** to delete the URL for a website on which you no longer want to host shortcuts to resources available through the Citrix Receiver for Web site.
3. Click **Get shortcuts** and copy the URLs you require for your website.



Add trusted websites using PowerShell SDK

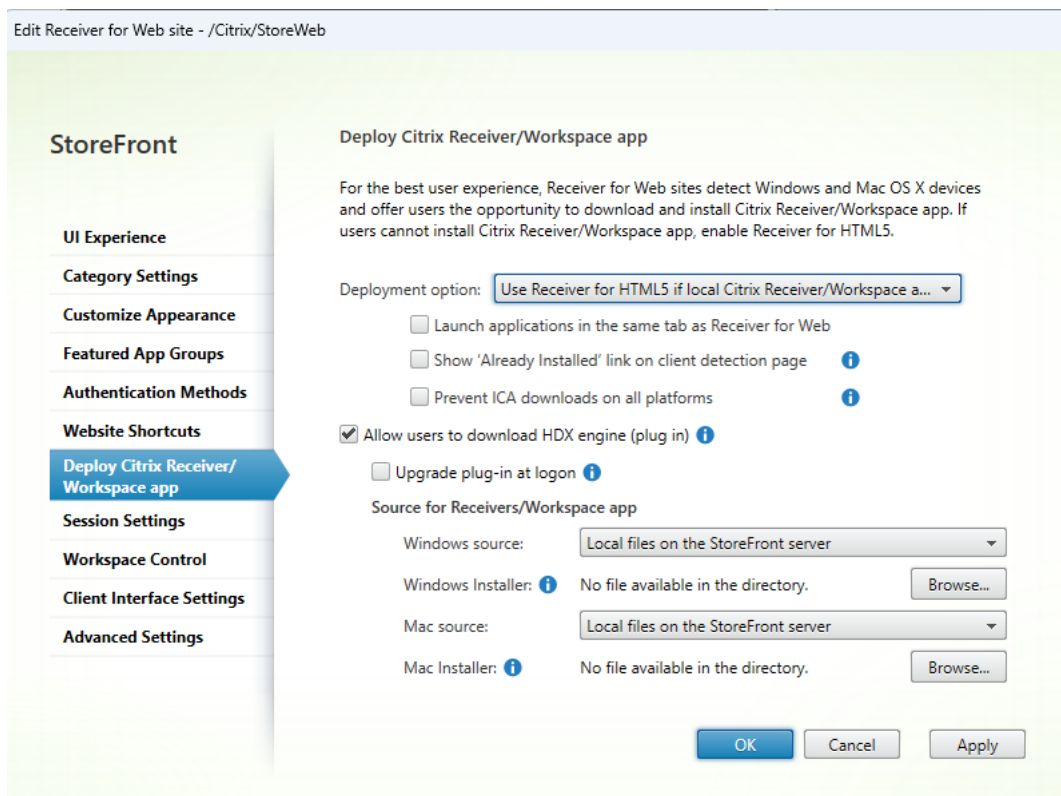
You can add trusted URLs using the [Set-STFWebReceiverApplicationShortcuts](#) PowerShell cmdlet.

Citrix Workspace app deployment

April 26, 2024

By default, when a user first browses to a store using a web browser on Windows, macOS or Linux, StoreFront automatically attempts to determine whether Citrix Workspace app is installed locally.

If a locally deployed Citrix Workspace app cannot be detected, the user is prompted to download and install it. The default download location is the Citrix website, but you can also host the installers on the StoreFront server or elsewhere. Users who cannot install Citrix Workspace app locally can use Citrix Workspace app for HTML5 through their web browser.



To modify deployment options, go to [Edit Receiver for web site](#) and select the **Deploy Citrix Receiver/-Workspace app** tab.

Deployment option

- Select **Always use Receiver for HTML5** if you want the user to always to access resources through a web browser without prompting the user to download and install Citrix Workspace app locally. With this option selected, Workspace for HTML5 users always access resources directly through their browsers.
- Select **Use Receiver for HTML5 if local Receiver is unavailable** if you want the store web site to prompt the user to download and install Citrix Workspace app locally, but fall back to accessing resources through a browser if Citrix Workspace app cannot be installed. Users without Citrix Workspace app are prompted to download and install it every time they log on to the site.
- Select **Install locally** if you want the site always to access resources through a locally installed Citrix Workspace app. Users are prompted to download and install the appropriate Citrix Workspace app for their platform. Users can continue to access the store through a web browser but when the launch a resource it opens in the locally installed Workspace app.

Launch applications in the same tab

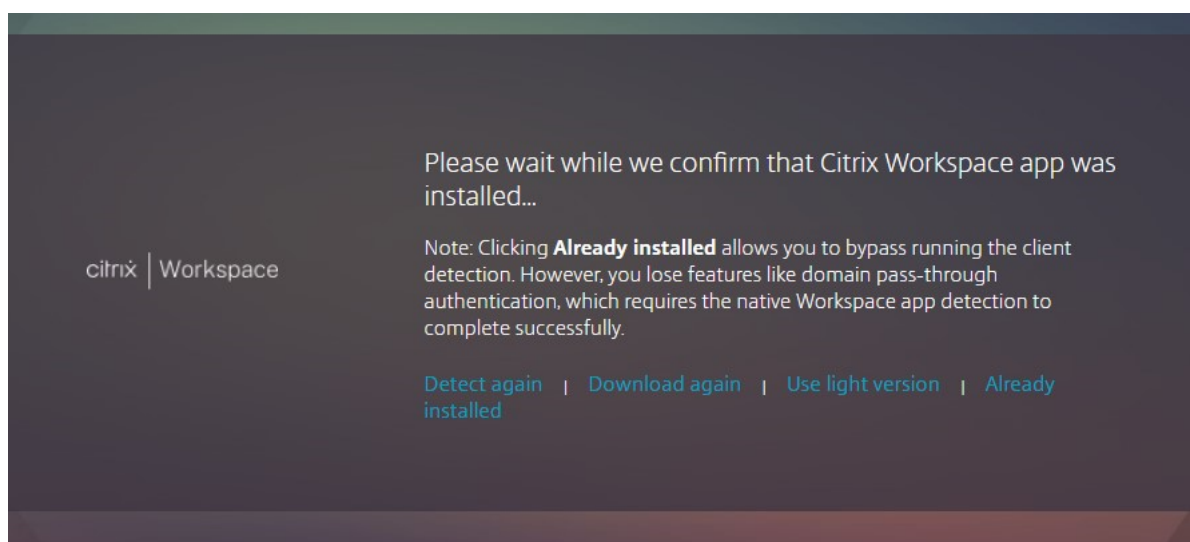
If you have chosen **Always use Receiver for HTML5** or **Use Receiver for HTML5 if local Receiver is unavailable**, by default, resources launched in the browser open a new browser tab. If you want your resources to open in the same tab, replacing Workspace app for HTML5, select **Launch applications in the same tab as Receiver for Web**.

Show the Already installed option on the client detection page

Note:

This setting is applicable only for Windows, MacOS, and Linux devices. If a user has installed Workspace web extensions, then the client detection and launch is handled by the web extensions. In such cases, this setting is not applicable.

When end users open a store in their browser for the first time on Windows, macOS, or Linux, the website attempts to detect the locally installed app using the Citrix Workspace launcher. Subsequently, when a user launches a resource, the Citrix Workspace launcher communicates with the locally installed Citrix Workspace app. If users click the **Already installed** option, the client detection process is skipped. As a result, when the user launches a resource, an **.ica** file is downloaded that users can open with their locally installed Citrix Workspace app. This does not support features such as domain pass-through and app protection.



This downloaded **.ica** file may pose a security risk. Citrix recommends that you clear the **Show Already installed link on the client detection page** checkbox to hide the **already installed** option.

Prevent Ica downloads on all platforms

This provides an additional level of protection by completely blocking `.ica` downloads across all platforms. As Citrix Workspace launcher is not available on iOS, Android or Chrome, users must either select **Use Light version** if available, or they must add their store to their locally installed Citrix Workspace app.

Important:

This option should not be used in conjunction with the **Show Already installed** option on the client detection page.

Allow users to download Citrix Workspace app for Windows or Mac

If you choose **Install locally** or **Use Receiver for HTML5 if local Receiver is unavailable** and enable **Allow users to download HDX engine (plug in)**, if Workspace app for HTML5 does not detect Workspace app installed locally then it gives the user the option to download Citrix Workspace app for Windows or Mac.

Upgrade Workspace app on logon

If you select **Upgrade plug-in at logon**, Workspace app for HTML5 offers users a choice to upgrade the Citrix Workspace app locally installed client when they log on. Users may choose to skip the upgrade and will not be prompted to upgrade again unless their browser cookies are cleared. To enable this feature, ensure the Citrix Workspace app files are available on the StoreFront server.

Download source

When end users click the download button you can choose whether they are redirected to the Citrix website or to download files directly from the server. You can choose **Citrix website**, **Local files on the StoreFront server** or **Files on remote server (through URL)**.

Configure session settings

March 11, 2024

To modify session settings, go to the [Edit Receiver for web site](#) screen, select the **Session Settings** tab.

Edit Receiver for Web site - /Citrix/StoreWeb

StoreFront

- Category Settings
- Customize Appearance
- Featured App Groups
- Authentication Methods
- Website Shortcuts
- Deploy Citrix Receiver/Workspace app
- Session Settings**
- Workspace Control
- Client Interface Settings
- Advanced Settings

Session Settings

Configure the settings to control the end user experience and specific timeout durations when the inactive users are logged off.

Server Communication attempts: ⓘ

Communication timeout duration: ⓘ

Minutes
 Seconds

Session timeout: ⓘ

Hour
 Minutes

Sign in timeout: ⓘ

 Minutes

Server communication attempts

The number of attempts for calls between the web proxy and store services, internal to StoreFront. Normally there is no need to modify this setting.

Communication timeout duration

The amount of time allowed for calls between the web proxy and store services, internal to StoreFront. Normally there is no need to modify this setting.

Session inactivity timeout

While accessing a StoreFront store through a web browser, after a period of inactivity, the user sees the message **Your session has timed out due to inactivity**. You can change the **Session timeout** to suit your users' usage pattern. This does not affect Citrix Workspace apps.

Alternatively you can use PowerShell. For example to set the timeout for the website '/Citrix/StoreWeb' to 30 minutes:

```
1 $rfw = Get-STFWebReceiverService '/Citrix/StoreWeb'  
2 Set-STFWebReceiverService $rfw -SessionStateTimeout 30  
3 <!--NeedCopy-->
```

If you modify the session timeout so that it is greater than the Authentication token lifetime or Maximum token lifetime then this also updates the authentication token lifetime and Maximum token lifetime to match.

Authentication token lifetime

When a user accesses a StoreFront store through a browser, by default the user is logged out after eight hours, regardless of any activity. This does not affect Citrix Workspace apps. To increase this timeout:

1. On StoreFront, navigate to **c:\inetpub\wwwroot\Citrix<StoreWeb>**.
2. Open the **web.config** file.
3. Locate the entry: **<authentication tokenLifetime="08:00:00"method="Auto" />**
4. Change the **tokenLifetime** to the desired value. To enter a value of 1 day or more, use the format **d.h:m:s**.

If you increase the session timeout to be more than 20 hours, you must also increase the Maximum token lifetime of Authentication Service.

Maximum token lifetime of Authentication Service

The Authentication Service issues tokens that are used when connecting to a store through a web browser or Citrix Workspace apps. For Citrix Workspace apps this is the only login timeout that needs to be updated. When accessing StoreFront through a browser, this timeout is used with the other timeouts. Unlike other settings described on this page this applies to all websites for the store.

When fronting StoreFront with Citrix Gateway, Citrix Gateway has the user credentials and does SSO to StoreFront. If the StoreFront token expires, StoreFront would issue a CitrixAG Basic challenge and Citrix Gateway would supply the credentials to log in to StoreFront. So if you are also using Citrix Gateway, then you also need configure its own session timeout.

1. For the Citrix Workspace app installed on the StoreFront Server, navigate to the path of your store's auth service **c:\inetpub\wwwroot\Citrix\<Store>Auth** (which could be one of several auth services depending on how many Stores you have).
2. In the **web.config** file, locate the **Authentication Token Producer** service, and within that, find the **add** element whose **id** matches that of the **Authentication Token Producer**. In the

following example, you need the `add` element with `id="f7cac185-57c1-4629-a33c-88a89dd4295d"encipherId="2948f7ad-735e-4e03-8e01-8d4f5d3ca75b"`:

```
1 <service id="f7cac185-57c1-4629-a33c-88a89dd4295d" displayName="
  Authentication Token Producer">
2   <relyingParties signingId="2948f7ad-735e-4e03-8e01-8
    d4f5d3ca75b" defaultLifetime="01:00:00" maxLifetime="
    01:00:00">
3   <clear />
4   <add id="f7cac185-57c1-4629-a33c-88a89dd4295d" encipherId="
    2948f7ad-735e-4e03-8e01-8d4f5d3ca75b" defaultLifetime="
    01:00:00" maxLifetime="20:00:00" />
5 <!--NeedCopy-->
```

3. Change the **maxLifetime** to the desired value. The default is 20:00:00. To enter a value of 1 day or more, use the format `dd.hh:mm:ss`.
4. Run the **isreset** command to apply the changes. Running this command logs off the users from Citrix StoreFront Web but it doesn't impact their current ICA session.

Workspace control

April 9, 2024

As users move between devices, workspace control ensures that the applications they are using follow them. Users can keep working with the same application instances across multiple devices rather than having to restart all their applications each time they log on to a new device. This enables, for example, clinicians in hospitals to save time as they move from workstation to workstation accessing patient data.

When users log on, they are automatically reconnected to any applications that they left running. For example, consider a user logging on to a store, and starting some applications. If the user then logs on to the same store using the same access method but on a different device, the running applications are automatically transferred to the new device. All the applications that the user starts from a particular store are automatically disconnected, but not shut down, when the user logs off from that store. In the case of accessing a store through a web browser, the same browser must be used to log on, start the applications, and log off.

Configure Workspace Control on Workspace App for HTML5

The workspace control settings within StoreFront management console only apply when accessing the store through a web browser. This is subject to the following requirements and restrictions:

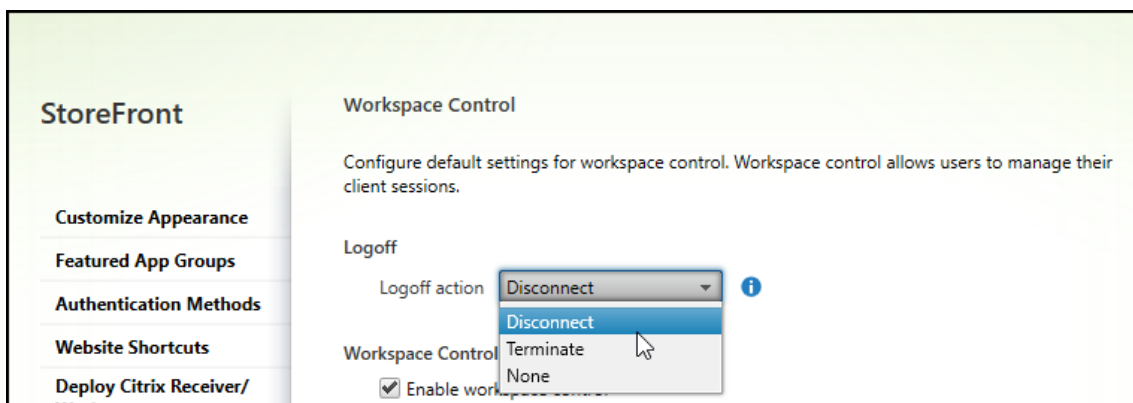
- Workspace control is not available when Workspace app for HTML is running within a hosted desktops or application.
- For users accessing websites from Windows devices, workspace control is only enabled if the site can detect that Citrix Workspace app for Windows is installed on users' devices or if Citrix Workspace app for HTML5 is used to access resources.
- To reconnect to disconnected applications, users accessing websites through Internet Explorer must add the site to the Local intranet or Trusted sites zones.
- If there is only one desktop available for a user on a website that is configured to start single desktops automatically when the user logs on, that user's applications are not reconnected, regardless of the workspace control configuration.
- Users must disconnect from their applications using the same browser that was originally used to start them. Resources started using a different browser, or started locally from the desktop or Start menu using Citrix Workspace app, cannot be disconnected or shut down by Citrix Workspace app for HTML5.
- Workspace control is not available when resources open within the same browser tab. To configure this, see [Citrix Workspace app deployment](#).

To modify workspace control settings when a store is accessed through a web browser, select **Workspace Control** on the [Edit Receiver for web site](#) screen.

The screenshot shows the 'StoreFront' configuration interface. On the left is a navigation menu with the following items: 'Customize Appearance', 'Featured App Groups', 'Authentication Methods', 'Website Shortcuts', 'Deploy Citrix Receiver/Workspace app', 'Session Settings', 'Workspace Control' (highlighted with a blue arrow), 'Client Interface Settings', and 'Advanced Settings'. The main content area is titled 'Workspace Control' and includes a description: 'Configure default settings for workspace control. Workspace control allows users to manage their client sessions.' Below this, the 'Logoff' section has a 'Logoff action' dropdown menu set to 'Disconnect' with an information icon. The 'Workspace Control' section contains a checked checkbox for 'Enable workspace control', followed by the 'Automatic reconnection when users log on' section with a checked checkbox for 'Automatically reconnect to the sessions when users log on'. The 'Reconnect and Disconnect Button' section has two unchecked checkboxes: 'Show reconnect button' and 'Show disconnect button'. At the bottom right are three buttons: 'OK', 'Cancel', and 'Apply'.

Configure settings for workspace control as follows:

- Specify the **Logoff action**. The log off actions are as follows:
 - **Disconnect**: When you log off from the site, the app and desktop sessions are automatically disconnected from the client device.
 - **Terminate**: When you log off the site, app and desktop sessions are automatically terminated on the server.
 - **None**: When you log off from the site, app and desktop sessions remain running.



- Select the **Enable workspace control** check box.
- Select the **Automatically reconnect to the sessions when users logon** check box under **Automatic reconnections when users logon**.

Configure Workspace Control using PowerShell SDK

You can configure workspace control using the PowerShell cmdlet [Set-STFWebReceiverUserInterface](#).

Configure Workspace Control on Workspace app for Windows

To configure Workspace Control on Workspace for Windows, see [Manage workspace control reconnect](#).

Configure Workspace Control on Workspace app for Mac

To configure Workspace control Workspace app for Mac, see [Configure workspace control settings](#).

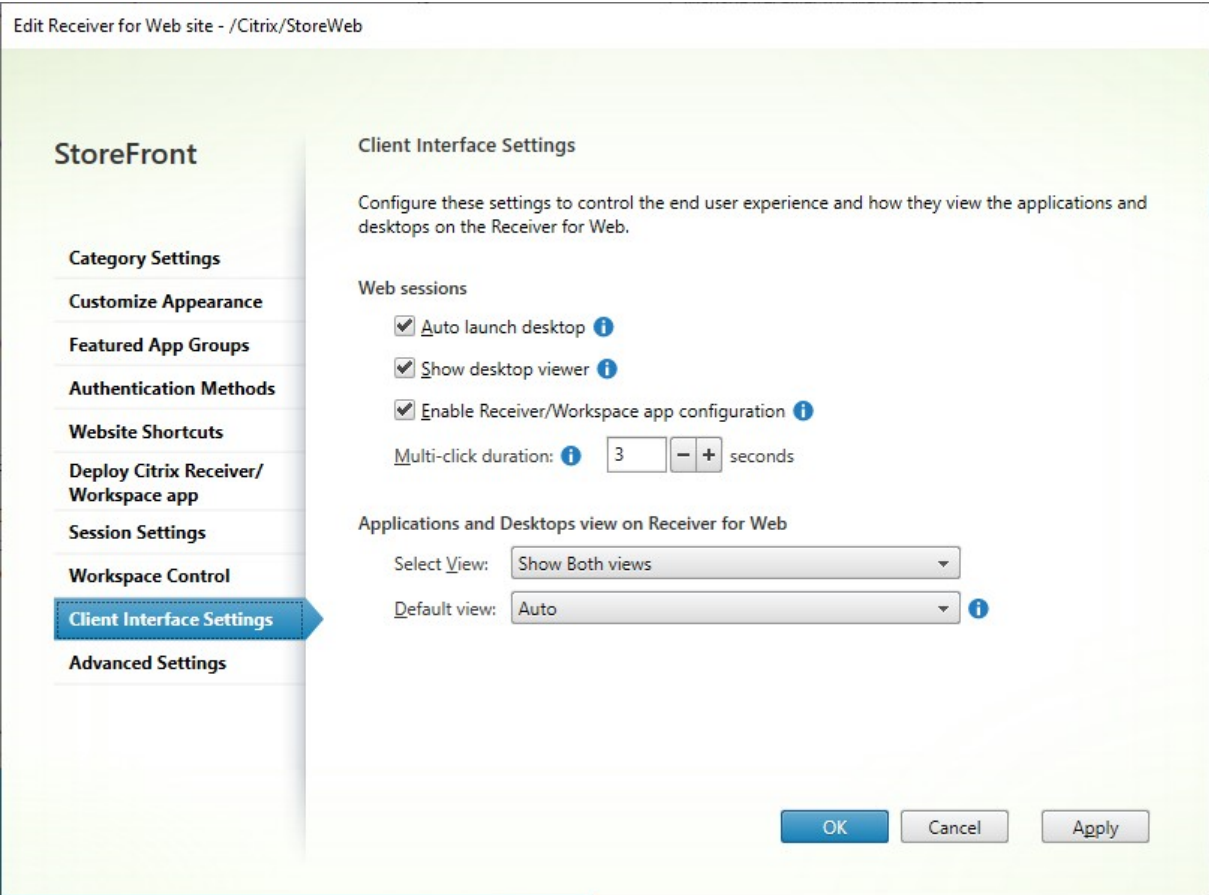
Disable Workspace Control across all apps

To disable session reconnect in StoreFront across Workspace apps, regardless of how they are configured, go to the **Advanced Settings** tab and uncheck **Allow session reconnect**.

Client Interface Settings

March 19, 2024

To modify client interface settings from the [Edit Receiver for web site](#) screen, select the **Client Interface Settings** tab.



Auto launch desktop

If this setting is enabled and a user only has one desktop, then the desktop is launched when the user signs in.

To use the PowerShell SDK to change auto launch desktop setting call cmdlet [Set-STFWebReceiverUserInterface](#) with parameter [AutoLaunchDesktop](#).

This setting only applies to Citrix Workspace app for HTML5. It does not apply to locally installed Citrix Workspace apps.

Show Desktop Viewer

The Desktop Viewer is the toolbar that provides easy access to HDX preferences. Use this setting to choose whether this is displayed.

This setting only applies to Citrix Workspace app for HTML5. It does not apply to locally installed Citrix Workspace apps.

Multi-click duration

Prevent users from launching the same application multiple times in the configured duration. This only applies to Citrix Workspace app for HTML5 and not to native Citrix Workspace app.

To use the PowerShell SDK to change the multi-click duration call cmdlet [Set-STFWebReceiverUserInterface](#) with parameter [MultiClickTimeout](#).

This setting only applies to Citrix Workspace app for HTML5. It does not apply to locally installed Citrix Workspace apps.

Enable Receiver/Workspace app configuration

If checked, Citrix Workspace app for HTML5 offers provisioning files that enable users to configure native Citrix Workspace app automatically for the associated store. The provisioning files contain connection details for the store that provides the resources on the site, including details of any Citrix Gateway deployments and beacons configured for the store.

To use the PowerShell SDK to change this option call cmdlet [Set-STFWebReceiverUserInterface](#) with parameter [ReceiverConfigurationEnabled](#).

Application and desktops view

When both desktops and applications are available, Citrix Workspace app displays separate desktop and application views by default. Favorites are displayed on the **Home** view. Users see the **Home** view first when they log on to the site.

From the **Select View** drop-down list, select whether to display apps or desktops, or both.

From the **Default** view drop-down list, select which view is displayed when the user logs in.

Option	Description
Auto	Display the Home view

Option	Description
Apps	Display the apps view
Desktops	Display the desktops view

To use the PowerShell SDK to change these options call cmdlet [Set-STFWebReceiverUserInterface](#) with parameters [ShowAppsView](#), [ShowDesktopsView](#) and [DefaultView](#).

App Protection

April 26, 2024

App Protection provides an extra level of security by blocking key logging and screen capture. For more information, see the [App Protection](#) documentation.

Workspace app

App Protection is available by default when accessing a store through Citrix Workspace apps for Windows, Mac, and Linux.

App Protection for hybrid launch

When accessing a store through a web browser, apps requiring App Protection are hidden by default. StoreFront can be configured to display protected apps when it detects the following minimum versions for the Citrix Workspace app:

App	Version
Citrix Workspace app for Windows	1912
Citrix Workspace app for Mac	2001
Citrix Workspace app for Linux	2108

StoreFront does not display protected apps when using earlier versions of Workspace app, or on iOS, Android, ChromeOS, or when launching apps in the browser using Citrix Workspace app for HTML5.

To allow StoreFront to display protected apps on supported Workspace versions, use the [PowerShell SDK](#) cmdlet [Set-STFWebReceiverAppProtection](#).

If the user has chosen to launch workspace apps through a browser (either through admin configuration or because the user chose to use **Workspace lite**), App Protection is not available. You can configure the store to always launch using locally installed Citrix Workspace app, see [Citrix Workspace app deployment](#).

StoreFront determines the Citrix Workspace app version Using [Citrix Workspace Web Extension](#) if it is available and configured (see [Browser extension based client detection](#)). Otherwise Storefront determines the Workspace app version as part of client detection the first time the user goes to the store website. If the user skips detection by choosing **Already installed** then StoreFront is unable to determine the app version so does not display protected applications. Therefore it is recommended that you disable the **Already installed** option, see [Citrix Workspace app deployment](#).

Warning

If Citrix Workspace Web Extension is not available, StoreFront determines the Citrix Workspace app version the first time the user goes to the website. If the user subsequently installs a different version of Workspace app then StoreFront will not be aware of the change, so may incorrectly allow or disallow launching protected apps. Citrix recommends configuring [App Protection Posture Check](#) which blocks launching virtual apps and desktops from Citrix Workspace app versions that do not support App Protection.

Remove website

February 27, 2024

1. Select the **Store** node in the left pane of the Citrix StoreFront management console, select the store for which you want to create the Citrix Receiver for Web site, and click **Manage Receiver for Web Sites** in the **Actions** pane.
2. Select a site and click **Remove**. When you remove a site, users can no longer use that webpage to access the store.

Configure Workspace app website

February 27, 2024

When you create a new store using StoreFront, a website is automatically created and associated with the store. When a store has multiple websites, select which website is displayed when users access the store using Citrix Workspace app.

1. Select the **Stores** node in the left pane of the Citrix StoreFront management console.
2. Select a store in the center pane, and click **Configure Unified Experience** in the **Actions** pane. If you don't have a Citrix Receiver for Web website created, a message displays including a link to the Add Receiver for Web site wizard.
3. Select the website which you wish Citrix Workspace app clients display when users access this store.
4. Click **OK**.

Configure server groups

March 11, 2024

The tasks below enable you to modify settings for multiple-server StoreFront deployments. To manage a multiple-server deployment, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Any configuration changes you make must be propagated to the other servers in the group to ensure a consistent configuration across the deployment.

You must configure servers comprising a StoreFront server group identically in terms of both StoreFront installation location and IIS website settings, such as physical path and site IDs.

Add a server to a server group

Use the Add Server task to obtain an authorization code to enable you to join a newly installed StoreFront server to your existing deployment. For more information about adding new servers to existing StoreFront deployments, see [Join an existing server group](#). See the *Scalability* section of [Plan your Storefront deployment](#) to assess how many servers you need in your group.

Remove servers from a server group

Use the **Remove Server** task to delete servers from a multiple-server StoreFront deployment. You can remove any server in the group apart from the server on which you are running the task. Before removing a server from a multiple-server deployment, first remove the server from the load-balancing environment.

Before a removed StoreFront server can be added again, to the same or to a different server group, you must reset it to a factory default state. See [Reset a server to factory defaults](#)

Propagate local changes to a server group

Use the Propagate Changes task to update the configuration of all the other servers in a multiple-server StoreFront deployment to match the configuration of the current server. Propagation of configuration information is initiated manually so that you retain control over when and if the servers in the group are updated with configuration changes. While running this task, you cannot make any further changes until all the servers in the group have been updated.

Important:

Any changes made on other servers in the group are discarded during propagation. If you update the configuration of a server, propagate the changes to the other servers in the group to avoid losing those changes if you later propagate changes from different server in the deployment.

The information propagated between servers in the group includes the following:

- Contents of all web.config files, which contain the StoreFront configuration.
- Contents of `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients`, such as `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\Windows\CitrixWorkspaceAppWeb.exe` and `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\MAC\CitrixWorkspaceAppWeb.dmg`.
- Contents of `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\contrib`.
- Contents of `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\custom` folder, such as copied images and customisation.js files.
- Contents of the Citrix Delivery Services certificate store, except any manually imported Certificate Revocation Lists (CRLs). (For details on distributing local CRLs, see [Certificate Revocation List \(CRL\) checking](#).)

Note:

Subscription data is synchronized with the other servers independently of the Propagate Changes mechanism. It happens automatically without the Propagate Changes task being initiated.

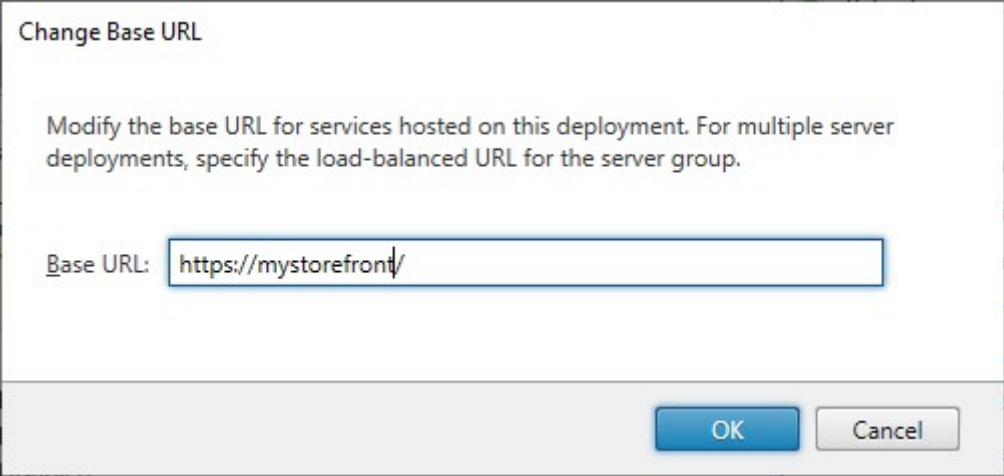
Change the base URL for a deployment

The base URL is used as the root of the URLs for the stores and other StoreFront services hosted on a deployment. For multiple-server deployments, specify the load-balanced URL.

To change the base URL:

1. In the Citrix StoreFront management console left pane, select the **Server Group** node.

- 2. In the actions pane click **Change Base URL...**
- 3. Enter the new URL
- 4. Press **OK**.



Integrate with Citrix Gateway and NetScaler ADC

April 18, 2024

Use Citrix Gateway with StoreFront to provide secure remote access for users outside the corporate network and NetScaler ADC to provide load balancing.

Task	Detail
Import a Citrix Gateway	Export configuration from your Citrix Gateway and import it into StoreFront
Manage Citrix Gateways	Add, remove and edit Citrix Gateway connection settings
Load balancing with NetScaler ADC	Configure NetScaler ADC as a load balancer in front of a StoreFront server group
Configure NetScaler ADC and StoreFront for Delegated Forms Authentication (DFA)	
Authenticate using different domains	Configure StoreFront and Citrix Gateway so that users first authenticate with the gateway on one domain, then authenticate to StoreFront on a different domain.

Task	Detail
Configure beacon points	Configure beacon URLs that Citrix Workspace app can use to determine whether it is inside or outside your corporate network.
Create a single FQDN used internally and externally	Create a single fully qualified domain name (FQDN) that can access a store directly from within your corporate network and remotely via the Citrix Gateway.

Configure Citrix Gateways

March 19, 2024

Use Citrix Gateways to provide remote access to StoreFront. Citrix Gateways run on a hardware or software NetScaler ADC or NetScaler Gateway appliance.

For more information about configuring your Gateway, see [Integrate NetScaler Gateway with StoreFront](#).

You must configure your gateway within StoreFront before StoreFront allows access through that gateway.

View Gateways

To view the gateways configured within StoreFront, select the Stores node in the left pane of the Citrix StoreFront management console and pane, click **Manage Citrix Gateways**. This displays the **Manage Citrix Gateways** window.

Manage Citrix Gateways

Add, edit or remove the Citrix Gateway appliances through which remote access is provided. Remote access through a Citrix Gateway cannot be applied to unauthenticated stores.

Alternatively, Citrix Gateway appliances can be [imported from file](#).

Citrix Gateways:

Display Name	Role	Used by Sto...	URL
Gateway	Authenticati...	Yes	https://gateway.example.com/

Add...

Edit...

Remove

Close

PowerShell

To get a list of gateways and their configuration call [Get-STFRoamingGateway](#).

Add Citrix Gateway

Important:

In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, [propagate your configuration changes to the server group](#) so that the other servers in the deployment are updated.

1. In the **Manage Citrix Gateways** window click **Add**.

2. On the General Settings tab enter the settings then press **Next**.

- Specify a **Display name** for the Citrix Gateway deployment that will help users to identify it.

Users see the display name you specify in Citrix Workspace app, so include relevant information in the name to help users decide whether to use that deployment. For example,

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

242

you can include the geographical location in the display names for your Citrix Gateway deployments so that users can easily identify the most convenient deployment for their location.

- Enter the URL of the gateway.

The fully qualified domain name (FQDN) for your StoreFront deployment must be unique and different from the Citrix Gateway virtual server FQDN. Using the same FQDN for StoreFront and the Citrix Gateway virtual server is not supported. The gateway adds the URL to the `X-Citrix-Via` HTTP header. StoreFront uses this header to determine which gateway is in use.

Using the GUI it is only possible to add a single gateway URL. If a gateway can be access by multiple URLs then you need to add the same gateway twice with identical configuration apart from the URL. To simply configuration, you can configure a secondary URL used to access the gateway. This option is not available using the GUI so you must configure this using PowerShell. You should close the management console before running any PowerShell commands. For example if you have multiple gateways behind a global server load balancer, typically it is useful to add both the GSLB URL and a URL that can be used to access each specific regional gateway, for example for testing or troubleshooting purposes. Once you have created the gateway you can add an additional URL using `Set-STFRoamingGateway`, using the `-GSLBurl` parameter for the secondary URL. Although the parameter is called `GSLBurl` this can be used for any situation where you wish to add a second URL. For example:

```
1 Set-STFRoamingGateway -Name "Europe Gateway" -GSLBurl "
   eugateway.example.com" -GatewayUrl "gslb.example.com"
2 <!--NeedCopy-->
```

Note:

Counterintuitively in this example, the `GSLBurl` parameter contains the regional URL while the `GatewayUrl` parameter contains the GSLB URL. For most purposes the URLs are treated identically and if the store is only accessed through a web browser they can be configured either way around. However when accessing StoreFront through Citrix Workspace app, it reads the `GatewayUrl` from StoreFront and subsequently uses it for remote access and it is preferable for it to be configured to always connect to the GSLB URL.

If you need more than two URLs then you will need to configure this as a separate gateway.

- Select the Usage or Role:

Usage or role	Description
Authentication and HDX routing	Use the gateway for both providing remote access to StoreFront and to access the VDAs.
Authentication only	Select this if the gateway is used only for remote access to StoreFront.
HDX routing only	Select this if the gateway is used only for providing HDX access to VDAs, e.g. at a site that does not have a StoreFront instance.

Add Citrix Gateway Appliance

StoreFront

General Settings

Secure Ticket Authority

Authentication Settings

Summary

General Settings

Complete these settings to configure access to stores through Citrix Gateway for users connecting from public networks. Remote access through a Citrix Gateway cannot be applied to unauthenticated stores.

Display name:

Europe gateway

Citrix Gateway URL:

https://eugateway.example.com

Usage or role:

Authentication and HDX routing

Next

Cancel

3. Fill out the settings on the **Secure Ticketing Authority** tab.

The secure ticketing authority issues session tickets in response to connection requests. These session tickets form the basis of authentication and authorization for access to Citrix Virtual Apps and Desktops resources.

- Enter at least one Secure Ticket Authority server URL. If you are using Citrix Virtual Apps and Desktops then you can use the delivery controller as a STA. If you are using Citrix Desktop as a Service then you can enter the cloud connectors, which proxy requests to the Citrix cloud ticketing authority. The entries on this list must exactly match the list configured in the Citrix Gateway.

© 1999–2024 Cloud Software Group, Inc. All rights reserved.

244

- Tick **Load balance multiple STA servers** to distribute requests between the STA servers. If unticked then StoreFront will try the servers in the order in which they are listed.
- If StoreFront cannot reach an STA server then it avoids using that server for a period of time. By default this is 1 hour but you can customize this value.
- If you want Citrix Virtual Apps and Desktops to keep disconnected sessions open while Citrix Workspace app attempts to reconnect automatically, select the Enable session reliability check box. If you configured multiple STAs and want to ensure that session reliability is always available, select the **Request tickets from two STAs, where available** check box.

When the Request tickets from two STAs, where available check box is selected, StoreFront obtains session tickets from two different STAs so that user sessions are not interrupted if one STA becomes unavailable during the course of the session. If, for any reason, StoreFront is unable to contact two STAs, it falls back to using a single STA.

The screenshot shows the 'Add Citrix Gateway Appliance' wizard with the 'StoreFront' tab selected. The 'Secure Ticket Authority (STA)' settings are displayed. The left sidebar shows 'General Settings' as the active tab, with 'Secure Ticket Authority', 'Authentication Settings', and 'Summary' as sub-tabs. The main content area for 'Secure Ticket Authority (STA)' includes a description: 'STA is hosted on Citrix Virtual Apps and Desktops servers and issues session tickets in response to connection requests. These session tickets form the basis of authentication and authorization for access to Citrix Virtual Apps and Desktops resources.' Below this, there is a section for 'Secure Ticket Authority URLs' with an information icon. A list box contains two URLs: 'https://ddc1.example.com/scripts/cbxsta.dll' and 'https://ddc2.example.com/scripts/cbxsta.dll'. Below the list box are 'Add...', 'Edit...', and 'Remove' buttons. Further down, there are three checkboxes: 'Load balance multiple STA servers' (unchecked), 'Enable session reliability' (checked), and 'Request tickets from two STAs, where available' (unchecked). The 'Bypass failed STA for:' field is set to 1 hour, 0 minutes, and 0 seconds. At the bottom right are 'Back', 'Next', and 'Cancel' buttons.

Once you have completed filling out the settings press **Next**

4. Fill out settings on the **Authentication Settings** tab.

- Choose the NetScaler version.
- If there are multiple gateways with the same URL (typically when using a global server load balancer), and you have entered a callback URL then you must enter the VIP of the

gateway. This allows StoreFront to determine which gateway the request came from and hence which server to contact using the Callback URL. Otherwise you can leave this blank.

- Select from the **Logon type** list the authentication method you configured on the appliance for Citrix Workspace app users.

The information you provide about the configuration of your Citrix Gateway appliance is added to the provisioning file for the store. This enables Citrix Workspace app to send the appropriate connection request when contacting the appliance for the first time.

- If users are required to enter their Microsoft Active Directory domain credentials, select Domain.
- If users are required to enter a tokencode obtained from a security token, select Security token.
- If users are required to enter both their domain credentials and a tokencode obtained from a security token, select Domain and security token.
- If users are required to enter a one-time password sent by text message, select SMS authentication.
- If users are required to present a smart card and enter a PIN, select Smart card.

If you configure smart card authentication with a secondary authentication method to which users can fall back if they experience any issues with their smart cards, select the secondary authentication method from the Smart card fallback list.

- Optionally, enter the internally accessible URL of the gateway in the Callback URL box. This allows StoreFront to contact the Citrix Gateway authentication service to verify that requests received from Citrix Gateway originate from that appliance. It is required for smart access and for password-less authentication scenarios such as Smart Card or SAML otherwise you can leave it blank. If you have multiple Citrix Gateways with the same URL then this URL must be for the specific gateway server.

Add Citrix Gateway Appliance

StoreFront

- ✓ General Settings
- ✓ Secure Ticket Authority
- Authentication Settings**
- Summary

Authentication Settings

These settings specify how the remote user provides authentication credentials

Version: 10.0 (Build 69.4) or later

VServer IP address: 10.1.0.18
(optional)

Logon type: Domain

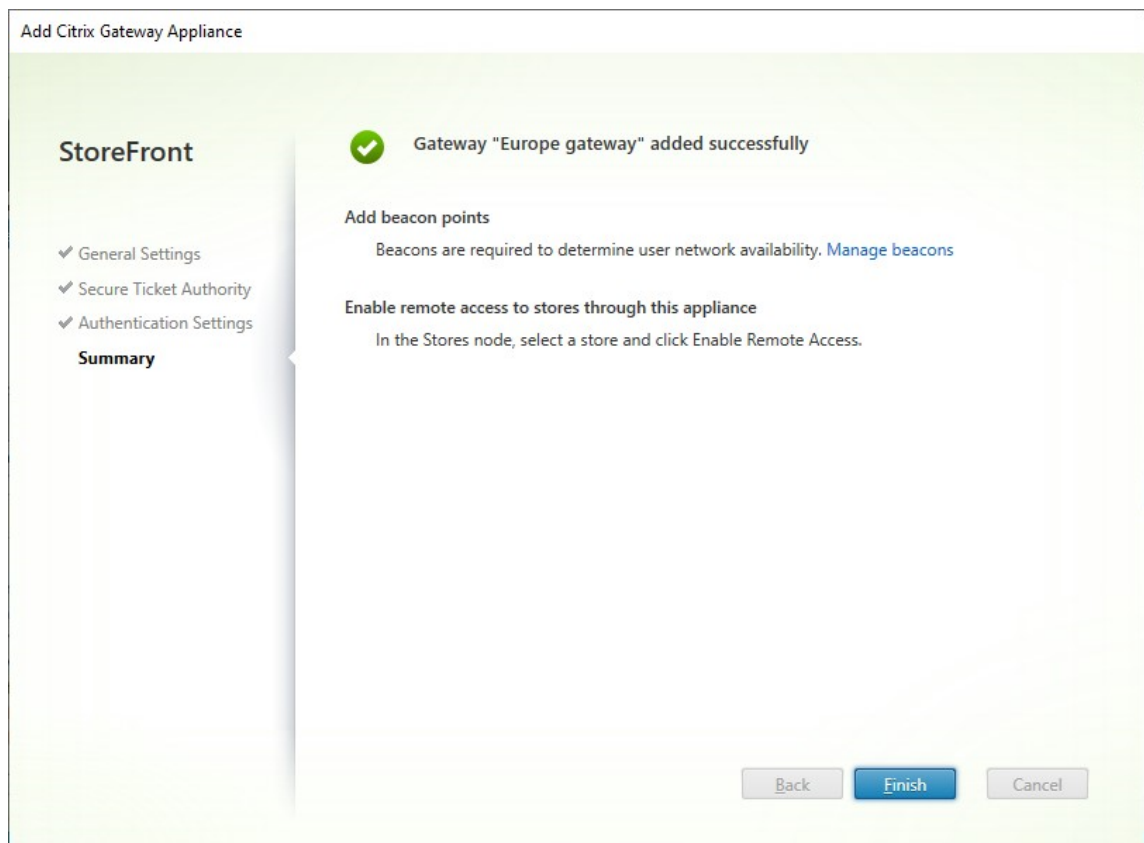
Smart card fallback: None

Callback URL: https://callback.example.com /CitrixAuthService/AuthService.asmx
(optional)

[Back](#) [Create](#) [Cancel](#)

Once you have completed filling out the settings press **Next**

5. Click **Create** to apply the configuration.



6. Once the deployment has been applied, click **Finish**.
7. To enable users to access your stores through the Gateway, configure [remote user access](#).

PowerShell SDK

To add a gateway using the PowerShell SDK call cmdlet [New-STFRoamingGateway](#).

Edit Citrix Gateway

1. In the **Manage Citrix Gateways** window, click on the gateway you wish to change and press **Edit**.

For a description of the parameters, see Add Citrix Gateway

2. Press **Save** to save your changes.

PowerShell SDK

To modify gateway configuration using the PowerShell SDK call cmdlet [Set-STFRoamingGateway](#).

Remove Citrix Gateway

1. In the **Manage Citrix Gateways** window, click on the gateway you wish to change and press **Remove**.
2. In the confirmation window press **Yes**.

PowerShell SDK

To remove the gateway using the PowerShell SDK call [Remove-STFRoamingGateway](#).

Import a Citrix Gateway

March 11, 2024

Remote access settings configured within the Citrix Gateway administration console have to be identical to those configured in StoreFront. This article shows you how to import details of a Citrix Gateway virtual server so that Citrix Gateway and StoreFront are configured correctly to work together.

Requirements

- NetScaler 11.1.51.21 or later is required to export multiple gateway vServers to a ZIP file.

Note:

Citrix Gateways can only export gateway vServers created using the Citrix Virtual Apps and Desktops wizard.

- It must be possible for DNS to resolve, and for StoreFront to contact, all STA (Secure Ticket Authority) server URLs in the GatewayConfig.json file within the ZIP file generated by the Citrix Gateway.
- The GatewayConfig.json file within the ZIP file generated by the Citrix Gateway must contain the URL of an existing Citrix Receiver for Web site on the StoreFront server. Citrix Gateway 11.1 and later takes care of this by contacting the StoreFront server and enumerating all existing stores and Citrix Receiver for Web sites before generating the ZIP file for export.
- StoreFront must be able to resolve the callback URL in DNS to the gateway VPN vServer IP address for authentication using the imported gateway to succeed.

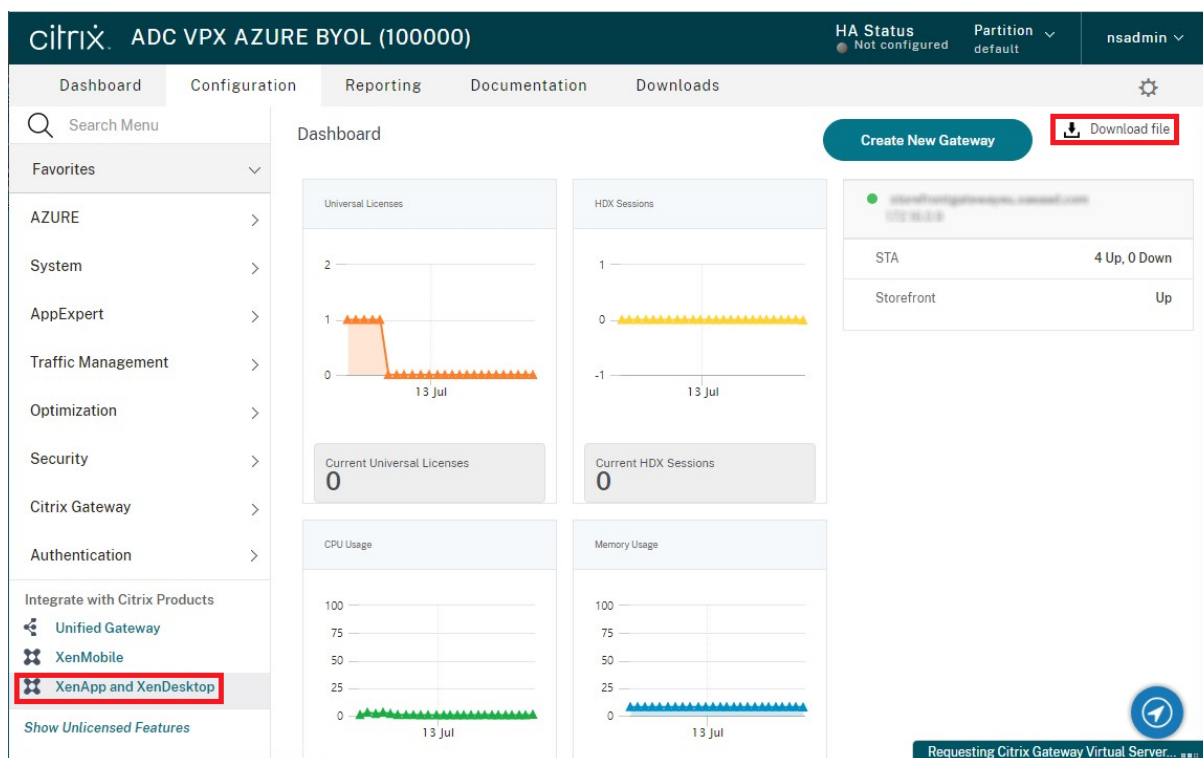
The callback URL and port combination you use is usually the same as the gateway URL and port combination, as long as StoreFront can resolve this URL.

or

The callback URL and port combination may be different from the gateway URL and port combination if you use different external and internal DNS namespaces in your environment. If your gateway is located in a DMZ and uses an `<example.com>` URL and StoreFront is on your private corporate network and uses an `<example.local>` URL you may use an `<example.local>` callback URL to point back to the gateway vServer in the DMZ.

Export configuration from Citrix Gateway

1. Log onto the Citrix Gateway.
2. Go to the Configuration tab
3. Under “Integrate with Citrix Products”, click XenApp and XenDesktop
4. On the top right click “Download file”.



1. Choose whether you wish to download the configuration for all gateways or a specific gateway.

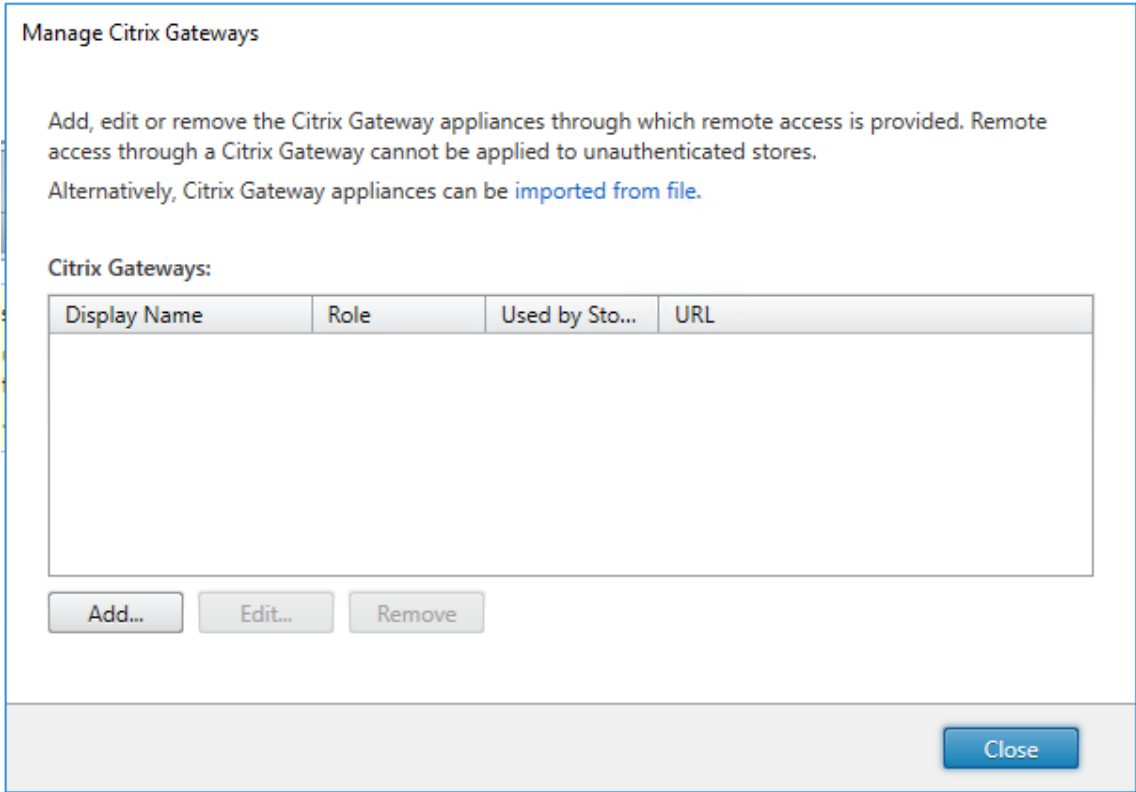
Import a Citrix Gateway using the console

You can import one or more Citrix Gateway virtual server configurations using the same import file. If you have multiple gateway virtual servers from different Citrix Gateway, you must use multiple import files.

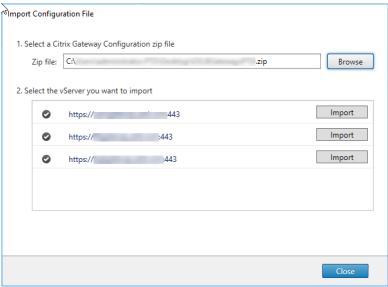
Important:

Citrix does not support manual editing of the configuration file exported from Citrix Gateway.

1. Select **Stores** in the left pane of the Citrix StoreFront management console, and in the **Actions** pane, click **Manage Citrix Gateways**.
2. On the Manage Citrix Gateways screen, click the **imported from file** link.



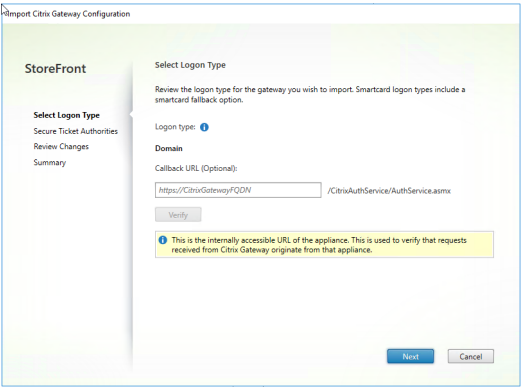
3. Browse to the Citrix Gateway virtual server configuration file.
4. A list of gateway vServers from the selected ZIP file is displayed. Select the gateway vServer you want to import and click **Import**. If you are repeating an import of a vServer, the Import button displays as Update. If you choose **Update**, you have the option later to overwrite or create a new gateway.



5. Review the **Logon type** for the selected gateway and specify a **Callback URL** if required. The

logon type is the authentication method that you configured on the Citrix Gateway for Citrix Workspace app users. Some logon types require callback URLs (see table).

- Click **Verify** to check that the Callback URL is valid and reachable from the StoreFront server.



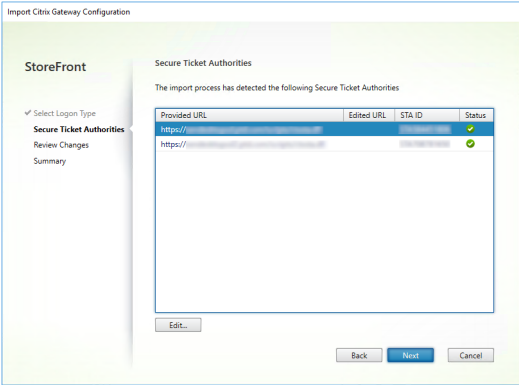
Logon type in console	LogonType in JSON file	Callback URL required
Domain	Domain	No
Domain and security token	DomainAndRSA	No
Security token	RSA	Yes
Smart card - no fallback	SmartCard	Yes
Smart card - domain	SmartCardDomain	Yes
Smart card - domain and security token	SmartCardDomainAndRSA	Yes
Smart card - security token	SmartCardRSA	Yes
Smart card - SMS authentication	SmartCardSMS	Yes
SMS authentication	SMS	Yes

If a callback URL is required, StoreFront will autofill Callback URL based on the gateway URL found in the ZIP file. You can change this to any valid URL that points back to the correct Citrix Gateway VIP. For GSLB gateways, unique callback URLs are required for each of the gateways you import.

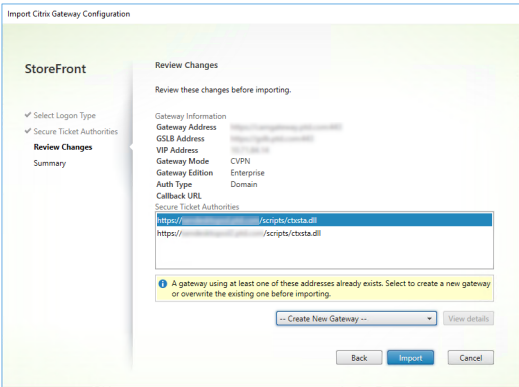
To use Smart Access or password-less authentication, a Callback URL is required.

6. Click **Next**.
7. StoreFront contacts all the STA (Secure Ticket Authorities) server URLs listed in the ZIP file using DNS, and validates that they are functional STA ticketing servers. The import will not continue

if one or more of the STA URLs is invalid.



- 8. Click **Next**.
- 9. Review the details of the import. If a gateway with the same gateway URL and port combination (GatewayURL:port) already exists, use the drop-down to select a gateway to overwrite it, or create a new gateway.



StoreFront uses the GatewayURL:port combination to determine whether a gateway you are trying to import matches an existing gateway that you may wish to update. If a gateway has a different GatewayURL:port combination then StoreFront treats it as a new gateway. This table of gateway settings shows which settings you can update.

Gateway Setting	Can be updated
Gateway URL:Port Combination	No
GSLB URL	Yes
Netscaler Trust Certificate & Thumbprint	Yes
Callback URL	Yes
Receiver for Web Site URL	Yes
Gateway Address/VIP	Yes

Gateway Setting	Can be updated
STA URL and STA ID	Yes
All Logon Types	Yes

10. Click **Import**. If the StoreFront server is part of a server group, a message is displayed reminding you to propagate the imported gateway settings to the other servers in the group.
11. Click **Finish**.

To import another vServer configuration, repeat the steps above.

Note:

The default gateway for a store is the gateway that Citrix Workspace apps try to connect through unless they are configured to use a different gateway. If no gateways are configured for the store, the first gateway imported from the ZIP file will become the default gateway used by Citrix Workspace apps. Importing subsequent gateways does not change the default gateway already set for the store.

Import multiple Citrix Gateways using PowerShell

Read-STFNetScalerConfiguration

- Copy the ZIP file to the desktop of the currently logged on StoreFront administrator.
- Read the contents of the Citrix Gateway virtual server configuration file ZIP file into memory and look at the three gateways it contains using their index values.

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
  USERPROFILE\desktop\GatewayConfig.zip"
2 <!--NeedCopy-->
```

View the three gateway objects in memory which were read in from the Netscaler ZIP import package using the **Read-STFNetScalerConfiguration** cmdlet.

```
1 $ImportedGateways.Document.Gateways[0]
2 $ImportedGateways.Document.Gateways[1]
3 $ImportedGateways.Document.Gateways[2]
4
5 GatewayMode           : CVPN
6 CallbackUrl           :
7 GslbAddressUri        : https://gslb.example.com/
8 AddressUri            : https://emeagateway.example.com/
9 Address               : https://emeagateway.example.com:443
10 GslbAddress           : https://gslb.example.com:443
```

```
11 VipAddress          : 10.0.0.1
12 Stas               : {
13   STA298854503, STA909374257 }
14
15 StaLoadBalance      : True
16 CertificateThumbprints : {
17   F549AFAA29EBF61E8709F2316B3981AD503AF387 }
18
19 GatewayAuthType     : Domain
20 GatewayEdition      : Enterprise
21 ReceiverForWebSites : {
22   Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
     ReceiverForWebSite }
23
24
25 GatewayMode         : CVPN
26 CallbackUrl         :
27 GslbAddressUri      : https://gslb.example.com/
28 AddressUri          : https://emeagateway.example.com/
29 Address             : https://emeagateway.example.com:444
30 GslbAddress         : https://gslb.example.com:443
31 VipAddress          : 10.0.0.2
32 Stas               : {
33   STA298854503, STA909374257 }
34
35 StaLoadBalance      : True
36 CertificateThumbprints : {
37   F549AFAA29EBF61E8709F2316B3981AD503AF387 }
38
39 GatewayAuthType     : DomainAndRSA
40 GatewayEdition      : Enterprise
41 ReceiverForWebSites : {
42   Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
     ReceiverForWebSite }
43
44
45 GatewayMode         : CVPN
46 CallbackUrl         : https://emeagateway.example.com:445
47 GslbAddressUri      : https://gslb.example.com/
48 AddressUri          : https://emeagateway.example.com/
49 Address             : https://emeagateway.example.com:445
50 GslbAddress         : https://gslb.example.com:443
51 VipAddress          : 10.0.0.2
52 Stas               : {
53   STA298854503, STA909374257 }
54
55 StaLoadBalance      : True
56 CertificateThumbprints : {
57   F549AFAA29EBF61E8709F2316B3981AD503AF387 }
58
59 GatewayAuthType     : SmartCard
60 GatewayEdition      : Enterprise
61 ReceiverForWebSites : {
```

```
62 Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.  
    ReceiverForWebSite }  
63  
64 <!--NeedCopy-->
```

Import-STFNetScalerConfiguration without specifying a CallbackURL

Copy the ZIP file to the desktop of the currently logged in StoreFront administrator. Read in the Citrix Gateway configuration ZIP import package into memory and look at the three gateways it contains using their index values.

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:  
    USERPROFILE\desktop\GatewayConfig.zip"  
2 <!--NeedCopy-->
```

Import three new gateways into StoreFront using the **Import-STFNetScalerConfiguration** cmdlet and specifying the gateway indexes you require. Using the **-Confirm:\$False** parameter prevents the Powershell GUI from prompting you to allow every gateway to be imported. Remove this if you wish to carefully import one gateway at a time.

```
1 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -  
    GatewayIndex 0 -Confirm:$False  
2 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -  
    GatewayIndex 1 -Confirm:$False  
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -  
    GatewayIndex 2 -Confirm:$False  
4 <!--NeedCopy-->
```

Import-STFNetScalerConfiguration specifying your own CallbackURL

Import three new gateways into StoreFront using the **Import-STFNetScalerConfiguration** cmdlet and specify a callback URL of your choice using the **-callbackURL** parameter.

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:  
    USERPROFILE\desktop\GatewayConfig.zip"  
2  
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -  
    GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.com:443 -  
    Confirm:$False  
4  
5 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -  
    GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.com:444 -  
    Confirm:$False  
6  
7 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -  
    GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.com:445 -  
    Confirm:$False
```

```
8 <!--NeedCopy-->
```

Import-STFNetScalerConfiguration override the authentication method stored in the import file and specify your own CallbackURL

Import three new gateways into StoreFront using the **Import-STFNetScalerConfiguration** cmdlet and specify a callback URL of your choice using the **-callbackURL** parameter.

```
1 $ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
  USERPROFILE\desktop\GatewayConfig.zip"
2
3 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
  GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://
  emeagatewaycb.example.com:443" -Confirm:$False
4
5 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
  GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://
  emeagatewaycb.example.com:444" -Confirm:$False
6
7 Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
  GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://
  emeagatewaycb.example.com:445" -Confirm:$False
8 <!--NeedCopy-->
```

Load balancing with NetScaler ADC

March 11, 2024

This article provides guidance on how to deploy a StoreFront server group containing two or more StoreFront servers in all active load balanced configuration. The article provides details of how to configure a NetScaler ADC appliance to load-balance incoming requests from Citrix Workspace app and web browsers between StoreFront servers in the server group.

Server certificate requirements for the load-balanced deployment

Consider the following options before purchasing a certificate from a commercial certificate authority or issuing one from your enterprise certificate authority.

- **Option 1:** Use a **.example.com* wildcard certificate on both the NetScaler ADC appliance load balancing virtual server and on the StoreFront server group nodes. This simplifies the configuration and allows you to add extra StoreFront servers in the future without the need to replace the certificate.

- **Option 2:** Use a certificate including Subject Alternative Names (SANs) on both the NetScaler ADC appliance load balancing virtual server and on the StoreFront server group nodes. Extra SANs within the certificate that match all of the StoreFront server fully qualified domain names (FQDNs) are optional, but recommended, as this allows greater flexibility in the StoreFront deployment.

Create DNS records for the StoreFront server group load balancer

Create a DNS A and PTR record for your chosen shared FQDN. Clients within your network use this FQDN to access the StoreFront server group using the NetScaler ADC appliance load balancer.

Example: `storefront.example.com` resolves to the load balancing virtual server virtual IP (VIP).

Configure StoreFront Servers

All of the StoreFront servers you wish to load balance between should be configured as part of a StoreFront Server Group which synchronized configuration between servers to ensure they are configured identically. For more details on adding servers to a Server Group see [Join an existing server group](#).

Each server should be configured for HTTPS so that communication between the load balancer and the StoreFront servers is encrypted. See [Securing StoreFront with HTTPS](#). The certificate must contain the load balanced FQDN as a Common Name (CN) or as a Subject Alternative Name (SAN).

Set the Server Group base URL to be the URL of the load balancer. To modify the Base URL, within the Citrix StoreFront management console, in the left hand pane right click **Server Group** and click **Change Base URL**. Enter the load balancer virtual server's URL.

Optionally Configure Citrix Service Monitor for HTTPS

A StoreFront installation includes the **Citrix Service Monitor** Windows service. This service has no other service dependencies and monitors the health of critical StoreFront services. This allows the NetScaler ADC and other third-party applications to Monitor the relative health of a StoreFront server deployment.

By default the Monitor uses HTTP on port 8000. You may optionally change this to use HTTPS on port 443.

1. Open the PowerShell Integrated Scripting Environment (ISE) on the primary StoreFront server and run the following commands to change the default Monitor to HTTPS 443:

```
1 $ServiceUrl = "https://localhost:443/StorefrontMonitor"
2 Set-STFServiceMonitor -ServiceUrl $ServiceUrl
3 Get-STFServiceMonitor
4 <!--NeedCopy-->
```

2. Once completed, propagate the changes to all other servers in the StoreFront server group.
3. To perform a quick test on the Monitor, enter the following URL into the browser on the StoreFront server or any other machine with network access to the StoreFront server. The browser returns an XML summary of the status of every StoreFront service.

<https://<loadbalancingFQDN>/StoreFrontMonitor/GetSFServicesStatus>

Configure NetScaler Load Balancer

Configure the server certificate on the NetScaler ADC

1. Log on to the NetScaler ADC appliance management GUI.
2. Select **Traffic Management > SSL > Certificates > Server Certificates**
3. Click **Install**.
4. On the **Install Server Certificate** page, enter a Certificate-Key Pair Name, click **Choose File** and browse for the certificate file. If the certificate file does not include the private key then in addition you need to select a **Key File**.

← Install Certificate[?]

Certificate-Key Pair Name*

wildcard.example.com

i

Certificate and Key files are stored in the folder /nsconfig/ssl/ on appliance.

Certificate File Name*

Choose File ▾

wildcard.example.com.cer

Add

i

Key File Name

Choose File ▾

wildcard.example.com.key

Add

i

Certificate Format

☒ PEM

☐ DER

Password

.....

i

☐ Certificate Bundle

☒ Notify When Expires

Notification Period

30

Install

Close

Add individual StoreFront server nodes to the NetScaler ADC appliance load balancer

1. Navigate to **Traffic Management > Load Balancing > Servers**. Click **Add** and add each of the StoreFront servers to be load balanced.

Example = 2 x StoreFront servers named StoreFront-eu-1 and StoreFront-eu-2

2. Use IP-based server configuration and enter the server IP address for each StoreFront node.

Traffic Management > Load Balancing > Servers

Servers 2

Add	Edit	Delete	Rename	Select Action ▼
<input type="text"/> Click here to search or you can enter Key : Value format				
<input type="checkbox"/>	NAME	STATE	IPADDRESS / DOMAIN	TRAFFIC DOMAIN
<input type="checkbox"/>	StoreFront-eu-1	● ENABLED	172.16.0.101	0
<input type="checkbox"/>	StoreFront-eu-2	● ENABLED	172.16.0.102	0
Total 2			25 Per Page ▼	Page 1 of 1

Define a StoreFront Monitor to check the status of all StoreFront nodes in the server group

1. Log on to the NetScaler ADC management GUI.
2. Select **Traffic Management > Load Balancing > Monitors > Add** and add a new Monitor called *StoreFront* and accept all default settings.
3. From the **Type** drop-down menu, select **StoreFront**.
4. If you have configured your StoreFront Monitor for HTTPS, then ensure that the **Secure** option is selected. Else leave this option unselected and enter a port of 8000.
5. Select the **Check Backend Services** option. This option enables monitoring of services running on the StoreFront server. StoreFront services are monitored by probing a Windows service that runs on the StoreFront server, which returns the status of the following services:
 - W3SVC (IIS)
 - WAS (Windows Process Activation Service)
 - CitrixCredentialWallet
 - CitrixDefaultDomainService

Create a service group containing all of the StoreFront servers

1. Navigate to **Traffic Management > Load Balancing > Service Groups**. Press **Add**. To connect to the StoreFront servers over HTTPS, select a protocol of SSL. Leave other settings as default. Press **OK**.

2. Within your Service Group, under **Service Group Members**, click **No Service Group Member**.
 - a) Click **Service Based**.
 - b) Select all of the Servers you defined previously.
 - c) To use SSL between the load balancer and the StoreFront server enter port 443. Else enter port 80.

Create Service Group Member

☐ IP Based ☒ Server Based

Select Server*

Storefront-eu-1, Storefront-eu-2 > Add Edit ⓘ

Note: The port number is mandatory only for DNS servers of query type A (domain name of the IP address)

Port

443 ⓘ

Weight

1

Server Id

Hash Id

☒ State

Create Close

3. Add the **Monitors** section and select the StoreFront Monitor you created earlier.

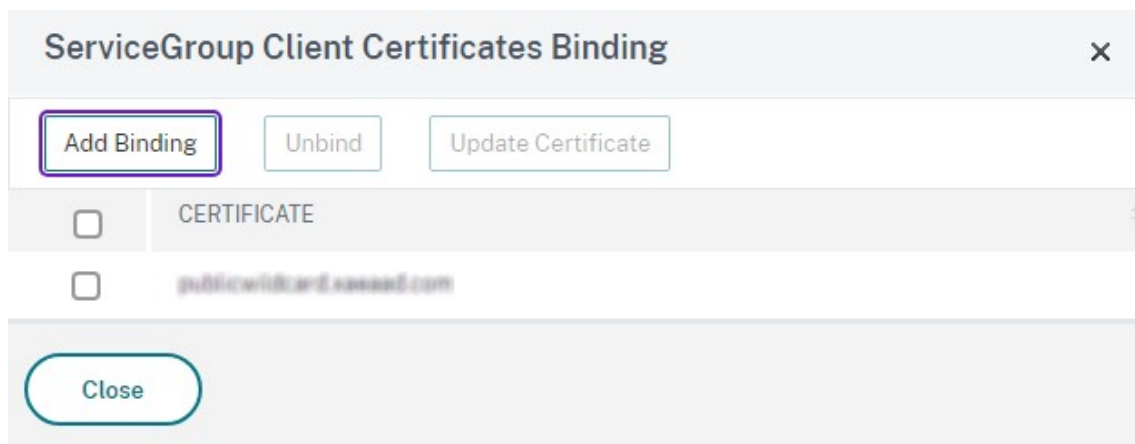
Monitors ×

Add Binding Edit Binding Unbind Edit Monitor

<input type="checkbox"/>	MONITOR NAME	WEIGHT	STATE
<input type="checkbox"/>	StoreFront	1	✓

Close

4. Add the **Certificates** section.
 - a) Bind the client certificate.
 - b) Bind the CA certificate used to sign the server certificate that you imported earlier, and any other CAs that might be part of the PKI chain of trust.



5. Add the **Settings** section. Select **Insert Client IP Header** and enter a header name of **X-Forwarded-For**. This allows the Client IP Address to be used in [Citrix Virtual Apps and Desktops Policies](#).

Create a load balancing virtual server for user traffic

1. Log on to the NetScaler ADC appliance management GUI.
2. Select **Traffic Management > Load Balancing > Virtual Servers > Add** to create a new virtual server.
3. Enter a name, choose a protocol of SSL and enter the **Port**. Click OK to create the Virtual Server.

Load Balancing Virtual Server

Basic Settings

Create a virtual server by specifying a name, an IP address, a port, and a protocol type. If an application is accessible from the Internet, the virtual server IP (VIP) address is a public IP address. If the application is accessible only from the local area network (LAN) or wide area network (WAN), the VIP is usually a private (ICANN non-routable) IP address.

You can configure multiple virtual servers to receive client requests, thereby increasing the availability of resources to process client requests.

Name*

StoreFrontLB

Protocol*

SSL

IP Address Type*

IP Address

IP Address*

172 . 16 . 0 . 8

Port*

443

More

OK

Cancel

- 4. Bind the **Service Group** you created earlier to the load balancing virtual server.
- 5. Bind the same server and CA certificate you previously bound to the service group.
- 6. Add the **Method** section and select the load-balancing method. Common choices for StoreFront load balancing are **round robin** or **least connection**.

Method ✕

Method is a load balancing algorithm that the Citrix ADC uses to select a service to which to direct the client request. In addition to selecting a method, you can specify a delay in accepting requests on a new service.

Load Balancing Method*

LEASTCONNECTION ▼ ⓘ

New Service Startup Request Rate

0

Backup LB Method*

ROUNDROBIN ▼

New Service Request unit*

PER_SECOND ▼

Increment Interval

OK

7. Add the **Persistence** section.

- Set the persistence method to be **COOKIEINSERT**.
- Set the time-out to be the same as the Session time out within StoreFront which by default is 20 minutes.
- Name the cookie. For example, **NSC_SFPersistence**, as this makes it easy to identify during debugging.
- Set backup persistence to **NONE**.

Note:

If the client is not allowed to store the HTTP cookie, the subsequent requests don't have the HTTP cookie, and Persistence is not used.

Persistence

×

Configure persistence to route all connections from the same user to the same service, such as an application that includes a shopping cart or that handles banking transactions. With some persistence types, you can configure backup persistence, which takes effect if the primary persistence type fails.

Select Persistence Type*

☐ SOURCEIP

☒ COOKIEINSERT

☐ OTHERS

Time-out (mins)*

Cookie Name

Backup Persistence

Backup Persistence*

NONE

▼

Backup Time-out (mins)

IPv4 Netmask

IPv6 Mask Length

OK

Configure StoreFront Loopback

When the base address is a load balancer, for the internal communication between StoreFront services, it could cause traffic to route to the load balancer and potentially to another server. This results in poor performance and unexpected behaviour. Use the StoreFront setting **Enable loopback communication** to avoid it. By default this is set to **On**, meaning it replaces the host part of the service address with the loopback IP address 127.0.0.1, while keeping the schema (HTTP or HTTPS) as-is. This works for a single server deployment and deployments with a non SSL-terminating load balancer.

Where the load balancer is SSL-terminating and communicates with StoreFront over HTTP (not recommended), it's necessary to configure StoreFront loopback communication to **OnUsingHttp**, which

means that StoreFront will also change the schema from HTTPS to HTTP.

1. Open Citrix StoreFront.
2. For each Store, go to **Manage Receiver for Web Sites**. For each Web site go to **Configure**.
3. Go to **Advanced Settings**
4. Change the **Enable loopback communication** setting to **OnUsingHttp**.

Edit Receiver for Web site - /Citrix/StoreWeb

StoreFront

Category Settings
Customize Appearance
Featured App Groups
Authentication Methods
Website Shortcuts
Deploy Citrix Receiver/
Workspace app
Session Settings
Workspace Control
Client Interface Settings
Advanced Settings

Advanced Settings

Configure advanced settings with caution.

Enable Fiddler tracing	<input type="checkbox"/>
Enable folder view	<input type="checkbox"/>
Enable loopback communication	On
Enable protocol handler	<input checked="" type="checkbox"/>
Enable strict transport security	<input type="checkbox"/>
ICA file cache expiry	90
Icon resolution	128
Loopback port when using HTTP	80
Prompt for untrusted shortcuts	<input checked="" type="checkbox"/>
Prompt to install Citrix Receiver/Workspace app after logon	<input type="checkbox"/>
Protocol handler skip double-hop check	<input type="checkbox"/>
Resource details	Default
Strict transport security policy duration	90.00:00:00

Enable loopback communication
Enables communication with StoreFront services using the loopback adaptor. Disable this when using Fiddler debugging. Default: On

OKCancelApply

Where the load balancer is SSL-terminating and communicates with StoreFront over HTTP (not recommended), it is necessary to configure StoreFront loopback communication to **OnUsingHttp**, which means that StoreFront will also change the schema from HTTPS to HTTP.

Configure NetScaler ADC load balancer for subscription synchronization between server groups

If you have a multisite deployment consisting of two or more StoreFront server groups, you can replicate subscription data between them using a pull strategy on a repeating schedule. StoreFront subscription replication uses TCP port 808, so using an existing load balancing virtual server on HTTP port 80 or HTTPS 443 fails. To provide high availability for this service, create a second virtual server

on each NetScaler ADC appliance in your deployment to load balance TCP port 808 for each of the StoreFront server groups.

Configure a service group for subscription synchronization

1. Log on to the NetScaler ADC appliance management GUI.
2. Select **Traffic Management > Load Balancing > Service Groups > Add**.
3. Enter a Service Group name, change the protocol to **TCP** and click **OK** to save.
4. **In the Service Group Members** section, add all of the StoreFront server nodes you defined previously in the Servers section and specify **Port** to **808**.
5. Add the **Monitors** section.
 - a) Click where it says **No Service Group to Monitor Binding**.
 - b) Click Add. Enter a Monitor **Name** and set its **Type** to **TCP**. Click **Create**.
 - c) Click **Bind**.

Monitors

Add Binding

Edit Binding

Unbind

Edit Monitor

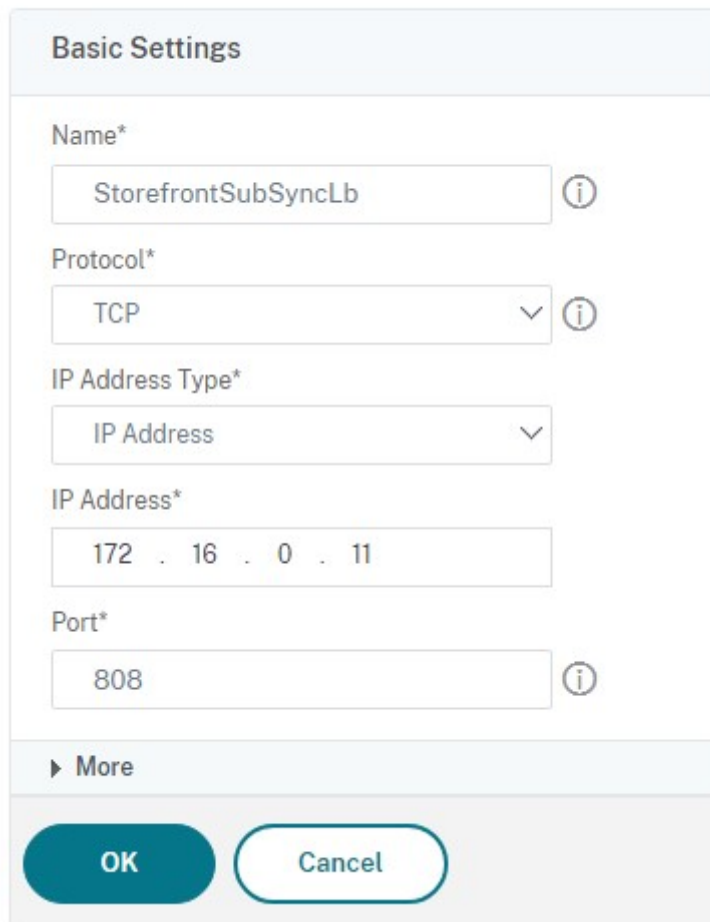
<input type="checkbox"/>	MONITOR NAME	WEIGHT	STATE
<input type="checkbox"/>	StoreFront-SubSync	1	✓

Close

Create a load balancing virtual server for subscription synchronization

1. Log on to the NetScaler ADC appliance management GUI.
2. Select **Traffic Management> Load Balancing > Virtual Servers > Add** and add a new service group.
3. Enter a **Name**
4. Change the protocol to **TCP**.
5. Enter an IP Address.
6. Enter a **Port** of **808**.

Load Balancing Virtual Server



The screenshot shows a configuration window titled "Load Balancing Virtual Server". It has a "Basic Settings" section with the following fields:

- Name***: A text box containing "StorefrontSubSyncLb" with an information icon (i) to its right.
- Protocol***: A dropdown menu showing "TCP" with a downward arrow and an information icon (i) to its right.
- IP Address Type***: A dropdown menu showing "IP Address" with a downward arrow.
- IP Address***: A text box containing the IP address "172 . 16 . 0 . 11".
- Port***: A text box containing the port number "808" with an information icon (i) to its right.

Below the "Basic Settings" section is a "More" section, indicated by a right-pointing triangle icon. At the bottom of the window are two buttons: "OK" (a solid teal button) and "Cancel" (a white button with a teal border).

7. Click **OK**.
8. Click **No Load Balancing Virtual Server ServiceGroup Binding**, select the Service Group you created earlier and click **Bind**.
9. Add the **Method** section and set the **Load Balancing Method** to **ROUNDROBIN**.
10. Click **Done** to complete your changes.

Configure StoreFront to pull subscription data via load balancer

See [Configure subscription synchronization](#).

When configuring the replication schedule, specify a server group address that matches the subscription syncing virtual server virtual load balancer IP address.

Configure Citrix Gateway and StoreFront for Delegated Forms Authentication (DFA)

February 27, 2024

Extensible authentication provides a single customization point for extension of the Citrix Gateway's and StoreFront's form-based authentication. To achieve an authentication solution using the Extensible Authentication SDK, you must configure Delegated Form Authentication (DFA) between the Citrix Gateway and StoreFront. The Delegated Forms Authentication protocol allows generation and processing of authentication forms, including credential validation, to be delegated to another component. For example, Citrix Gateway delegates its authentication to StoreFront, which then interacts with a third party authentication server or service.

Configuring Delegated Forms Authentication on Citrix Gateway is described in [CTX200383](#).

Installation recommendations

- To ensure communication between the Citrix Gateway and StoreFront is protected, use HTTPS instead of HTTP protocol.
- For cluster deployment, ensure that all the nodes have the same server certificate installed and configured in IIS HTTPS binding prior to configuration steps.
- Ensure that the Citrix Gateway has the issuer of StoreFront's server certificate as a trusted certificate authority when HTTPS is configured in StoreFront.

StoreFront cluster installation considerations

- Install a third party authentication plugin on all the nodes prior to joining them up together.
- Configure all the Delegated Forms Authentication related settings on one node and propagate the changes to the others. See the “Enable Delegated Forms Authentication.”

Enable Delegated Forms Authentication

Because there is no GUI to set up Citrix pre-shared key setting in StoreFront, use the PowerShell console to install Delegated Forms Authentication.

1. Install Delegated Forms Authentication. It is not installed by default and you need to install it using the PowerShell console.

```
1 PS C:\Users\administrator.PTD.000> cd 'C:\Program Files\Citrix\Receiver StoreFront\Scripts'
```

```

2 PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> & .\
  ImportModules.ps1
3 Adding snapins
4 Importing modules
5 Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.
  DeliveryServices.ConfigurationProvider.dll'
6 Loading 'C:\Program Files\Citrix\Receiver StoreFront\Admin\Citrix.
  DeliveryServices.ConfigurationProvider.dll'
7
8 PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Install-
  DSDFAServer
9 Id                                : bf694fbc-ae0a-4d56-8749-
  c945559e897a
10 ClassType                        : e1eb3668-9c1c-4ad8-bbae-
  c08b2682c1bc
11 FrameworkController              : Citrix.DeliveryServices.Framework
  .FileBased.FrameworkController
12 ParentInstance                   : 8dd182c7-f970-466c-ad4c-27
  a5980f716c
13 RootInstance                     : 5d0cdc75-1dee-4df7-8069-7375
  d79634b3
14 TenantId                         : 860e9401-39c8-4f2c-928d-34251102
  b840
15 Data                             : {
16   }
17
18 ReadOnlyData                     : {
19   [Name, DelegatedFormsServer], [Cmdlet, Add-DSWebFeature], [Snapin
    , Citrix.DeliverySer
20                                     vices.Web.Commands], [Tenant, 860
    e9401-39c8-4f2c-928d-34251102
    b840] }
21
22 ParameterData                    : {
23   [FeatureClassId, e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc], [
    ParentInstanceId, 8dd182c7-f
24                                     970-466c-ad4c-27a5980f716c], [
    TenantId, 860e9401-39c8-4f2c
    -928d-34251102b840] }
25
26 AdditionalInstanceDependencies : {
27   b1e48ef0-b9e5-4697-af9b-0910062aa2a3 }
28
29 IsDeployed                       : True
30 FeatureClass                     : Citrix.DeliveryServices.Framework
  .Feature.FeatureClass
31 <!--NeedCopy-->

```

2. Add Citrix Trusted Client. Configure the shared secret key (passphrase) between StoreFront and the Citrix Gateway. Your passphrase and client ID must be identical to what you configured on the Citrix Gateway.

```

1 PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Add-

```

```

DSCitrixPSKTrustedClient -clientId netscaler.fqdn.com -
passphrase secret
2 <!--NeedCopy-->

```

3. Set the Delegated Forms Authentication conversation factory to route all the traffic to the custom form. To find the conversation factory, look for ConversationFactory in C:\inetpub\wwwroot\Citrix\Authentication\web.config. This is an example of what you might see.

```

1 <example connectorURL="http://Example.connector.url:8080/adapters-
sf-aaconnector-webapp">
2 <routeTable order="1000">
3 <routes>
4 <route name="StartExampleAuthentication" url="Example-
Bridge-Forms/Start">
5 <defaults>
6 <add param="controller" value="
ExplicitFormsAuthentication" />
7 <add param="action" value="AuthenticateStart" />
8 <add param="postbackAction" value="Authenticate" />
9 <add param="cancelAction" value="CancelAuthenticate"
/>
10 <add param="conversationFactory" value="
ExampleBridgeAuthentication" />
11 <add param="changePasswordAction" value="
StartChangePassword" />
12 <add param="changePasswordController" value="
ChangePassword" />
13 <add param="protocol" value="CustomForms" />
14 </defaults>
15 </route>
16 <!--NeedCopy-->

```

4. In PowerShell, set the Delegated Forms Authentication conversation factory. In this example, to ExampleBridgeAuthentication.

```

1 PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Set-
DSDFAProperty -ConversationFactory ExampleBridgeAuthentication
2 <!--NeedCopy-->

```

PowerShell arguments are not case-sensitive: **-ConversationFactory** is identical to **-conversationfactory**.

Uninstall StoreFront

Before you uninstall StoreFront, uninstall any third party authentication plugin, as it will impact the functionality of StoreFront.

Authenticate using different domains

March 11, 2024

Some organizations have policies in place that do not allow them to give third-party developers or contractors access to published resources in a production environment. This article shows you how to give access to published resources in a test environment by authenticating through Citrix Gateway with one domain. You can then use a different domain to authenticate to StoreFront and the Receiver for Web site. Authentication through Citrix Gateway described in this article is supported for users logging on through the Receiver for Web site. This authentication method is not supported for users of native desktop or mobile Citrix Receiver or Citrix Workspace apps.

Set up a test environment

This example uses a production domain called `production.com` and a test domain called `development.com`.

production.com domain

The `production.com` domain in this example is set up as follows:

- Citrix Gateway with `production.com` LDAP authentication policy configured.
- Authentication through the gateway occurs using a `production\testuser1` account and password.

development.com domain

The `development.com` domain in this example is set up as follows:

- StoreFront, Citrix Virtual App and Desktops and VDAs are all on the `development.com` domain.
- Authentication to the Citrix Receiver for Web site occurs using a `development\testuser1` account and password.
- There is no trust relationship between the two domains.

Configure a Citrix Gateway for the store

To configure a Citrix Gateway for the store:

1. Select **Stores** in the left pane of the Citrix StoreFront management console, and in the **Actions** pane, click **Manage Citrix Gateways**.
2. On the Manage Citrix Gateways screen, click **Add**.
3. Complete the General Settings, Secure Ticket Authority, and Authentication steps.

Add NetScaler Gateway Appliance

The screenshot shows the 'Add NetScaler Gateway Appliance' wizard in the Citrix StoreFront management console. The left sidebar is titled 'StoreFront' and contains a list of settings: 'General Settings' (selected), 'Secure Ticket Authority', 'Authentication Settings', and 'Summary'. The main area is titled 'General Settings' and contains the following text: 'Complete these settings to configure access to stores through NetScaler Gateway for users connecting from public networks. Remote access through a NetScaler Gateway cannot be applied to unauthenticated stores.' Below this text are three input fields: 'Display name:' with the value 'ProductionGateway', 'NetScaler Gateway URL:' with the value 'https://gateway.production.com', and 'Usage or role:' with a dropdown menu showing 'Authentication and HDX routing'. At the bottom right of the form are two buttons: 'Next' and 'Cancel'.

StoreFront

General Settings

Secure Ticket Authority
Authentication Settings
Summary

General Settings

Complete these settings to configure access to stores through NetScaler Gateway for users connecting from public networks. Remote access through a NetScaler Gateway cannot be applied to unauthenticated stores.

Display name:

NetScaler Gateway URL:

Usage or role:

Next **Cancel**

Add NetScaler Gateway Appliance

StoreFront

✓ General Settings

Secure Ticket Authority

Authentication Settings

Summary

Secure Ticket Authority (STA)

STA is hosted on XenDesktop, XenApp, and VDI-in-a-Box servers and issues session tickets in response to connection requests. These session tickets form the basis of authentication and authorization for access to XenDesktop, XenApp, and VDI-in-a-Box resources.

Secure Ticket Authority URLs: ⓘ

https://sta1.development.com/scripts/ctxsta.dll

https://sta2.development.com/scripts/ctxsta.dll

Add...

Edit...

Remove

☐ Load balance multiple STA servers

Bypass failed STA for:

1

 hours

0

 minutes

0

 seconds

☒ Enable session reliability ⓘ

☐ Request tickets from two STAs, where available ⓘ

Back

Next

Cancel

Edit NetScaler Gateway appliance - ProductionGateway

StoreFront

General Settings

Secure Ticket Authority

Authentication Settings

Authentication Settings

These settings specify how the remote user provides authentication credentials

Version:

10.0 (Build 69.4) or later

VServer IP address:
(optional)

Logon type: ⓘ

Domain

Smart card fallback:

None

Callback URL: ⓘ
(optional)

https://callback.production.com

/CitrixAuthService/AuthService.asmx

OK

Cancel

Apply

Note:

DNS conditional forwarders may need to be added so that the DNS servers in use on both domains can resolve FQDNs on the other domain. The Citrix Gateway must be able to resolve the STA server FQDNs on the `development.com` domain using its `production.com` DNS server. StoreFront should also be able to resolve the callback URL on the `production.com` domain using its `development.com` DNS server. Alternatively, a `development.com` FQDN can be used which resolves to the Citrix Gateway virtual server virtual IP (VIP).

Enable pass-through from Citrix Gateway

1. Select **Stores** in the left pane of the Citrix StoreFront management console, and in the **Actions** pane, click **Manage Authentication Methods**.
2. On the Manage Authentication Methods screen, select **Pass-through from Citrix Gateway**.
3. Click **OK**.

Manage Authentication Methods - STORE

Select the methods which users will use to authenticate and access resources.

Method	Settings
<input checked="" type="checkbox"/> User name and password	
<input type="checkbox"/> SAML Authentication	
<input type="checkbox"/> Domain pass-through Can be enabled / disabled separately on Receiver for Web sites	
<input type="checkbox"/> Smart card Can be enabled / disabled separately on Receiver for Web sites	
<input type="checkbox"/> HTTP Basic	
<input checked="" type="checkbox"/> Pass-through from Citrix Gateway	

Installing and uninstalling the authentication methods and the authentication service settings are included in the advanced options.

Advanced

OK

Cancel

Configure the store for remote access using the Gateway

1. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the **Actions** pane, click **Configure Remote Access Settings**.
2. Select **Enable Remote Access**.
3. Ensure that you have registered the Citrix Gateway with your store. If you do not register the Citrix Gateway, the STA ticketing will not work.

Configure Remote Access Settings - Store

Enabling remote access allows users outside the firewall to securely access resources. After you enable remote access, add a NetScaler Gateway appliance.

☒ Enable Remote Access

Select the permitted level of access to internal resources

☒ Allow users to access only resources delivered through StoreFront (No VPN tunnel) ?

☐ Allow users to access all resources on the internal network (Full VPN tunnel) ?

Users may require the NetScaler Gateway Plug-in to establish a full VPN tunnel.

NetScaler Gateway appliances:

☒ ProductionGateway ?

Add...

Default appliance:

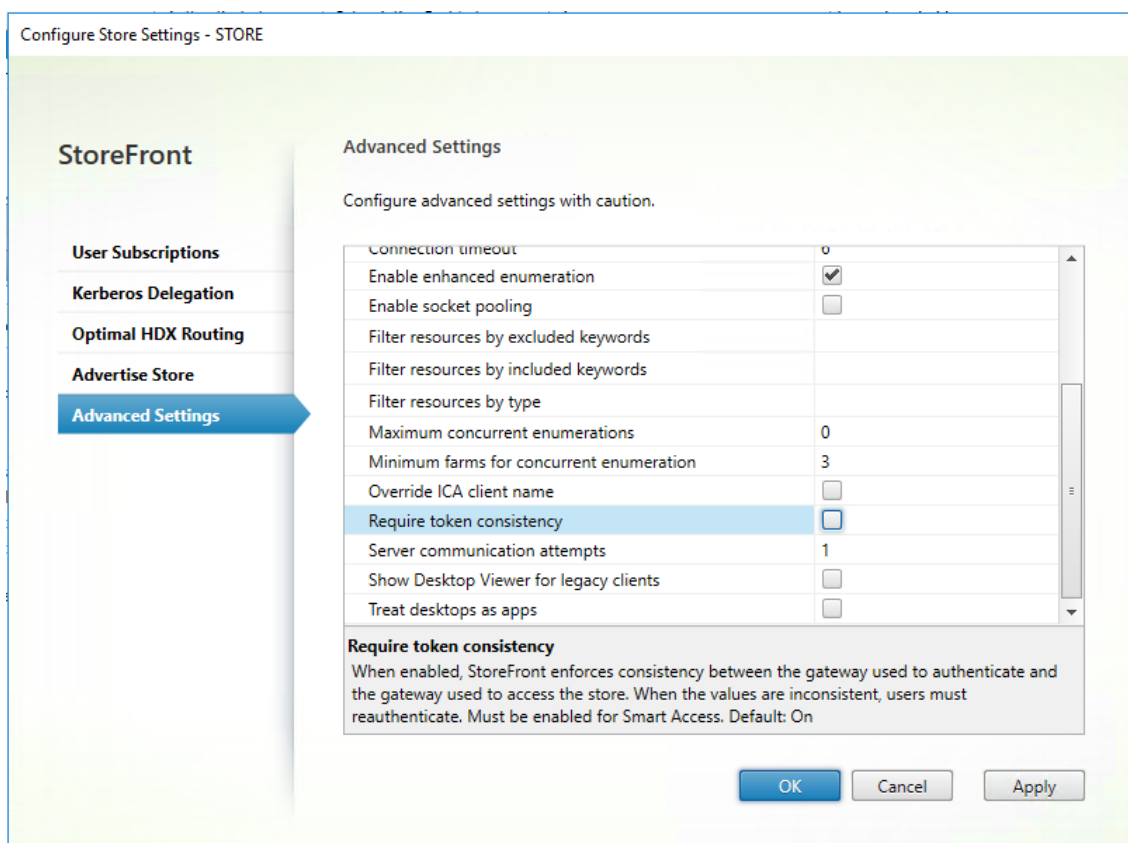
ProductionGateway ▼

OK

Cancel

Disable token consistency

1. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the **Actions** pane, click **Configure Store Settings**.
2. On the Configure Store Settings page, select **Advanced Settings**.
3. Clear the **Require token consistency** check box. For more information, see [Advanced store settings](#).



4. Click **OK**.

Note:

The Require token consistency setting is selected (on) by default. If you disable this setting, SmartAccess features used for Citrix Gateway End Point Analysis (EPA) stop working. For more information on SmartAccess, see [CTX138110](#).

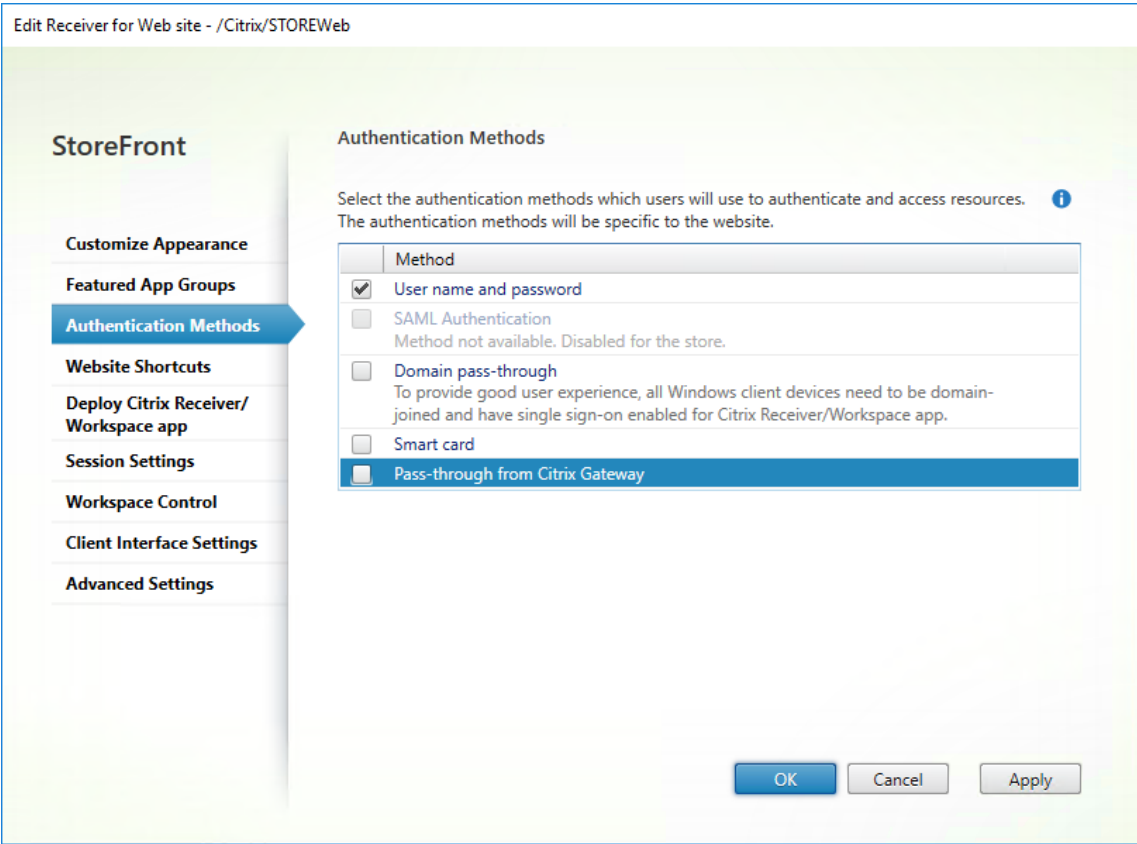
Disable pass-through from Citrix Gateway for the website

Important:

Disabling pass-through from Citrix Gateway prevents the website from trying to use the incorrect credentials from the [production.com](#) domain passed from the Citrix Gateway. Disabling pass-through from Citrix Gateway causes the website to prompt the user to enter credentials. These credentials are different from the credentials used to log on through the Citrix Gateway.

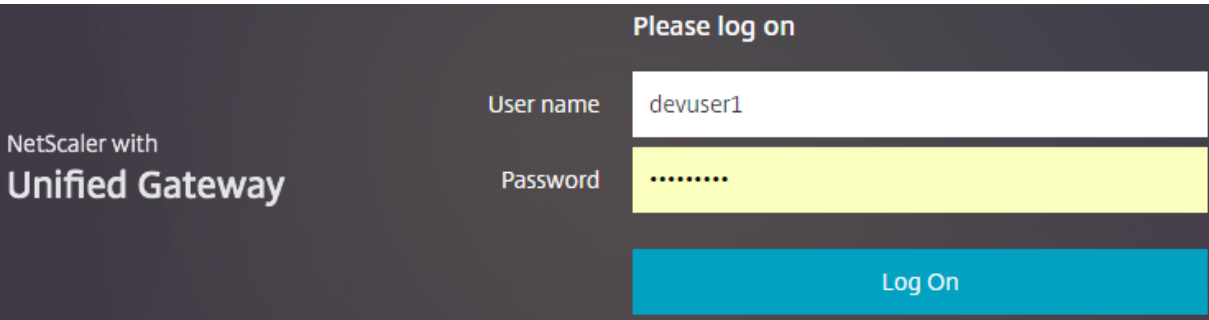
1. Select the **Stores** node in the left pane of the Citrix StoreFront management console.
2. Select the **store** that you want to modify.
3. In the **Actions** pane, click **Manage Receiver for Web Sites**.
4. In Authentication Methods, clear **Pass-through from Citrix Gateway**.

5. Click **OK**.

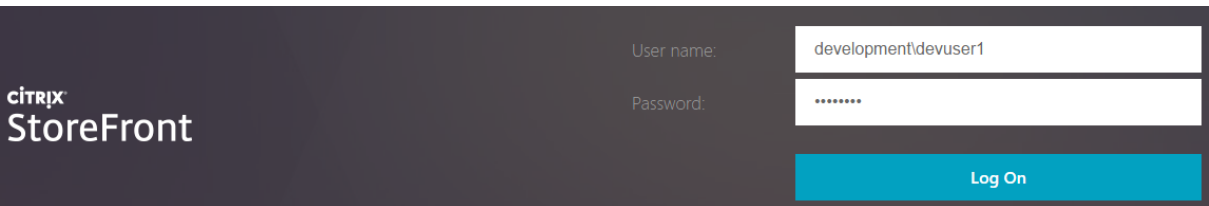


Log on to Gateway using a `production.com` user and credentials

To test, log on to Gateway using a `production.com` user and credentials.



After logon, the user is prompted to enter `development.com` credentials.



Add a trusted domain drop-down list in StoreFront (optional)

This setting is optional, but it may help prevent the user from accidentally entering the wrong domain to authenticate through the Citrix Gateway.

If the user name is the same for both domains, entering the wrong domain is more likely. New users may also be used to leaving out the domain when they log on through the Citrix Gateway. Users may then forget to enter domain\username for the second domain when they are prompted to log on to the Receiver for Web site.

1. Select **Stores** in the left pane of the Citrix StoreFront management console, and in the **Actions** pane, click **Manage Authentication Methods**.
2. Select the drop-down arrow next to **User name and password**.
3. Click **Add** to add `development.com` as a trusted domain, and select the **Show domains list in logon page** check box.
4. Click **OK**.

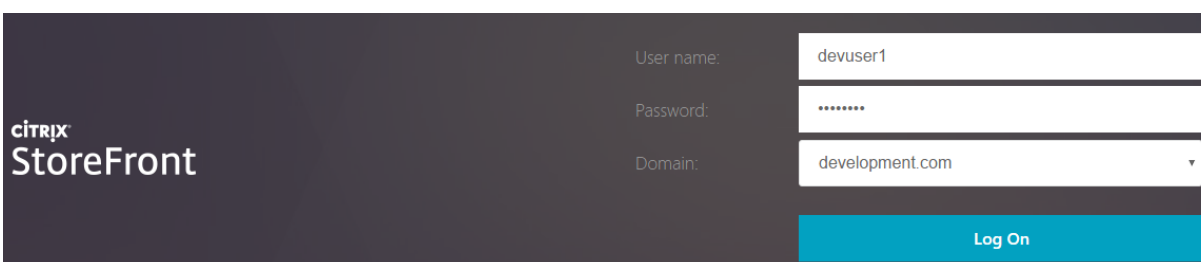
Configure Trusted Domains

Allow users to log on from: ☐ Any domain
☒ Trusted domains only

Trusted domains:

Default domain:

☒ Show domains list in logon page



The image shows the Citrix StoreFront login interface. On the left is the Citrix StoreFront logo. On the right, there are three input fields: 'User name:' with the value 'devuser1', 'Password:' with masked characters '*****', and 'Domain:' with a dropdown menu showing 'development.com'. Below these fields is a blue 'Log On' button.

Note:

Browser password caching is not recommended in this authentication scenario. If users have different passwords for the two different domain accounts, password caching can lead to a poor experience.

NetScaler session action policy

- If Single Sign-on to web applications is enabled within your Citrix Gateway session policy, incorrect credentials sent by Citrix Gateway to website are ignored because you disabled the **Pass-through from Citrix Gateway** authentication method on the website. The website prompts for credentials regardless of what this option is set to.
- Populating the Single Sign-on entries in the Client Experience and Published App tabs in Citrix Gateway does not change the behavior described in this article.

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration	Client Experience	Security	Published Applications
Accounting Policy			
<div></div>			
Override Global			
<input checked="" type="checkbox"/> Display Home Page			
Home Page			
<div>https://sf.development.com/Citrix/S</div> <input checked="" type="checkbox"/>			
URL for Web-Based Email			
<div></div> <input type="checkbox"/>			
Split Tunnel*			
<div>OFF</div> <input type="checkbox"/>			
Session Time-out (mins)			
<div>60</div> <input checked="" type="checkbox"/>			
Client Idle Time-out (mins)			
<div></div> <input type="checkbox"/>			
Clientless Access*			
<div>On</div> <input checked="" type="checkbox"/>			
Clientless Access URL Encoding*			
<div>Clear</div> <input checked="" type="checkbox"/>			
Clientless Access Persistent Cookie*			
<div>ALLOW</div> <input checked="" type="checkbox"/>			
Plug-in Type*			
<div>Windows/MAC OS X</div> <input type="checkbox"/>			
Windows Plugin Upgrade			
<div>Always</div> <input type="checkbox"/>			
Linux Plugin Upgrade			
<div>Always</div> <input type="checkbox"/>			
MAC Plugin Upgrade			
<div>Always</div> <input type="checkbox"/>			
AlwaysON Profile Name			
<div></div> <div><div>+</div><div></div></div> <input type="checkbox"/>			
<input type="checkbox"/> Single Sign-on to Web Applications <input type="checkbox"/>			
Credential Index*			
<div>PRIMARY</div> <input checked="" type="checkbox"/>			
KCD Account			
<div></div> <div><div>+</div><div></div></div> <input type="checkbox"/> ?			
Single Sign-on with Windows*			
<div>OFF</div> <input type="checkbox"/>			
Client Cleanup Prompt*			
<div>ON</div> <input type="checkbox"/>			
<input type="checkbox"/> Advanced Settings			

Unchecked Override Global check box indicates that the value is inherited from Global NetScaler Gateway Parameters.

Network Configuration	Client Experience	Security	Published App
Override Global			
ICA Proxy*			
<div>OFF</div>		<input checked="" type="checkbox"/>	
Web Interface Address			
<div>https://sf.development.com/Citrix/S</div>		<input checked="" type="checkbox"/>	
Web Interface Address Type*			
<div>IPV4</div>			
Web Interface Portal Mode*			
<div>NORMAL</div>		<input type="checkbox"/>	
Single Sign-on Domain			
<div></div>		<input type="checkbox"/>	
Citrix Receiver Home Page			
<div></div>		<input type="checkbox"/>	
Account Services Address			
<div></div>		<input type="checkbox"/>	

Configure beacon points

May 10, 2024

Important:

<http://ping.citrix.com> is currently unavailable so you must set an alternative beacon. Do not use third party websites that you do not own as an external beacon. Instead use websites controlled by your organization.

In the Manage Beacons screen, specify URLs inside and outside your internal network to be used as beacon points. Locally installed Citrix Workspace app attempts to contact beacon points and uses the responses to determine whether users are connected to local or public networks. When a user accesses a desktop or application, the location information is passed to the server providing the resource so that appropriate connection details can be returned to Citrix Workspace app. This ensures that users are not prompted to log on again when they access a desktop or application. Beacons are not used by Citrix Workspace app for HTML5.

Manage Beacons

Beacon points are used to determine whether users are connecting from internal or external networks. Two external addresses that can be resolved from the Internet are required.

Internal beacon: ☒ Use the service URL
☐ Specify beacon address:

`https://mycompany.net`

External beacons:

- `http://ping.citrix.com`
- `https://mygateway.example.com`

Add... Edit... Remove

OK Cancel

For example, if the internal beacon point is accessible, this indicates that the user is connected to the local network. However, if Citrix Workspace app cannot contact the internal beacon point and receives responses from both the external beacon points, this means that the user has an Internet connection but is outside the corporate network. Therefore, the user must connect to desktops and applications through Citrix Gateway. When the user accesses a desktop or application, the server providing the resource is notified to provide details of the Citrix Gateway appliance through which the connection must be routed. This means that the user does not need to log on to the appliance when accessing the desktop or application.

By default, StoreFront sets:

- The internal beacon to the base URL of your deployment.

- External beacons to <http://ping.citrix.com> and the URL of the first Citrix Gateway deployment you add.

To configure beacon points:

1. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the Actions pane, click **Manage Beacons**.
2. Specify the URL to use as the internal beacon point.
 - To use the server URL or load-balanced URL of your StoreFront deployment, select **Use the service URL**.
 - To use an alternative URL, select **Specify beacon address** and enter a highly available URL within your internal network.
3. Click **Add** to enter the URL of an external beacon point. To modify a beacon point, select the URL in the External beacons list and click **Edit**. Select a URL in the list and click **Remove** to stop using that address as a beacon point.

You must specify at least two highly available external beacon points that can be resolved from public networks. The beacon URLs should be fully qualified domain names (<http://example.com>) and not the abbreviated NetBIOS name (<http://example>). This enables Citrix Workspace app to determine whether users are located behind an Internet paywall, such as in a hotel or Internet café. In such cases, all the external beacon points connect to the same proxy. You should use URLs that are controlled by your organization, not third party websites.

If you change any beacon points, ensure that users update Citrix Workspace app with the modified beacon information. Users can obtain an updated Citrix Workspace app provisioning file from Citrix Workspace app for HTML5. Otherwise, you can [export a provisioning file](#) for the store and make this file available to your users.

PowerShell SDK

To get the current beacons use [Get-STFRoamingBeacon](#).

To add a beacon use [Set-STFRoamingBeacon](#).

To set the beacons to their defaults, use [Clear-STFRoamingBeacon](#).

Create a single FQDN used internally and externally

March 11, 2024

You can create a single fully qualified domain name (FQDN) that can access a store directly from within your corporate network and remotely via a Citrix Gateway.

In the following document, it uses as examples:

- <https://storefront.example.com> as the single URL used for users to access StoreFront. When inside the network it resolves to the StoreFront server or load balancer. When outside the network it resolves to the gateway.
- <https://storefrontcb.example.com> as the callback url. This resolves internally to the gateway. This is only required for smart access or password-less authentication. You must ensure that the certificate on the gateway includes this address as a SAN, use a wildcard certificate.

Server Group base URL

Change the base URL to be the single URL. See [Change the base URL for a deployment](#).

StoreFront beacons for locally installed Citrix Workspace app

Locally installed Citrix Workspace app attempts to contact beacon points and uses the responses to determine whether users are connected to local or public networks.

By default, StoreFront uses the server group base URL as the internal beacon URL. In this configuration, the same URL is valid both internally and externally so cannot be used as a beacon. Therefore, you must set the internal beacon to a URL that you know is only accessible internally.

See [Configure beacon](#).

External DNS

- storefront.example.com resolves to the externally facing IP of the Citrix Gateway Virtual Server.

Internal DNS

- storefront.example.com resolves to the storefront load balancer or single StoreFront server IP.
- storefrontcb.example.com resolves to the gateway vServer VIP. If a firewall exists between the DMZ and the enterprise local network, allow for this.

Export and import the StoreFront configuration

March 11, 2024

Note:

You can only import StoreFront configurations which are the same StoreFront version as the target StoreFront installation.

You can export the entire configuration of a StoreFront deployment. This includes both single server deployments and server group configurations. If an existing deployment is already present on the importing server, the current configuration is erased and then replaced by the configuration contained within the backup archive. If the target server is a clean factory default installation, a new deployment is created using the imported configuration stored within the backup. The exported configuration backup is in the form of a single .zip archive if unencrypted, or a .ctxzip if you choose to encrypt the backup file when it is created.

Scenarios where configuration export and import can be used

- Only backup StoreFront deployments in a working and trusted state. Any changes to the configuration requires a new backup to be taken to replace the old one. You cannot modify existing backups as a file hash of the backup.zip file prevents modification.
- Backup BEFORE upgrading StoreFront for disaster recovery.
- Cloning existing testing StoreFront deployments to put into production
- Creating user acceptance environments by cloning production deployments into a test environment.
- Moving StoreFront during OS migrations such as upgrading the hosting from Window Server 2019 to Windows 2022. In-place OS upgrades are not supported.
- Building extra server groups in multigeo deployments such as in large enterprises with multiple datacenters.

Things to consider when exporting and importing a StoreFront configuration

- Do you currently use any Citrix published authentication SDK examples, such as Magic Word authentication or third party authentication customizations? If so, you must install these packages on ALL importing servers BEFORE importing a configuration containing extra authentication methods. The configuration import fails if required authentication SDK packages are not installed on any of the importing servers. If importing a configuration into a server group, install the authentication packages on all members of the group.

- You can encrypt or decrypt your configuration backups. The exporting and importing PowerShell cmdlets support both use cases.
- You can decrypt encrypted backups (.ctxzip) later, but StoreFront cannot re-encrypt unencrypted backup files (.zip). If an encrypted backup is required, perform the export again using a PowerShell credential object containing a password of your choice.
- The SiteID of the website in IIS where StoreFront is currently installed (exporting server) must match the SiteID of the target website in IIS (importing server) where you want to restore the backed up StoreFront configuration.

PowerShell cmdlets

Export-STFConfiguration

Parameter	Description
-TargetFolder (String)	The export path to the backup archive. Example: "\$env:userprofile\desktop\"
-Credential (PSCredential Object)	Specify a credential object to create an encrypted .ctxzip backup archive during export. The PowerShell credential object should contain the password to use for encryption and decryption. Do not use -Credential at the same time as the -NoEncryption parameter. Example: \$CredObject
-NoEncryption (Switch)	Specify that the backup archive should be an unencrypted .zip. Do not use -NoEncryption at the same time as the -Credential parameter.
-ZipFileName (String)	The name for the StoreFront configuration backup archive. Do not add a file extension, such as .zip or .ctxzip. The file extension is added automatically depending on whether the -Credential or -NoEncryption parameter is specified during export. Example: "backup"
-Force (Boolean)	This parameter automatically overwrites backup archives with the same file name as existing backup files already present in the specified export location.

Important:

The **SiteID** parameter found in StoreFront 3.5 was deprecated in version 3.6. It is no longer necessary to specify the **SiteID** when performing an import, as the SiteID contained within the backup archive is always be used. Ensure the SiteID matches the existing StoreFront website already configured within IIS on the importing server. **SiteID 1** to **SiteID 2** configuration imports are NOT supported.

Import-STFConfiguration

Parameter	Description
-ConfigurationZip (String)	The full path to the backup archive you want to import. This should also include the file extension. Use .zip for unencrypted and .ctxzip for encrypted backup archives. Example: <code>\$env:userprofile\desktop\backup.ctxzip</code>
-Credential (PSCredential Object)	Specify a credential object to decrypt an encrypted backup during import. Example: <code>\$CredObject</code>
-HostBaseURL (String)	If this parameter is included, the Host base URL you specify is used instead of the Host base URL from the exporting server. Example: <code>https://<importingserver>.example.com</code>

Unprotect-STFConfigurationBackup

Parameter	Description
-TargetFolder (String)	The export path to the backup archive. Example: <code>\$env:userprofile\desktop</code>
-Credential (PSCredential Object)	Use this parameter to create an unencrypted copy of the encrypted backup archive. Specify the PowerShell credential object containing the password to use for decryption. Example: <code>\$CredObject</code>

Parameter	Description
-EncryptedConfigurationZip (String)	The full path of the encrypted backup archive you want to decrypt. You must specify the file extension .ctxzip. Example: <code>\$env:userprofile\desktop\backup.ctxzip</code>
-OutputFolder (String)	The path to create an unencrypted copy (.zip) of the encrypted (.ctxzip) backup archive. The original encrypted copy of the backup is retained so it can be reused. Do not specify a file name and file extension for the unencrypted copy. Example: <code>\$env:userprofile\desktop</code> This parameter automatically overwrites backup archives with the same file name as existing backup files already present in the specified export location.
-Force (Boolean)	

Configuration export and import examples

Import the StoreFront cmdlets into the current PowerShell session

Open the PowerShell Integrated Scripting Environment (ISE) on the StoreFront server and run:

```
1 $env:PSModulePath = [Environment]::GetEnvironmentVariable('PSModulePath', 'Machine')
2 $SDKModules = 'C:\Program Files\Citrix\Receiver StoreFront\PowerShellSDK\Modules\Citrix.StoreFront'
3 Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose
4 Import-Module "$SDKModules.Authentication\Citrix.StoreFront.Authentication.psd1" -verbose
5 Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1" -verbose
6 Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -verbose
7 Import-Module "$SDKModules.WebReceiver\Citrix.StoreFront.WebReceiver.psd1" -verbose
8 <!--NeedCopy-->
```

Single server scenarios

Create an unencrypted backup of an existing configuration on Server A and restore it onto the same deployment Export the configuration of the server you wish to back up.

```
1 Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -  
  zipFileName "backup" -NoEncryption  
2 <!--NeedCopy-->
```

Copy the backup.zip file to a safe location. You can use this backup for disaster recovery to restore the server to its previous state.

```
1 Import-STFConfiguration -configurationZip "$env:userprofile\desktop\  
  backup.zip" -HostBaseURL "https://storefront.example.com"  
2 <!--NeedCopy-->
```

Back up an existing configuration on Server A and restore it onto Server B to create a clone of an existing server Export the configuration of the server you wish to back up.

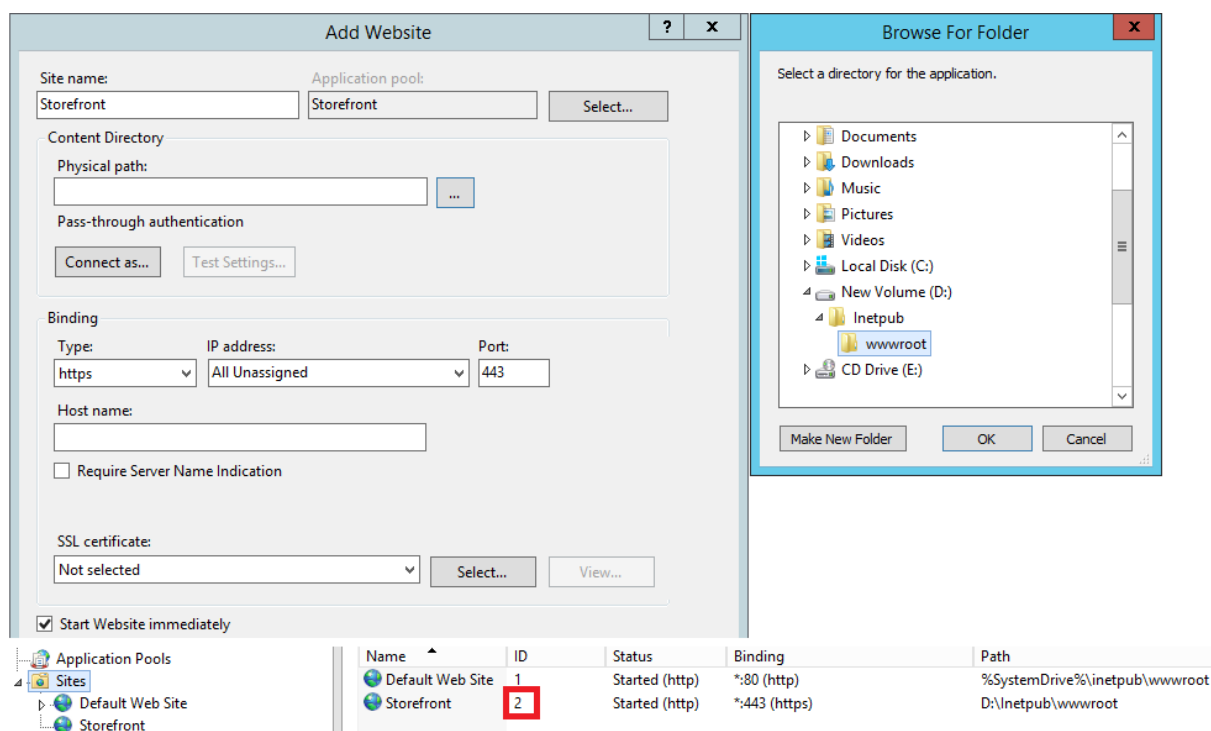
```
1 Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -  
  zipFileName "backup" -NoEncryption  
2 <!--NeedCopy-->
```

Copy the backup.zip file to the desktop of server B.

```
1 Import-STFConfiguration -configurationZip "$env:userprofile\desktop\  
  backup.zip" -HostBaseURL "https://serverB.example.com"  
2 <!--NeedCopy-->
```

StoreFront is already deployed onto a custom website in IIS. Restore the configuration onto another custom website deployment Server A has StoreFront deployed on a custom website location rather than the usual default website within IIS. The IIS SiteID for the second website created in IIS is 2. The StoreFront website's physical path can be on another nonsystem drive such as d:\ or on the default c:\ system drive but should use an IIS SiteID greater than 1.

A new website called StoreFront has been configured within IIS, which uses **SiteID = 2**. StoreFront is already deployed on the custom website in IIS with its physical path on drive **d:\inetpub\wwwroot**.



1. Export a copy of the Server A configuration.
2. On Server B, configure IIS with a new website called **StoreFront**, which also uses **SiteID 2**.
3. Import the Server A configuration onto Server B. The site ID contained in the backup is used and must match the target website where you want to import the StoreFront configuration.

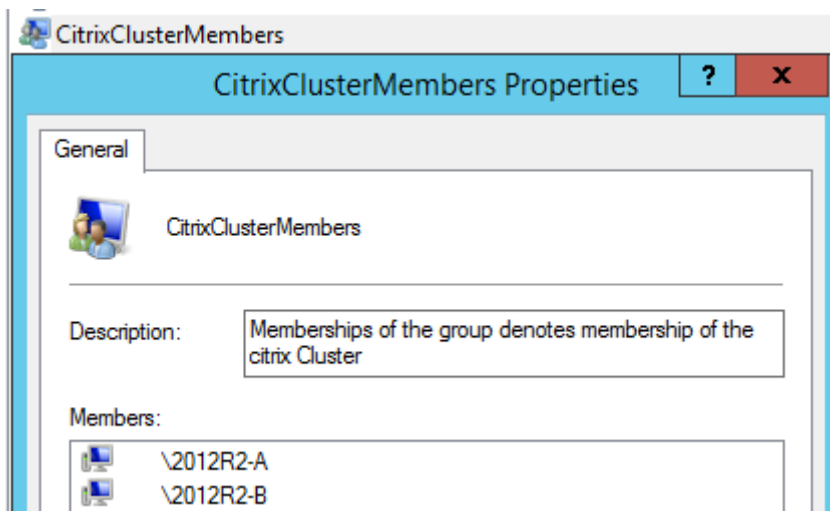
```
1 Import-STFConfiguration -configurationZip "$env:userprofile\
  desktop\backup.ctxzip" -HostBaseURL "https://serverB.example.
  com"
2 <!--NeedCopy-->
```

Server group scenarios

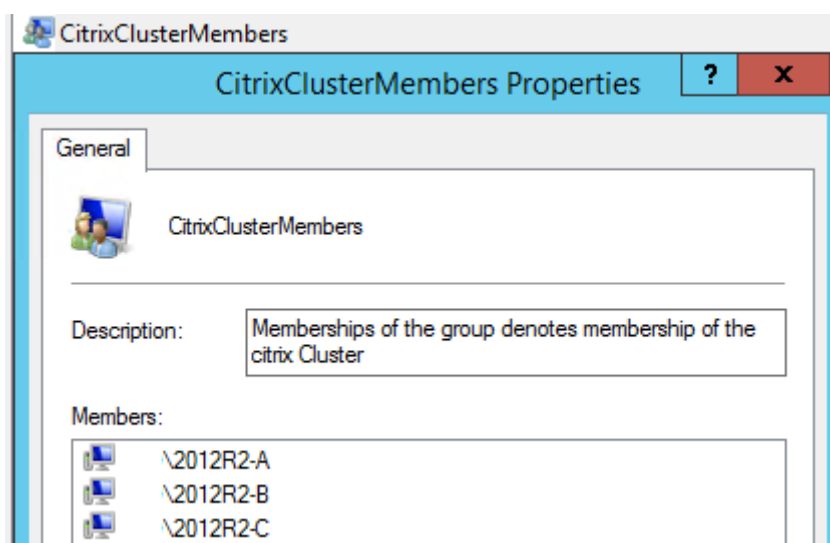
Scenario 1: Backup an existing server group configuration and restore it later onto the same server group deployment A previous configuration backup was taken while only two StoreFront servers, 2012R2-A and 2012R2-B, were members of the server group. Within the backup archive is a record of the **CitrixClusterMembership** at the time the backup was taken containing only the two original servers 2012R2-A and 2012R2-B. The StoreFront server group deployment has subsequently increased in size since the original backup was taken due to business demand, so an additional node 2012R2-C has been added to the server group. The underlying StoreFront configuration of the server group held in the backup has not changed. The current CitrixClusterMembership of three servers must be maintained even if an old backup containing only the two original server group nodes is imported. During import the current cluster membership is preserved and then written back once the configura-

tion has been successfully imported onto the primary server. The import also preserves the current CitrixClusterMembership if server group nodes were removed from the server group since the original backup was taken.

1. Export the Server Group 1 configuration from 2012R2-A, which is the primary server used to manage the entire server group.



2. Later you add an additional server, 2012R2-C to the existing server group.



3. The configuration of the server group must be restored to a known previously working state. StoreFront backs up the current CitrixClusterMembership of three servers during the import process, and then restores it after the import has succeeded.
4. Import the Server Group 1 configuration back onto node 2012R2-A.

```
1 Import-STFConfiguration -configurationZip "$env:userprofile\
  desktop\backup.ctxzip" -HostBaseURL "https://servergroup1.
  example.com"
```

```
2 <!--NeedCopy-->
```

5. Propagate the newly imported configuration to the entire server group, so all servers have a consistent configuration after import.

Scenario 2: Backup an existing configuration from Server Group 1 and use it to create a new Server Group on a different factory default installation. You can then add other new server group members to the new primary server Server Group 2 is created containing two new servers, 2012R2-C and 2012R2-D. The Server Group 2 configuration will be based on the configuration of an existing deployment, Server Group 1, which also contains two servers 2012R2-A and 2012R2-B. The CitrixClusterMembership contained within the backup archive is not used when creating a new server group. The current CitrixClusterMembership is always backed up and then restored after the import is successful. When creating a new deployment using an imported configuration, the CitrixClusterMembership security group contains only the importing server until additional servers are joined to the new group. Server Group 2 is a new deployment and intended to coexist alongside Server Group 1. Specify the -HostBaseURL parameter. Server Group 2 will be created using a new factory default StoreFront installation.

1. Export the Server Group 1 configuration from 2012R2-A, which is the primary server used to manage the entire server group.
2. Import the Server Group 1 configuration onto node 2012R2-C, which will be the primary server used to manage the newly created Server Group 2.

```
1 Import-STFConfiguration -configurationZip "$env:userprofile\
  desktop\backup.ctxzip" -HostBaseURL "https://servergroup2.
  example.com"
2 <!--NeedCopy-->
```

3. Join any additional servers that will be part of the new Server Group 2 deployment. Propagation of the newly imported configuration from Server Group 1 to all new members of Server Group 2 is automatic, as this forms part of the normal join process when a new server is added.

Scenario 3: Backup an existing configuration from Server Group A and use it to overwrite the existing Server Group B configuration Server Group 1 and Server Group 2 already exist in two separate data centers. Many StoreFront configuration changes are made on Server Group 1, which you should apply to Server Group 2 in the other data center. You can port the changes from Server Group 1 to Server Group 2. Do not use the **CitrixClusterMembership** within the backup archive on Server Group 2. Specify the **-HostBaseURL** parameter during import, as the Server Group 2 host base URL should not be changed to the same FQDN that is currently in use by Server Group 1. Server Group 2 is an existing deployment.

1. Export the Server Group 1 configuration from 2012R2-A, which is the primary server used to manage the entire server group.
2. Import the Server Group 1 configuration onto the factory default installation on node 2012R2-C, which will be the primary server of the new Server Group 2.

```
1 Import-STFConfiguration -configurationZip "$env:userprofile\
  desktop\backup.zip" -NoEncryption -HostBaseURL "https://
  servergroup2.example.com"
2 <!--NeedCopy-->
```

Create an encrypted backup of your server configuration

A PowerShell credential object comprises both a Windows account username and a password. PowerShell credential objects ensure that your password stays protected in memory.

Note:

To encrypt a configuration backup archive, you need only the password to perform encryption and decryption. The username stored within the credential object is not used. You must create a credential object containing the same password within the PowerShell session that is used on both the exporting and importing servers. Within the credential object you can specify any user.

PowerShell requires that you specify a user when creating a new credential object. This example code obtains the currently logged on Windows user for convenience.

Create a PowerShell Credential Object within your Powershell session on the exporting server.

```
1 $User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
2 $Password = "Pa55w0rd"
3 $Password = $Password | ConvertTo-SecureString -asPlainText -Force
4 $CredObject = New-Object System.Management.Automation.PSCredential(
  $User,$Password)
5 <!--NeedCopy-->
```

Export the configuration to backup.ctxzip which is an encrypted zip file.

```
1 Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -
  zipFileName "backup" -Credential $CredObject
2 <!--NeedCopy-->
```

Create an identical PowerShell Credential Object within your Powershell session on the importing server.

```
1 Import-STFConfiguration -configurationZip "$env:userprofile\desktop\
  backup.ctxzip" -Credential $CredObject -HostBaseURL "https://
  storefront.example.com"
2 <!--NeedCopy-->
```

Unprotect an existing encrypted backup archive

```
1 $User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
2 $Password = "Pa55w0rd"
3 $Password = $Password | ConvertTo-SecureString -asPlainText -Force
4 $CredObject = New-Object System.Management.Automation.PSCredential(
    $User,$Password)
5
6 Unprotect-STFConfigurationExport -encryptedConfigurationZip "$env:
    userprofile\desktop\backup.ctxzip" -credential $CredObject -
    outputFolder "c:\StoreFrontBackups" -Force
7 <!--NeedCopy-->
```

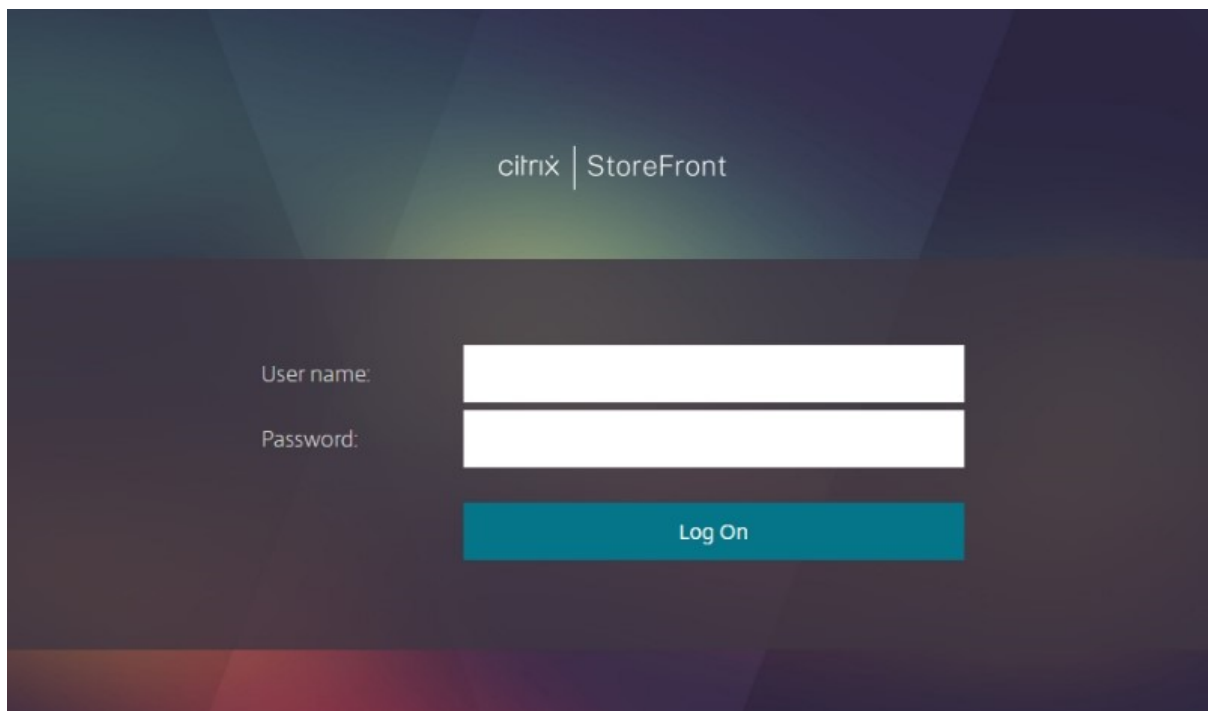
End user guide

March 11, 2024

This section describes the features and appearance of a store when viewed either through a web browser or through Citrix Workspace app.

Log On

Depending on the authentication method and whether single sign-on is enabled, you may be required to log on.



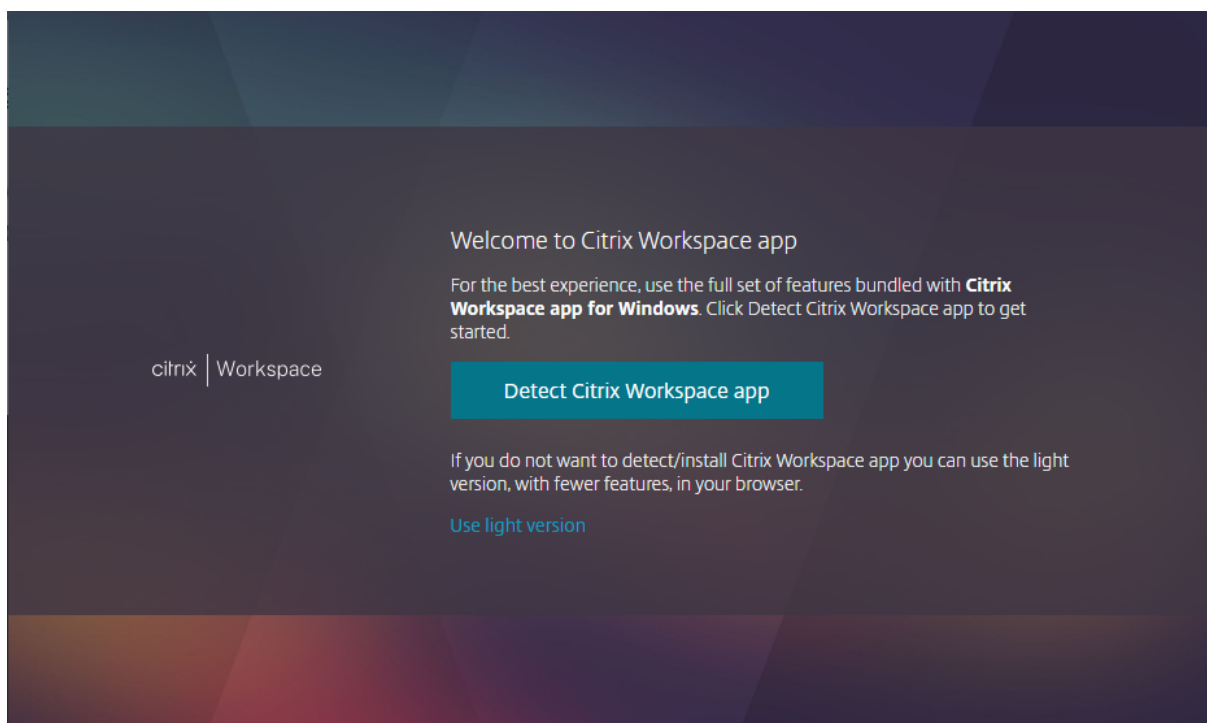
Citrix Workspace app detection

Note:

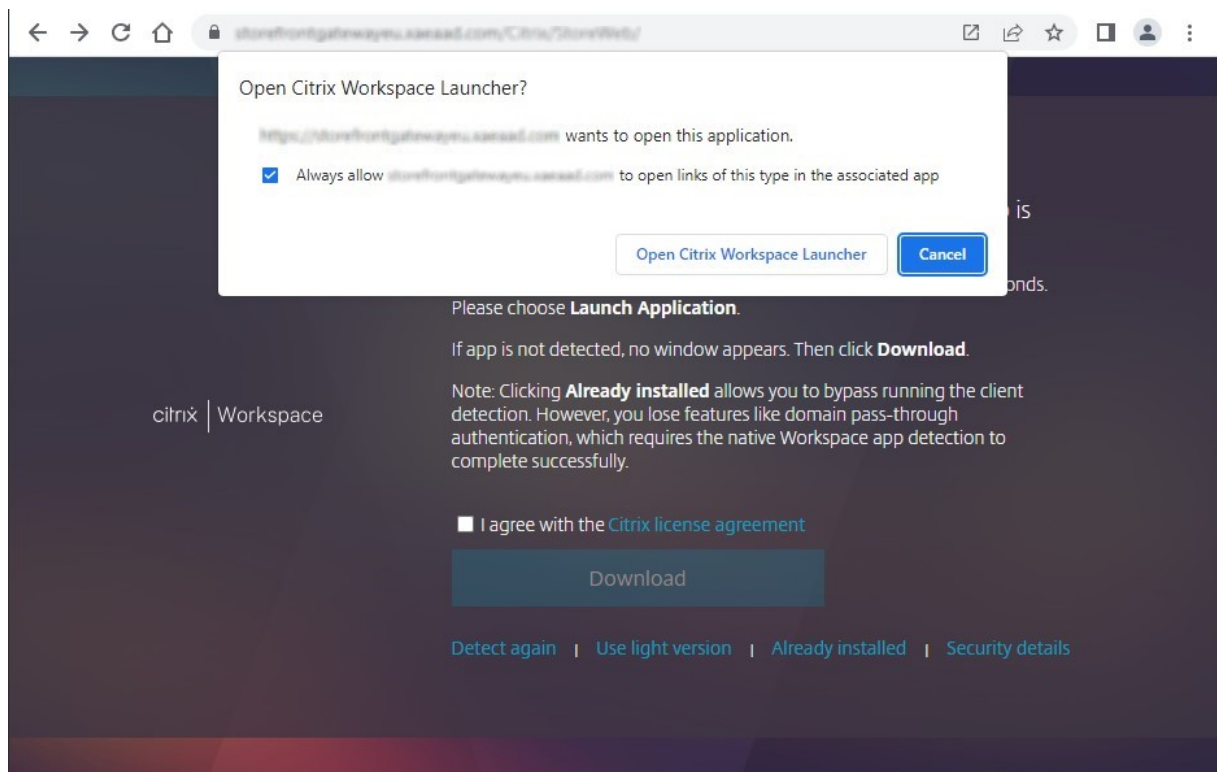
This step only applies when accessing the store through a web browser, not through locally installed Citrix Workspace app. This step may occur before or after log on depending on configuration.

Depending on configuration, when accessing the store through a web browser for the first time or after clearing your cookies, you may see the **Welcome to Citrix Workspace app** screen. Either:

- Click **Detect Citrix Workspace app** if you wish to launch resources in the locally installed Citrix Workspace app. This is recommended for the best experience.
- Click **Use light version** (if available) to always launch resources within the browser.



When you click **Detect Citrix Workspace app**, it tries to detect a locally installed Citrix Workspace app. First it tries using the [Citrix Workspace web extensions](#). If this is not installed or fails to detect locally installed Citrix Workspace app then it attempts to open **Citrix Workspace Launcher** which is a component of Citrix Workspace app. If Citrix Workspace app is installed then your browser pops up a window asking to run the **Citrix Workspace Launcher**. Click **Open Citrix Workspace Launcher** or **Open link** (depending on the browser). It is recommend you also tick **Always allow domain to open links of this type in the associated app** to avoid this window appearing every time you launch a resource.



If a locally installed Citrix Workspace app is detected then after a few seconds it continues to the next screen. When you subsequently launch a resource it will either use Citrix Workspace web extensions or Citrix Workspace Launcher, depending on which was detected, to open resources in the locally installed Citrix Workspace app.

If Citrix Workspace app is not installed, or you cancel the launcher then depending on configuration you have the following options:

- **Download** - Downloads Citrix Workspace app from the Citrix website or from the StoreFront server. After installing Citrix Workspace app, click **Detect again**.
- **Detect again** - Attempts to detect the locally installed Citrix Workspace app again.
- **Use light version** - Skips Workspace app detection and always opens resources in your web browser.
- **Already installed** - use this option if you have a legacy version of Citrix Receiver installed that does not support the Citrix Workspace Launcher or Citrix Workspace web extensions. If you select this option, when you launch a virtual app or desktop then your browser downloads a file **launch.ica** that you can open with Citrix Receiver. This option results in reduced functionality so is not recommended.

Home tab

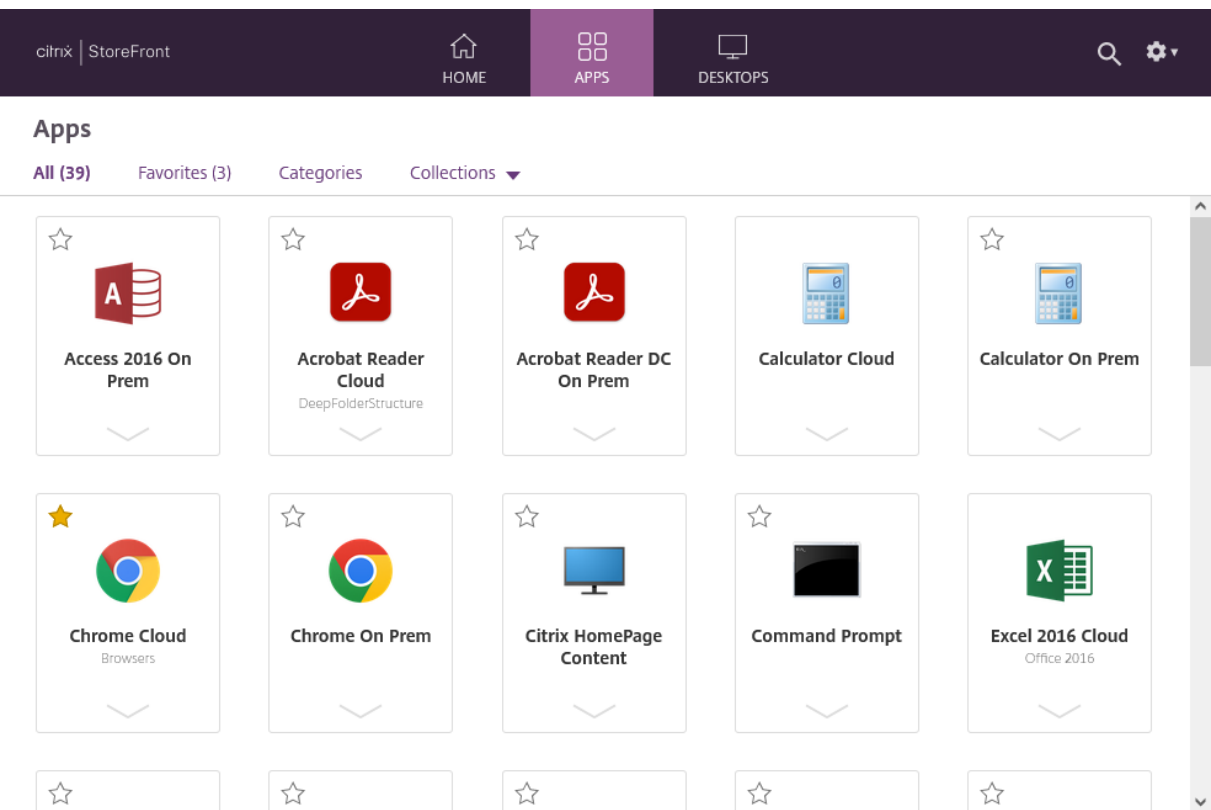
The **Home** tab displays any featured app groups along with any favorite or mandatory apps and desktops. The **Home** tab is only shown if favorites are enabled for the store.



Apps tab

The **Apps** tab has a number of sub-views:

- **All** - displays all apps.
- **Favorites** - Displays all favorite apps.
- **Categories** - Displays categories and the apps within those categories. The way categories are displayed depend on the [Category settings](#).
- **Collections** Displays the [Featured app groups](#).



Desktops tab

The **Desktops** tab has two sub-views:

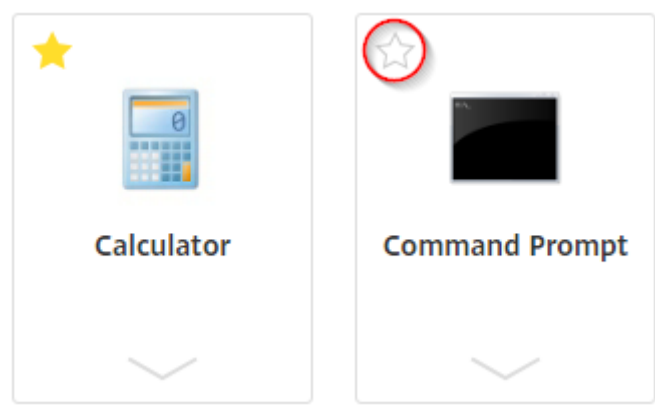
- **All** - Displays all desktops.
- **Favorites** - Displays your favorite desktops.

App and desktop tiles

Click on an icon to launch the app or desktop.

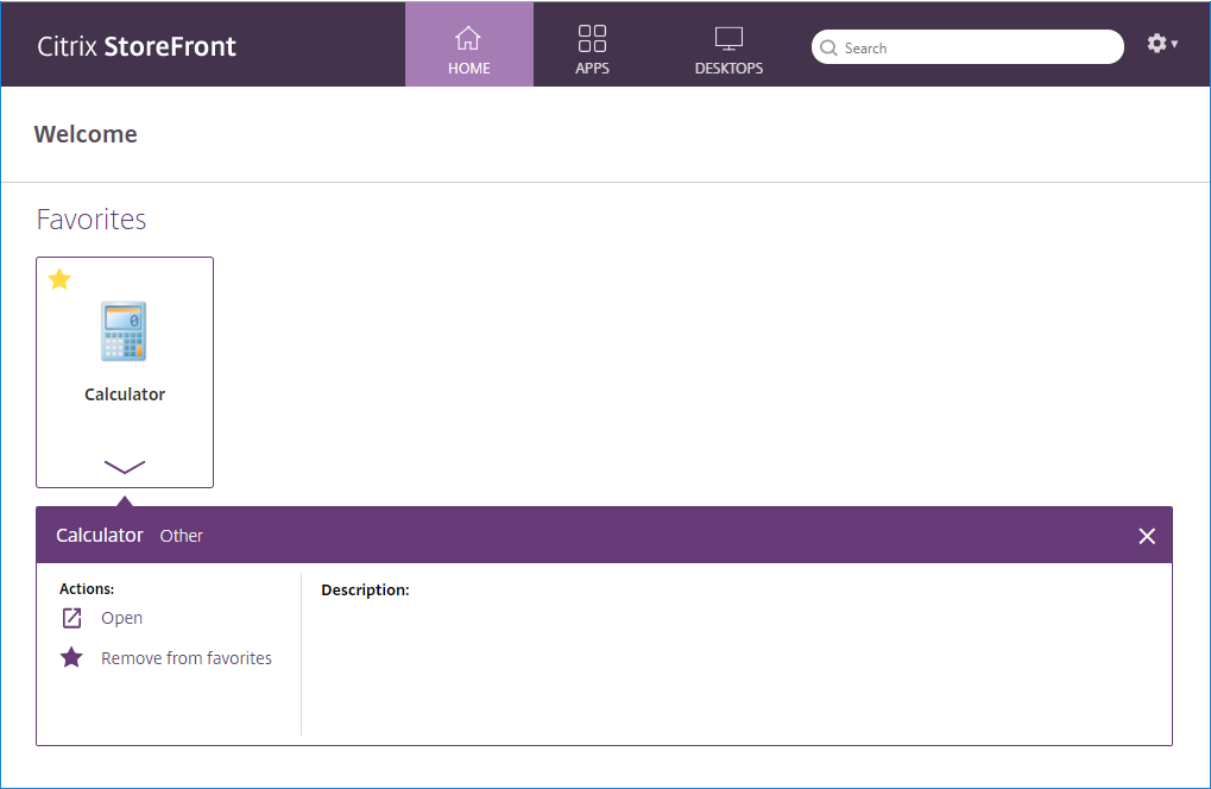
Favorites

Click or tap the star to make an item a favorite:



View details and actions

You can expand a panel below each icon to show the app description and actions.



The following actions may be available:

- **Open** - Launches or re-connects to the app or desktop.
- **Add to favorites** - If the item is not a favorite, is not mandatory, and favorite are enable for the store then adds the app or desktop to your favorite.
- **Remove from favorites** - If the item is a favorite, is not mandatory, and favorite are enable for the store then removes the app or desktop from your favorites.

- **Restart** - For assigned desktops where restart is available, this restarts the desktop.

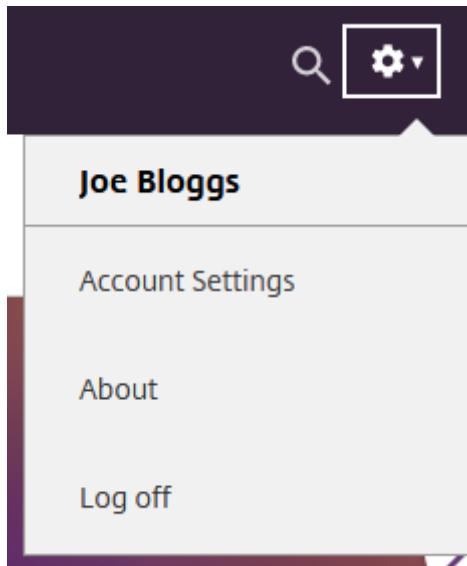
Search

Click the magnifying glass icon to bring up the search box. Search across all apps, desktops, and categories:



Settings

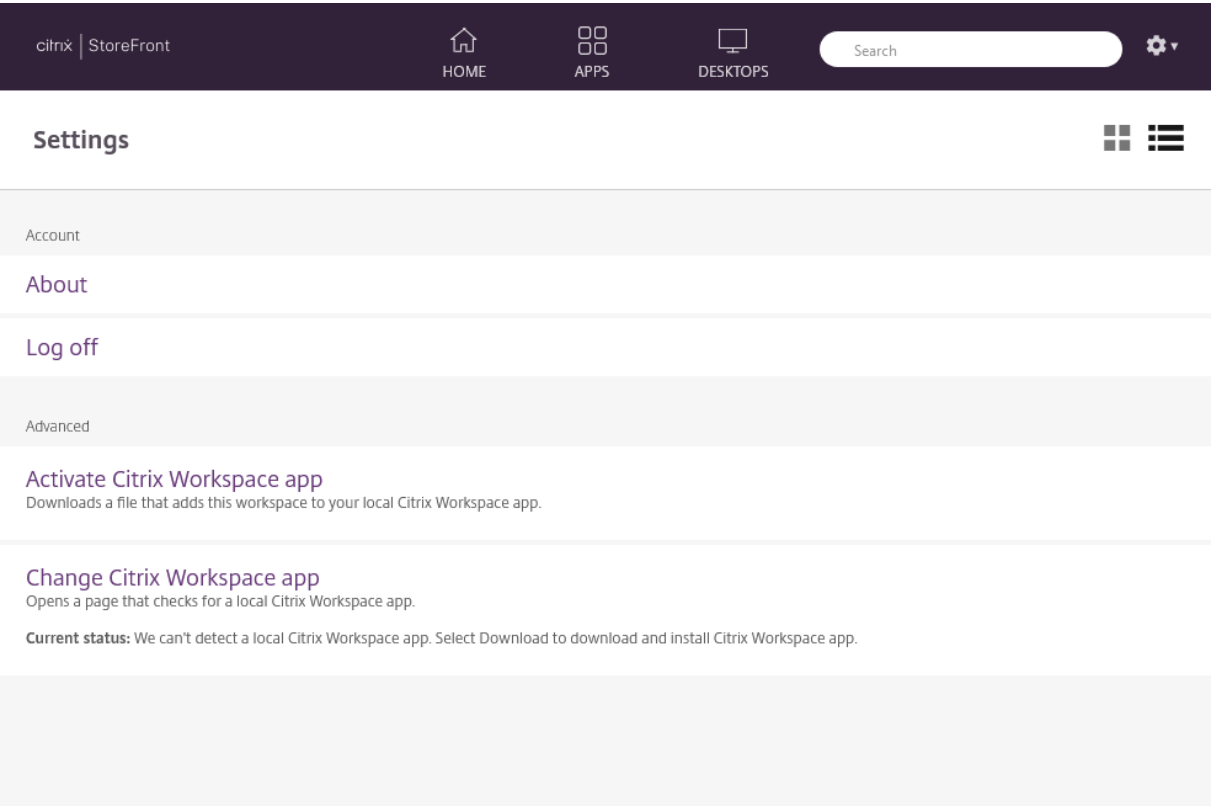
The settings menu is available only when accessing the store through a web browser.



The settings menu has the following options:

- **Account Settings** - opens the settings page.
- **About** - Displays information about the application.
- **Log off** - Logs off the website.

Account Settings



The following options may be available:

Connect. Resumes any disconnected sessions.

Disconnect. Disconnects all of your current sessions and logs you off.

Activate Citrix Workspace app. Downloads a file that adds this store to the local Citrix Workspace app.

Change Citrix Workspace app. Opens a page that checks for a locally installed Citrix Workspace app. This also allows users to switch between launching resources using the locally installed Citrix Workspace app, and launching them in a web browser.

Log off

To log off, open the settings menu and click **Log off**. This logs you off the store. If you are connected to any resources then depending configuration it will either:

- Terminate the resources.
- Disconnect from the resources
- Leave the resources connected.

StoreFront SDK

April 9, 2024

Citrix StoreFront provides an SDK based on a number of Microsoft Windows PowerShell version 2.0 modules. With the SDK, you can perform the same tasks as you would with the StoreFront MMC console, together with tasks you cannot do with the console alone.

Note:

The PowerShell SDK is not compatible with PowerShell 6 or higher.

For the SDK Reference, see [StoreFront SDK](#).

Use the SDK

The SDK comprises of a number of PowerShell snap-ins installed automatically by the installation wizard when you install and configure various StoreFront components.

To access and run the cmdlets:

1. Start a PowerShell command line prompt or **Windows PowerShell ISE** as administrator.

You must run the shell or script using a member of the local administrators group on the StoreFront server.

2. To use SDK cmdlets within scripts, set the execution policy in PowerShell.

For more information about PowerShell execution policy, see your Microsoft documentation.

3. Add the modules you require into the PowerShell environment using the **Add -Module** command in the Windows PowerShell console. For example, type:

```
Import-Module Citrix.StoreFront
```

To import all the cmdlets, type:

```
Get-Module -ListAvailable | Where-Object { $_.Name.StartsWith("Citrix.StoreFront")} | Import-Module
```

After importing, you have access to the cmdlets and their associated help.

Get started with the SDK

To create a script, perform the following steps:

1. Take one of the provided SDK examples installed by StoreFront into the **%Program-Files%\Citrix\Receiver StoreFront\PowerShellSDK\Examples** folder.
2. To help you customize your own script, review the example script to understand what each part is doing. For more information, see the example use case, which explains in detail the script's actions.
3. Convert and adapt the example scripts to turn them into a script that is more consumable. To do this:
 - Use the PowerShell ISE or a similar tool to edit the script.
 - Use variables to assign values that are to be reused or modified.
 - Remove any commands that are not required.
 - Note that StoreFront cmdlets can be identified by the prefix STF.
 - Use the **Get-Help** cmdlet supplying the cmdlet name and **-Full** parameter for more information on a specific command.

Examples

Note:

When creating a script, to ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described above rather than copying and pasting the example scripts.

Examples	Description
Create a Simple Deployment	Script: creates a simple deployment with a StoreFront controller configured with a single XenDesktop server.
Create a Remote Access Deployment	Script: builds on the previous script to add remote access to the deployment.
Create a Remote Access Deployment with Optimal Launch Gateway	Script: builds on the previous script to add preferred optimal launch gateways for a better user experience.

Example: Create a simple deployment

The following example shows how to create a simple deployment configured with one XenDesktop controller.

Before you begin, make sure you follow the steps detailed in [Get Started with the SDK](#). This example can be customized using the methods described to produce a script for automating StoreFront deployment.

Note:

To ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described in this document, rather than copying and pasting the example script.

Understand the script This section explains what each part of the script produced by StoreFront is doing. This will help you with the customization of your own script.

- Sets the error handling requirements and imports the required StoreFront modules. Imports are not required in newer versions of PowerShell.

```

1 Param(
2     [Parameter(Mandatory=$true)]
3     [Uri]$HostbaseUrl,
4     [long]$SiteId = 1,
5     [ValidateSet("XenDesktop","XenApp","AppController","VDIinaBox
        ")]
6     [string]$Farmtype = "XenDesktop",
7     [Parameter(Mandatory=$true)]
8     [string[]]$FarmServers,
9     [string]$StoreVirtualPath = "/Citrix/Store",
10    [bool]$LoadbalanceServers = $false,
11    [int]$Port = 80,
12    [int]$SSLRelayPort = 443,
13    [ValidateSet("HTTP","HTTPS","SSL")]
14    [string]$TransportType = "HTTP"
15 )
16 \# Import StoreFront modules. Required for versions of
    PowerShell earlier than 3.0 that do not support
    autoloading
17 Import-Module Citrix.StoreFront
18 Import-Module Citrix.StoreFront.Stores
19 Import-Module Citrix.StoreFront.Authentication
20 Import-Module Citrix.StoreFront.WebReceiver
21 <!--NeedCopy-->

```

- Automates the virtual path of the authentication and Citrix Receiver for Web services based on the **\$StoreVirtualPath** supplied. **\$StoreVirtualPath** is equivalent to **\$StoreIISpath** because Virtual paths are always the path in IIS. Therefore in Powershell they have a value such as “/Citrix/Store”, “/Citrix/StoreWeb”, or “/Citrix/StoreAuth”.

```

1 \# Determine the Authentication and Receiver virtual path to use
    based of the Store
2 $authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"
3 $receiverVirtualPath = "$($StoreVirtualPath.TrimEnd('/'))Web"
4 <!--NeedCopy-->

```

- Creates a new deployment if one is not already present in preparation for adding the required StoreFront services. **-Confirm:\$false** suppresses the requirement to confirm the deployment can proceed.

```
1  \# Determine if the deployment already exists
2  $existingDeployment = Get-STFDeployment
3  if(-not $existingDeployment)
4  {
5
6      \# Install the required StoreFront components
7      Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -
        Confirm:$false
8  }
9
10 elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)
11 {
12
13     \# The deployment exists but it is configured to the desired
        hostbase url
14     Write-Output "A deployment has already been created with the
        specified hostbase url on this server and will be used."
15 }
16
17 else
18 {
19
20     Write-Error "A deployment has already been created on this
        server with a different host base url."
21 }
22
23 <!--NeedCopy-->
```

- Creates a new authentication service if one does not exist at the specified virtual path. The default authentication method of username and password is enabled.

```
1  \# Determine if the authentication service at the specified
        virtual path exists
2  $authentication = Get-STFAuthenticationService -VirtualPath
        $authenticationVirtualPath
3  if(-not $authentication)
4  {
5
6      \# Add an Authentication service using the IIS path of the
        Store appended with Auth
7      $authentication = Add-STFAuthenticationService
        $authenticationVirtualPath
8  }
9
10 else
11 {
12
```



```

13     Write-Output "An Authentication service already exists at the
        specified virtual path and will be used."
14 }
15
16 <!--NeedCopy-->

```

- Creates the new store service configured with one XenDesktop controller with the servers defined in the array **\$XenDesktopServers** at the specified virtual path if one does not already exist.

```

1  \# Determine if the store service at the specified virtual path
    exists
2  $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
3  if(-not $store)
4  {
5
6  \# Add a Store that uses the new Authentication service
    configured to publish resources from the supplied servers
7  $store = Add-STFStoreService -VirtualPath $StoreVirtualPath -
    AuthenticationService $authentication -FarmName $Farmtype -
    FarmType $Farmtype -Servers $FarmServers -LoadBalance
    $LoadbalanceServers \
8      -Port $Port -SSLRelayPort $SSLRelayPort -TransportType
    $TransportType
9  }
10
11 else
12 {
13
14     Write-Output "A Store service already exists at the specified
        virtual path and will be used. Farm and servers will be
        appended to this store."
15     \# Get the number of farms configured in the store
16     $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.
        Count
17     \# Append the farm to the store with a unique name
18     Add-STFStoreFarm -StoreService $store -FarmName "Controller$(
        $farmCount + 1)" -FarmType $Farmtype -Servers $FarmServers
        -LoadBalance $LoadbalanceServers -Port $Port \
19         -SSLRelayPort $SSLRelayPort -TransportType $TransportType
20 }
21
22 <!--NeedCopy-->

```

- Adds a Citrix Receiver for Web service at the specified IIS virtual path to access applications published in the store created above.

```

1  \# Determine if the receiver service at the specified virtual
    path exists
2  $receiver = Get-STFWebReceiverService -VirtualPath
    $receiverVirtualPath
3  if(-not $receiver)

```

```
4 {
5
6     \# Add a Receiver for Web site so users can access the
       applications and desktops in the published in the Store
7     $receiver = Add-STFWebReceiverService -VirtualPath
       $receiverVirtualPath -StoreService $store
8 }
9
10 else
11 {
12
13     Write-Output "A Web Receiver service already exists at the
       specified virtual path and will be used."
14 }
15
16 <!--NeedCopy-->
```

- Enables XenApp services for the store so older Citrix Receiver or Citrix Workspace app clients can connect to published applications.

```
1 \# Determine if PNA is configured for the Store service
2 $storePnaSettings = Get-STFStorePna -StoreService $store
3 if(-not $storePnaSettings.PnaEnabled)
4 {
5
6     \# Enable XenApp services on the store and make it the default
       for this server
7     Enable-STFStorePna -StoreService $store -AllowUserPasswordChange
       -DefaultPnaService
8 }
9
10 <!--NeedCopy-->
```

Example: Create a remote access deployment

The following example builds on the previous script to add a deployment with remote access.

Before you begin, make sure you follow the steps detailed in [Get Started with the SDK](#). This example can be customized using the methods described to produce a script for automating StoreFront deployment.

Note:

To ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described in this document, rather than copying and pasting the example script.

Understand the script This section explains what each part of the script produced by StoreFront is doing. This will help you with the customization of your own script.

- Sets the error handling requirements and import the required StoreFront modules. Imports are not required in newer versions of PowerShell.

```

1 Param(
2     [Parameter(Mandatory=$true)]
3     [Uri]$HostbaseUrl,
4     [Parameter(Mandatory=$true)]
5     [long]$SiteId = 1,
6     [string]$Farmtype = "XenDesktop",
7     [Parameter(Mandatory=$true)]
8     [string[]]$FarmServers,
9     [string]$StoreVirtualPath = "/Citrix/Store",
10    [bool]$LoadbalanceServers = $false,
11    [int]$Port = 80,
12    [int]$SSLRelayPort = 443,
13    [ValidateSet("HTTP","HTTPS","SSL")]
14    [string]$TransportType = "HTTP",
15    [Parameter(Mandatory=$true)]
16    [Uri]$GatewayUrl,
17    [Parameter(Mandatory=$true)]
18    [Uri]$GatewayCallbackUrl,
19    [Parameter(Mandatory=$true)]
20    [string[]]$GatewaySTAUrls,
21    [string]$GatewaySubnetIP,
22    [Parameter(Mandatory=$true)]
23    [string]$GatewayName
24 )
25 Set-StrictMode -Version 2.0
26
27 \# Any failure is a terminating failure.
28 $ErrorActionPreference = 'Stop'
29 $ReportErrorShowStackTrace = $true
30 $ReportErrorShowInnerException = $true
31 \# Import StoreFront modules. Required for versions of PowerShell
    earlier than 3.0 that do not support autoloading
32 Import-Module Citrix.StoreFront
33 Import-Module Citrix.StoreFront.Stores
34 Import-Module Citrix.StoreFront.Roaming
35 <!--NeedCopy-->

```

- Create an internal access StoreFront deployment by calling the previous examples script. The base deployment will be extended to support remote access.

```

1 \# Create a simple deployment by invoking the SimpleDeployment
    example
2 $scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
    Definition -Parent
3 $scriptPath = Join-Path $scriptDirectory "SimpleDeployment.ps1"
4 & $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
    FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
    Farmtype $Farmtype \`
5     -LoadbalanceServers $LoadbalanceServers -Port $Port -
    SSLRelayPort $SSLRelayPort -TransportType $TransportType

```

```
6 <!--NeedCopy-->
```

- Gets services created in the simple deployment as they need to be updated to support the remote access scenario.

```
1 \# Determine the Authentication and Receiver sites based on the
  Store
2 $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
3 $authentication = Get-STFAuthenticationService -StoreService
  $store
4 $receiverForWeb = Get-STFWebReceiverService -StoreService $store
5 <!--NeedCopy-->
```

- Enables CitrixAGBasic on the Citrix Receiver for Web service required for remote access using Citrix Gateway. Get the Citrix Receiver for Web CitrixAGBasic and ExplicitForms authentication method from the supported protocols.

```
1 \# Get the Citrix Receiver for Web CitrixAGBasic and
  ExplicitForms authentication method from the supported
  protocols
2 \# Included for demonstration purposes as the protocol name can
  be used directly if known
3 $receiverMethods = Get-
  STFWebReceiverAuthenticationMethodsAvailable | Where-Object {
4   $_ -match "Explicit" -or $_ -match "CitrixAG" }
5
6 \# Enable CitrixAGBasic in Receiver for Web (required for remote
  access)
7 Set-STFWebReceiverService $receiverForWeb -AuthenticationMethods
  $receiverMethods
8 <!--NeedCopy-->
```

- Enables CitrixAGBasic on the authentication service. This is required for remote access.

```
1 \# Get the CitrixAGBasic authentication method from the protocols
  installed.
2 \# Included for demonstration purposes as the protocol name can
  be used directly if known
3 $citrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-
  Object {
4   $_ -match "CitrixAGBasic" }
5
6 \# Enable CitrixAGBasic in the Authentication service (required
  for remote access)
7 Enable-STFAuthenticationServiceProtocol -AuthenticationService
  $authentication -Name $citrixAGBasic
8 <!--NeedCopy-->
```

- Adds a new remote access Gateway, adding the optional subnet ipaddress is supplied and registers it with the store to be accessed remotely.

```
1 \# Add a new Gateway used to access the new store remotely
```

```

2  Add-STFRoamingGateway -Name "NetScaler10x" -LogonType Domain -
    Version Version10_0_69_4 -GatewayUrl $GatewayUrl '
3  \-CallbackUrl $GatewayCallbackUrl -SecureTicketAuthorityUrls
    $GatewaySTAUrls
4  \# Get the new Gateway from the configuration (Add-
    STFRoamingGateway will return the new Gateway if -PassThru is
    supplied as a parameter)
5  $gateway = Get-STFRoamingGateway -Name $GatewayName
6  \# If the gateway subnet was provided then set it on the gateway
    object
7  if($GatewaySubnetIP)
8  {
9
10     Set-STFRoamingGateway -Gateway $gateway -SubnetIPAddress
        $GatewaySubnetIP
11 }
12
13 \# Register the Gateway with the new Store
14 Register-STFStoreGateway -Gateway $gateway -StoreService $store -
    DefaultGateway
15 <!--NeedCopy-->

```

Example: Create a remote access deployment with optimal launch Gateway

The following example builds on the previous script to add a deployment with optimal launch Gateway remote access.

Before you begin, make sure you follow the steps detailed in [Get Started with the SDK](#). This example can be customized using the methods described to produce a script for automating StoreFront deployment.

Note:

To ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described in this document, rather than copying and pasting the example script.

Understand the script This section explains what each part of the script produced by StoreFront is doing. This will help you with the customization of your own script.

- Sets the error handling requirements and imports the required StoreFront modules. Imports are not required in newer versions of PowerShell.

```

1  Param(
2      [Parameter(Mandatory=$true)]
3      [Uri]$HostbaseUrl,
4      [long]$SiteId = 1,
5      [string]$Farmtype = "XenDesktop",
6      [Parameter(Mandatory=$true)]

```

```

 7      [string[]]$FarmServers,
 8      [string]$StoreVirtualPath = "/Citrix/Store",
 9      [bool]$LoadbalanceServers = $false,
10      [int]$Port = 80,
11      [int]$SSLRelayPort = 443,
12      [ValidateSet("HTTP","HTTPS","SSL")]
13      [string]$TransportType = "HTTP",
14      [Parameter(Mandatory=$true)]
15      [Uri]$GatewayUrl,
16      [Parameter(Mandatory=$true)]
17      [Uri]$GatewayCallbackUrl,
18      [Parameter(Mandatory=$true)]
19      [string[]]$GatewaySTAUrls,
20      [string]$GatewaySubnetIP,
21      [Parameter(Mandatory=$true)]
22      [string]$GatewayName,
23      [Parameter(Mandatory=$true)]
24      [Uri]$OptimalGatewayUrl,
25      [Parameter(Mandatory=$true)]
26      [string[]]$OptimalGatewaySTAUrls,
27      [Parameter(Mandatory=$true)]
28      [string]$OptimalGatewayName
29  )
30  Set-StrictMode -Version 2.0
31  \# Any failure is a terminating failure.
32  $ErrorActionPreference = 'Stop'
33  $ReportErrorShowStackTrace = $true
34  $ReportErrorShowInnerException = $true
35  \# Import StoreFront modules. Required for versions of PowerShell
    earlier than 3.0 that do not support autoloading
36  Import-Module Citrix.StoreFront
37  Import-Module Citrix.StoreFront.Stores
38  Import-Module Citrix.StoreFront.Roaming
39  <!--NeedCopy-->

```

- Calls into the remote access deployment script to configure the basic deployment and add remote access.

```

 1  \# Create a remote access deployment
 2  $scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
    Definition -Parent
 3  $scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.
    ps1"
 4  & $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
    FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
    Farmtype $Farmtype \
 5      -LoadbalanceServers $LoadbalanceServers -Port $Port -
    SSLRelayPort $SSLRelayPort -TransportType $TransportType
    \
 6      -GatewayUrl $GatewayUrl -GatewayCallbackUrl
    $GatewayCallbackUrl -GatewaySTAUrls $GatewaySTAUrls -
    GatewayName $GatewayName
 7  <!--NeedCopy-->

```

- Adds the preferred optimal launch gateway and get it from the list of configured gateways.

```
1 \# Add a new Gateway used for remote HDX access to desktops and  
  apps  
2 $gateway = Add-STFRoamingGateway -Name $OptimalGatewayName -  
  LogonType UsedForHDXOnly -GatewayUrl $OptimalGatewayUrl -  
  SecureTicketAuthorityUrls $OptimalGatewaySTAUrls -PassThru  
3 <!--NeedCopy-->
```

- Gets the store service to use the optimal gateway, register it assigning it to launches from the farm named.

```
1 \# Get the Store configured by SimpleDeployment.ps1  
2 $store = Get-STFStoreService -VirtualPath $StoreVirtualPath  
3 \# Register the Gateway with the new Store for launch against all  
  of the farms (currently just one)  
4 $farmNames = @($store.FarmsConfiguration.Farms | foreach {  
5   $_.FarmName }  
6 )  
7 Register-STFStoreOptimalLaunchGateway -Gateway $gateway -  
  StoreService $store -FarmName $farmNames  
8 <!--NeedCopy-->
```

Troubleshoot StoreFront

April 9, 2024

Installation Logs

When StoreFront is installed or uninstalled, the following log files are created by the StoreFront installer in the `C:\Windows\Temp\StoreFront` directory. The file names reflect the components that created them and include time stamps.

- Citrix-DeliveryServicesRoleManager-*.log—Created when StoreFront is installed interactively.
- Citrix-DeliveryServicesSetupConsole-*.log—Created when StoreFront is installed silently and when StoreFront is uninstalled, either interactively or silently.
- CitrixMsi-CitrixStoreFront-x64-*.log—Created when StoreFront is installed and uninstalled, either interactively or silently.

Event Logs

StoreFront supports Windows event logging for the authentication service, stores, and Receiver for Web sites. Any events that are generated are written to the StoreFront application log, which can be

viewed using Event Viewer under either **Application and Services Logs > Citrix Delivery Services** or **Windows Logs > Application**. You can control the number of duplicate log entries for a single event by editing the configuration files for the authentication service, stores, and Receiver for Web sites.

Log throttling

1. Use a text editor to open the *web.config* file for the authentication service, store, or Receiver for Web site, which are typically located in the C:\inetpub\wwwroot\Citrix\Authentication\, C:\inetpub\wwwroot\Citrix\storename\, and C:\inetpub\wwwroot\Citrix\storenameWeb\ directories, respectively, where storename is the name specified for the store when it was created.

2. Locate the following element in the file.

```
<logger duplicateInterval="00:01:00"duplicateLimit="10">
```

By default, StoreFront is configured to limit the number of duplicate log entries to 10 per minute.

3. Change the value of the duplicateInterval attribute to set the time period in hours, minutes, and seconds over which duplicate log entries are monitored. Use the duplicateLimit attribute to set the number of duplicate entries that must be logged within the specified time interval to trigger log throttling.

When log throttling is triggered, a warning message is logged to indicate that further identical log entries will be suppressed. Once the time limit elapses, normal logging resumes and an informational message is logged indicating that duplicate log entries are no longer being suppressed.

Powershell and management console logs

Configuration changes made through PowerShell or the management console are logged at C:\Program Files\Citrix\Receiver StoreFront\Admin\logs. The log file names contain command actions and subjects, along with time stamps that can be used to differentiate command sequences.

Diagnostics logging

StoreFront writes diagnostics logs to c:\Program Files\Citrix\Receiver StoreFront\admin\trace

By default, messages of level **Error**, **Warning**, and **Info** are logged. In most cases this includes sufficient information to diagnose any issues.

You can enable additional verbose logging for troubleshooting purposes. This is only required if requested by Citrix support. This may have an impact on performance so you should revert the `TraceLevel` to `Info` once troubleshooting is complete.

To enable Verbose logging:

1. Using an account with local administrator permissions, start Windows PowerShell
2. Enter command:

```
1 Set-STFDiagnostics -All -TraceLevel "Verbose" -confirm:$False
2 <!--NeedCopy-->
```

This enables “Verbose” logging for all services, without prompting for confirmation. When this command is entered it restarts the Storefront services. Wait for the PowerShell prompt to return to verify that the services have finished restarting. While these services are restarting, the StoreFront server will not be accessible by users.

3. Reproduce the issue to create the logs.
4. Set the logging back to default level for all services

```
1 Set-STFDiagnostics -All -TraceLevel "Info" -confirm:$False
2 <!--NeedCopy-->
```

You can further customize the diagnostics logging:

- StoreFront writes a separate log file for each service. By default, each log file is up to 200Mb and StoreFront writes up to five log files per service before purging old log files. If you need to customize the size or number of logs written then you can do this using the `-FileSizeKb` and `-FileCount` parameters.
- Change the level of detail logged using `-TraceLevel`. Allowed values are `Off`, `Error`, `Warning`, `Info`, or `Verbose`.
- Using the parameter `-All` sets the logging parameters for all services. You can customize logging for an individual service using `-Service [Service name]`

For more information on the `Set-STFDiagnostics` cmdlet, see the [StoreFront PowerShell SDK documentation](#).

Launch.ica file logging

When a user launches an app or desktop, StoreFront generates a file called `launch.ica` that Workspace app reads to determine how to connect to the app or desktop. Depending on configuration this file may be stored in memory so not directly accessible. To diagnose launch errors it can be useful to view the contents of `launch.ica`.

To enable logging of the launch.ica file on the client PC, complete the following steps:

1. Navigate to the following registry key by using the registry editor:

32-bit Systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

64-bit Systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

2. Set the following two string key values:

- `LogFile="path to the log file"`
- `LogICAFile=true`

For example:

```
1 LogFile=C:\ica\ica.log
2 LogICAFile=true
3 <!--NeedCopy-->
```

Note:

The use of an ICA file in your environment for anything other than troubleshooting purposes is further outlined in [CTX200126](#).

Third Party Notices

April 30, 2024

StoreFront may include third party software components licensed under the following terms. This list was generated using third party software as of the date listed. This list may change with specific versions of the product and may not be complete; it is provided “As-Is.” TO THE EXTENT PERMITTED BY APPLICABLE LAW, CITRIX AND ITS SUPPLIERS MAKE NO REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, WITH REGARD TO THE LIST OR ITS ACCURACY OR COMPLETENESS, OR WITH RESPECT TO ANY RESULTS TO BE OBTAINED FROM USE OR DISTRIBUTION OF THE LIST. BY USING OR DISTRIBUTING THE LIST, YOU AGREE THAT IN NO EVENT SHALL CITRIX BE HELD LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY OTHER DAMAGES WHATSOEVER RESULTING FROM ANY USE OR DISTRIBUTION OF THIS LIST.

Castle Windsor 3.3.0

Copyright 2004-2013 Castle Project - <http://www.castleproject.org/>

Licensed under the Apache License, Version 2.0

Microsoft Unity Application Block (Unity) 2.1

Copyright © 2011 Microsoft Corporation.

Licensed under the Microsoft Public License (MS-PL) <https://msdn.microsoft.com/en-us/library/hh237493.aspx>

Microsoft Patterns and Practices: Prism 2.2

Copyright © 2010 Microsoft Corporation.

Licensed under the Microsoft Public License (MS-PL) <http://compositewpf.codeplex.com/releases/view/46046>

Microsoft patterns & practices: Common Service Locator 1.0

Copyright © Microsoft Corporation.

Licensed under the Microsoft Public License (MS-PL)

Microsoft .Net Reference Source

Copyright © Microsoft Corporation. Licensed under the MIT license.

ManagedEsent Release 1.9.4

Copyright © Microsoft Corporation.

Licensed under the Microsoft Public License (MS-PL) <http://managedesent.codeplex.com/license>

jQuery UI - v1.10.4 - 2014-03-12

<http://jqueryui.com/>

Copyright 2014 jQuery Foundation and other contributors; Licensed MIT

jQuery JavaScript Library v1.12.4

<http://jquery.com/>

Includes Sizzle.js

<http://sizzlejs.com/>

Copyright jQuery Foundation and other contributors

Released under the MIT license

<http://jquery.org/license>

Date: 2016-05-20T17:17Z

jQuery jScrollPane v2.0.0beta11

jQuery jScrollPane - v2.0.0beta11 - 2011-07-04 <http://jscrollpane.kelvinluck.com/>

Copyright (c) 2010 Kelvin Luck

Dual licensed under the MIT and GPL licenses.

jquery.contextmenu.js

jQuery Plugin for Context Menus

<http://www.JavascriptToolbox.com/lib/contextmenu>

Copyright (c) 2008 Matt Kruse (javascripttoolbox.com)

Dual licensed under the MIT and GPL licenses.

jQuery plugin for Hammer.JS - v1.0.0 - 2014-01-02

<http://eightmedia.github.com/hammer.js>

Copyright (c) 2014 Jorik Tangelder j.tangelder@gmail.com;

Licensed under the MIT license

jQuery MouseWheel

Copyright (c) 2011 Brandon Aaron (<http://brandonaaron.net>)

Licensed under the MIT License (LICENSE.txt).

WPF Toolkit 3.5

WPF Toolkit (<http://wpf.codeplex.com/>) Copyright (c) 2006-2014 Microsoft

MS-PL license <http://wpf.codeplex.com/license>

9

Extended WPF Toolkit 3.0

Copyright (C) 2007-2013 Xceed Software Inc.

This program is provided to you under the terms of the Microsoft Public License (Ms-PL) as published at <http://wpftoolkit.codeplex.com/license>

For more features, controls, and fast professional support, pick up the Plus Edition at <http://xceed.com/wpftoolkit>

Stay informed: follow @datagrid on Twitter or Like <http://facebook.com/datagrids>

WiX Toolset

Copyright (c) Outercurve Foundation. Common Public License Version 1.0.

CLR Security

Copyright (c) Microsoft Corporation. Microsoft Limited Permissive License (MS-LPL)

Stack Exchange Redis 1.1

StackExchange.Redis.StrongName 1.1 <https://stackexchange.github.io/StackExchange.Redis> Copyright (c) 2014 Stack Exchange

Licensed under the MIT license

Newtonsoft JSON

Copyright (c) 2007 James Newton-King

Licensed under the MIT license.

jQuery JavaScript Library v3.7.0

<https://jquery.com/>

Includes Sizzle.js

<https://sizzlejs.com/>

Copyright JS Foundation and other contributors

Released under the MIT license

<https://jquery.org/license>

Date: 2020-05-04T22:49Z

jQuery UI - v1.13.2 - 2022-07-14

<http://jqueryui.com>

Copyright jQuery Foundation and other contributors; Licensed MIT

Hammer.JS - v2.0.4 - 2014-09-28

Hammer.JS - v2.0.8 - 2016-04-23

<http://hammerjs.github.io/>

Copyright (c) 2016 Jorik Tangelder;

Licensed under the MIT license

VelocityJS.org (1.5.0)

velocity-animate (C) 2014-2017 Julian Shapiro.

Licensed under the MIT license. See LICENSE file in the project root for details.

slick.js - 1.8.0

The MIT License (MIT)

Copyright (c) 2013-2016

jQuery UI Touch Punch 0.2.3

Copyright 2011–2014, Dave Furfero

Dual licensed under the MIT or GPL Version 2 licenses.

APPENDIX: Referenced Licenses

MIT License

```
1  Permission is hereby granted, free of charge, to any person obtaining a
2    copy
3  of this software and associated documentation files (the "Software"),
4    to deal
5  in the Software without restriction, including without limitation the
6    rights
7  to use, copy, modify, merge, publish, distribute, sublicense, and/or
8    sell
9  copies of the Software, and to permit persons to whom the Software is
10   furnished to do so, subject to the following conditions:
11
12  The above copyright notice and this permission notice shall be included
13   in
14   all copies or substantial portions of the Software.
15
16  THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS
17   OR
18   IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY
19   ,
20   FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL
21   THE
22   AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER
23   LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
24   FROM,
25   OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS
26   IN
27   THE SOFTWARE.
28  <!--NeedCopy-->
```

Apache License, Version 2.0

```
1                                     Apache License
2                                     Version 2.0, January 2004
3                                     http://www.apache.org/licenses/
4
5
6  TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION
7
8  1. Definitions.
9
10     "License" shall mean the terms and conditions for use, reproduction,
11     and distribution as defined by Sections 1 through 9 of this document
12     .
13
14     "Licenser" shall mean the copyright owner or entity authorized by
15     the copyright owner that is granting the License.
16
17     "Legal Entity" shall mean the union of the acting entity and all
18     other entities that control, are controlled by, or are under common
19     control with that entity. For the purposes of this definition,
20     "control" means (i) the power, direct or indirect, to cause the
```

20 direction or management of such entity, whether by contract or
21 otherwise, or (ii) ownership of fifty percent (50%) or more of the
22 outstanding shares, or (iii) beneficial ownership of such entity.
23
24 "You" (or "Your") shall mean an individual or Legal Entity
25 exercising permissions granted by **this** License.
26
27 "Source" form shall mean the preferred form **for** making modifications
28 ,
29 including but not limited to software source code, documentation
30 source, and configuration files.
31
32 "Object" form shall mean any form resulting from mechanical
33 transformation or translation of a Source form, including but
34 not limited to compiled object code, generated documentation,
35 and conversions to other media types.
36
37 "Work" shall mean the work of authorship, whether in Source or
38 Object form, made available under the License, as indicated by a
39 copyright notice that is included in or attached to the work
40 (an example is provided in the Appendix below).
41
42 "Derivative Works" shall mean any work, whether in Source or Object
43 form, that is based on (or derived from) the Work and **for** which the
44 editorial revisions, annotations, elaborations, or other
45 modifications
46 represent, as a whole, an original work of authorship. For the
47 purposes
48 of **this** License, Derivative Works shall not include works that
49 remain
50 separable from, or merely link (or bind by name) to the interfaces
51 of,
52 the Work and Derivative Works thereof.
53
54 "Contribution" shall mean any work of authorship, including
55 the original version of the Work and any modifications or additions
56 to that Work or Derivative Works thereof, that is intentionally
57 submitted to Licensor **for** inclusion in the Work by the copyright
58 owner
59 or by an individual or Legal Entity authorized to submit on behalf
60 of
61 the copyright owner. For the purposes of **this** definition, "submitted
62 "
63 means any form of electronic, verbal, or written communication sent
64 to the Licensor or its representatives, including but not limited to
65 communication on electronic mailing lists, source code control
66 systems,
67 and issue tracking systems that are managed by, or on behalf of, the
68 Licensor **for** the purpose of discussing and improving the Work, but
69 excluding communication that is conspicuously marked or otherwise
70 designated in writing by the copyright owner as "Not a Contribution."
71
72

63 **"Contributor"** shall mean Licensor and any individual or Legal Entity
64 on behalf of whom a Contribution has been received by Licensor and
65 subsequently incorporated within the Work.
66

67 2. Grant of Copyright License. Subject to the terms and conditions of
68 **this** License, each Contributor hereby grants to You a perpetual,
69 worldwide, non-exclusive, no-charge, royalty-free, irrevocable
70 copyright license to reproduce, prepare Derivative Works of,
71 publicly display, publicly perform, sublicense, and distribute the
72 Work and such Derivative Works in Source or Object form.
73

74 3. Grant of Patent License. Subject to the terms and conditions of
75 **this** License, each Contributor hereby grants to You a perpetual,
76 worldwide, non-exclusive, no-charge, royalty-free, irrevocable
77 (except as stated in **this** section) patent license to make, have made
78 use, offer to sell, sell, **import**, and otherwise transfer the Work,
79 where such license applies only to those patent claims licensable
80 by such Contributor that are necessarily infringed by their
81 Contribution(s) alone or by combination of their Contribution(s)
82 with the Work to which such Contribution(s) was submitted. If You
83 institute patent litigation against any entity (including a
84 cross-claim or counterclaim in a lawsuit) alleging that the Work
85 or a Contribution incorporated within the Work constitutes direct
86 or contributory patent infringement, then any patent licenses
87 granted to You under **this** License **for** that Work shall terminate
88 as of the date such litigation is filed.
89

90 4. Redistribution. You may reproduce and distribute copies of the
91 Work or Derivative Works thereof in any medium, with or without
92 modifications, and in Source or Object form, provided that You
93 meet the following conditions:
94

95 (a) You must give any other recipients of the Work or
96 Derivative Works a copy of **this** License; and
97

98 (b) You must cause any modified files to carry prominent notices
99 stating that You changed the files; and
100

101 (c) You must retain, in the Source form of any Derivative Works
102 that You distribute, all copyright, patent, trademark, and
103 attribution notices from the Source form of the Work,
104 excluding those notices that **do** not pertain to any part of
105 the Derivative Works; and
106

107 (d) If the Work includes a **"NOTICE"** text file as part of its
108 distribution, then any Derivative Works that You distribute must
109 include a readable copy of the attribution notices contained
110 within such NOTICE file, excluding those notices that **do** not
111 pertain to any part of the Derivative Works, in at least one
112 of the following places: within a NOTICE text file distributed
113 as part of the Derivative Works; within the Source form or
114 documentation, **if** provided along with the Derivative Works; or,

115 within a display generated by the Derivative Works, **if** and
116 wherever such third-party notices normally appear. The contents
117 of the NOTICE file are **for** informational purposes only and
118 **do** not modify the License. You may add Your own attribution
119 notices within Derivative Works that You distribute, alongside
120 or as an addendum to the NOTICE text from the Work, provided
121 that such additional attribution notices cannot be construed
122 as modifying the License.
123

124 You may add Your own copyright statement to Your modifications and
125 may provide additional or different license terms and conditions
126 **for** use, reproduction, or distribution of Your modifications, or
127 **for** any such Derivative Works as a whole, provided Your use,
128 reproduction, and distribution of the Work otherwise complies with
129 the conditions stated in **this** License.
130

131 5. Submission of Contributions. Unless You explicitly state otherwise,
132 any Contribution intentionally submitted **for** inclusion in the Work
133 by You to the Licensor shall be under the terms and conditions of
134 **this** License, without any additional terms or conditions.
135 Notwithstanding the above, nothing herein shall supersede or modify
136 the terms of any separate license agreement you may have executed
137 with Licensor regarding such Contributions.
138

139 6. Trademarks. This License does not grant permission to use the trade
140 names, trademarks, service marks, or product names of the Licensor,
141 except as required **for** reasonable and customary use in describing
142 the
143 origin of the Work and reproducing the content of the NOTICE file.

144 7. Disclaimer of Warranty. Unless required by applicable law or
145 agreed to in writing, Licensor provides the Work (and each
146 Contributor provides its Contributions) on an "AS IS" BASIS,
147 WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or
148 implied, including, without limitation, any warranties or conditions
149 of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A
150 PARTICULAR PURPOSE. You are solely responsible **for** determining the
151 appropriateness of using or redistributing the Work and assume any
152 risks associated with Your exercise of permissions under **this**
153 License.

154 8. Limitation of Liability. In no event and under no legal theory,
155 whether in tort (including negligence), contract, or otherwise,
156 unless required by applicable law (such as deliberate and grossly
157 negligent acts) or agreed to in writing, shall any Contributor be
158 liable to You **for** damages, including any direct, indirect, special,
159 incidental, or consequential damages of any character arising as a
160 result of **this** License or out of the use or inability to use the
161 Work (including but not limited to damages **for** loss of goodwill,
162 work stoppage, computer failure or malfunction, or any and all
163 other commercial damages or losses), even **if** such Contributor
164 has been advised of the possibility of such damages.
165

```
166 9. Accepting Warranty or Additional Liability. While redistributing
167 the Work or Derivative Works thereof, You may choose to offer,
168 and charge a fee for, acceptance of support, warranty, indemnity,
169 or other liability obligations and/or rights consistent with this
170 License. However, in accepting such obligations, You may act only
171 on Your own behalf and on Your sole responsibility, not on behalf
172 of any other Contributor, and only if You agree to indemnify,
173 defend, and hold each Contributor harmless for any liability
174 incurred by, or claims asserted against, such Contributor by reason
175 of your accepting any such warranty or additional liability.
176
177 END OF TERMS AND CONDITIONS
178 <!--NeedCopy-->
```

Microsoft Public License (MS-PL)

```
1 This license governs use of the accompanying software. If you use the
2 software, you accept this license. If you do not accept the license,
3 do not use the software.
4
5 1. Definitions
6 The terms “reproduce,” “reproduction,” “derivative works,” and “
7 distribution” have the
8 same meaning here as under U.S. copyright law.
9
10 A “contribution” is the original software, or any additions or
11 changes to the software.
12
13 A “contributor” is any person that distributes its contribution under
14 this license.
15
16 “Licensed patents” are a contributor’s patent claims that read
17 directly on its contribution.
18
19 2. Grant of Rights
20
21 (A) Copyright Grant- Subject to the terms of this license, including
22 the license conditions and limitations in section 3, each
23 contributor grants you a non-exclusive, worldwide, royalty-free
24 copyright license to reproduce its contribution, prepare derivative
25 works of its contribution, and distribute its contribution or any
26 derivative works that you create.
27
28 (B) Patent Grant- Subject to the terms of this license, including the
29 license conditions and limitations in section 3, each contributor
30 grants you a non-exclusive, worldwide, royalty-free license under
31 its licensed patents to make, have made, use, sell, offer for sale,
32 import, and/or otherwise dispose of its contribution in the software
33 or derivative works of the contribution in the software.
34
35 3. Conditions and Limitations
```

20
21 (A) No Trademark License- This license does not grant you rights to use
any contributors' name, logo, or trademarks.
22
23 (B) If you bring a patent claim against any contributor over patents
that you claim are infringed by the software, your patent license
from such contributor to the software ends automatically.
24
25 (C) If you distribute any portion of the software, you must retain all
copyright, patent, trademark, and attribution notices that are
present in the software.
26
27 (D) If you distribute any portion of the software in source code form,
you may **do** so only under **this** license by including a complete copy
of **this** license with your distribution. If you distribute any
portion of the software in compiled or object code form, you may
only **do** so under a license that complies with **this** license.
28
29 (E) The software is licensed "as-is." You bear the risk of using it.
The contributors give no express warranties, guarantees or
conditions. You may have additional consumer rights under your local
laws which **this** license cannot change. To the extent permitted
under your local laws, the contributors exclude the implied
warranties of merchantability, fitness **for** a particular purpose and
non-infringement.
30 <!--NeedCopy-->



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).