



StoreFront™ 2507 LTSR

Contents

StoreFront 2507 Long Term Service Release Overview	5
What's new	6
Cumulative Update 1 (CU1)	6
What's new in 2507 (initial release)	7
Get started	21
Plan your StoreFront deployment	22
System requirements	26
Configure resources	32
Install StoreFront	34
Create a new deployment	38
End user access	40
Manage Deployment	48
StoreFront™ Management console	49
StoreFront PowerShell modules	51
Configure the base URL	60
Configure server groups	61
Manage the subscriptions database	64
Manage subscriptions data	65
Store subscription data using Microsoft SQL Server	70
Subscriptions synchronization	90
Upgrade StoreFront™	93
Export and import the StoreFront configuration	97
Default website for deployment	106

Reset a server to factory defaults	107
Uninstall StoreFront	108
Manage stores	109
Create store	112
Manage sites	119
Set Workspace app website	142
Authentication	143
Active Directory username and password authentication	145
SAML authentication	155
Domain pass-through authentication	161
Smart card authentication	163
Pass-through from Citrix Gateway	167
Manage websites	172
UI Experience	178
Citrix Workspace app deployment	179
Category Settings	184
Appearance	188
Featured app groups	190
Authentication methods	194
Website shortcuts	196
Launch Preferences	198
Store timeouts	201
Session reconnect	205
User interface settings	208

Pinned links	212
Custom announcements	215
Dialog after login	217
App Protection	218
Advanced settings	220
Configure remote access settings	224
Configure a Store	226
Favorites	227
Kerberos delegation	230
Configure optimal HDX™ routing for a store	231
Advertise or hide stores to users	235
Advanced store settings	236
Federated Authentication Service Configuration	243
Export store provisioning files for users	245
Configure session settings	246
Citrix Workspace™ app configuration	247
Integrate with Citrix Gateway and NetScaler ADC	249
Configure Citrix Gateways	249
Import a Citrix Gateway	262
Load balancing with NetScaler® ADC	271
Configure Citrix Gateway and StoreFront for Delegated Forms Authentication (DFA)	285
Authenticate using different domains	288
Configure beacon points	298
Create a single FQDN used internally and externally	301

Require Citrix Workspace™ app when connecting through a gateway	302
Entra ID authentication via OIDC and single sign-on to VDA	305
End user experience	315
Classic experience	316
Modern experience	327
Require Citrix Workspace app	341
Citrix Workspace app detection	344
Activity Manager	347
Assigned desktop power management	356
Secure your StoreFront deployment	358
Securing StoreFront with HTTPS	370
Certificate Revocation List (CRL) checking	375
ICA® file signing	384
Logs and Analytics	385
Log files	386
Event Log	388
Performance counters	389
Telemetry	389
Citrix Workspace app analytics	394
Deprecation notices	404
Third Party Notices	407

StoreFront 2507 Long Term Service Release Overview

October 22, 2025

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 store.
- What [authentication methods](#) users use to log on.
- Whether the store can be [remotely accessed through a NetScaler gateway](#)..

Users can use locally installed [Citrix Workspace app](#) or 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

December 2, 2025

The 2507 LTSR includes the following releases.

- [2507 LTSR CU1](#)
- [2507 initial release](#)
- [Known issues](#)

Cumulative Update 1 (CU1)

December 12, 2025

Release date: December 12, 2025

About this release

[StoreFront \(initial release\)](#)

[Known issues in this release](#)

[Citrix Product Subscription Advantage Eligibility Dates](#)

Citrix Workspace app for HTML5

This release includes [Citrix Workspace app for HTML5 2511](#).

What's new in 2507 LTSR CU1

Cumulative Update 1 (CU1) is the latest release of the StoreFront 2507 LTSR. See [What's new](#).

Starting with the CU1 release, when you sign in to StoreFront, you can see timely and relevant information about the launch status of Citrix Workspace app for HTML5. For more information, see [Improved Virtual Apps and desktops launch experience](#).

StoreFront Entra ID integration with NetScaler Gateway

StoreFront now supports authentication to Entra ID using OIDC. In this configuration, users can either have hybrid identities, or Entra only identity without an Active Directory account. In Studio, you can define user access using either either Entra ID directory membership, or for hybrid users Active Directory membership.

Fixed issues

StoreFront 2507 LTSR CU1 contains the following fixes:

- StoreFront **Favorites** do not synchronize between StoreFront servers when NTLM authentication is disabled. [CVADHELP-26155]
- Users encounter a **Cannot start app** error when they attempt to access certain applications through the internal StoreFront (SF) URL. [CVADHELP-29201]
- StoreFront servers intermittently log events 4010 and 4011, which indicates XML health check failures to the Delivery Controllers (DDCs). This causes occasional enumeration failures for users. [CVADHELP-28016]
- When you install the Citrix Web extension and disable the protocol handler, ICA files download instead of launching applications. This occurs because the system fails to detect Citrix Workspace app properly when the protocol handler is disabled. The fix now displays “Citrix Workspace app is successfully detected via the browser extension” and allows users to redo client detection when needed. [CVADHELP-29591]

Known issues

- There are no new known issues in Cumulative Update 1.

What’s new in 2507 (initial release)

December 12, 2025

StoreFront 2507 LTSR includes the following new features and enhancements since StoreFront 2402 LTSR:

Remove Citrix Workspace™ app detection as a prerequisite for App Protection for hybrid launch scenarios

Starting with the 2507 LTSR release, Citrix Workspace app detection is no longer a prerequisite for [App Protection for hybrid launches](#) to function. This change simplifies the enablement of App Protection for hybrid launch scenarios.

Previously, when StoreFront™ was configured to enable App Protection for hybrid launches, the user interface only displayed resources requiring App Protection if it detected certain versions of Citrix Workspace app via Citrix Workspace web extensions or Citrix Workspace launcher. This prevented use of App Protection in situations where it was not possible to use Citrix Workspace launcher or Citrix Workspace web extensions. This check has been removed and the user interface now displays such resources regardless of whether Citrix Workspace app was detected.

With this change, resources requiring App Protected are displayed in situations where ICA files are downloaded and when using legacy versions of Citrix Workspace app that do not implement App Protection. This makes it possible for users to avoid applying App Protection by tampering with the ICA file or using a version of Citrix Workspace app that does not enable App Protection. Therefore if you have enabled App Protection for hybrid launches, it is important that you also enable [App Protection Posture Check](#) and [Policy Tampering Detection](#).

Enhanced Scout functionality

Scout now supports displaying the Add machine button on the Collect page. This enhancement enables you to manually add multiple StoreFront Server machines in the same cluster and trigger collection simultaneously, improving the efficiency of data collection across StoreFront deployments.

Removal Citrix Customer Experience Improvement Program

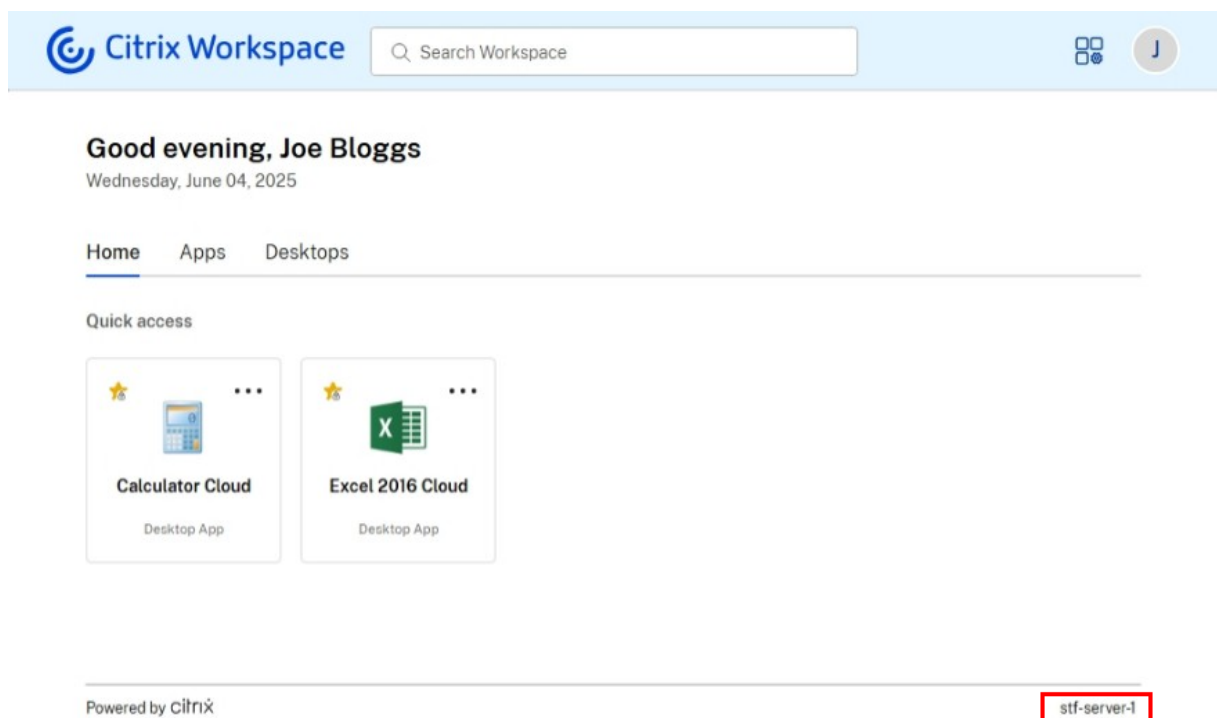
StoreFront no longer sends data to the Citrix Customer Experience Improvement Program.

Citrix Workspace app for HTML5 HDX Client

This release includes [Citrix Workspace app for HTML5 HDX client 2505](#).

Display StoreFront server name in end-user UI

When using the modern experience, the name of the server the user is connected to is displayed at the bottom of the screen on desktop, and in error messages on all platforms. This helps support team to quickly locate relevant server logs.



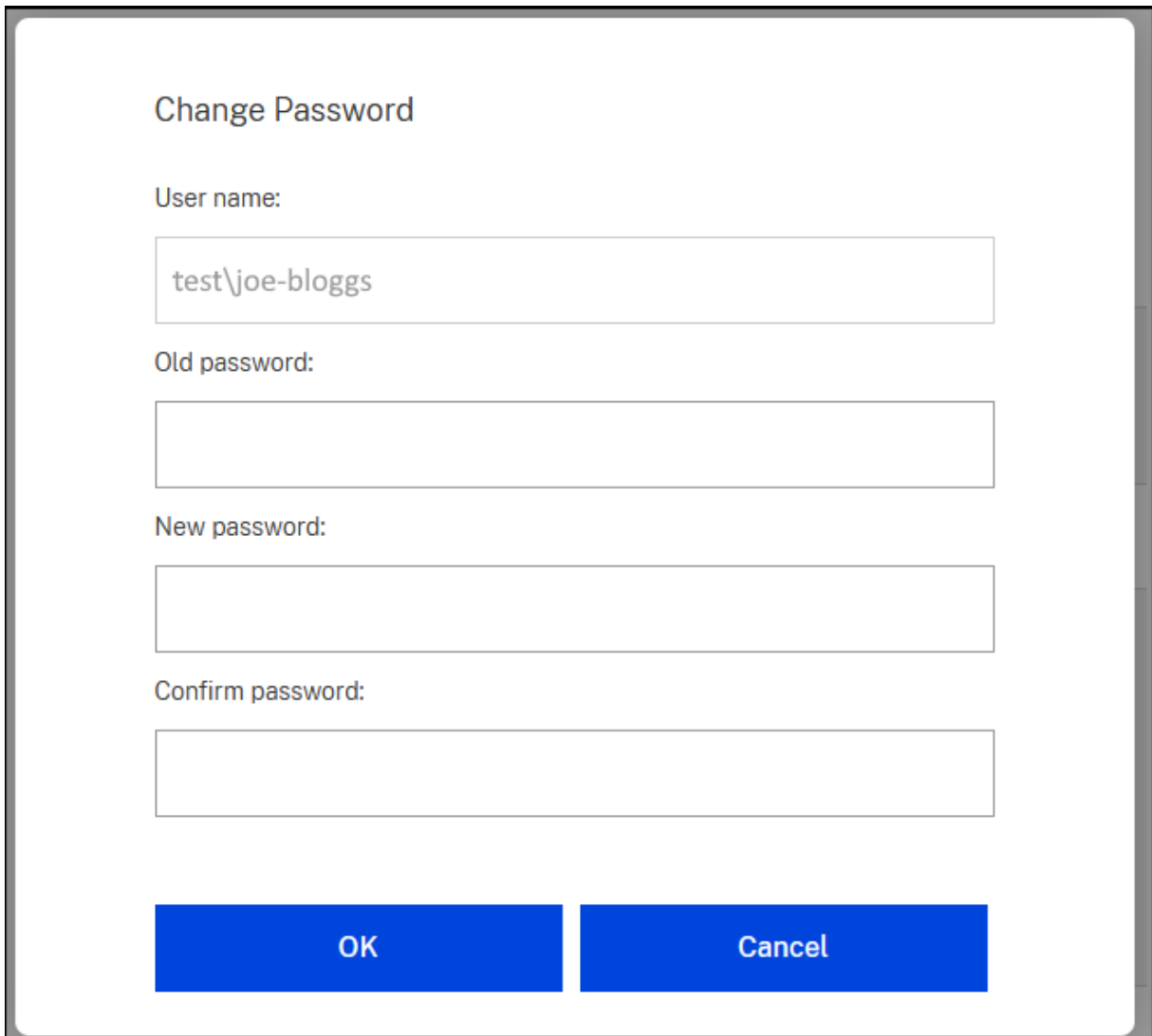
Citrix Workspace Launcher for Android, iPhone, and iPad devices

Citrix Workspace Launcher allows web browsers to communicate with Citrix Workspace app to launch resources without downloading ICA files. Previously this was only available on Windows, macOS and Linux. Citrix Workspace launcher is now supported on Android, iPhone, and iPad. When an Android, iPhone or iPad user first opens a store website in their web browser, the website detects Citrix Workspace app using Citrix Workspace Launcher. If detected successfully, Citrix Workspace Launcher is used for all subsequent launches. This streamlines the launch experience and improves security by avoiding saving ICA files to the device.

This requires Citrix Workspace app for Android 25.03 or higher and Citrix Workspace app for iOS 25.03 or higher. It is available with both the Classic and Modern experience.

Change passwords at any time using modern experience

Previously, when using the modern experience, users could change expired passwords at log in but had no way to change them at other times. With StoreFront 2503, if configured in [password options](#), there is an option in account settings to change passwords at any time, similar to the classic experience.

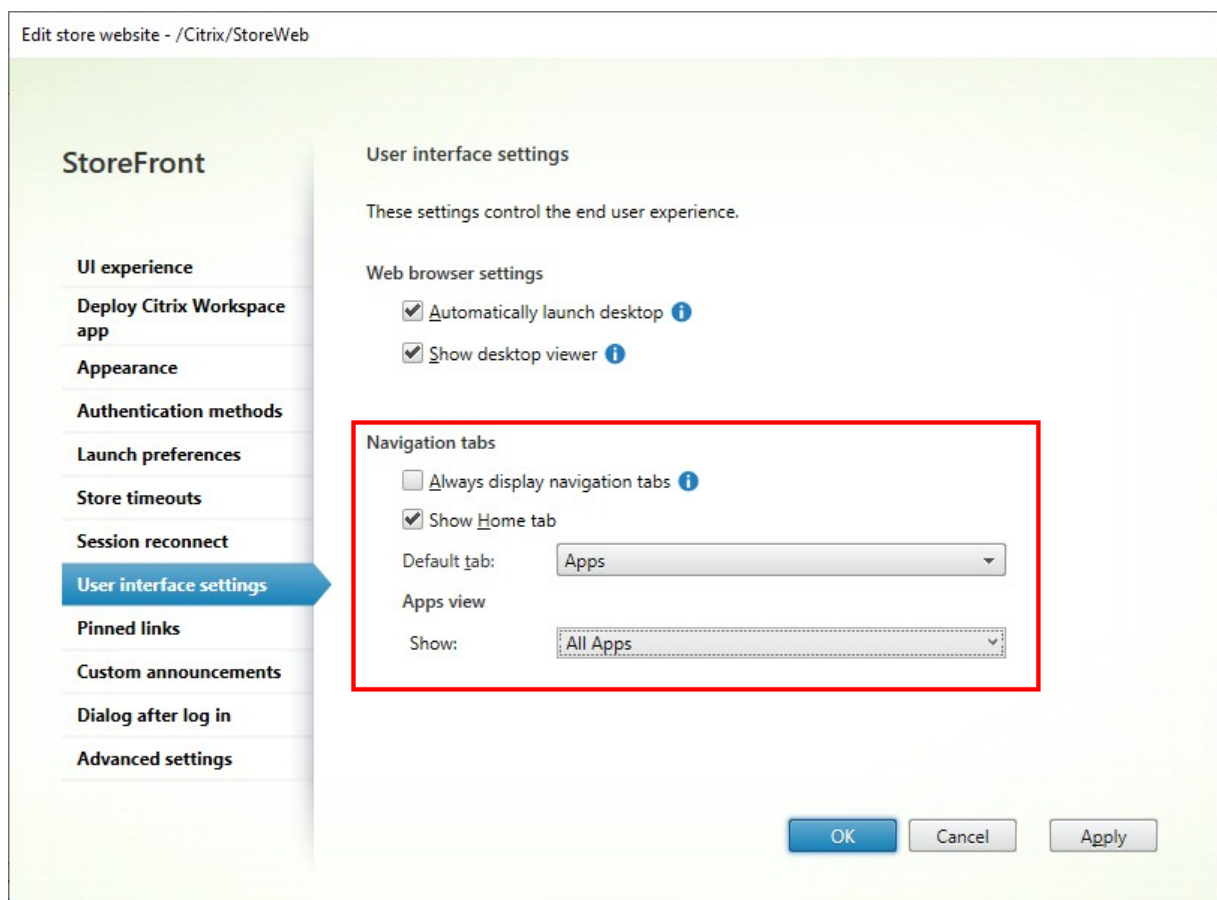
A screenshot of a 'Change Password' dialog box. The dialog has a title bar at the top. Below the title, the text 'Change Password' is centered. There are four input fields: 'User name:' with the text 'test\joe-bloggs', 'Old password:', 'New password:', and 'Confirm password:'. At the bottom, there are two blue buttons labeled 'OK' and 'Cancel'.

For more information, see [Change password](#).

Enhanced navigation and default tab configuration using modern experience

When using the modern experience, administrators can customize the end-user navigation tabs. Administrators can configure the following options:

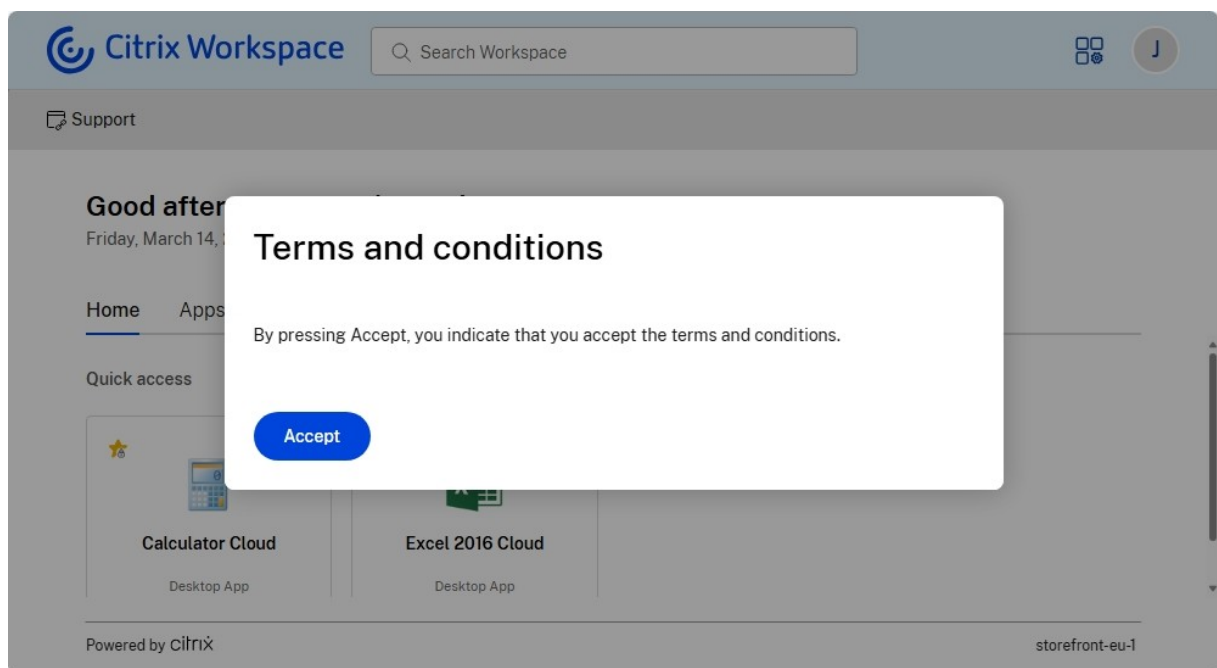
- Always display navigation tabs.
- Show home tab
- Default tab



For more information, see [Navigation tabs](#)

Display dialog after login

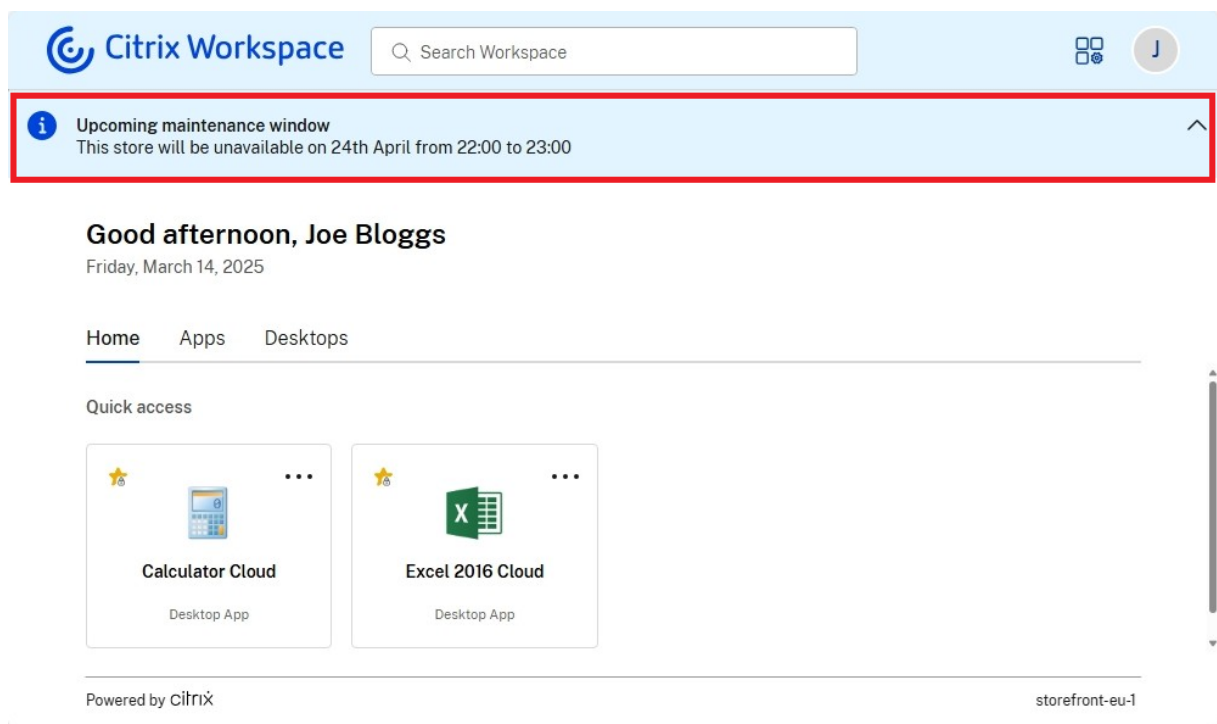
When using the modern experience, administrators can configure a pop-up dialog that appears to end users after login, which users must accept before interacting with StoreFront. You can use this to inform users about important information such as regulatory information, policy acknowledgments, internal policies, instructional content, security notices, system updates, and legal disclaimers. This is only available when using the modern experience.



For more information on how to configure this, see [Dialog after login](#).

Custom announcements

When using the modern experience, administrators can configure a banner that is displayed to the end-users, for instance to notify them of upcoming changes or maintenance windows. For more information, see [Custom announcements](#).



Session reconnect using the modern experience

Session reconnect (formerly known as Workspace Control) is now available when using the modern experience. Previously it was only available when using the classic experience. With session reconnect, you can configure the following settings for users connecting through a web browser:

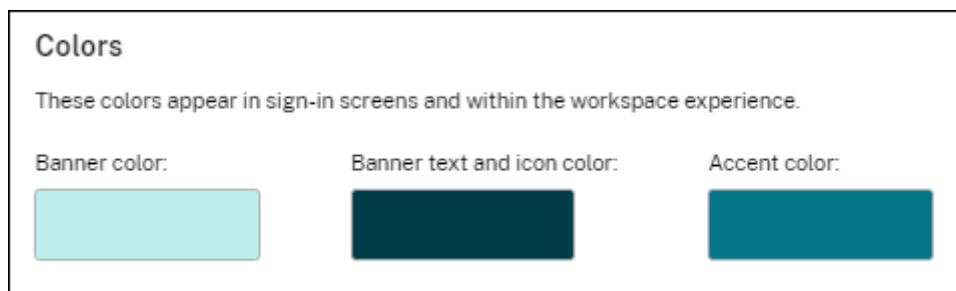
- Store log out action - whether to leave sessions active, disconnect them or log them out.
- Whether to automatically reconnect to sessions when users log in.

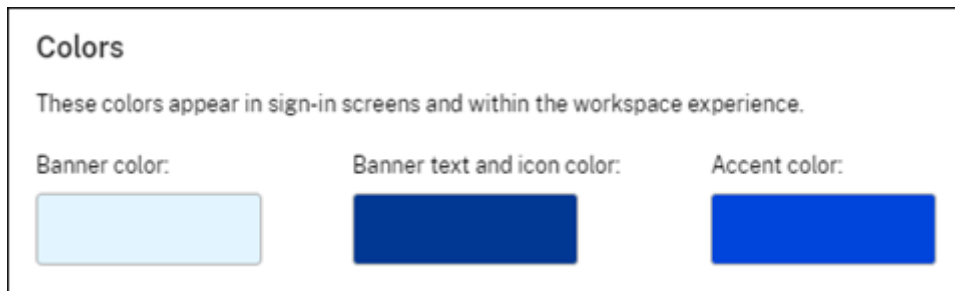
For more information, see [Session reconnect](#)

Color customization using the modern experience

The default colors have been updated.

Old default color:



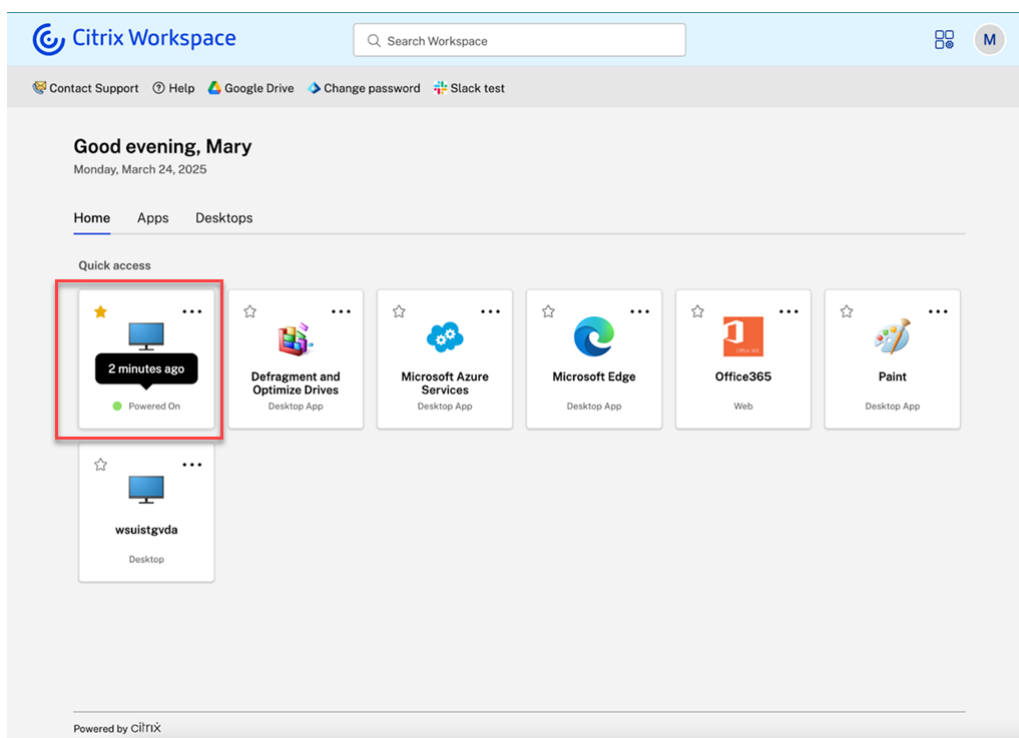
New default color:

Furthermore, the colors are now applied more consistently to buttons, links and spinners.

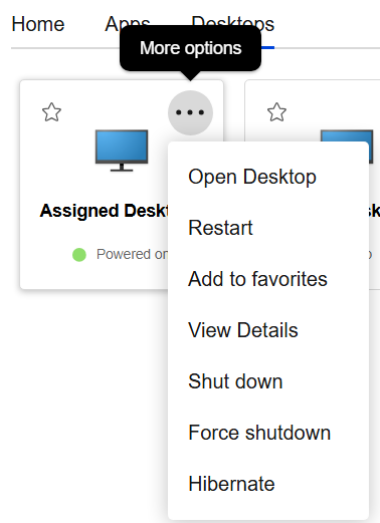
For more information, see [Appearance](#).

Display power state of assigned desktops

The end user interface now provides visibility into the power state of the user's assigned desktops, when using the modern experience with DaaS. The power state indicates whether an assigned desktop is Powered On, Powered Off, or in a suspended state (in hibernation). This enhancement allows users to quickly identify the status of their desktops, enabling them to make informed decisions and manage their resources more effectively.



Users can perform power-related actions directly from the desktop tile using the **More** options menu (ellipsis icon). Available actions dynamically change based on the desktop's current power state.



For more information, see [Assigned desktop power status](#) and [Tile actions](#).

Note:

- This functionality requires Citrix DaaS. It is not currently available with Citrix Virtual Apps and Desktops.
- Power states are not displayed for desktops where App Protection is enabled.
- Power states are only displayed for assigned desktops, not pooled desktops.

Updated terminology in management console

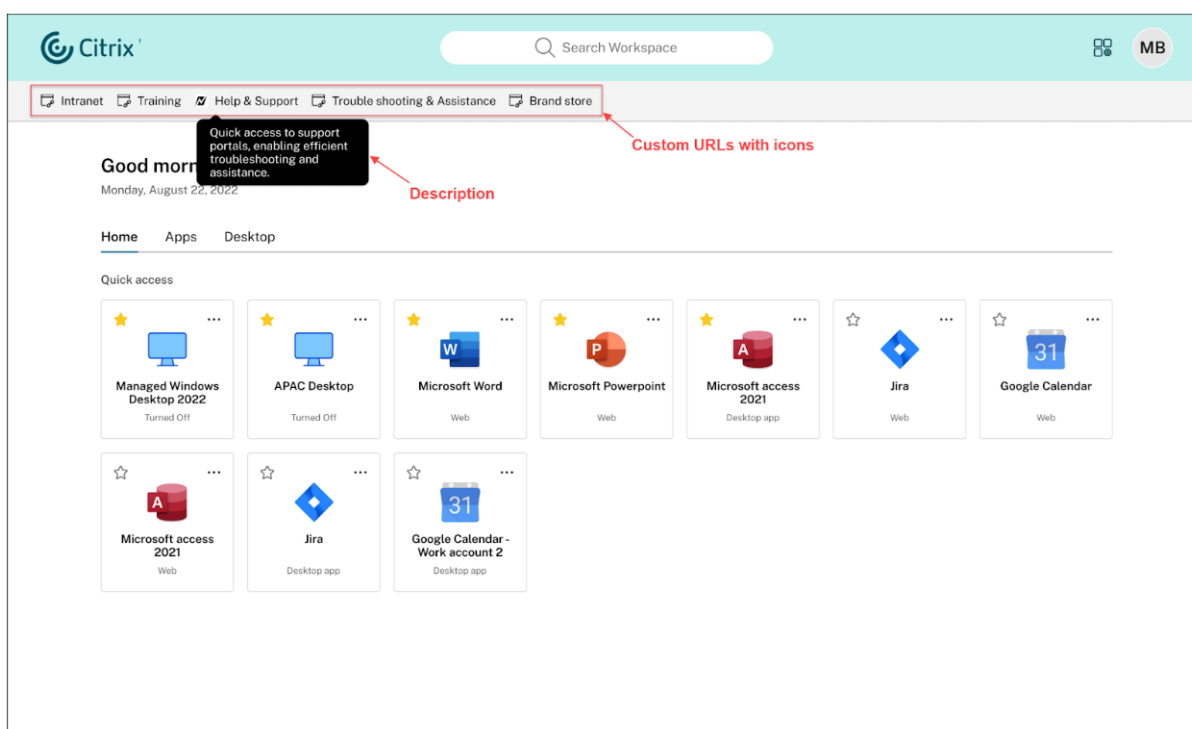
The management console uses updated terminology. In particular the follow have been updated:

Old term	New term	Notes
Citrix Receiver	Citrix Workspace app	Citrix Receiver is not supported and has been replaced by Citrix Workspace app.
HDX™ engine (plug in)	Citrix Workspace app	The HDX client is a component of Citrix Workspace app.
Receiver for Web	website	
Unified experience	Classic experience	On the UI Experience tab when editing a website.
Next generation experience	Modern experience	On the UI Experience tab when editing a website.
Configure Unified Experience	Set Citrix Workspace app website	The link on the actions pane.

Old term	New term	Notes
Delivery controller™	Site	This reflects that each entity is a site consisting of multiple delivery controllers, or a DaaS tenant or SPA server.
Workspace control	Session reconnect	

Pinned links

Custom URLs on StoreFront UI refer to customer-defined hyperlinks that provide quick access to specific websites. This feature functions as a shortcut that helps users to efficiently navigate to websites directly from the StoreFront UI. Important links, such as support websites or company portals, can be made available to the users without needing them to search for these links. It makes the navigation effortless and faster. This feature is only available on the modern experience.



For more information, see [Pinned links](#)

Require end users to use the locally installed Citrix app only

Administrators can enforce the use of the native Citrix Workspace app, eliminating the option for users to access the Citrix Workspace web client on browsers. This feature is designed for customers who

want to leverage the full benefits of the native app. The native app offers advantages such as built-in App Protection service, no browser version compatibility issues, enhanced security and telemetry for monitoring and troubleshooting.

For more information, see [Require end users to use the locally installed Citrix app only](#)

XenApp® Services off by default for new stores

When you create a new store, XenApp Services is disabled by default. You can enable it manually in the GUI or using PowerShell. Note that XenApp Services is deprecated and will be removed in a future release.

Progressive Web App [Technical Preview]

The Progressive Web App (PWA) feature allows you to install the store website so that it can be launched from your start menu or desktop, similar to a native app. This is available only in the old UI. For more information, see [Progressive Web App](#)

Citrix Licensing Telemetry

StoreFront collects telemetry on user log-ins and your configuration. For more information, see [Citrix Licensing data collection programs](#).

Citrix Gateway Service for StoreFront

Citrix Gateway Service for StoreFront provides HDX routing to your resources without needing to host your own gateway. For more information, see [Gateway Service for StoreFront](#) and [Add Citrix Gateway Service](#).

If you've opted the [Citrix Gateway Service for StoreFront \(Technical Preview\)](#) with StoreFront 2311 or 2402 and you've configured a CloudGateway, the configuration is no longer valid with StoreFront 2507. You must delete the existing gateway and create new gateways following the updated documentation.

Citrix web extensions

[Citrix web extensions](#) is enabled for all installations without needing to manually configure StoreFront using PowerShell.

Windows Server 2025 support

Storefront 2407 can be installed on Windows Server 2025 Datacenter and Standard editions.

Removal of support for Windows Server 2016

StoreFront 2407 can't be installed on Windows Server 2016. Install StoreFront on Windows Server 2019, 2022 or 2025. For more information on removed items, see [Deprecation notices](#).

Fixed issues

This release includes the following fixes since StoreFront 2503.1:

- In the management console > Manage authentication methods screen, if you clear all authentication methods except HTTP Basic, when you press OK to save changes, an error appears. [WSP-27352]
- When you change the **Launch option** to **Open in Citrix Workspace app** and save the changes, StoreFront might display an error. The error occurs when the HTML5 HDX version installed on the server differs from the version installed by default by the current version of StoreFront. [WSP-27357]
- When configuring a custom announcement it is possible to enter a very long title and description that does not display correctly. [WSUI-10550]
- When you add a StoreFront server to a server group, the new server's **Citrix Receiver for Web** application pool is set to recycle periodically, which might log out users unexpectedly. With this fix, the application pool is set to recycle at a time between 01:00 and 03:55 to avoid working hours. [WSP-27426]
- Multiple telemetry exception events are logged when installing StoreFront on a non-English system [WSP-27768]
- StoreFront Management console refers to obsolete term "Unified Experience". [WSP-27609]
- The PowerShell command `Get-STFWebReceiverSiteStyle` might fail with error **Value cannot be null**. [CVADHELP-27988]
- The PowerShell command `Set-STFWebReceiverSiteStyle` might fail with error **Value cannot be null**. [CVADHELP-28231]
- Changes on the website **Appearance** tab might not be correctly saved. [WSP-28464]
- The PowerShell command `Set-STFWebReceiverSiteStyle` resets unspecified parameters to the default rather than preserving their existing value. [WSP-28264]
- When Cloud Connectors operate in LHC mode and a user attempts to launch a resource that is accessible from multiple locations, the session might fail to start if the resource isn't immediately available. The issue occurs because, after checking the resource's readiness, StoreFront

might send the request to a different connector than the one initially used to launch the resource. [CTXENG-64445]

- Once StoreFront selects a FAS server, if that FAS server later became unavailable the launch fails. With this fix, StoreFront will instead select a different FAS server allowing the launch to proceed. [WSP-25742]
- If a FAS server fails to respond, StoreFront continues to attempt to contact it for every user, adding delay to the log-in or launch time (depending on configuration). With this fix, when a FAS server fails to respond, StoreFront avoids attempting to use the same server for a period of time so subsequent users are not impacted by the delay. [WSP-25742]
- When socket pooling is enabled, StoreFront might show high memory usage and port exhaustion causing service unavailability. [CVADHELP-26838]
- An upgrade to a newer version of StoreFront fails and the logs contain text “VersionData:Load Failed due to exception: System.IndexOutOfRangeException”. The issue occurs when a user group created by StoreFront has an empty description. [CVADHELP-25433] [WSP-22426]
- Intermittently, StoreFront upgrade fails. The installer either fails silently before the wizard appears, or the wizard becomes unresponsive, or after clicking through the wizard the upgrade fails. The issue occurs because the installation files are deleted before they are needed. [CVADHELP-25435] [WSP-23961]
- Upgrade fails with message “There was an error adding user accounts in the Administrators local group to the CitrixStorefrontAdministrators local group” or similar. This occurs when a user group used by StoreFront contains a deleted user. [WSP-23111]
- During an outage, when the connectors go into Local Host Cache mode, StoreFront needs to send launch requests to the connector in the same zone as the resource. When a resource is available in multiple zones, previously, StoreFront would only try to launch the resource in one zone. With this enhancement, if the attempt to start a resource in one zone fails, in some cases StoreFront server tries to make another attempt to start the resource using connectors in other available zones to improve resilience. [WSP-23898]
- Remove additional notification shown in Citrix Workspace app for Windows 2309 or higher, when connecting to StoreFront 2402 using a XenApp Services URL [WSP-23122].
- In the [StoreFront Web API](#), the list endpoint should set `isSubscriptionEnabled` according to whether favorites are enabled. [WSP-22503]
- In the Store Services API, the [Resource Enumeration](#) endpoint should set subscription status according to whether favorites are enabled. [WSP-22503]
- When you upgrade StoreFront, you might notice duplicate copies of customization files, which were placed in the custom folder (`\StoreWeb\custom`), can also be found in the root of the website folder (`\StoreWeb`) after the upgrade process is complete. [CVADHELP-25405]

Fixes to the Classic UI experience:

- When **Launch option** is set to **Let the user choose**, the **Welcome to Citrix Workspace app** screen displays text **undefined**. [STRFRNTUI-695]

- After disabling **Allow users to skip Citrix Workspace app detection**, users who previously skipped Citrix Workspace app detection are not affected. With this fix, the next time such users open the store website they are required to complete Citrix Workspace app detection. [STRFRNTUI-659]
- When using Microsoft Edge, after downloading Citrix Workspace app, instructions on how to launch Citrix Workspace launcher are missing. [STRFRNTUI-615]
- When using Safari, on the Citrix Workspace app detection screen, instructions for opening the Citrix Workspace launcher are missing. [STRFRNTUI-673]
- When **Launch option to Let the user choose** and Citrix web extension is installed and has detected Citrix Workspace app, it is not possible to change the launch method to open resources in a web browser. [STRFRNTUI-691]
- When Citrix Workspace app has been successfully detected by Citrix web extension, the link to **Download Citrix Workspace app** should be hidden from the settings page. [STRFRNTUI-692]
- Auto launch desktop does not work after one year following the first time the user accesses the website. [CVADHELP-26817]
- The content security policy should include **default-src: none**. [STRFRNTUI-665]
- The UI hangs if Citrix web extension is disabled/removed after detecting Citrix Workspace app [STRFRNTUI-689]
- The copyright symbol is not displayed correctly when using non-English languages. [STRFRNTUI-704]
- On the settings screen, indicate whether Citrix Workspace web extension will be used to launch apps and desktops. [STRFRNTUI-700]
- Some cookies do not have **SameSite** set. With this change, **SameSite** is set to **Lax** for all cookies. [WSP-26464]
- Update translation on the client detection screen when using Mozilla FireFox in the Brazilian Portuguese language. [STRFRNTUI-564]
- Updated the Content Security Policy defined in the **http-equiv** tag of the HTML file to block inline scripts. If you have customized StoreFront in a way that uses eval or adds inline scripts to the DOM then this action causes those customizations to fail.

Fixes to the modern UI experience:

- When using Google Chrome on macOS with Citrix web extension installed and session reconnect might not work. [WSUI-10534]
- The desktop tab should be hidden if the user does not have any desktops. [WSUI-10922]
- On the desktop tile of a hibernated resource, the **Resume** option is not available. [WSUI-10569]
- When a user tries to restart a desktop from Activity Manager, they get error **Cannot Restart desktop**. [WSUI-10224]
- Resource filtering rules should not apply to sessions listed by **Activity Manager**. [WSP-28345]
- On mobile, the **Cancel** button next to the search bar should be black rather than blue. [WSUI-10547]

- When all resources require App Protection and the user has chosen to launch in their browser, the option to connect to Citrix Workspace app is not available. [WSUI-10830]
- On a hibernated persistent desktop tile, the menu doesn't include an option to resume the desktop. [WSUI-10569].
- The modern experience does not load on Citrix Workspace app for Linux [CVADHELP-27746]
- Allow Activity manager to handle more sites than can be enumerated concurrently. [WSP-24122]

Known issues

- When using Safari on iOS, after completing Citrix Workspace app detection and returning to Safari, the webpage may become stuck on a loading screen. To work around this, the user must refresh the webpage. [WSUI-10515]

Get started

October 22, 2025

Pre-requisites

1. [Plan your StoreFront deployment](#)
2. Install and configure the resource providers that you wish StoreFront to aggregate:
 - [Citrix Virtual Apps and Desktops](#)
 - [Citrix DaaS](#)
 - [Secure Private Access](#).

For more information on configuring the resources optimally see [Configure resources](#).

3. Review the [System Requirements](#) and ensure that you have the pre-requisites to install StoreFront.

Deploy StoreFront

To create your StoreFront™ deployment, complete the following steps:

1. [Install StoreFront](#) onto a new server.
2. [Create a new deployment](#) with your first store.
3. [Determine how users will access the store](#).

Optimize your deployment

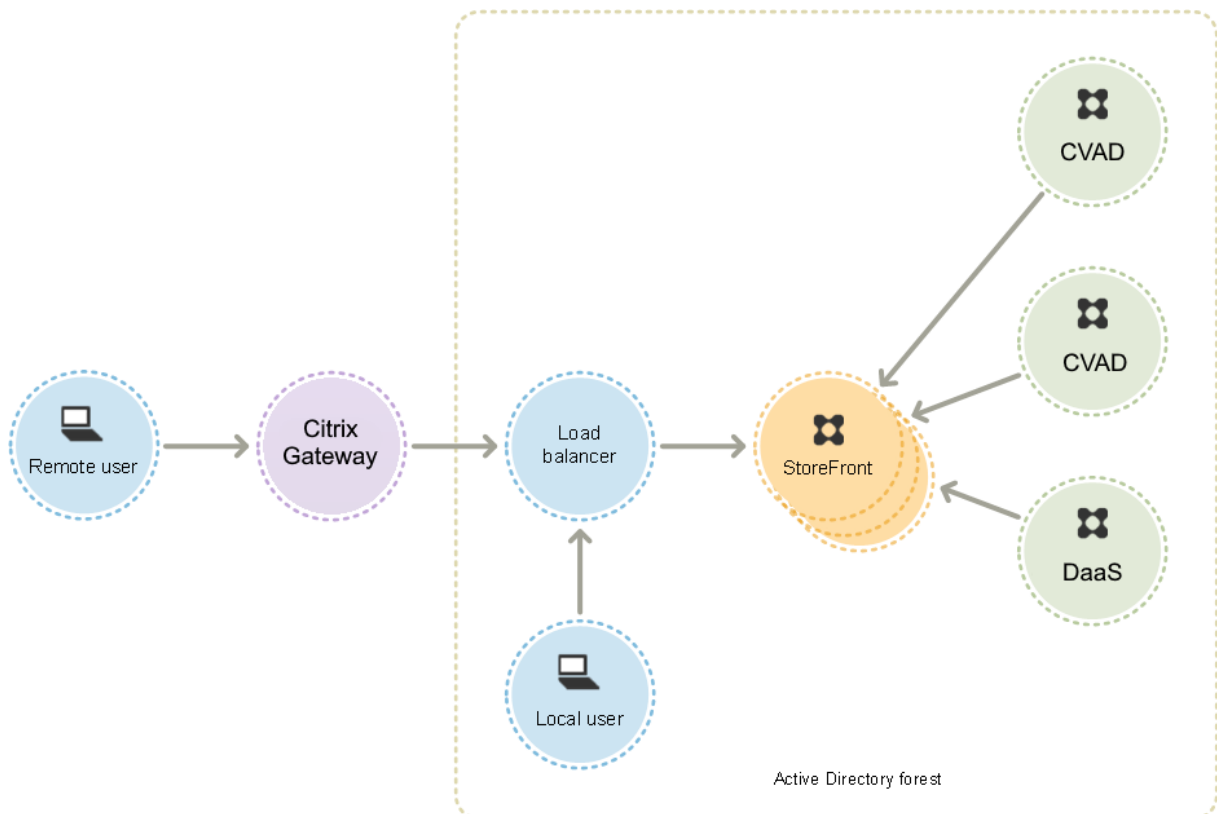
1. For redundancy and scalability, deploy a [load balancer](#) and add further servers to the [StoreFront server group](#).
2. [Secure your deployment](#).
3. Optimize the [end user experience](#).
4. Enable remote access using a [Citrix Gateway](#).

Plan your StoreFront deployment

October 22, 2025

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:

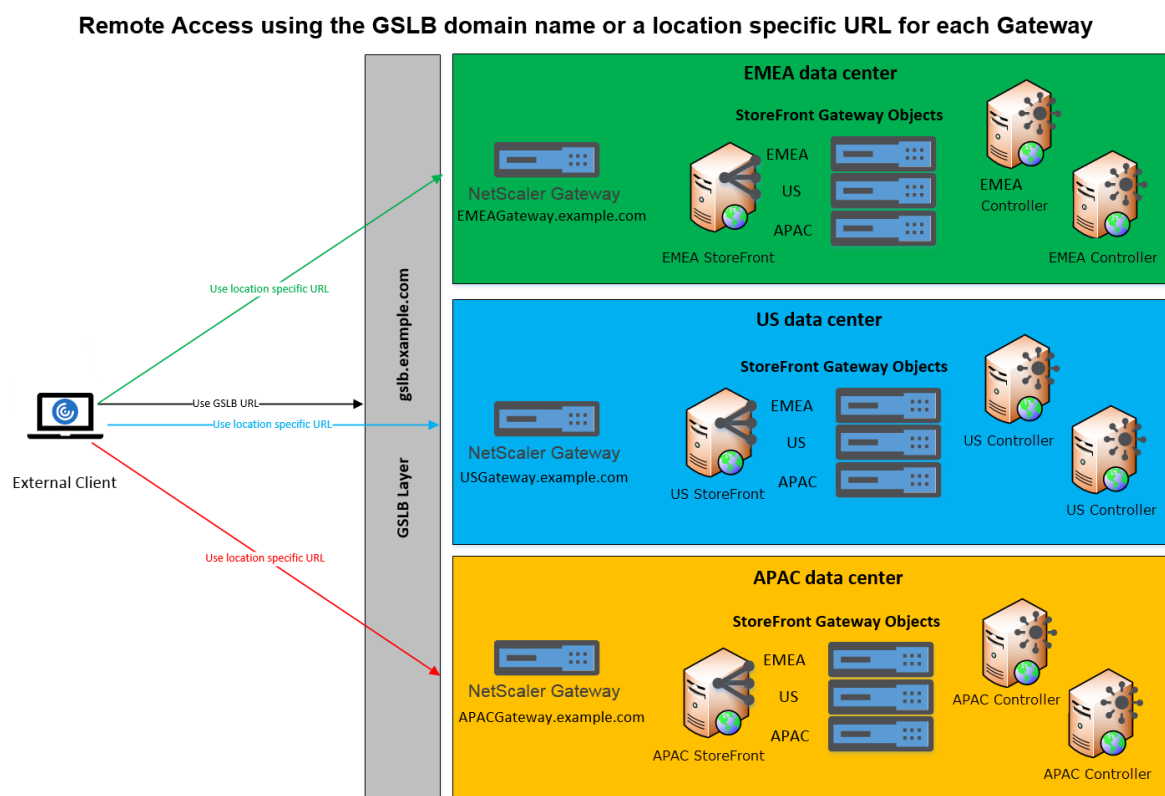
[emeagateway.example.com](#) - Europe gateway

[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 ensure 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](#).

When you add a store to Citrix Workspace app, it identifies the store by base URL and store name. Therefore, if you have multiple StoreFront deployments behind a GSLB then each deployment must have the same [base URL](#).

Note:

When Citrix Workspace app roams between different StoreFront deployments behind a GSLB, the user is required to re-authenticate. Therefore you should configure persistence so a user's requests are always routed to the same deployment if possible.

User access

See [User access options](#).

System requirements

October 22, 2025

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 2025 Datacenter and Standard editions
- Windows Server 2022 Datacenter and Standard editions
- Windows Server 2019 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 4.8.0 then the installer automatically installs .NET Framework 4.8.0. Note this requires that the NET-Framework-45-Core Windows feature is already installed. In addition StoreFront requires .NET 8. If it is not already installed then the installer automatically installs .NET 8.

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). For more information, see [Log files](#).

Network

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

- Clients connect to StoreFront using HTTPS or HTTP, normally over port 443 or 80 respectively, depending on IIS configuration. It is recommended that you enable HTTPS and disable HTTP within IIS.
- 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.
- If you are using a NetScaler load balancer with a StoreFront monitor, it needs to connect to the Citrix Service monitor. By default this runs on TCP port 8000 but can alternatively be configured to run over HTTPS on port 443. See [Load balancing with NetScaler ADC](#).

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. StoreFront cannot be installed on a domain controller.

For StoreFront to authenticate users against Microsoft Active Directory, ensure the StoreFront server is joined to either the domain containing your users' accounts or a domain that has a trust relationship with the user accounts domain. This is always required for [domain pass-through](#). For [username and password](#) authentication this is required by default, alternatively you can configure StoreFront to delegate authentication to the delivery controllers.

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 2507 LTSR
- Citrix Virtual Apps and Desktops 2503
- Citrix Virtual Apps and Desktops 2411
- Citrix Virtual Apps and Desktops 2407
- Citrix Virtual Apps and Desktops 2402 LTSR
- Citrix Virtual Apps and Desktops 2203 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

Connections through Citrix Gateway can be made using the ICA proxy, Citrix Gateway plug-in, or client-less 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 within their browser. For more information, see [User access options](#).

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>.

Older versions of Citrix Workspace™ app and Citrix Receiver™ may work but are not supported.

On Android, iOS and iPadOS using Citrix Workspace app versions earlier than 24.12, it is not possible to connect to a store configured with the modern experience through a gateway.

Web browsers

End-users can access stores using a web browser. Apps and desktops can be launched either via a locally 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*

* Internet Explorer can be used to connect to store websites configured to use the classic experience, not the modern experience. The HTML5 HDX client does not support Internet Explorer so you must use Citrix Workspace app to connect 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](#).

Citrix web extensions For an improved experience, it is recommended that users add Citrix web extension to their web browser. For requirements, see [Citrix web extension](#).

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.

Configure resources

October 22, 2025

When delivering resources with Citrix Virtual Apps and Desktops, Citrix Desktops as a Service or Secure Private access, consider the following when configuring resources. For more information about delivering applications with Citrix Virtual Apps and Desktops, see [Applications](#).

- Enter the resource name as you wish it to appear within your store.
- Optionally enter a description. This is displayed on the store when you expand the app details, alongside any keywords.
- Choose an icon to help users visually identify an application on the StoreFront website.
- 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 a resource 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 favorites, users cannot remove mandatory applications from the Home tab. Has no effect if favorites are disabled for the store.
Auto	When users log on to the store, the application or desktop is automatically favorited and added to their Home tab. Users can unfavorite such applications. Has no effect if favorites 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.
prefer="application"	Where <i>application</i> identifies a locally installed application. Applies only to published apps 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 .

Smart Access Tags

StoreFront™ sets certain Smart Access Tags. You can define Access Policies within Studio that can be used to allow or deny access to a delivery group based on these smart access tags. This requires:

- Citrix Virtual Apps and Desktops 2407 or higher. For more information, see [About access policy rules](#).
- Citrix Desktops as a Service. For more information, see [About access policy rules](#).

StoreFront sets the following Smart Access Tags:

Name	Description	Example
<code>Citrix.ClientUserAgent</code>	The user agent of the client	<code>Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36</code>
<code>Citrix.StoreFrontStoreUrl</code>	The URL of the store the user is connected to	<code>https://storefront.example.com/Citrix/Store</code>

Install StoreFront

November 16, 2025

Before installing

Before you install and configure StoreFront, review the [System Requirements](#).

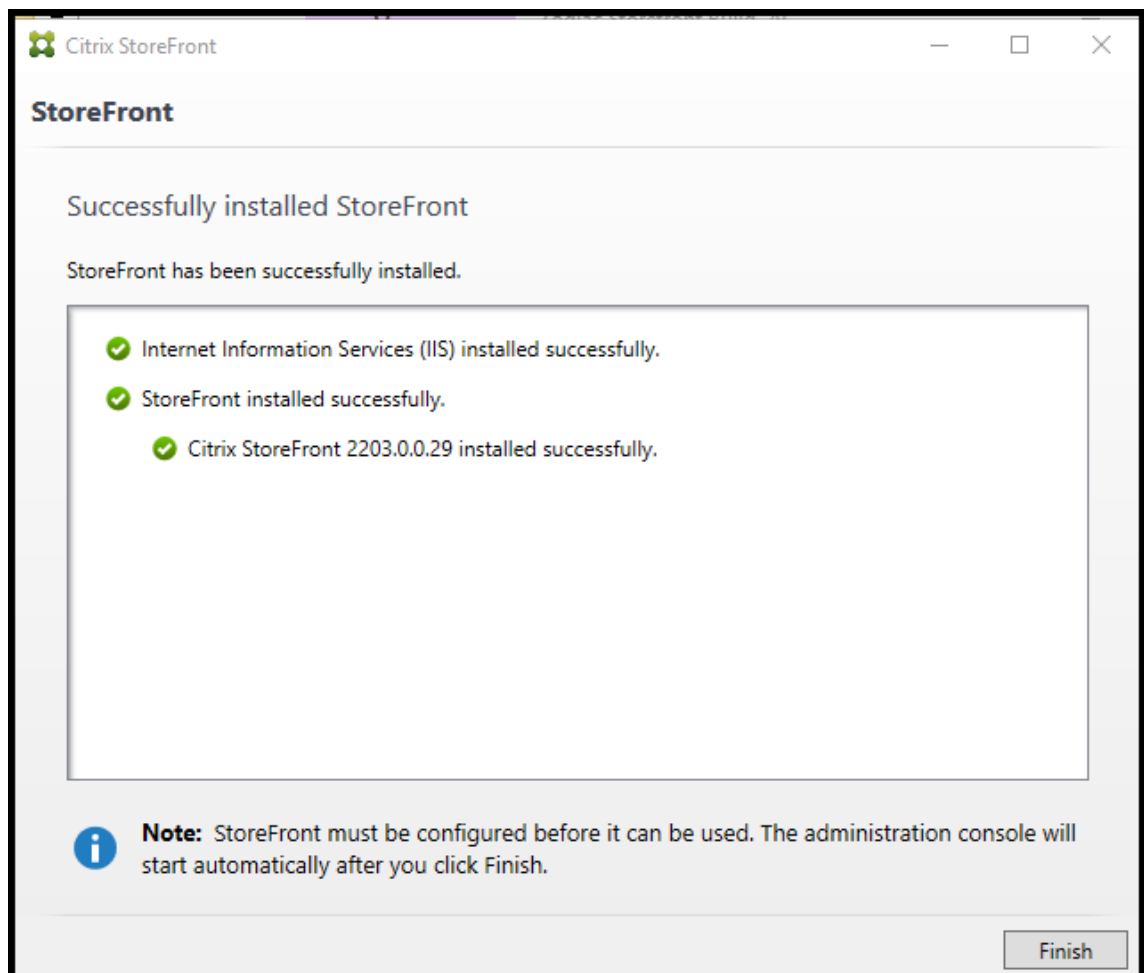
Install StoreFront

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 [StoreFront download page](#). The installer can also be found on the Citrix Virtual Apps and Desktops image in the `\x64\Storefront` directory.
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. Browse your installation media or download package, locate CitrixStoreFront-x64.exe, and copy the file to a temporary location on the server.

3. 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]
```

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.

.Net Framework 4.8 reboot step with Windows Server 2019

The .Net Framework 4.8 is a pre-installed component on Windows Server 2022 but not on Windows Server 2019. The CitrixStoreFront-x64.exe installer runs the .Net Framework 4.8 installer if it's not present. If existing .Net Framework libraries are in use, a server reboot may be required for the .Net Framework 4.8 install to complete before StoreFront can be installed. This may occur if you have a PowerShell session running.

When a reboot is required the CitrixStoreFront-x64.exe will exit and will need to be manually restarted afterwards. If the install is in silent mode it will exit with an error code otherwise the user will be prompted to allow reboot. The CitrixStoreFront-x64.exe process will return any non success exit code from the .Net Framework 4.8 installer in those situations. The specific reboot exit codes are:

- ERROR_SUCCESS_REBOOT_REQUIRED **3010**

- ERROR_SUCCESS_REBOOT_INITIATED **1641**

For silent installation of CitrixStoreFront-x64.exe via PowerShell script, pre-install .Net Framework 4.8 on the server if it's not already present.

Installing as part of Citrix Virtual Apps and Desktops™

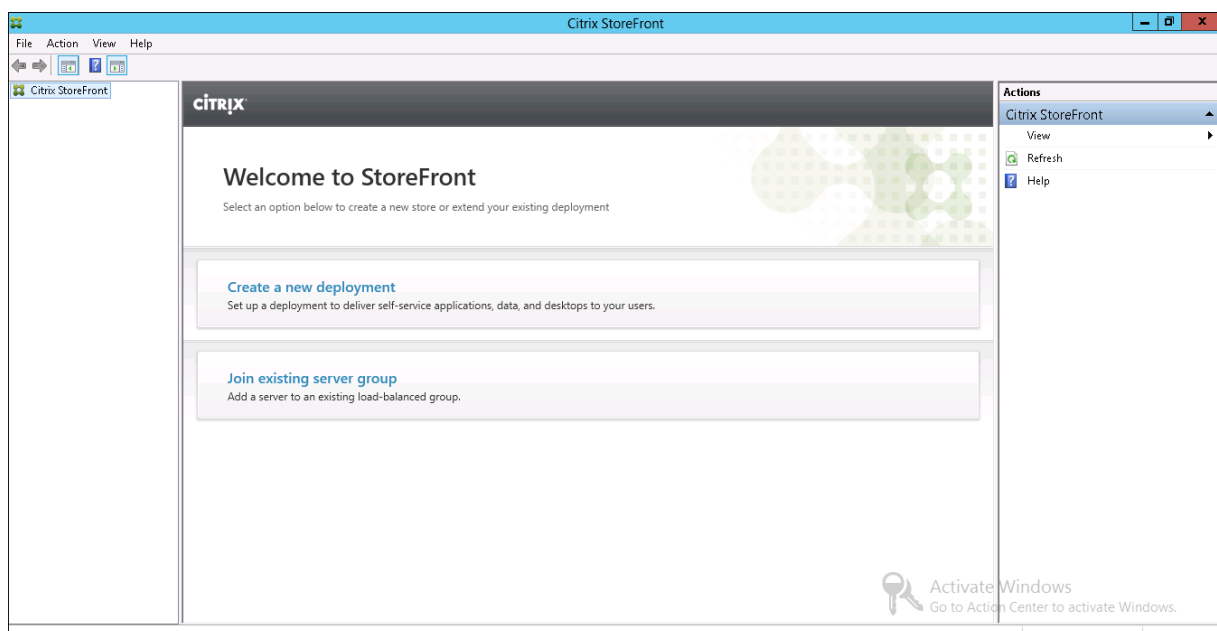
You can install StoreFront on the same server as Citrix Virtual Apps and Desktops. Run the Citrix Virtual Apps and Desktops installer and under **Extend Deployment** choose **Citrix StoreFront**.

Installation logs

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

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.

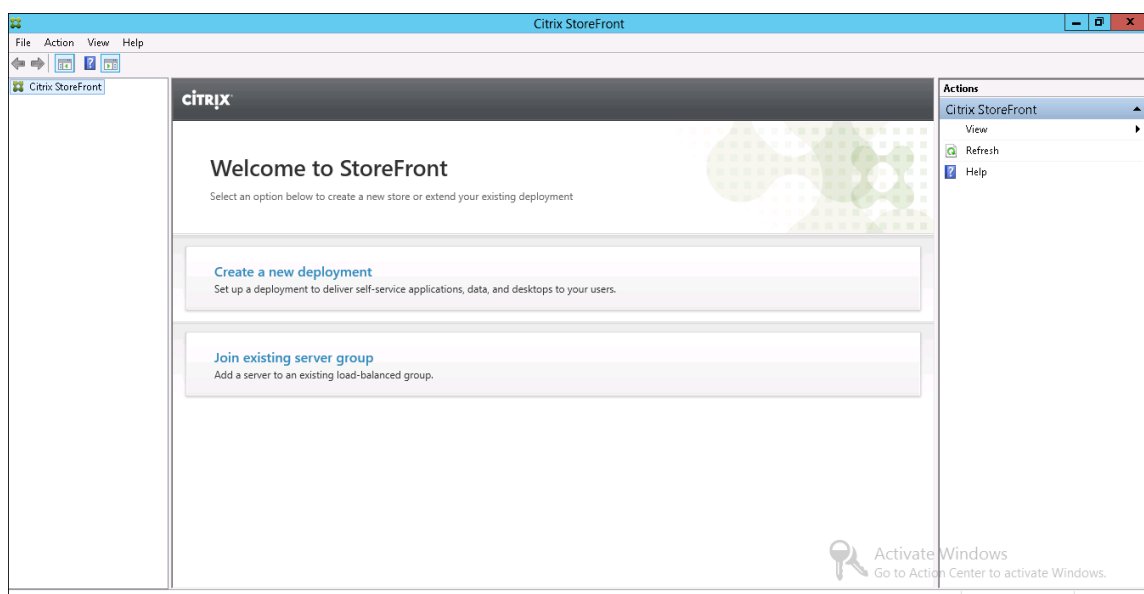
- [Join existing server group](#). Add another server to an existing StoreFront deployment. Select this option to rapidly increase the capacity of your StoreFront deployment. External load balancing is required for multiple server deployments. To add a server, you need access to an existing server in the deployment.

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

Create a new deployment

November 5, 2025

1. If the StoreFront [management console](#) is not already open after installation of StoreFront, open it.



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.

Create New Deployment

StoreFront

Base URL

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

Enter a Base URL

Confirm the base URL for services hosted on this deployment. For multiple server deployments, specify the load-balanced URL for the server group.

Base URL:

Next Cancel

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 PowerShell

To create a deployment using [PowerShell](#), run 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 [PowerShell](#). 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"
```

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 perform all StoreFront configuration using the PowerShell modules and include the [SiteID](#) in each command.

End user access

November 12, 2025

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

- **Locally installed Citrix Workspace app** - 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.
- **Web browser** - 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

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

Citrix Workspace app offers the following advantages compared to using a web browser:

- **Enhanced security** as [.ica](#) files are handled securely and never downloaded.
- **Enhanced reliability** for opening apps and desktops without needing to deploy on the Citrix web extensions.
- **In-built App Protection service** provides an additional layer of security to protect against key-logging and screen-capturing malware.
- **Better telemetry** because the native app offers extensive information for monitoring purposes.

- **Enhanced HDX™ capabilities** with enhanced features such as optimized codec compression and efficient audio-video compression. These improvements ensure high quality and performance for tasks involving high-definition content or graphics-intensive apps.

Typically a store has a single website which is displayed within Citrix Workspace app. It is possible to configure multiple [websites](#), in which case you can [configure](#) which website is displayed within Citrix Workspace app.

Beacons

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. It uses this information to connect directly to StoreFront or through a Citrix Gateway. For more information, see [Configure beacon points](#).

Require use of Citrix Workspace app

You can configure StoreFront so that when users open a store website in their browser, it automatically opens Citrix Workspace app and does not allow users to continue in their web browser. If Citrix Workspace app is not detected then the website gives the user the option to install it. Furthermore, the website automatically configures Citrix Workspace app to connect to the store. For more information, see [Require use of Citrix Workspace app](#). This functionality can also be implemented in the Citrix Gateway using a plug-in, see [Require Citrix Workspace app when connecting through a gateway](#).

Add Store to Citrix Workspace App

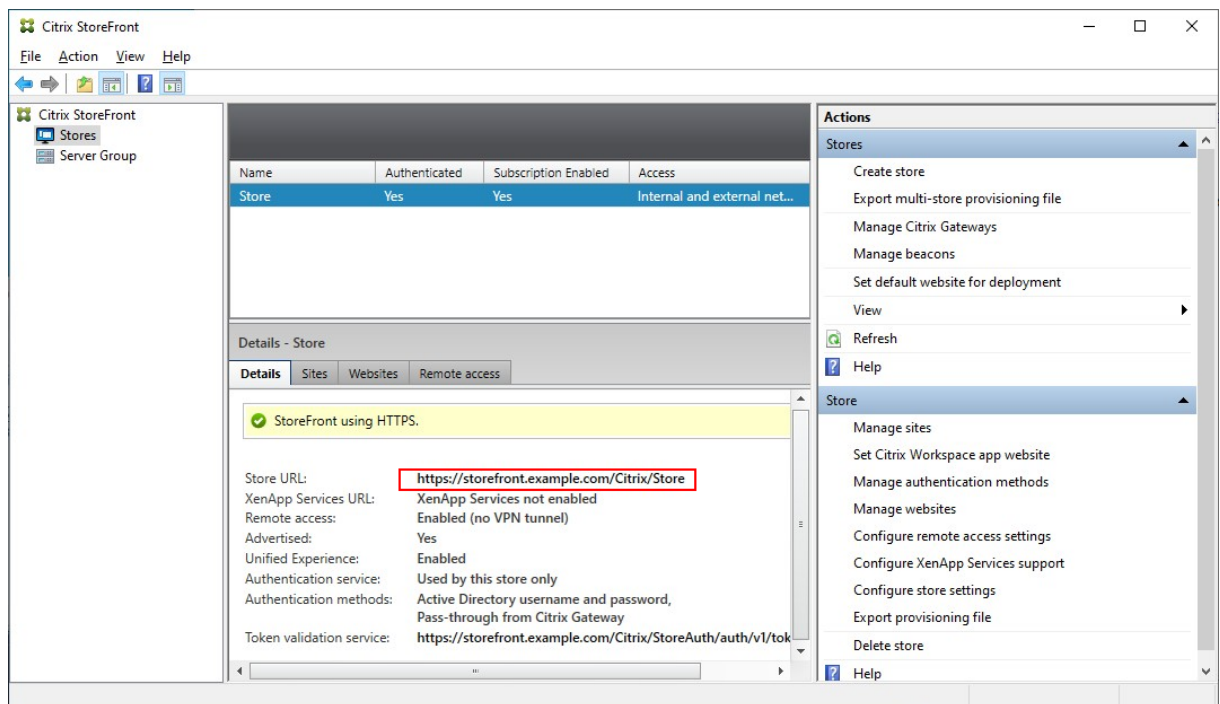
After installation, Citrix Workspace app must be configured with connection details for the stores providing users' desktops and applications. You can configure Citrix Workspace app using the store URL, a provisioning file or configure email discovery.

For more information on configuring Citrix Workspace app for Windows, see [Citrix Workspace app for Windows documentation](#).

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.

Store URL To get the store URL, within the management console, select the store. The store URL is displayed on the store details.



If you right click the store URL there is an option to copy it to clipboard.

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](#).

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](#).

Web browser

As an alternative to using a locally installed Citrix Workspace app, users can access their store through a web browser.

Normally there is a single website for a store but you can configure multiple websites, each with its own URL and configuration. For more information, see [Manage websites](#).

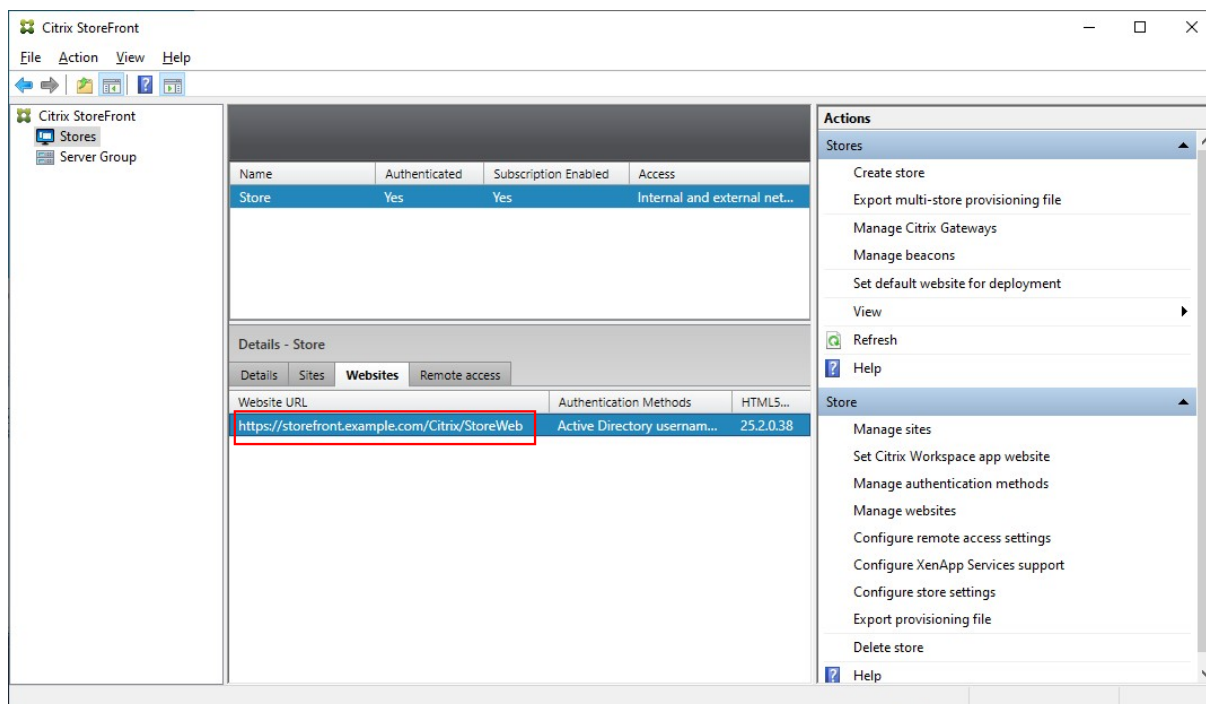
Internal users can navigate directly to the store website URL. Where there are multiple websites in your StoreFront deployment, you can configure one of them as the default URL that users are redirected to when the user navigates to the base URL.

If you have deployed a Citrix Gateway, then external users navigate to the gateway URL. This is normally a different URL, though can be configured to use the [same URL](#).

Note:

The Store website URL used from a web browser is different to the Store URL used to configure Citrix Workspace app.

To get the store website URL, within the management console, select the store. The website URLs are displayed on the **Websites** tab.



If you right click the website URL there is an option to copy it to clipboard.

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 **Let the user choose** then when the user first opens the store website in their browser, the user has the option to click **Use web browser** to launch resources within their web browser.

Requirements for opening resources in your browser

For users on the internal network, access through a web browser to resources provided by Citrix Virtual Apps and Desktops is disabled by default. To enable local access to desktops and applications using a web browser, 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 a store in their web 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 web extensions

For the best user experience, deploy [Citrix web extensions](#). These 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:

- 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, select **Change launch method** (classic experience) or **Verify connection** (modern experience) to re-detect Citrix Workspace app.

Important

If users do not have Citrix web extensions installed, then Citrix Workspace app detection takes an additional 6s to time out attempting to contact Citrix web extensions. If you have not deployed Citrix web extensions then you may wish to disable it or modify the timeouts. For more information, see [Launch preferences](#).

Citrix Workspace launcher

When the user first goes to a StoreFront web site with a supported operating system and browser and Citrix web extensions are not installed, it attempts to invoke the Citrix Workspace Launcher. For more information on the user experience see [Classic experience](#) and [Modern experience](#).

If a supported version of Citrix Workspace app is installed then the app notifies StoreFront. The browser remembers this and when it launches an app it uses Citrix Workspace Launcher.

The store website invokes Citrix Workspace Launcher 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 Workspace app or Citrix Receiver.

- Citrix Receiver for Windows 4.3 or higher or any version of Citrix Workspace app for Windows with the WebHelper component (this is installed by default)
- Citrix Receiver for Mac 12.0 or higher or any version of Citrix Workspace app for Mac
- Citrix Workspace app for Linux 2003 or higher
- Citrix Workspace app for iOS 2503 or higher
- Citrix Workspace app for Android 2503 or higher

If Citrix Workspace 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 file downloads. The user can later try again by going to the Settings screen and clicking **Change Citrix Workspace app**.

Citrix Workspace launcher has the following limitations:

- 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. For more information, see [CTX460312](#).

- When connecting to the website via a Citrix Gateway, 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 is unable to connect to StoreFront. To work around this, ensure your Citrix Gateway is configured for HDX routing with appropriate STA servers. [Edit the Citrix Gateway](#), set the **Usage or role** to **Authentication and HDX routing** and configure the STA servers.
- If there is an authenticated proxy in front of the Citrix Gateway then Citrix Workspace app is unable to make a SOCKS connection to Citrix Gateway so Citrix Workspace launcher fails.

As an alternative, deploy Citrix web extensions.

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 the website is unable to detect a locally installed Citrix Workspace app by any other means, or the user clicks **Skip detection**, 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. This launch method is not recommended as:

- Storing ICA files on disk is a security risk.
- When using [Session reconnect](#), the website cannot reconnect to existing sessions.
- Domain pass-through authentication is not available.

This option can be disabled, for more information see [Launch preferences](#).

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-logon or post-logon screen, and add language packs. For more information see [Customize Appearance](#).

XenApp Services URLs

Note:

XenApp Services (also known as PNAgent) is deprecated as of StoreFront 2308. 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.

Manage Deployment

October 22, 2025

This section describes how to manage your StoreFront deployment. It contains the following topics:

Topic	Description
StoreFront Management Console	Open the StoreFront management console GUI to configure StoreFront

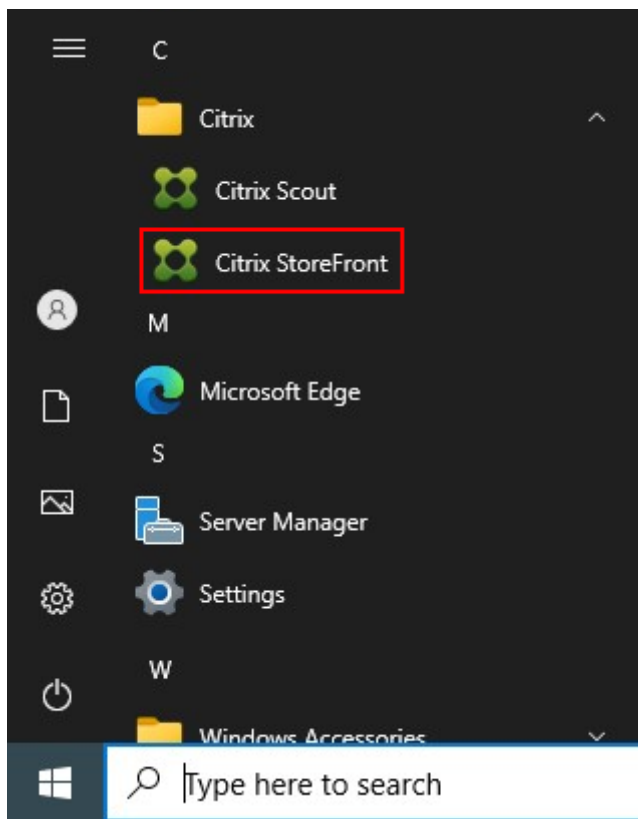
Topic	Description
StoreFront PowerShell modules	Use the StoreFront PowerShell modules to automate StoreFront configuration
Configure the base URL	Configure the base URL that users enter to connect to the deployment.
Configure server group	Add and remove servers in your StoreFront server group and propagate configuration to the other servers in the group.
Manage the subscriptions database	Choose where StoreFront store subscriptions, manage the data within the database and synchronize data between server groups.
Upgrade StoreFront	Upgrade older versions of StoreFront to this version.
Export and import the StoreFront configuration	Export configuration from one StoreFront deployment and import it into another deployment.
Default website for deployment	Configure which website users are redirected to when they go to the base URL in their web browser.
Reset a server to factory defaults	Remove all StoreFront configuration so that you can re-configure it, or add it to an existing server group.
Uninstall StoreFront	Remove StoreFront from your server

StoreFront™ Management console

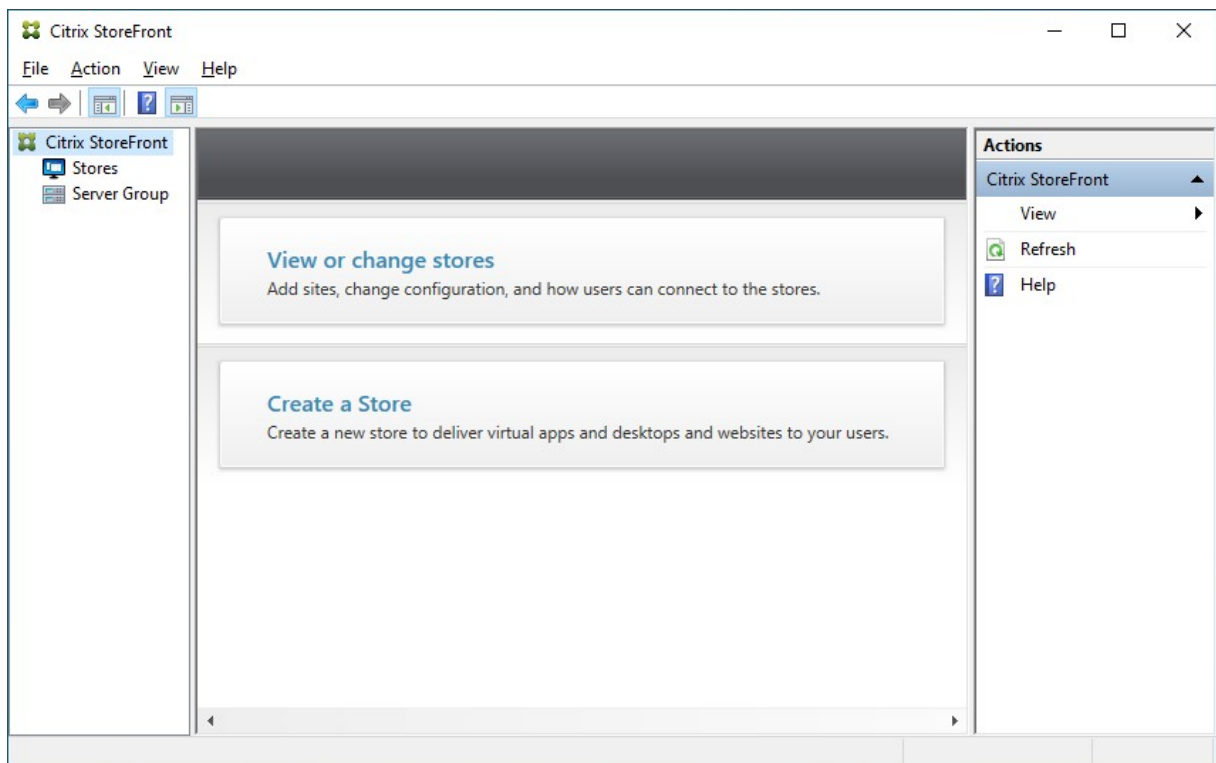
October 22, 2025

Most of aspects of StoreFront can be configured using the StoreFront management console.

To open the management console open the **Start** menu, expand the **Citrix** folder and select **Citrix StoreFront**.



This opens the StoreFront management console.



Once you have [created a deployment](#), on the left hand side there is a tree view containing the following

items:

- **Stores.** Select this to [view and manage stores](#) and [gateways](#)..
- **Server Group.** Select this to [manage the server group](#) and to configure the [base URL](#).

When you select a node in the tree view, the rest of the screen updates accordingly.

The central part of the window contains information about the stores or server group.

On the right hand side is the **Actions** pane.

Some advanced configuration tasks are not available in the management console and require the use of [StoreFront PowerShell modules](#).

StoreFront PowerShell modules

November 5, 2025

Citrix StoreFront provides a number of Microsoft Windows PowerShell version 2.0 modules that are included when you install StoreFront. With the modules, you can perform the same tasks as you would with the [StoreFront management console](#), together with tasks you cannot do with the console alone.

Note:

The StoreFront PowerShell modules are not compatible with PowerShell 6 or higher.

For the PowerShell modules reference, see [StoreFront developer documentation](#).

Get started

1. Ensure that the StoreFront management console is closed.
2. 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.
3. To use cmdlets within scripts, set the execution policy in PowerShell to RemoteSigned. For more information about PowerShell execution policy, see [Microsoft documentation](#).
4. You can use the Example scripts as a starting point.
5. Use the **Get-Help** cmdlet supplying the cmdlet name and **-Full** parameter for more information on a specific command.

Virtual Path

Cmdlets to get or create a store, website or authentication services take a **VirtualPath** parameter. This is the path to where the application is hosted within IIS. The store and website path can also be found in StoreFront management console. Typically, by convention the auth path is the same as the store path with suffix **Auth** and the website is the same as the store path with the suffix **Web**. E.g. for store virtual path **/Citrix/Store**, the auth service has path **/Citrix/StoreAuth** and the website has path **/Citrix/StoreWeb**.

E.g. to get a store service whose path is **/Citrix/Store**, run command:

```
1 Get-STFStoreService -VirtualPath '/Citrix/Store'
```

If you omit the VirtualPath then it returns all services. If there is only one service, then PowerShell treats this as a single object.

Site ID

Some cmdlets include a **SiteId** parameter. If you have multiple deployments on the same server on different IIS sites then you must specify the **SiteId**. If you only have one site then the parameter is not required.

Example scripts

StoreFront includes a few example scripts which can be found in the **%ProgramFiles%\Citrix\Receiver\StoreFront\PowerShellSDK\Examples** folder. You can use these as templates for creating your own scripts.

- ```
1 - Use the PowerShell ISE, Visual Studio Code or a similar tool to edit
 the script.
2 - Use variables to assign values that are to be reused or modified.
3 - Remove any commands that are not required.
4 - Note that StoreFront cmdlets can be identified by the prefix STF.
```

---

| Examples                          | Description                                                                                          |
|-----------------------------------|------------------------------------------------------------------------------------------------------|
| Create a Simple Deployment        | Script: creates a simple deployment with a StoreFront controller configured with a single CVAD site. |
| Create a Remote Access Deployment | Script: builds on the previous script to add remote access to the deployment.                        |

| Examples                                                      | Description                                                                                                  |
|---------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| 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. |

## Create a simple deployment

The following example shows how to create a simple deployment configured with one CVAD site.

Before you begin, make sure you follow the steps detailed in Get Started. This example can be customized to produce a script for automating StoreFront deployment.

This section explains what each part of the script 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 modern versions of PowerShell.

```

1 Param(
2 [Parameter(Mandatory=$true)]
3 [Uri]$HostbaseUrl,
4 [long]$SiteId = 1,
5 [ValidateSet("XenDesktop","XenApp","AppController","VDIinaBox
6 ")]
7 [string]$Farmtype = "XenDesktop",
8 [Parameter(Mandatory=$true)]
9 [string[]]$FarmServers,
10 [string]$StoreVirtualPath = "/Citrix/Store",
11 [bool]$LoadbalanceServers = $false,
12 [int]$Port = 80,
13 [int]$SSLRelayPort = 443,
14 [ValidateSet("HTTP","HTTPS","SSL")]
15 [string]$TransportType = "HTTP"
16)
17 # Import StoreFront modules. Required for versions of
18 # PowerShell earlier than 3.0 that do not support
19 # autoloading
20 Import-Module Citrix.StoreFront
21 Import-Module Citrix.StoreFront.Stores
22 Import-Module Citrix.StoreFront.Authentication
23 Import-Module Citrix.StoreFront.WebReceiver

```

- 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"
```

- 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 }
```

- 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 }

```

- Creates the new store service configured with one site (also known as a farm) 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 }

```

- Adds a website 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 }
```

- 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 }
```

### 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. This example can be customized using the methods described to produce a script for automating StoreFront deployment.

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 modern 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

```

- 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

```

- 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

```

- 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

```

- 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

```

- 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

**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. This example can be customized using the methods described to produce a script for automating StoreFront deployment.

**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 modern 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
```

- 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 -GatewaySTAOUrls $GatewaySTAOUrls -
 GatewayName $GatewayName
```

- 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 $OptimalGatewaySTAOUrls -PassThru
```

- Gets the store service to use the optimal gateway, register it assigning it to launches from the site 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
```

## Configure the base URL

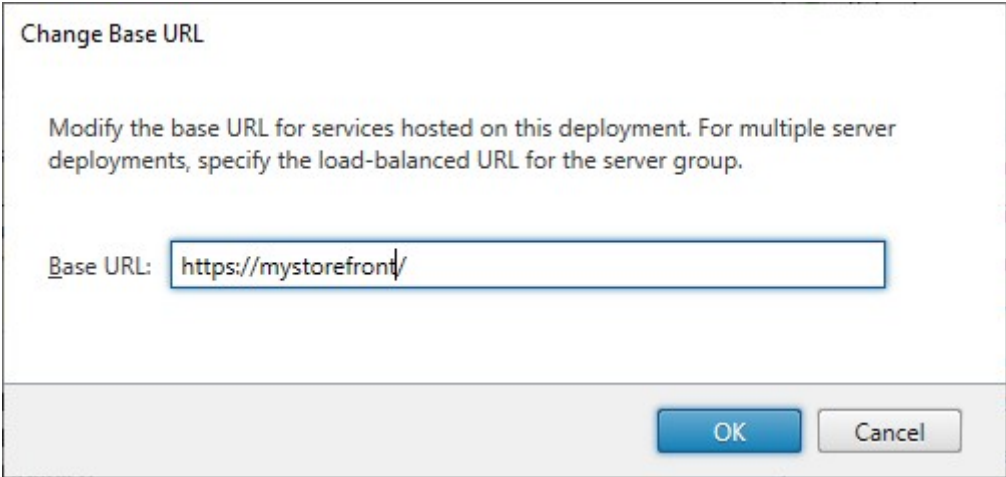
October 22, 2025

The base URL is used as the root of the URLs for the stores and other StoreFront services hosted on a deployment. You must enter the URL users use to connect directly to the deployment (not via a Citrix Gateway) e.g. <https://storefront.example.com>. The scheme must be [http](#) or [https](#). It is recommended that you always use [https](#).

- For a single server deployment without a load balancer, enter the URL of the server.
- If users connect via a load balancer, enter the URL the load balancer. You must also [enable loopback communication](#) so that StoreFront bypasses the load balancer for internal communication.

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**.



Change Base URL

Modify the base URL for services hosted on this deployment. For multiple server deployments, specify the load-balanced URL for the server group.

Base URL:

OK Cancel

## Configure server groups

October 22, 2025

For redundancy and scalability, you should deploy 2 or more identical StoreFront servers in a server group, behind a load balancer. StoreFront synchronizes configuration and favorites data between the servers.

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. Once you have completed your changes, propagate

local changes to the other servers in the server group to ensure a consistent configuration across the deployment.

## View server group

In the StoreFront management console, in the tree view on the left hand side, select **Server Group**. This shows the number of servers in the server group, the base URL, the list of servers and their synchronization status.

## Add a server to a server group

Before you install StoreFront on a server that you're adding to the group, ensure the following:

- The server you're adding must have the same version of StoreFront as other servers in the group.
- The server you're adding is co-located with the other servers in the group. Ensure low latency and a reliable connection between the servers.
- The server you're 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 aren't supported.
- IIS is configured with the same website configuration, such as physical path and site IDs, as 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](#)

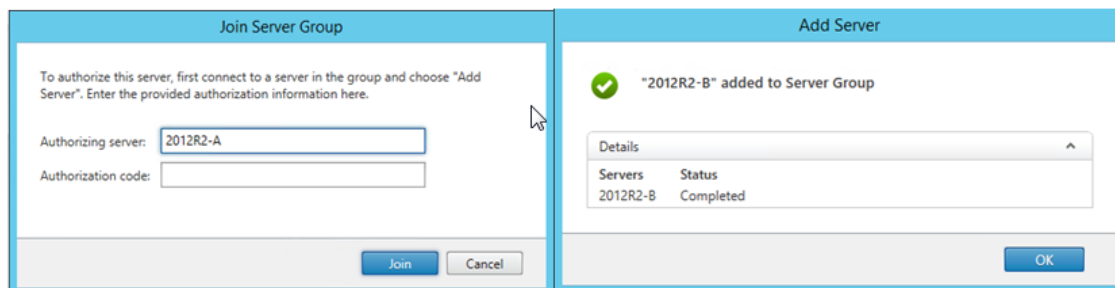
### Important:

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. 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, select **Add Server**. Make a note of the authorization code that is displayed.

2. Connect to the new server. In the StoreFront management console, select **Join existing server group**.
3. 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 select **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.



4. Add the server to the load balancer.

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.

### Remove servers from a server group

1. Remove the server from the load balancer.
2. Log in to one of the servers in the server group other than the one you wish to remove.
3. Open the StoreFront management console.
4. In the tree view Select **Server Group**
5. Select **Remove Server**.
6. Choose the server you wish to remove.

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

Once you have made configuration changes to one server, you must propagate those changes to all the other servers in the server group. 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 propagation, you cannot make any further changes until all the servers in the group have been updated.

To propagate changes, select **Propagate changes** from the actions pane.

**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`.
- For each store website, e.g. `c:\inetpub\wwwroot\Citrix\StoreWeb`, the contents of the `contrib`, `custom` and `customweb` folders. These folders are used to hold website customizations.
- 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 needing to initiate the Propagate Changes task.

## Manage the subscriptions database

October 22, 2025

When you create a store, StoreFront creates a Microsoft Extensible Storage Engine (ESENT) database locally on the server to hold favorites (also known as subscription) data. In StoreFront server group environments, each server maintains its own copy of the database. Any changes to favorites are propagated to other servers to ensure users see the same favorites regardless of which server they connect to.

Alternatively, you can store favorites in a SQL Server database. For more information, see [Store subscription data using Microsoft SQL Server](#).

To view whether a store is using a local ESENT database or a SQL server database, use the PowerShell script:

```
1 $store=Get-STFStoreService -VirtualPath '/Citrix/Store'
2 Get-STFStoreSubscriptionsDatabase -StoreService $store
```

## Managing favorites data

When using an ESENT database, you can use PowerShell to manage the favorites data. For more information, see [Manage favorites data](#). When use a SQL server database, you can use SQL to manage the records.

## Syncing favorites between server groups

Subscriptions automatically synchronize between servers in a server group. If you have multiple server groups, then you can configure Citrix Files to periodically synchronize subscriptions between server groups. For more information, see [Subscriptions synchronization](#).

## Manage subscriptions data

November 5, 2025

If you are using a local database, you can manage favorites for a store using PowerShell cmdlets.

### Purge subscription data

A folder and datastore containing favorites 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.

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 $SubsPath = "C:\Windows\ServiceProfiles\NetworkService\AppData\
13 Roaming\Citrix\SubscriptionsStore\1__Citrix_$Store*"
14
15 Stop-Service -displayname $SubsService
16
17 Remove-Item $SubsPath -Force -Verbose
18
19 Start-Service -displayname $SubsService
20
21 Get-Service -displayname $SubsService
22 }
23
24 Remove-SubscriptionData -Store "YourStore"
```

## Export subscription data

You can obtain a backup of the Store subscription data in the form of a tab separated .txt file using the cmdlet [Export-STFStoreSubscriptions](#), for example:

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
2 yourstore>"
3 Export-STFStoreSubscriptions -StoreService $StoreObject -FilePath "$env
4 :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"
```

For more information on `Restore-STFStoreSubscriptions`, see <https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/2507/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"
```

For more information on Import-STFStoreSubscriptions, see <https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/2507/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  |

---

| No of Records | Size MB |
|---------------|---------|
| 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"
```

## Store subscription data using Microsoft SQL Server

October 22, 2025

### 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 you can easily use SQL update statements 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.

**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. |
| Simpler to configure replication between different server groups using subscription syncing and pull schedules. See <a href="#">Configure subscription synchronization</a> | 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.                                                                                                                                                                                                                                                     |
| SQL unnecessary when subscription management is not needed. If the subscription data will never need updating, ESENT is likely to meet customer needs.                     | 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.                                                                                                                                                                                                                                                                                                                                               |

### Disadvantages of ESENT and SQL server

| ESENT                                                                                                                                                                                                                                                                                                                                                                | SQL                                                                                                                                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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. | 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. |

---

**ESENT**

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.

---

**SQL**

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.

Data migration from ESENT and transformation to SQL friendly format required. This process is only required once.

Extra windows servers and licenses may be needed.

Extra steps to deploy StoreFront.

---

**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.

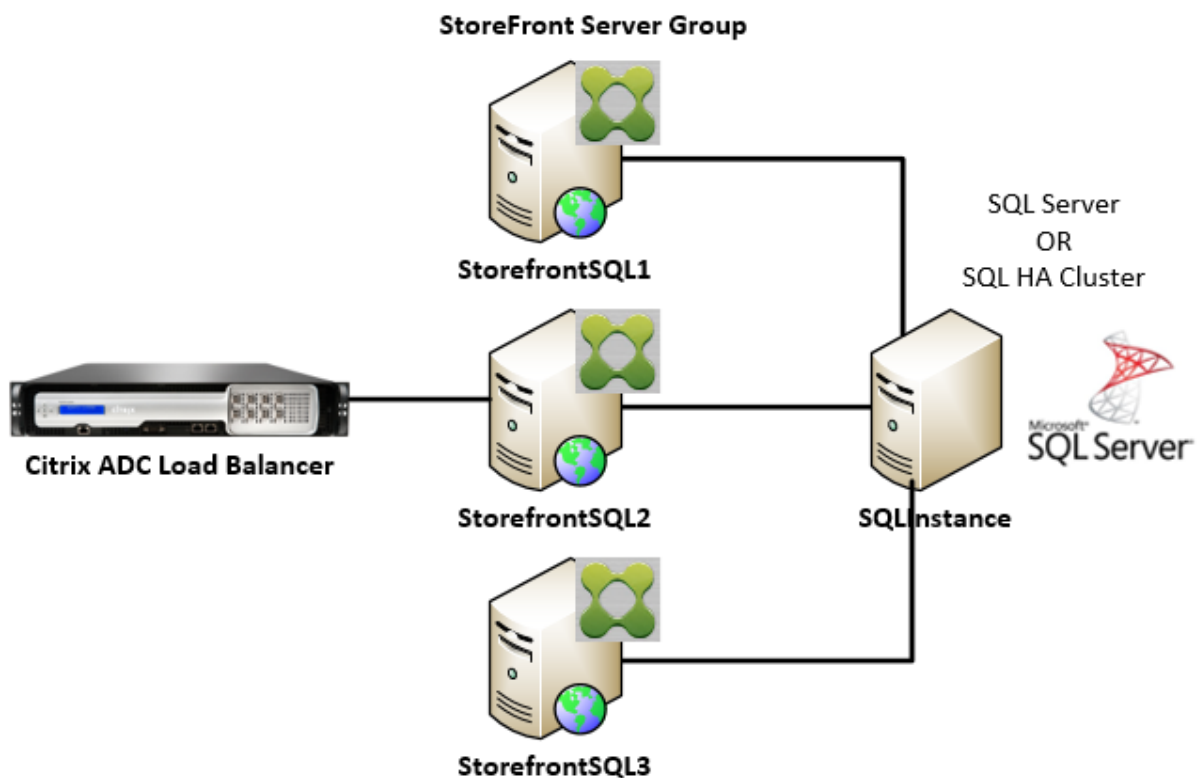
There are four scenarios you can use for storing subscription data in SQL Server:

**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.



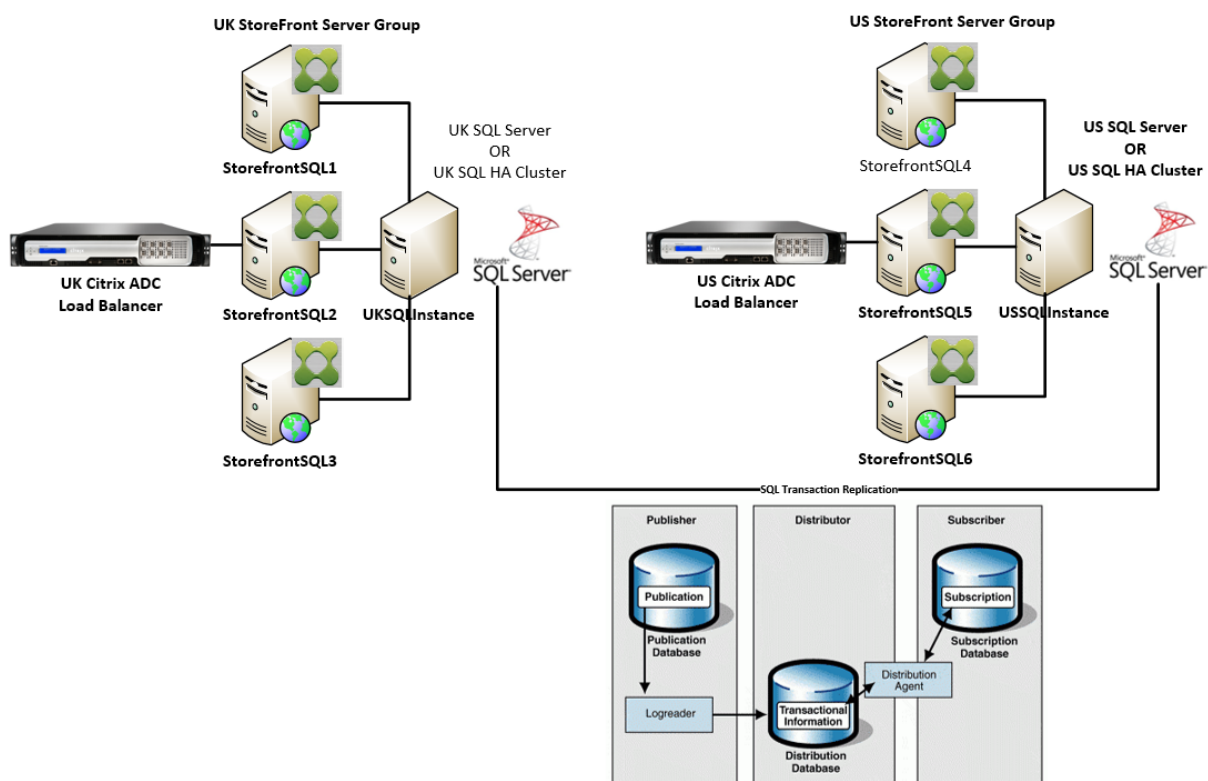
**Scenario 4: Multiple StoreFront server groups and a dedicated Microsoft SQL server instance in each data center per server group**

**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"

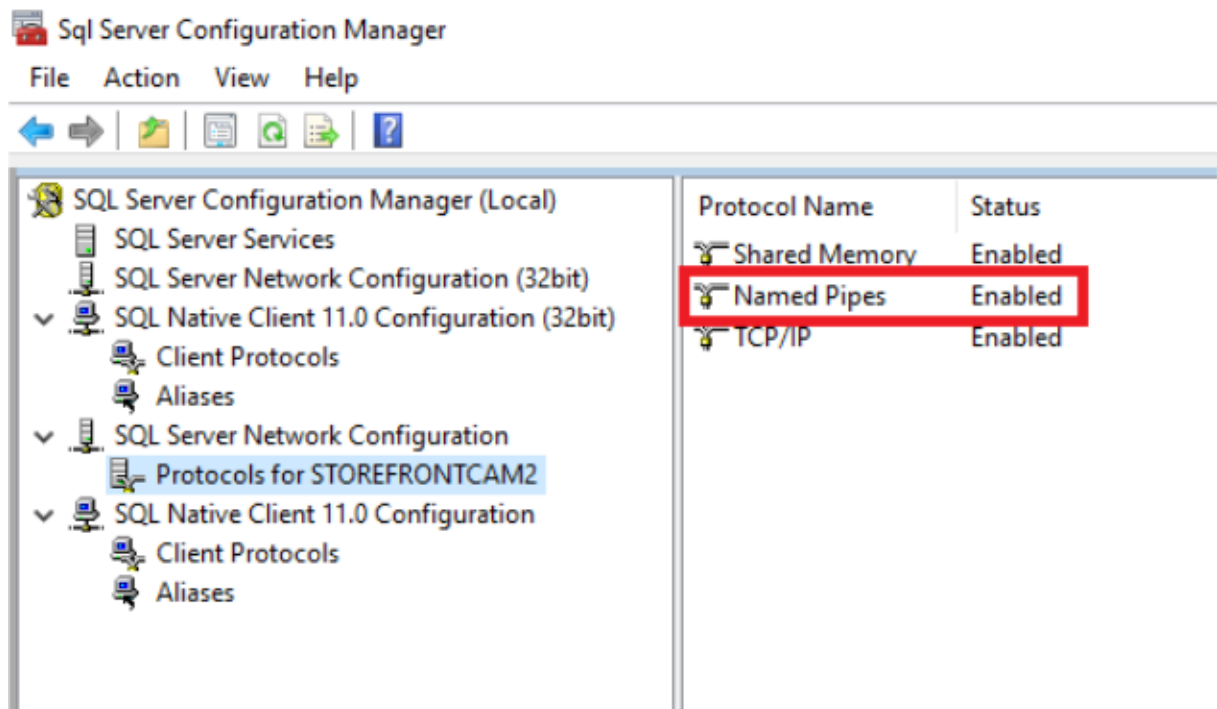
```

```

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"

```

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.



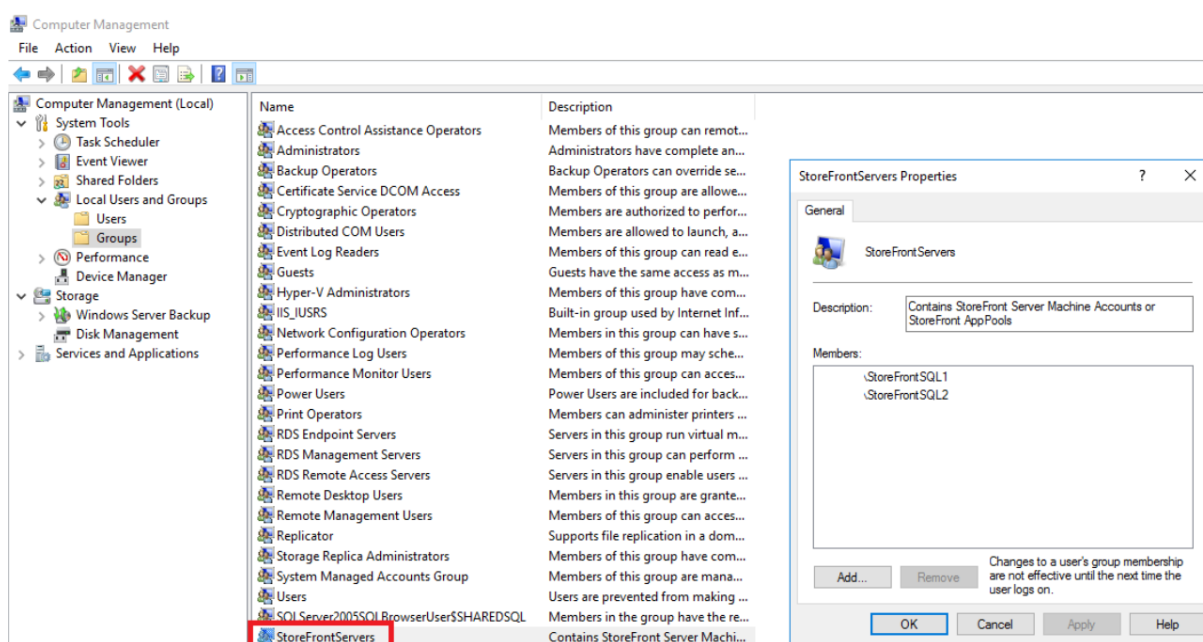
Ensure the Windows firewall rules are correctly configured to allow SQL server connections using either a specific port or dynamic ports. Refer to Microsoft documentation for how to do this in your environment.

**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.

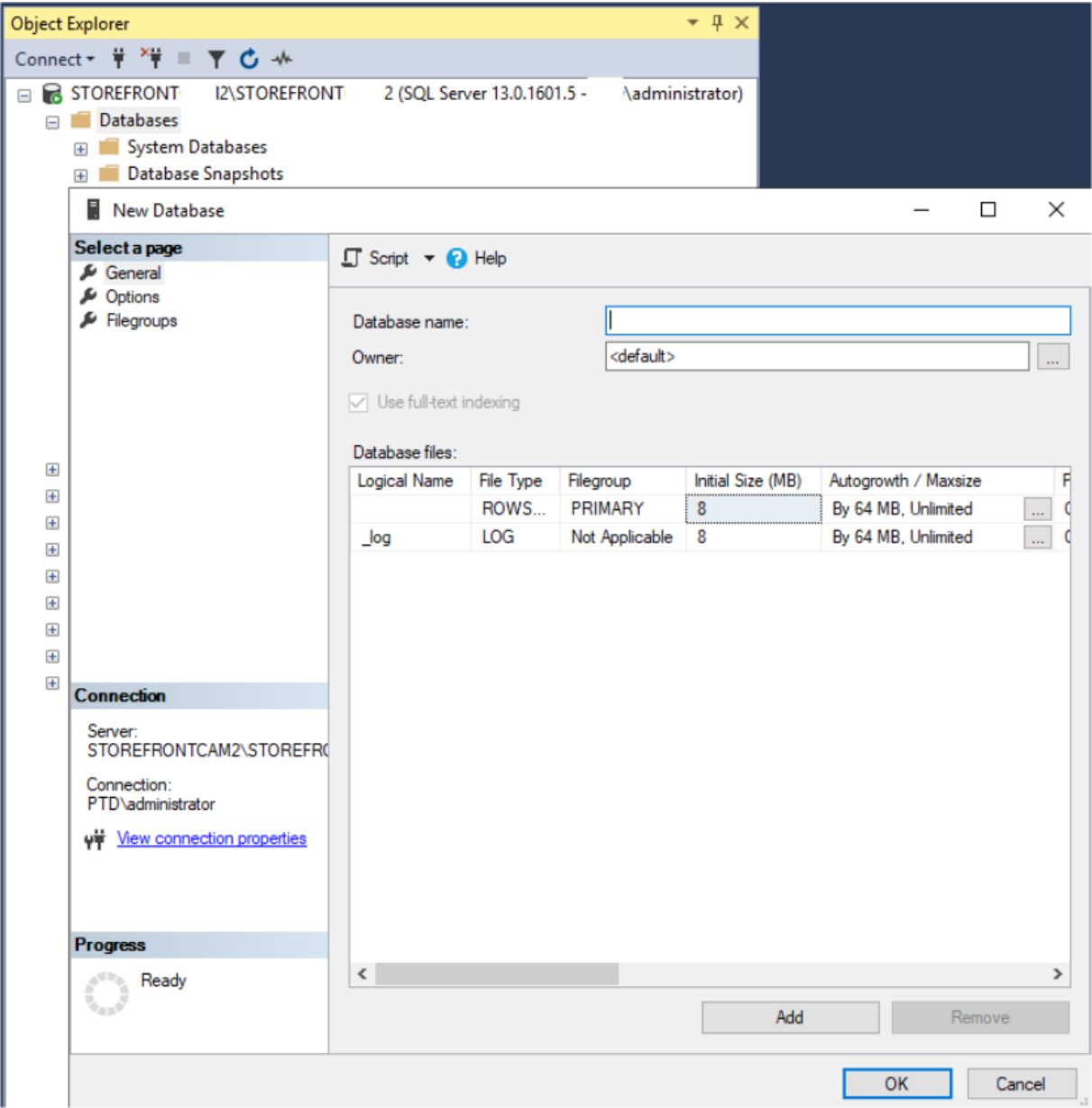
```
1 function Add-RemoteSTFMachineAccounts
2 {
```

```
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")
```

**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.

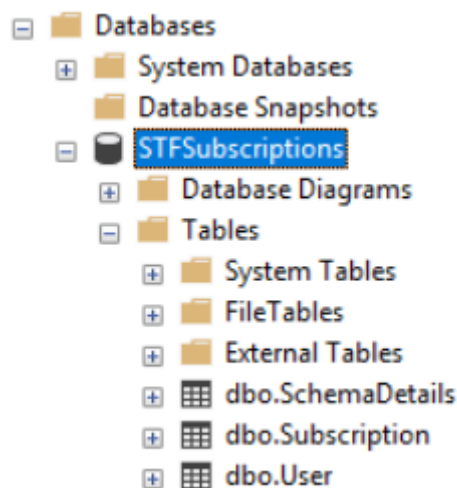
```
C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\STFSubscriptions.mdf
```

```
C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\STFSubscriptions.ldf
```

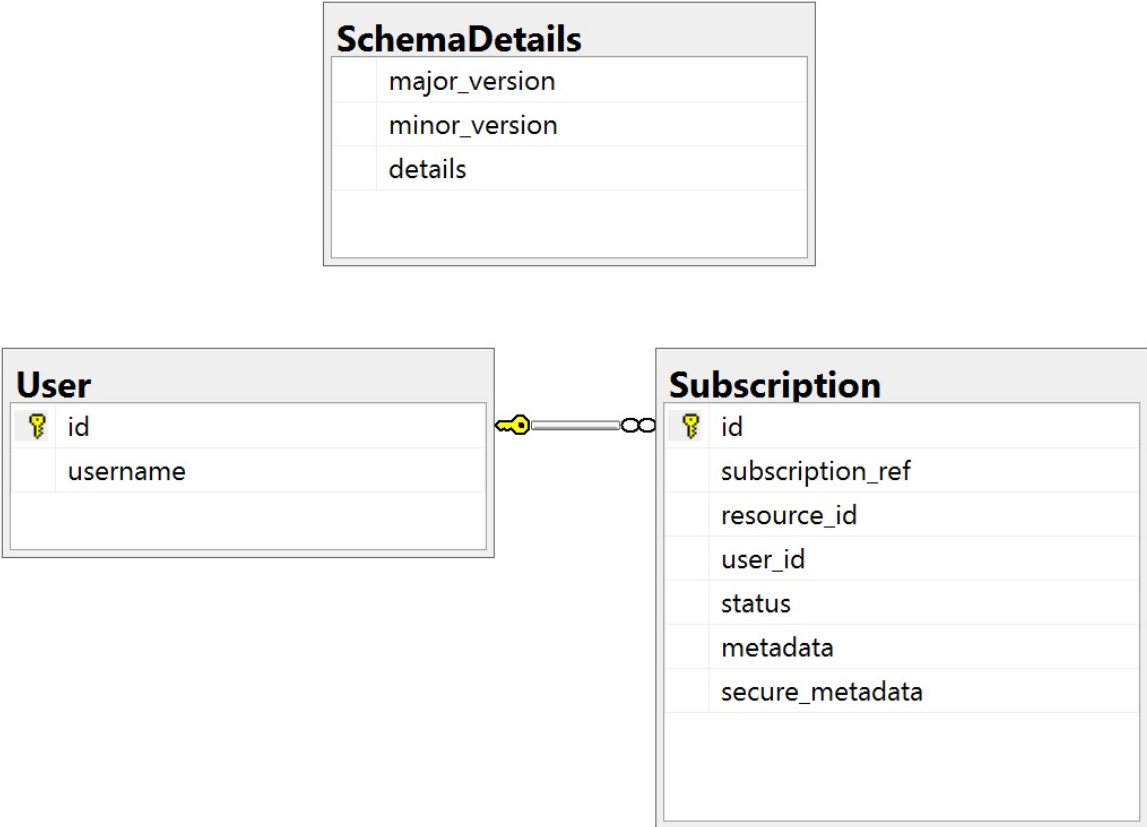
- Set the reference to your SQL server's name within the script:

```
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
```

### 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;"
```

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
```

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_ref               | resource_id                             | user_id | status | metadata                                                                                                                                                                                                      | secure_metadata |
| 1                | D0026484B489708BDC08F03A7009   | XenDesktopSSL.Netscape+ 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                | 2A3C2F8F874624C40C78B0C03110C7 | 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                | 4258EAF08102B64C0009E0E00E423  | 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                | 9632ACE317D011816779C3A26929CA | 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  | count |
|----|-----------|-------|
| 1  | S-1-5-21- | 6099  |

**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.

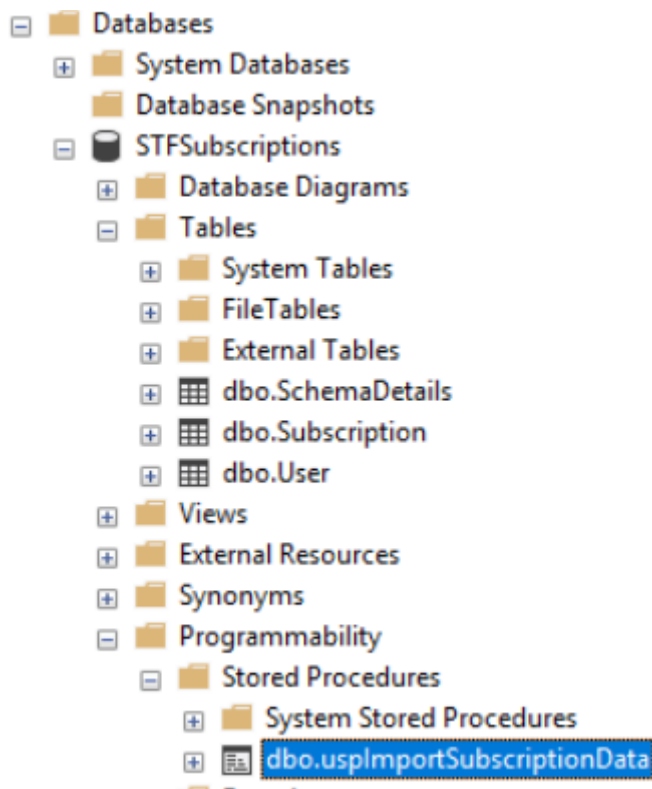
The [Create-ImportSubscriptionDataSP.sql](#) script creates a T-SQL stored procedure to bulk import the subscription data. It removes duplicate entries for each unique user so the resulting SQL data is correctly normalized and split into the correct tables.

Before executing *Create-ImportSubscriptionDataSP.sql*, change **USE [STFSubscriptions]** to match the database under which you want to create the Stored Procedure.

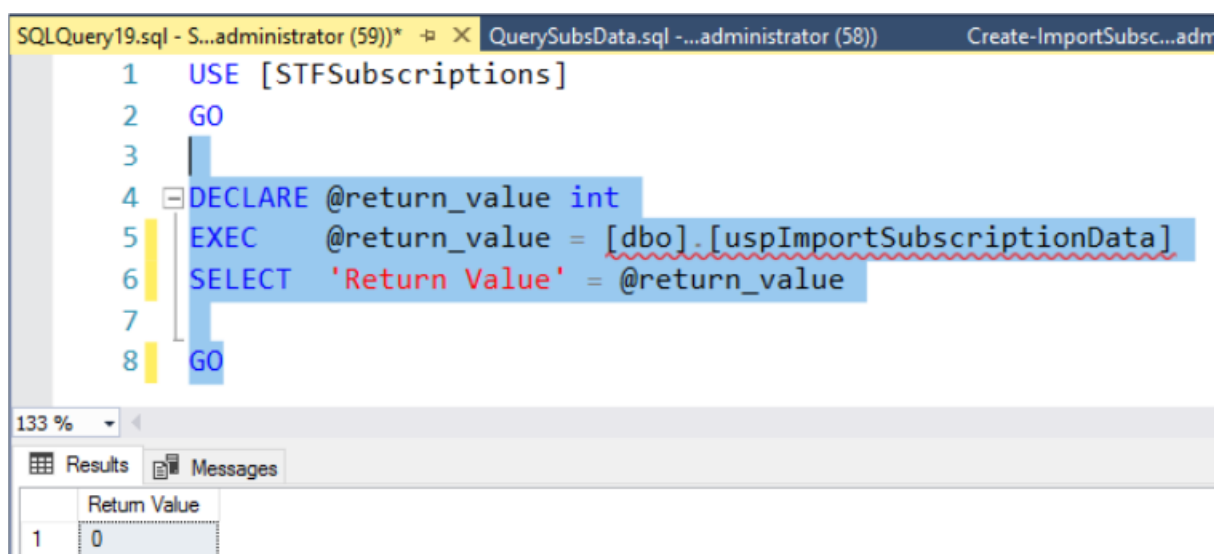
Open the *Create-ImportSubscriptionDataSP.sql* file using SQL Server Management Studio and execute the code within it. This script adds the *ImportSubscriptionDataSP* Stored Procedure to the database you created earlier.

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]

```

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]

```

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]
```

```
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'
```

```
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'
```

## 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 redun-

dant copy of the production data away from the live production database.

**Note:**

All Site names are case sensitive and must exactly match the case and name used within StoreFront.

```
1 -- Update the site name used in all subscriptions.
2 Use [STFSubscriptions]
3 UPDATE [Subscription]
4 SET [resource_id] = REPLACE(resource_id,'OldSiteName.','NewSiteName.')
5 WHERE [resource_id] LIKE 'OldDeliveryController.%'
```

```
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.%'
```

```
1 -- Delete all subscription records for a particular site
2 Use [STFSubscriptions]
3 DELETE FROM [Subscription]
4 WHERE [resource_id] LIKE 'site.%'
```

```
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.%'
```

```
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'
```

```
1 -- Delete all subscription records for an application published via a
 specific site
2 Use [STFSubscriptions]
3 DELETE FROM [Subscription]
4 FROM [Subscription]
5 WHERE [resource_id] = 'Site.Application'
```

```
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'
```

```
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)
```

## Subscriptions synchronization

November 5, 2025

StoreFront automatically synchronizes favorites, also known as 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 sites must be named identically between the synchronized Stores including the case. Failing to duplicate the site 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. Site 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
```

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"
```

- Run on UK data center StoreFront servers to pull data from the US datacenter servers:

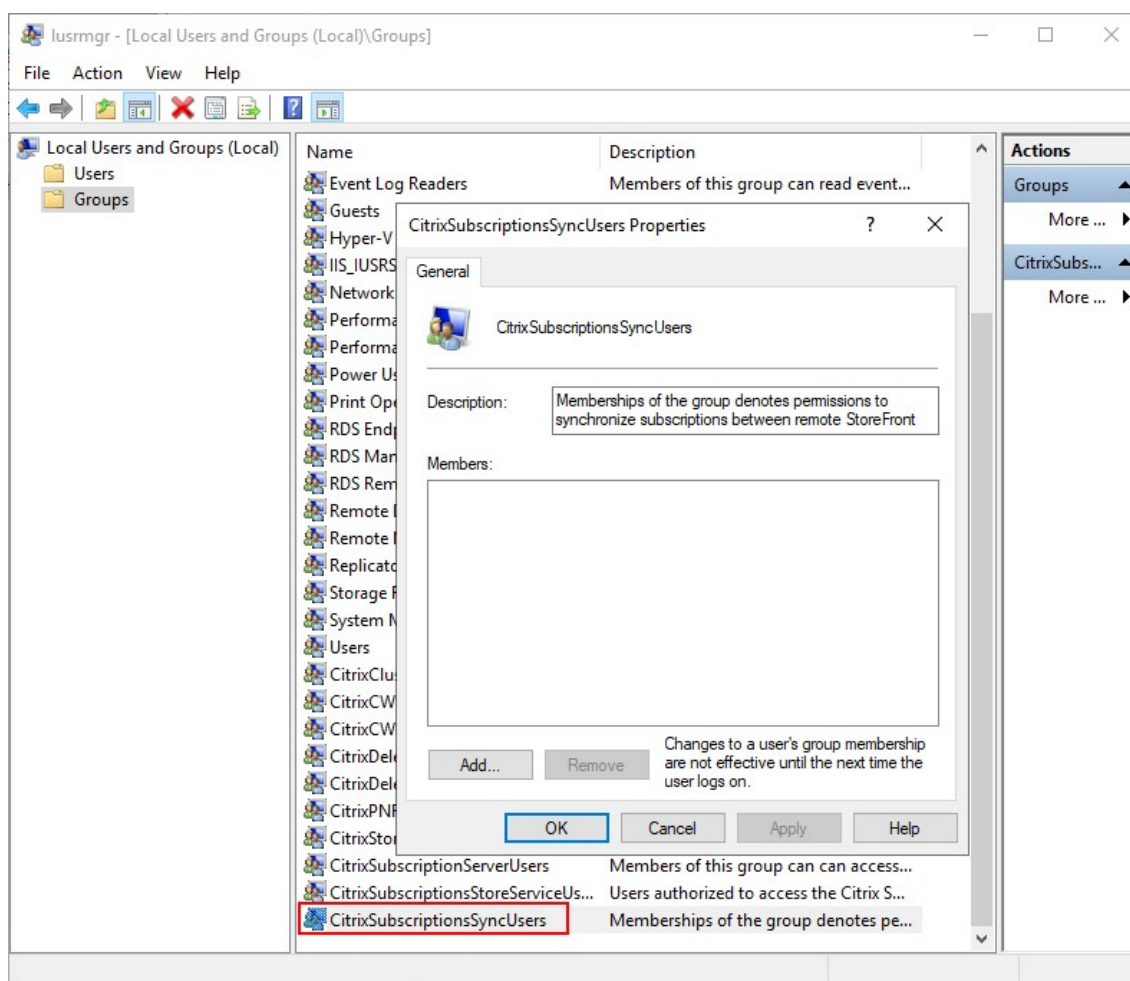
```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/"
 Citrix/Store"
2 Add-STFSubscriptionSynchronizationSource -FriendlyName "
 SyncFromUSStore" -StoreService $StoreObject -
 RemoteStoreFrontAddress "USloadbalancedStoreFront.example.
 com"
```

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)).





- 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
```

For more information about propagating changes in a multiple server StoreFront deployment, see [Configure server groups](#).

- 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
```

- 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
```

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
```

9. To list the subscription synchronization schedules currently configured for your StoreFront deployment, run the following command.

```
1 Get-STFSubscriptionSynchronizationSchedule
```

10. To list the subscription synchronization sources currently configured for your StoreFront deployment, run following command.

```
1 Get-STFSubscriptionSynchronizationSource
```

## Upgrade StoreFront™

October 22, 2025

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.

### Supported upgrade paths

You can upgrade to StoreFront 2507 from:

- StoreFront 2503.1
- StoreFront 2503
- StoreFront 2407
- StoreFront 2402 LTSR (any CU)
- StoreFront 2203 LTSR (any CU)
- StoreFront 1912 LTSR CU10

It is not possible to upgrade from 2402 CU2 or later CUs to 2407 or 2411.

## Good to know

- 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 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 upgrading from a supported version.
- 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` or `C:\inetpub\wwwroot\Citrix\<StoreName>Auth\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 server group during scheduled maintenance downtime**

This describes upgrading a StoreFront server group of multiple servers, 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. Upgrade each server by following the instructions in Upgrade a single StoreFront server.
3. Check all servers are functioning correctly.
4. 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.

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 5, 7, 10 and 11 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.

## Troubleshoot upgrade issues

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](#).

## Export and import the StoreFront configuration

October 22, 2025

### 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 <b>-Credential</b> at the same time as the <b>-NoEncryption</b> parameter. Example: \$CredObject |
| -NoEncryption (Switch)            | Specify that the backup archive should be an unencrypted .zip. Do not use <b>-NoEncryption</b> at the same time as the <b>-Credential</b> 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 <b>-Credential</b> or <b>-NoEncryption</b> 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://&lt;importingserver&gt;.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> |
| -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>                                |

| Parameter              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -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: \$env:userprofile\desktop<br>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

```

### 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

```

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"
```

**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.

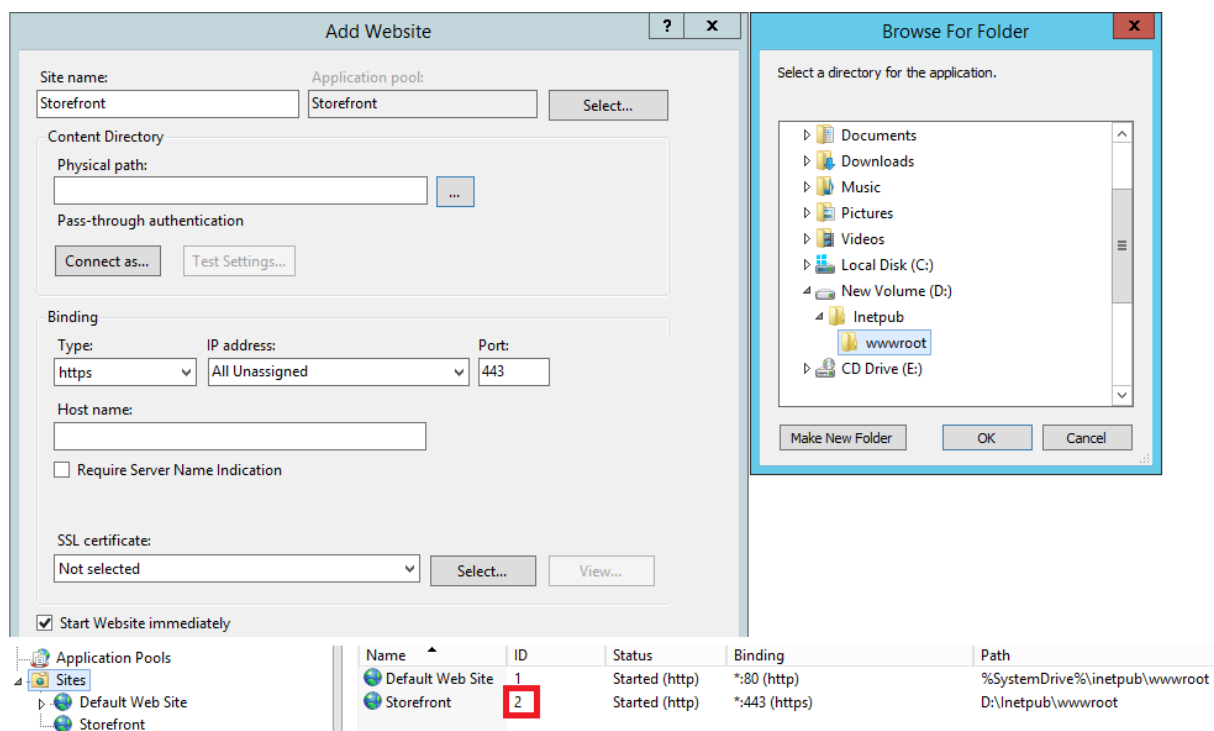
```
1 Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -
 zipFileName "backup" -NoEncryption
```

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"
```

**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.

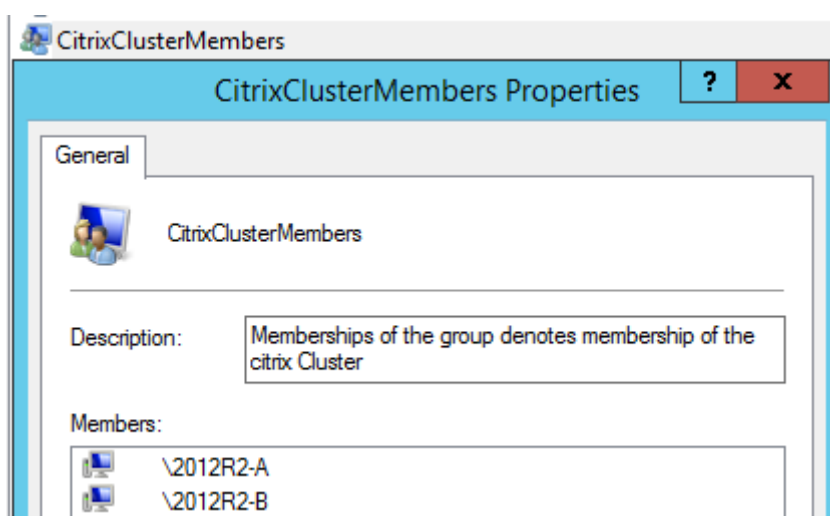
```
1 Import-STFConfiguration -configurationZip "$env:userprofile\
 desktop\backup.ctxzip" -HostBaseURL "https://serverB.example.
 com"
```

## Server group scenarios

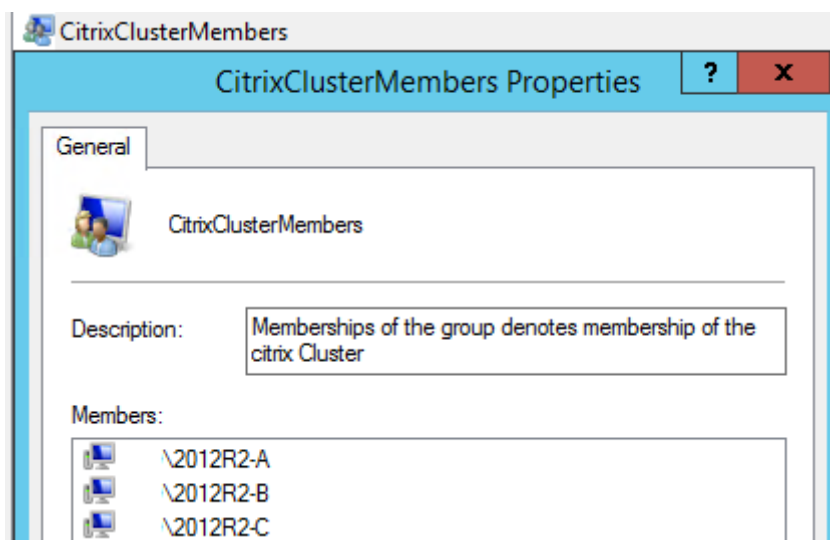
### Scenario 1: Backup an existing server group configuration and restore it later onto the same server group deployment

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 configuration 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"
```

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"
```

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"
```

### 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)
```

Export the configuration to backup.ctxzip which is an encrypted zip file.

```
1 Export-STFConfiguration -targetFolder "$env:userprofile\desktop\" -
 zipFileName "backup" -Credential $CredObject
```

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"
```

#### 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
```

## Default website for deployment

October 22, 2025

When users open the base URL in their web browser, you can configure StoreFront to redirect the user to a particular website.

1. Open the StoreFront management console.
2. From the **Actions** pane, select **Set default website for deployment**.
3. If you wish to set a default website then
  1. Select **Set a default website for server**
    1. Select a **Store**
      1. Select a **Website path**.
4. Select **OK** to save the changes.

**Set default website**

Select which website the user gets redirected to when they open the base URL in their browser.

☒ Set a default website for server

Base URL:

Store:

Website path:

OK Cancel

## Reset a server to factory defaults

November 5, 2025

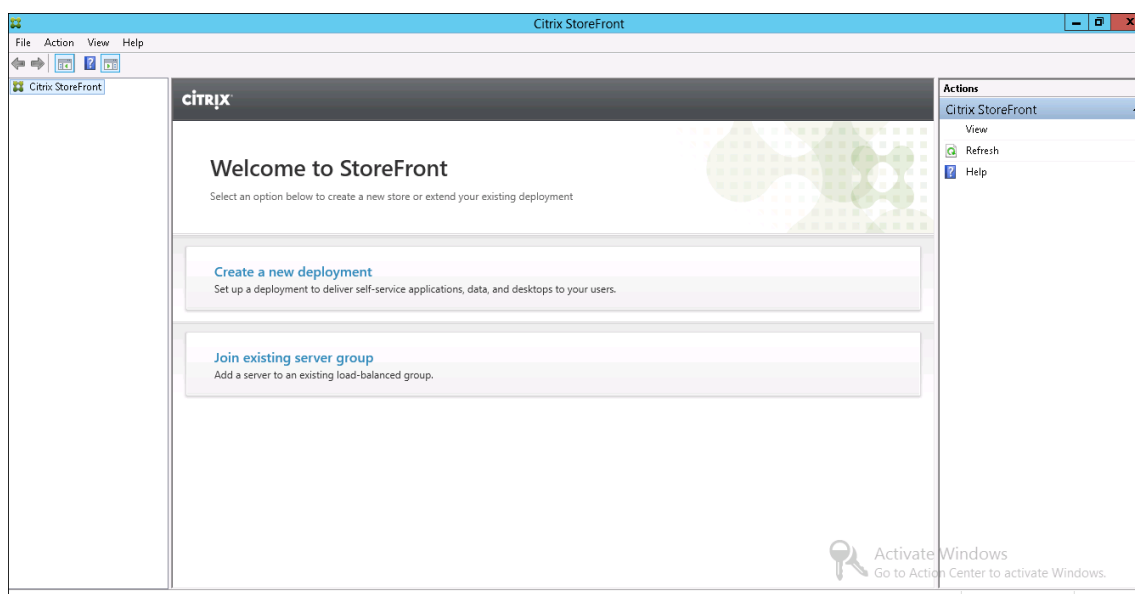
In some situations, there is a need to reset a StoreFront installation to its initial installation state. This is necessary, for example, before you can re-add a StoreFront server to a server group. A manual uninstall and reinstall can be performed, but this is more time consuming and may cause other unforeseen issues. Instead you can use [PowerShell modules](#) to reset configuration to defaults.

1. Ensure that the StoreFront management console is closed.
2. Open a PowerShell console.
3. Run cmdlet [Clear-STFDeployment](#).

```
1 Clear-STFDeployment -Confirm $False
```

4. 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

October 22, 2025

In addition to the product itself, uninstalling StoreFront removes the authentication service, stores, websites, 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.
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 the **Web Server (IIS)** Role. For more information, see [Microsoft learn](#).
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](#).

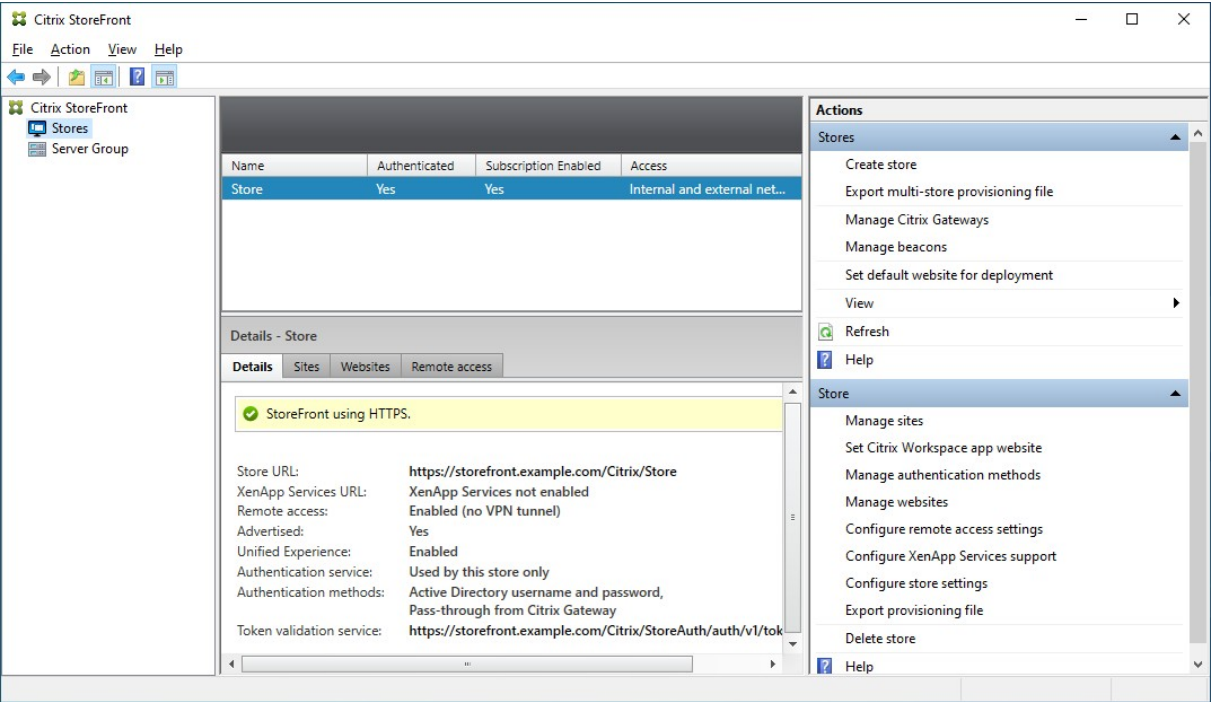
## Manage stores

October 22, 2025

In Citrix StoreFront, you create one or more stores to allow end-users to access their resources. Each store defines how the user authenticates, which resources are aggregated and the appearance. End users can open these stores through a web browser or by adding them to their locally installed Citrix Workspace app.

### View Stores

1. From the [management console](#), select the **Stores** node in the left pane.
2. Select the store you wish to view.



In the **Details** pane you can view the following tabs:

| Tab           | Detail                                                             |
|---------------|--------------------------------------------------------------------|
| Details       | Gives store details such as the URL and authentication methods     |
| Sites         | Lists all sites that have been configured for the store            |
| Websites      | Lists all <a href="#">websites</a> configured for the store.       |
| Remote Access | Details of whether remote access is enabled using a Citrix Gateway |

Create a store

From the **Actions** pane **Stores** section, press **Create store**. For more details, see [Create Store](#).

Configure store

From the Actions pane **Store** section, you can perform the following store configuration actions:

| Action                                           | Detail                                                                                                                                                                                                                                           |
|--------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Manage sites</a>                     | Add and remove sites.                                                                                                                                                                                                                            |
| <a href="#">Set Citrix Workspace app website</a> | Configure which website is used when accessing the store using Citrix Workspace app                                                                                                                                                              |
| <a href="#">Manage authentication methods</a>    | Choose which methods users can use to authenticate to the store                                                                                                                                                                                  |
| <a href="#">Manage websites</a>                  | Manage the website used to access the store                                                                                                                                                                                                      |
| <a href="#">Configure remote access settings</a> | Configure access to stores through Citrix Gateway for users connecting from public networks.                                                                                                                                                     |
| Configure XenApp® services support               | Enable or disable the XenApp services URL                                                                                                                                                                                                        |
| <a href="#">Configure store settings</a>         | Opens the Configure store settings windows where you can configure <a href="#">Favorites</a> , <a href="#">Kerberos Delegation</a> , <a href="#">Optimal HDX routing</a> , <a href="#">Advertise Store</a> and <a href="#">Advanced Settings</a> |

You can perform the following advanced store configuration outside of the management console:

| Task                                                       | Detail                                                                      |
|------------------------------------------------------------|-----------------------------------------------------------------------------|
| <a href="#">Default ica settings</a>                       | Configure HDX settings by adding them to default.ica                        |
| <a href="#">Citrix Workspace app Configuration</a>         | Use StoreFront to configure Citrix Workspace app                            |
| <a href="#">Configure Federated authentication service</a> | Configure Federated authentication service (FAS) for single sign-on to VDAs |

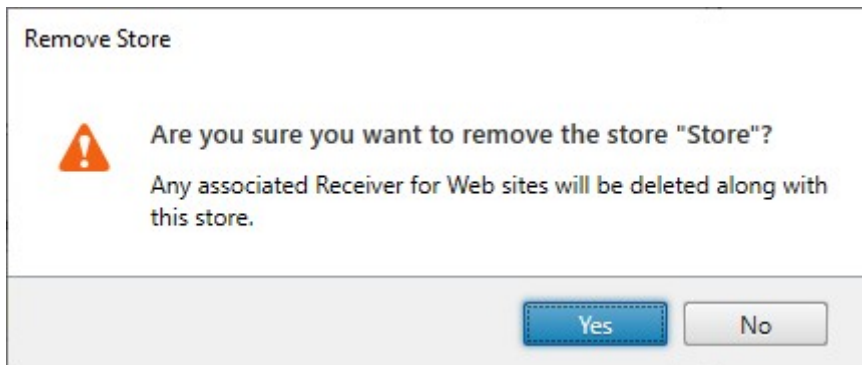
## Export provisioning files

You can generate files containing connection details for one or multiple stores, including any Citrix Gateway deployments and beacons configured for the store. For more information, see [Export provisioning files](#).

## Delete a store

To delete a store:

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



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

## Create store

November 5, 2025

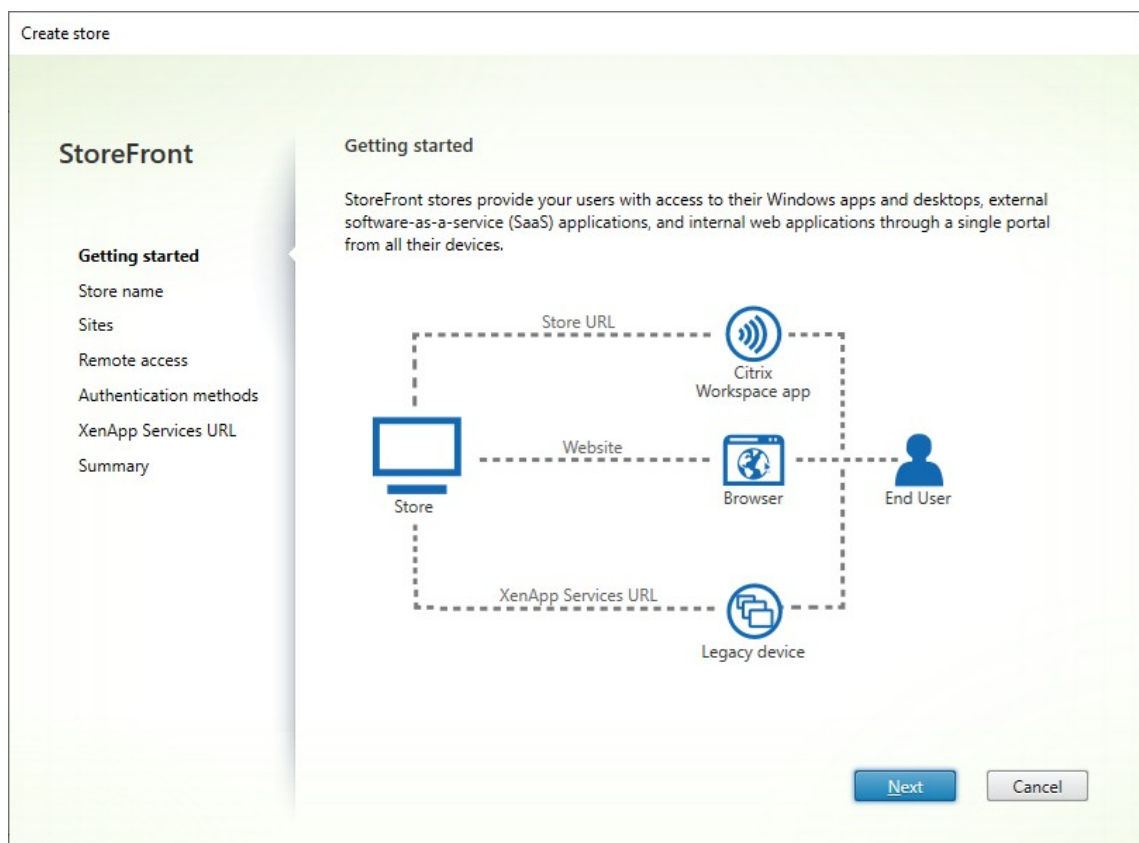
You can create as many stores as you need; for example, you can create a store for a particular group of users or to group together a specific set of resources.

### 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 non-domain-joined servers.)

Create store

## StoreFront

- ✓ Getting started
- Store name**
- Sites
- 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 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:

☐ Do not require authentication when accessing this store.  
Unauthenticated users can access the store without presenting credentials.

### Website settings

☐ Set this website as the default for this deployment  
If selected, when a web browser goes to the deployment's base URL, it is redirected to this website.

[Back](#) [Next](#) [Cancel](#)

Click **Next**

3. On the **Sites** tab, add sites for your virtual desktops and applications. For more details, see [Manage sites](#)

Create store

StoreFront

✓ Getting started

✓ Store name

**Sites**

Remote access

Authentication methods

XenApp Services URL

Summary

Sites

Specify the sites for this store.

| Name   | Type                                     | Servers             |
|--------|------------------------------------------|---------------------|
| London | Citrix Virtual Apps and Desktops or D... | ddc1.london.exam... |

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 the Citrix StoreFront console, specifically the 'Remote access' tab. On the left, a sidebar lists the steps: 'Getting started', 'Store name', 'Sites', 'Remote access' (which is highlighted), 'Authentication methods', 'XenApp Services URL', and 'Summary'. The main area contains instructions and configuration options for remote access. It includes a checkbox to 'Enable remote access', which is checked. Below this, there are two radio button options for the level of access: '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 'Citrix Gateway' list shows 'netscaler-01' as the selected gateway. An 'Add...' button is present below the list. The 'Default Gateway' dropdown also shows 'netscaler-01'. At the bottom right, there are 'Back', 'Next', and 'Cancel' buttons.

Create store

**StoreFront**

- ✓ Getting started
- ✓ Store name
- ✓ Sites
- Remote access**
- Authentication methods
- XenApp Services URL
- Summary

**Remote access**

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.

☒ 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 must install the Citrix Access client to establish a full VPN tunnel.

Citrix Gateway: ☒ netscaler-01 ⓘ

Default Gateway: netscaler-01 ▼

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
- ✓ Sites
- ✓ 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"/> Active Directory username and password                       |
| <input type="checkbox"/> SAML Authentication                                                     |
| <input type="checkbox"/> Domain pass-through<br>Can be enabled / disabled separately on websites |
| <input type="checkbox"/> Smart card<br>Can be enabled / disabled separately on websites          |
| <input type="checkbox"/> HTTP Basic                                                              |
| <input checked="" 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 select **Enable XenApp Services URL**, otherwise clear it.

Create store

**StoreFront**

- ✓ Getting started
- ✓ Store name
- ✓ Sites
- ✓ Remote access
- ✓ Authentication methods
- XenApp Services URL**
- Summary

**Configure XenApp Services URL (Deprecated)**

Enable a XenApp Services URL to allow legacy devices to connect to the store.

☒ **Enable XenApp Services URL**  
URL: `https://storefront.example.com/Citrix/store2/PNAgent/config.xml`

☐ **Make this the default store for XenApp Services**  
XenApp Services will use this store to deliver resources.

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

Click **Create**

**Note:**

XenApp services is deprecated and will be removed from a future release.

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

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

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 site. Further sites must be configured separately.

## Manage sites

November 19, 2025

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

### View sites

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 sites**.

### View sites using PowerShell

To view sites using [PowerShell](#), run cmdlet [Get-STFStoreFarm](#).

### Add site

#### Add sites for Citrix Virtual Apps and Desktops™

1. In the **Manage sites** 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 or DaaS**.
4. Under **Servers** for each DDC, click **Add** and enter the address of the DDC (or corresponding load balancer).
  - If you have placed load balancer(s) in front of the DDCs then enter the address of the load balancer(s). If you are not using a load balancer then list each DDC individually.
  - Include at least 2 DDCs for redundancy.

- If your servers are using HTTPS (recommended), ensure that the names you specify in the servers list match exactly (including the case) the names on the certificates for those servers.
5. Optionally select **Servers are load balanced**. If selected, StoreFront randomly selects a server. If cleared, StoreFront uses the first server on the list unless it is unavailable, in which case it proceeds down the list until it finds a responsive server. You can use the up and down arrows to define the priority order.
- If all DDCs have similar latencies then it is recommended that you select **Servers are load balanced** so that StoreFront distributes the load across all DDCs.
  - If you have a multi-zone geographically diverse deployment where DDCs have different latencies, you may wish to place those with the lowest DDCs at the top of the list and clear **Servers are load balanced**, so StoreFront prefers servers with lower latency. Consider using a separate load balancer to distribute the load between different DDCs in the same location.
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 (not recommended), 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 TLS connections (recommended), select **HTTPS**. You must [Enable TLS on Delivery Controllers](#) or on the load balancers in front of the DDCs.

The following TLS 1.3 cipher suites are supported:

- TLS\_AES\_256\_GCM\_SHA384
- TLS\_AES\_128\_GCM\_SHA256

The following TLS 1.2 cipher suites are supported:

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256

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.
8. Press **OK**

**Add site**

Display name:

Type: ☒ Citrix Virtual Apps and Desktops or DaaS  
☐ Secure Private Access

Servers (load balanced):

☒ Servers are load balanced

Transport type:

Port:

---

**Advanced settings**  
 Configure bypass durations and other advanced settings using the 'Settings' dialog.

9. If you have configured [Security keys](#) (recommended), then you must add the key using PowerShell. For example:

```
1 $store = Get-STFStoreService -VirtualPath [path to store]
2 $farm = Get-STFStoreFarm -StoreService $store -FarmName [site name]
3 Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true -
 XMLValidationSecret [Security key]
```

### Add sites for Citrix Desktops as a Service

1. In the **Manage sites** 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 or DaaS**.

4. Under **Servers** for each Cloud Connector, click **Add** and enter the name of the Cloud Connector (or corresponding load balancer).
  - If you have placed a load balancer in front of the Cloud Connectors or DDCs then enter the name of the load balancer. If you are not using a load balancer then list each DDC or Cloud Connector individually.
  - If you have multiple resource locations, Citrix recommends that you add the Cloud Connectors from all resource locations containing VDAs so that in the event of an outage StoreFront can use the Local Host Cache to launch VDAs at the appropriate location.
  - If you are using a load balancer then it is important that you use a separate load balancer for each resource location. If a load balancer fronts servers in multiple resource locations then this does not matter in normal operation. However in Local Host Cache mode, it would prevent StoreFront from being able to direct launch requests to the correct resource location, resulting in failed launches.
  - If your servers are using HTTPS (recommended), ensure that the names you specify in the servers list match exactly (including the case) the names on the certificates for those servers.
5. Optionally select **Servers are load balanced**. If selected, StoreFront randomly selects a server. If cleared, StoreFront uses the first server on the list unless it is unavailable, in which case it proceeds down the list until it finds a responsive server. You can use the up and down arrows to define the priority order.
  - If all servers have similar latencies then it is recommended that you select **Servers are load balanced** so that StoreFront distributes the load across all DDCs.
  - If you have a multi-zone geographically diverse deployment where DDCs have different latencies, you may wish to place those servers with the lowest latency at the top of the list and clear **Servers are load balanced**, so StoreFront prefers servers with lower latency. Consider using a separate load balancer to distribute the load between different servers in the same resource location or zone.
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 (not recommended), 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**. You must [configure the Cloud Connectors for HTTPS](#).

The following TLS 1.3 cipher suites are supported:

- TLS\_AES\_256\_GCM\_SHA384
- TLS\_AES\_128\_GCM\_SHA256

The following TLS 1.2 cipher suites are supported:

- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256

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.

8. Press **OK**.

**Add site**

Display name:

Type: ☒ Citrix Virtual Apps and Desktops or DaaS  
☐ Secure Private Access

Servers (load balanced):

☒ Servers are load balanced

Transport type:

Port:

---

**Advanced settings**  
Configure bypass durations and other advanced settings using the 'Settings' dialog.

9. If you have configured [Security keys](#) (recommended), then you must add the key using PowerShell. For example:



```
1 $store = Get-STFStoreService -VirtualPath [Path to store]
2 $farm = Get-STFStoreFarm -StoreService $store -FarmName [Site name]
3 Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true -
 XMLValidationSecret [Security key]
```

## Add sites for Citrix Secure Private Access

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

1. Navigate to **Stores > Manage sites** on StoreFront.
2. Select **Add**.
3. In the **Add site** 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 (not recommended).
  - **HTTPS**: sends data over secure HTTPS connections (recommended) using 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. Select **OK**.

## Add a site using PowerShell

To add a site, also known as a farm, run cmdlet [Add-STFStoreFarm](#)

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

## Edit a site

In the **Manage sites** screen, select a site and click **Edit**.

**Warning:**

If you rename a site then:

- The site is deleted from any [Optimal HDX routing](#) configuration. You must add the site back into your Optimal HDX routing configuration.
- Any user favorites [Favorites](#) for that site disappear (unless you are using multi-site aggregation). This is because the favorite record references the site by name. The favorite records are not deleted so if you rename the site back to its original name then the favorites re-appear. To fix this, if you are using a SQL server database you can update the records in the database. Otherwise you can export the favorites, correct the names and re-import. For more information, see [manage subscription data](#).

**Edit a site using PowerShell**

To modify a site using PowerShell, run cmdlet [Set-STFStoreFarm](#)

**Delete a site**

In the **Manage sites** screen, select a site and click **Remove**.

**Delete a site using PowerShell**

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

**Health check and 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. This avoids delays trying to connect to servers that are unavailable.

Use these parameters to specify the duration of the bypass behavior:

- **Background health-check polling period** - Specifies how often StoreFront checks whether each server is available. Default is 1 minute. To configure this see [Background health check polling period](#).
- **Bypass duration** - When the background health check is enabled, this should be set to at least the polling period but beyond that the value has no impact. If background health-check is disabled (not recommended) then the servers will be bypassed until the duration expires. Defaults to 60 minutes.

- **All failed bypass duration** - Only used when background health-check is disabled (not recommended). Specifies a reduced duration in minutes that StoreFront uses instead of **Bypass duration** if all servers for a particular site are being bypassed. The default is 0 minutes meaning that StoreFront does not bypass any servers.

### To change the bypass parameters

Normally there is no need to modify these settings.

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 sites**.
4. Select a controller, click **Edit**, and then click **Settings** on the **Edit site** 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 sites

By default, users accessing a store see an aggregate of all the resources available to them from all the sites 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 sites. In addition, within a site, applications may be filtered by user group within Citrix Virtual Apps and Desktops Studio configuration.


To configure specific sites for particular user groups:


1. From the **Manage sites** screen, under **User mapping and multi-site aggregation configuration**, click **Configure**. This option is only available if two or more sites 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** No mappings  
Use this setting to provide access to deployments based on user's membership of Active Directory groups.

 **Aggregate resources** No aggregation  
Use this optional setting to help de-duplicate overlapping resources across multiple controllers. At least one user mapping must be defined before aggregating resources.

OK Cancel

2. Click **Map users to sites**. 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

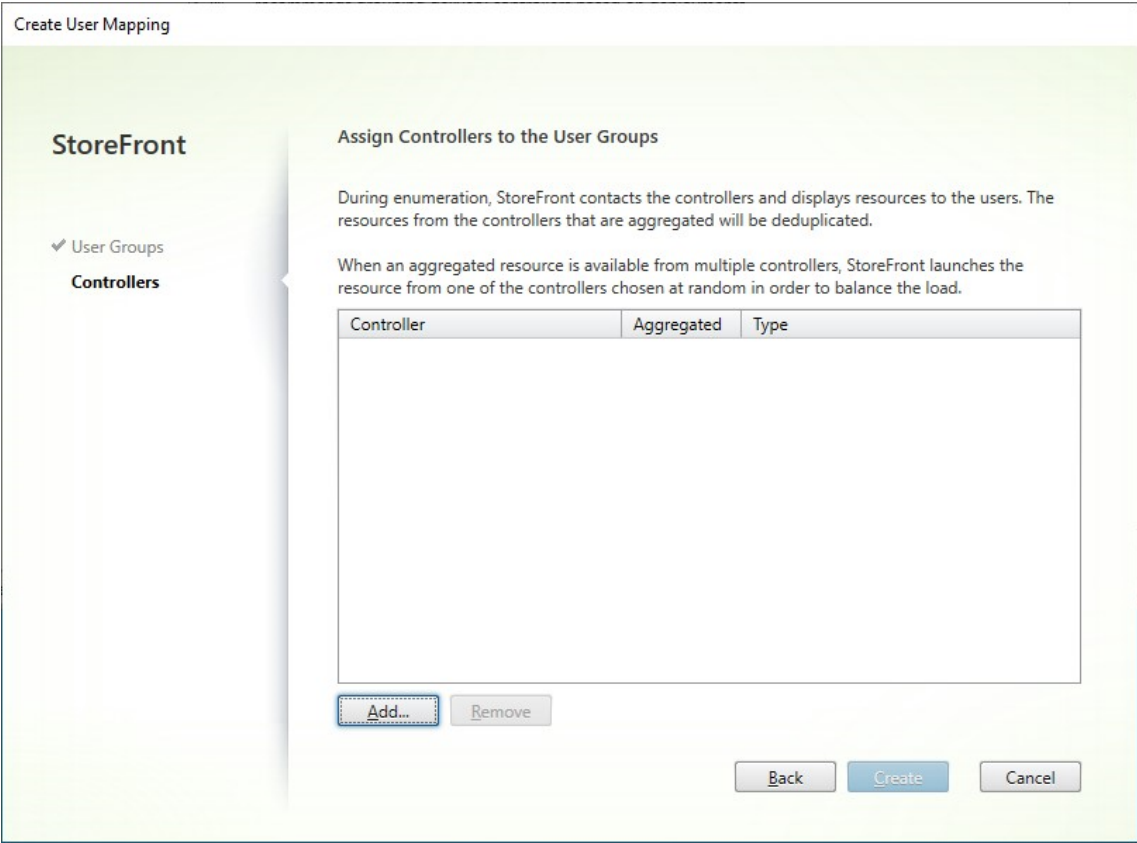
☒ Specific User Groups

XAEEAAD\DesktopOnly Users

Add... View Remove

Next Cancel

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



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

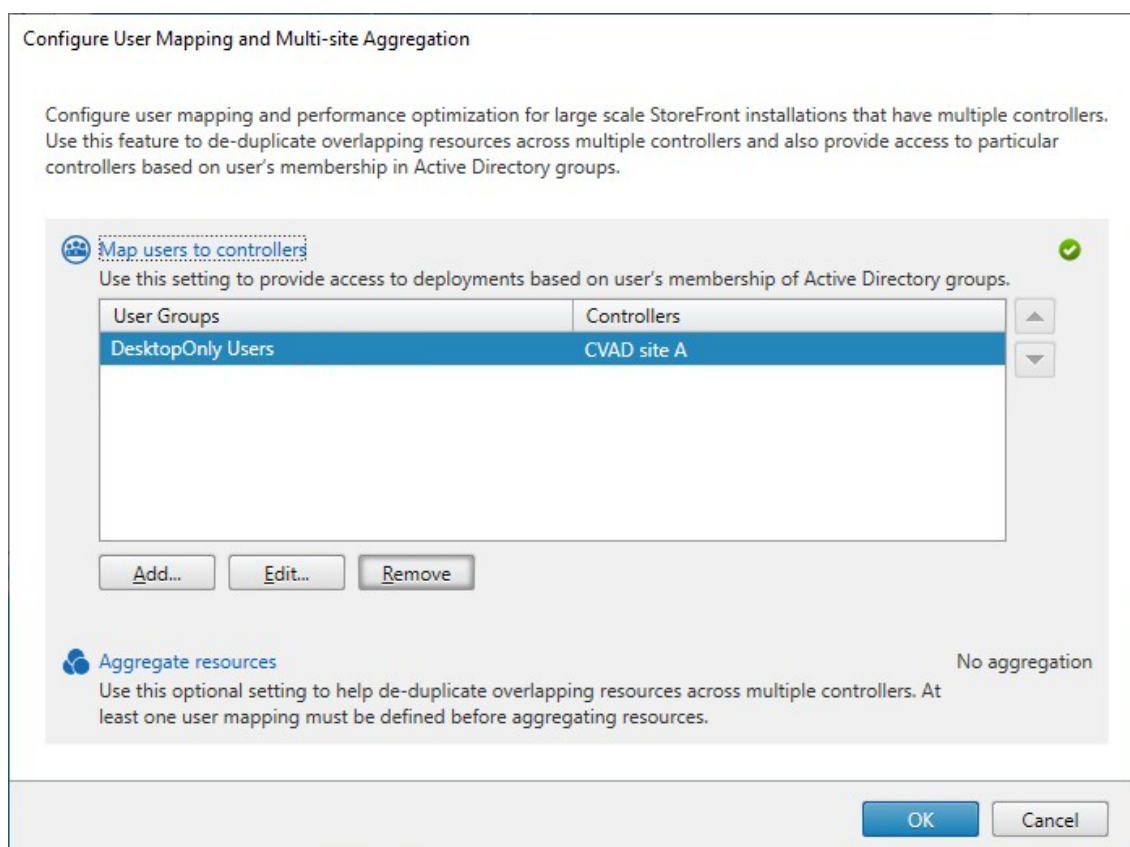
Back

Create

Cancel

6. Click **Create**.





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

## Map users to resources using PowerShell

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

1. For each site (known as a farm within the SDK), create an EquivalentFarmset. All sites must be part of a farmset, 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 site (farm).
2. For each set of users who require access to a different set of sites, 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 site (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 launches an aggregated resource, StoreFront determines the most appropriate instance of that resource for the user, taking into account:

- Server availability.
- Whether the user already has an active session.
- **Primary** and **Secondary** keywords.
- The user's zone preference.
- The order of the delivery feeds 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.

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.

As part of the StoreFront site configuration you can specify which zones those resources are in. If users access StoreFront via a GSLB, you can configure the GSLB to insert a zone preference header. StoreFront then tries to launch applications hosted on the preferred deployment before contacting other deployments.

After checking the other factors, 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.

If a launch fails from one site then StoreFront tries other suitable sites, unless:


- A controller reports that the user has reached their assigned desktop limit.
- A controller reports a credential failure (e.g. invalid, expired or out of hours). StoreFront does not try again with any other delivery controllers as it would expect to get the same result, and to avoid repeated attempts causing an account lock out.
- The launch times out. This would only occur in extreme cases where there are a large number of controllers with high latency.


To configure multi-site aggregation:

1. On the **Manage sites** screen, under **User mapping and multi-site aggregation configuration** click **Configure**. This option is only available if two or more sites are configured.

**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** No mappings  
 Use this setting to provide access to deployments based on user's membership of Active Directory groups.

 **Aggregate resources** No aggregation  
 Use this optional setting to help de-duplicate overlapping resources across multiple controllers. At least one user mapping must be defined before aggregating resources.

OK Cancel

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

Aggregate Do not aggregate

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

☐ Controllers publish identical resources  
☒ Load balance resources across controllers

OK Cancel

3. Choose the sites 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                             |
|--------------------------|-------------|----------------------------------|
| <b>Aggregated</b>        |             |                                  |
| <input type="checkbox"/> | CVAD Site B | Citrix Virtual Apps and Desktops |
| <input type="checkbox"/> | CVAD site A | Citrix Virtual Apps and Desktops |
| <b>Not Aggregated</b>    |             |                                  |
| 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:
- **Sites 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 sites. When not selected, launches are directed to the first site specified in the user mapping dialog screen, failing over to subsequent site 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.

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** No mappings  
Use this setting to provide access to deployments based on user's membership of Active Directory groups.

**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.

OK Cancel

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 sites**. This opens the **Create user mapping** screen.

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

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 sites. You must add all of the aggregated sites, 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.

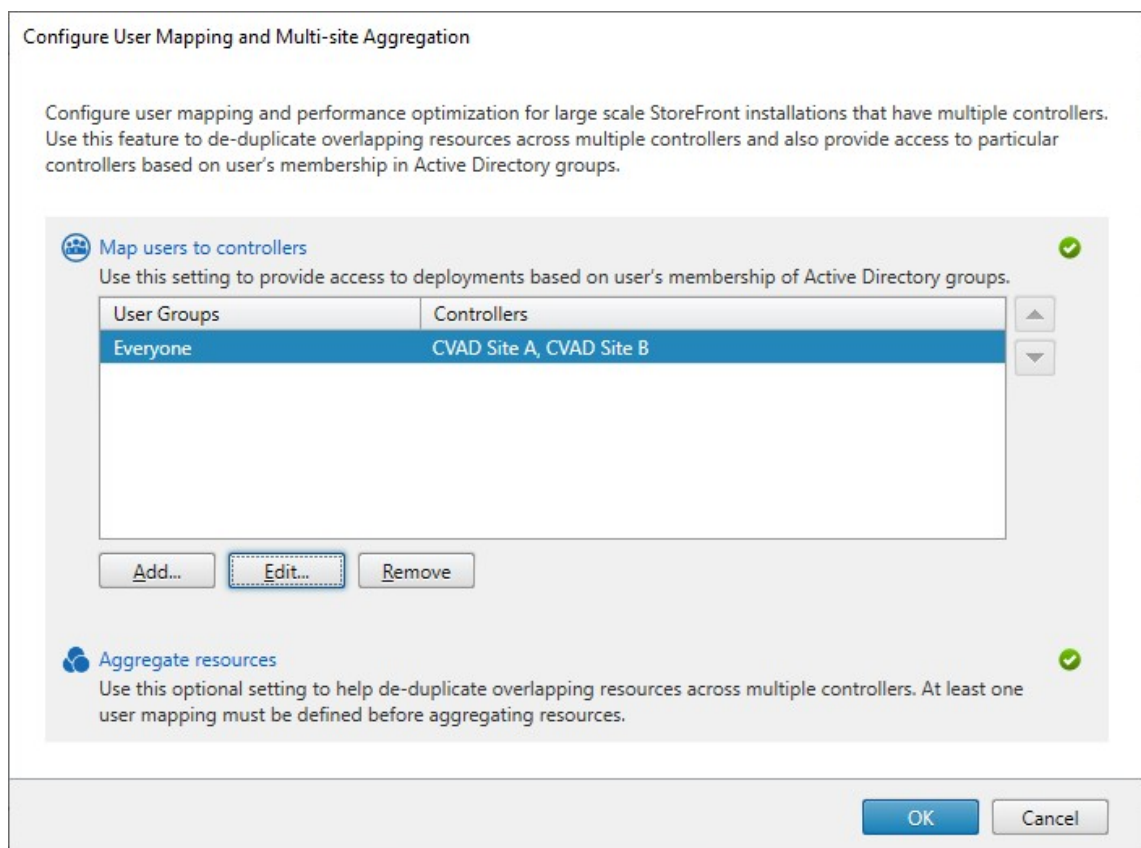
| Controller  | Aggregated | Type                             |
|-------------|------------|----------------------------------|
| CVAD Site A | Yes        | Citrix Virtual Apps and Desktops |
| CVAD Site B | Yes        | Citrix Virtual Apps and Desktops |

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 site is mapped to a user group, otherwise those resources will not be usable by anyone.
12. Click **OK**.

### Advanced configurations using PowerShell

You can configure many common multi-site and high availability operations with the StoreFront management console. You can also configure StoreFront using [PowerShell](#), 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 sites (known in the SDK as farms) that you wish to aggregate. If different sites 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 site 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 site not part of an aggregation group, create an EquivalentFarmset without specifying an [AggregationGroupName](#). All sites (farms) 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 sites, 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 sites are evaluated. This sets the order of preference of which site to use to launch a resource.

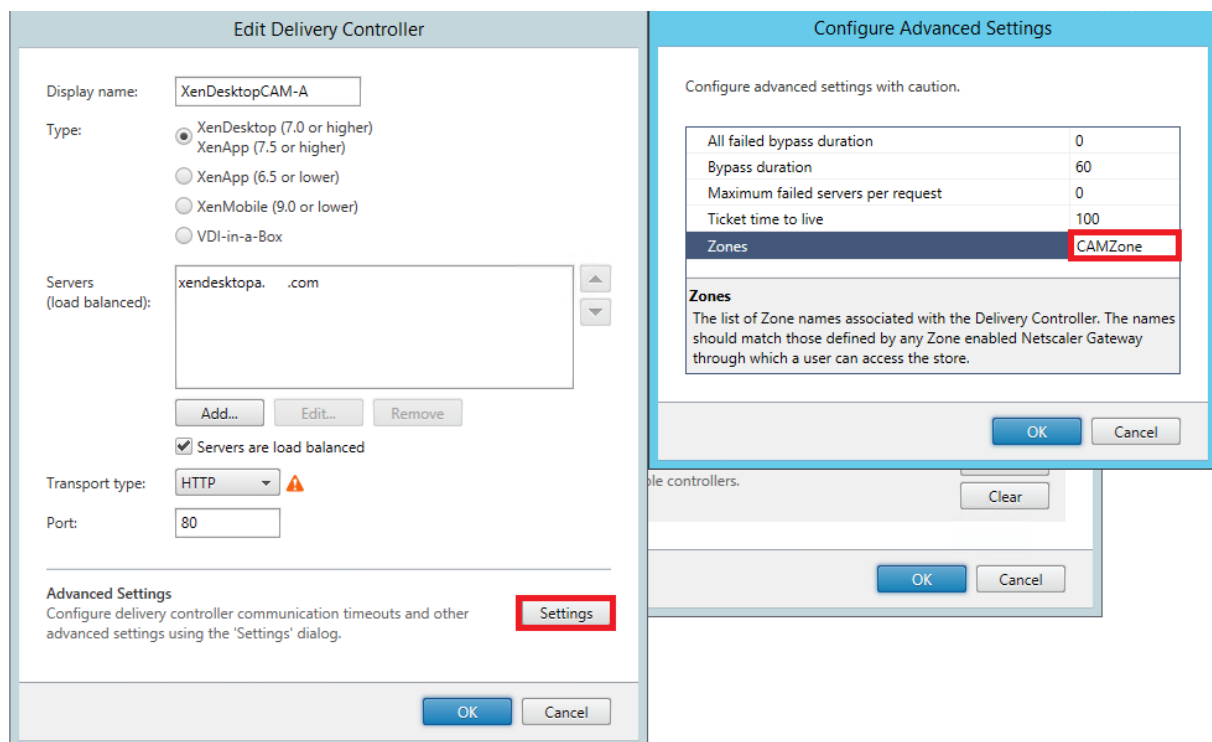
You must ensure that every site (farm) is included in at least one UserFarmMapping, otherwise no users would be able to access that resource.

## Zone preference

If you have multiple CVAD deployments in different regions, you can configure your NetScaler ADC to notify StoreFront of the user's preferred CVAD deployments. For more information, see [Global Server Load Balancing \(GSLB\) Powered Zone Preference](#).

You must manually configure StoreFront to tell it which CVAD deployment contains which zones:

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 sites**.
4. Select a site, click **Edit**, and then click **Settings** on the **Edit site** screen.
5. Under Advanced Settings click **Settings**.
6. In the Configure Advanced Settings dialog, on the **Zones** row, click in the second column.
7. Click **Add...**, enter the zone name and press **OK**. Repeat for each zone in the deployment.
8. In the Configure Advanced Settings dialog, click **OK**.



When the user launches an aggregated resource, StoreFront goes through the list of zones in the **X-Citrix-ZonePreference** header and looks for a site configured with that zone name. If there is a match it sends the launch request to that CVAD deployment. If there is no match then it tries other deployments.

If the CVAD deployment contains multiple zones, it is not possible to direct the launch request to a specific zone within that deployment.

## Set Workspace app website

October 22, 2025

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 from the **Actions** pane, select **Set Citrix Workspace™ app website**. If you don't have a website, a message displays including a link to the create website wizard.
3. Select the website which you wish display when users access this store using Citrix Workspace app.

4. Click **OK**.

# Authentication

November 5, 2025

## Authentication methods

Normally users either authenticate directly to StoreFront™, or to a Citrix Gateway in front of StoreFront. Depending on your requirements, there are several authentication methods available.

| Method                                                 | Detail                                                                                                                                                                                                                                                                  |
|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Active Directory username and password</a> | Users enter their Active Directory username and password.                                                                                                                                                                                                               |
| <a href="#">Domain pass-through</a>                    | Windows devices single sign-on using the account they used to log in to Windows.                                                                                                                                                                                        |
| <a href="#">Smart card</a>                             | Users swipe a smart card and enter a PIN. This uses the certificate stored on the smart card to authenticate the user.                                                                                                                                                  |
| <a href="#">SAML</a>                                   | Delegate authentication to third party identity providers using SAML.                                                                                                                                                                                                   |
| HTTP Basic                                             | Allows third party integrations to authenticate users using their Active Directory username and password. See the Post Credentials API in the <a href="#">Web API developer documentation</a> . HTTP Basic does not provide a user interface for users to authenticate. |
| <a href="#">Pass-through from Citrix Gateway</a>       | Allow users to authenticate at a Citrix Gateway.                                                                                                                                                                                                                        |

Alternatively, when creating a new store, you can disable authentication and instead allow anonymous access to the stores. See [Create store](#).

## Select 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<br><small>Can be enabled / disabled separately on Receiver for Web sites</small> |          |
| <input type="checkbox"/> Smart card<br><small>Can be enabled / disabled separately on Receiver for Web sites</small>                     |          |
| <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

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](#).

### Select authentication methods using PowerShell

To configure authentication using [PowerShell](#):

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.

## Authentication method settings

Some authentication methods have additional settings. Select the **Settings** drop down list to see available options. For more information see the page for that authentication method.

## Shared authentication service settings

You can configure one store to share the authentication service of another store, enabling single sign-on between them.

1. Open **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.

## Install or uninstall authentication methods

You can customize existing methods or create your own authentication methods using the [Authentication SDK](#).

If you have installed a new custom authentication method on the server then you must also install it for each existing store where you wish to use it. From the **Manage authentication methods** screen select **Advanced** then **Install or uninstall authentication methods**.

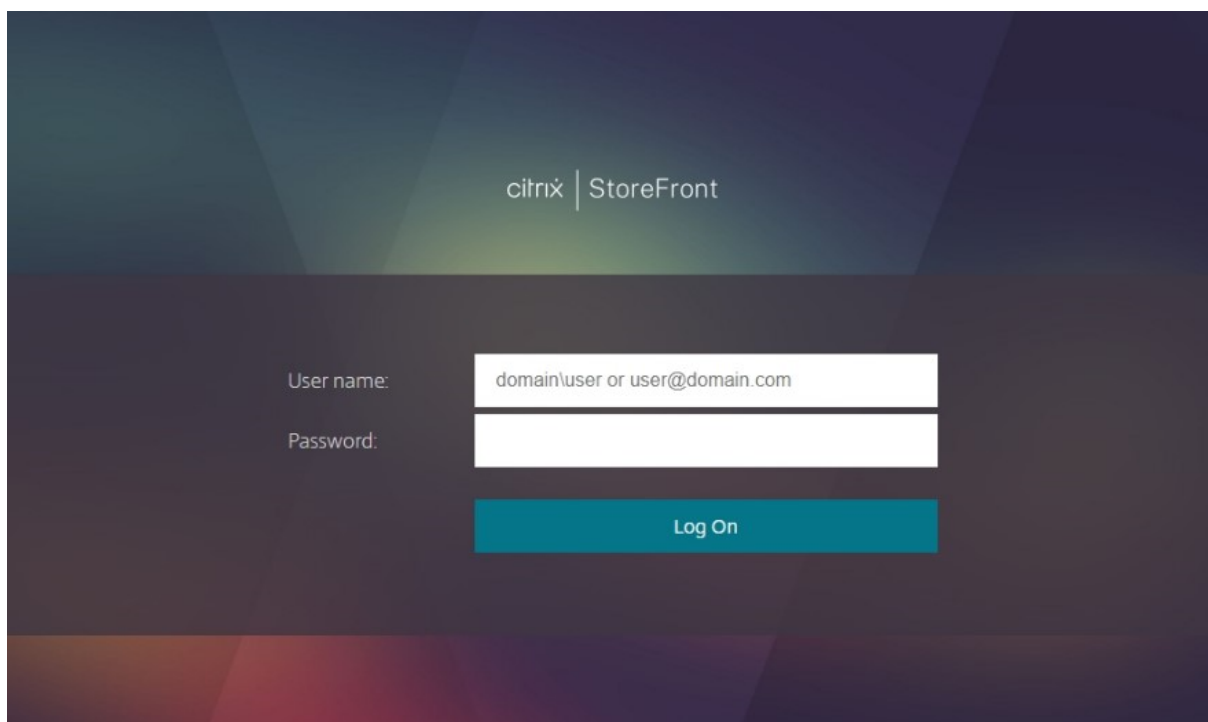
## Single sign-on to VDAs

Some authentication methods include the ability to SSO to VDAs, see each individual authentication method for more details. Otherwise single sign-on can be achieved using [Federated Authentication Service](#).

## Active Directory username and password authentication

November 5, 2025

Users are prompted to enter their active directory username and password.



If the user's password has expired, or is about to expire, then depending on configuration, the user might be given the option to change their password.

To enable or disable username and password authentication for a store when using Citrix Workspace app, in the [Authentication Methods](#) window tick or untick **Active Directory username and password**.

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

## Configure trusted user domains

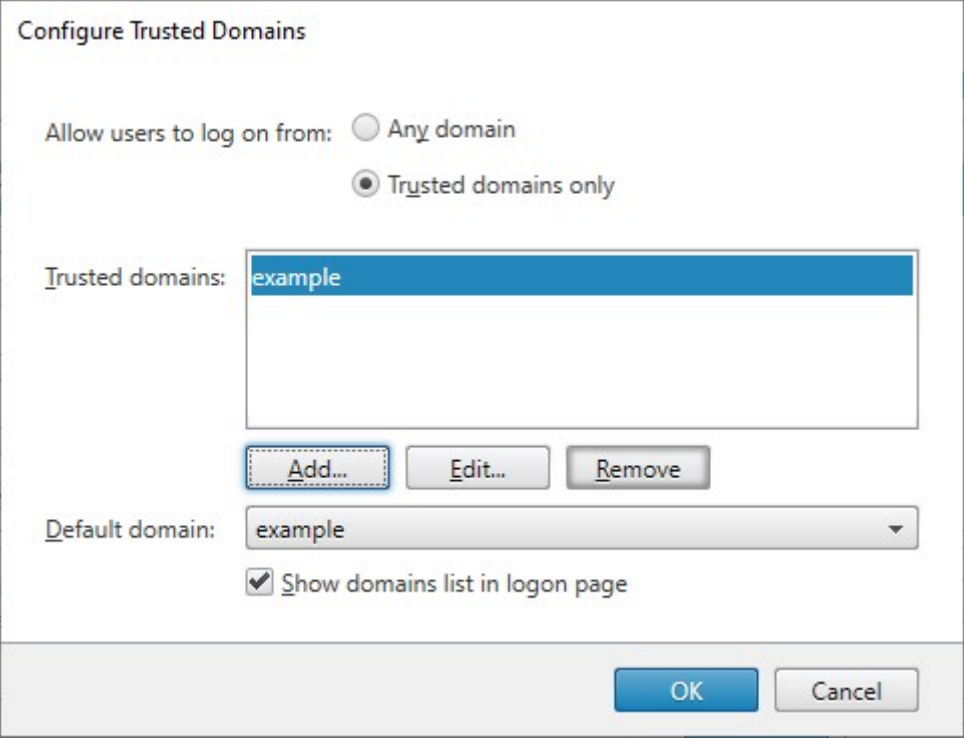
You can restrict access to stores for users logging on with explicit domain credentials, either directly or using pass-through authentication from Citrix Gateway.

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 **username 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 username 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 username 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.



The image shows a 'Configure Trusted Domains' dialog box. It has a title bar with the text 'Configure Trusted Domains'. Inside, there are two radio buttons under the label 'Allow users to log on from:'. The first is 'Any domain' and the second is 'Trusted domains only', which is selected. Below this is a list box labeled 'Trusted domains:' containing the text 'example'. Under the list box are three buttons: 'Add...', 'Edit...', and 'Remove'. Below these is a dropdown menu labeled 'Default domain:' with 'example' selected. At the bottom left is a checked checkbox labeled 'Show domains list in logon page'. At the bottom right are 'OK' and 'Cancel' buttons.

## PowerShell

To get the list of configured domains, use cmdlet `Get-STFExplicitCommonOptions`.

To update the trusted domains, use cmdlet `Set-STFExplicitCommonOptions`.



### 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:

| Citrix Workspace apps | 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 |
|-----------------------|--------------------------------------------------------------|--------------------------------------------|---------------------------------------------------------------------|
| 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 **Active Directory username 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.

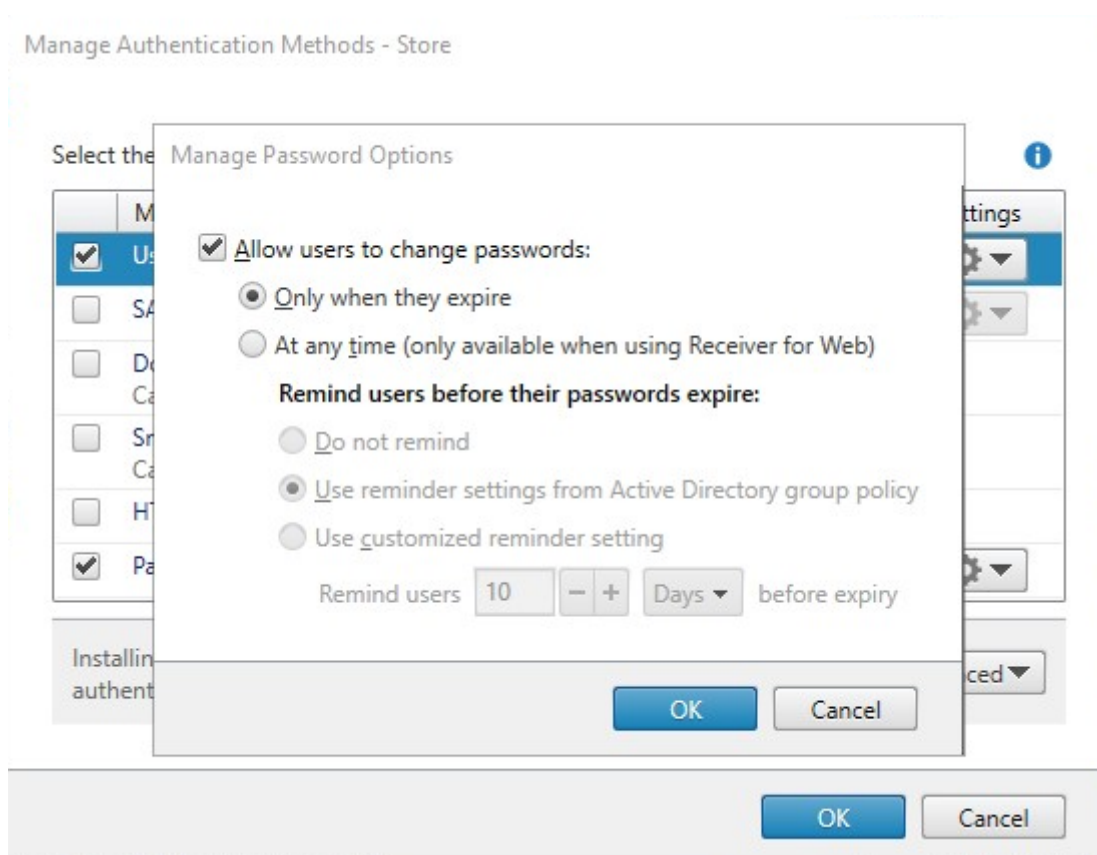
3. Choose whether to allow users to change passwords **Only when they expire** or **At any time**.
4. Choose whether to remind users before their passwords expire. You can choose from the following options:

- **Do not remind** - The UI does not display password expiry reminders. It only notifies users as the point the password has expired.
- **Use reminder settings from Active Directory group policy** - After logging in, the user interface notifies if their password is going to expire in the number days configured in [group policy](#). The user is given the option to change their password.

**Note:**

StoreFront does not take into account [fine grained password policies](#). Therefore if you are using fine grain password policies, you should not select this option.

- **Use customized reminder setting** - After logging in, the user interface notifies the user if their password is going to expire in the given number days. The user is given the option to change their password.



## Notes

### Note 1:

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 2:

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.

## PowerShell

To get the list of trusted domains, use cmdlet `Get-STFExplicitCommonOptions`.

To update the trusted domains, use cmdlet `Set-STFExplicitCommonOptions`.

## Password validation

Normally StoreFront asks Windows to validate the credentials in Active Directory. This requires that the Windows server is on the same domain as the user, or there is a trust relationship between the two domains. When 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 credentials. This also affects HTTP Basic and Gateway Pass-through authentication.

To configure how StoreFront validates passwords:

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

**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<br><small>Can be enabled / disabled separately on Receiver for Web sites</small> |          |
| <input type="checkbox"/> Smart card<br><small>Can be enabled / disabled separately on Receiver for Web sites</small>                     |          |
| <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

2. From the **Validate Password Via** drop down, choose:

- **Active Directory** - Asks Windows to validate credentials in Active Directory
- **Delivery Controllers** - Ask the configured Delivery Controller™ to validate credentials.

## 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. If you selected **Delivery Controllers** then select **Configure**. In 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):  ▲ ▼

☒ Servers are load balanced

Transport type:

Port:

4. Select **OK**.

## PowerShell

To get how passwords are validated, use cmdlet [Get-STFExplicitAuthenticator](#).

To do password validation via delivery controllers, use cmdlet [Set-STFExplicitAuthenticator](#) to set the validator to [xmlServiceAuthenticator](#). To set which delivery controller to use to authenticate credentials, use cmdlet [Enable-STFXmlServiceAuthentication](#)

## Single sign-on to VDAs

When users launch a resource, StoreFront passes through the credentials the user used to log in to the store to single sign-on to the VDAs.

If [Federated Authentication Service \(FAS\)](#) is enabled for the store then StoreFront contacts a FAS server to provide a certificate to single sign-on to the store. This certificate is passed through to the VDA instead of the credentials. If StoreFront is unable to contact a FAS server then there is no single sign-on to the VDA.

## 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`. The template is defined using [Forms Template Language](#).

The following examples add a title and prevent Citrix Workspace app for Windows from caching passwords:

### 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") *@
```

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

```
1 @Heading("ExplicitAuth:AuthenticateHeadingText")
```

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>
```

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"))
```

3. Comment the statement as shown below.

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

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 log in to the gateway using their domain username and password, and optionally a second factor. 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](#).

## SAML authentication

November 5, 2025

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 [CTX220638](#).
- 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 using Citrix Workspace app, 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"
```

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
```

## 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
 :\\Users\\exampleusername\\Downloads\\FederationMetadata.xml"
```

## Configure Identity Provider

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

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 checked="" type="checkbox"/> SAML Authentication                                                  | ▼                                                 |
| <input type="checkbox"/> Domain pass-through<br>Can be enabled / disabled separately on Receiver for Web | <div>Identity Provider<br/>Service Provider</div> |
| <input type="checkbox"/> Smart card<br>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

Identity Provider

**Identity Provider**

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

SAML Binding ⓘ

Address ⓘ

Signing Certificates

| Subject Name | Thumbprint |
|--------------|------------|
|              |            |

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**.

The screenshot shows a 'Service Provider' configuration window. At the top, it says 'Service Provider' and 'The Identity Provider requires this information to configure the trust for this Service Provider.' Below this, there are three fields: 'Export Signing Certificate' with a 'Browse...' button, 'Export Encryption Certificate' with a 'Browse...' button, and 'Service Provider Identifier' which is pre-filled with 'https://storefrontlb.xaaad.com/Citrix/StoreAuth'. At the bottom right, there are 'OK' and 'Cancel' buttons.

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

Using [PowerShell](#):

- 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.

## Domain pass-through authentication

October 22, 2025

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 websites 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](#).

### Web browser configuration

You might 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.

## 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.

For more information on configuring Microsoft Edge for Windows Integrated Authentication, see [Microsoft documentation](#).

## 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

To single sign-in to VDAs using domain credentials, you must use Citrix Workspace app for Windows with the **Enable single sign-on** component, see [Configure domain pass-through authentication](#). Alternatively you can configure [Federated Authentication Service](#) to single sign-on to VDAs.

## Smart card authentication

October 22, 2025

With Smart card authentication, users authenticate using smart cards and PINs when they access their stores. Smart card authentication can be enabled for users connecting to stores through Citrix Workspace app, web browsers, and XenApp Services URLs.

### Note:

Where the users log in to Windows using their smart card, it is recommended that you enable [domain pass-through authentication](#), instead of, or as well as, smart card authentication. This enables single sign-on to the store without needing to re-authenticate with their smart card.

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.

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 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 websites 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.

Alternatively you can configure [Federated Authentication Service](#) to single sign-on to VDAs

## 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.

## Pass-through from Citrix Gateway

December 12, 2025

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 locally installed 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 and password.
- **RSA** Users log on to Citrix Gateway using passcodes that are derived from token codes 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.

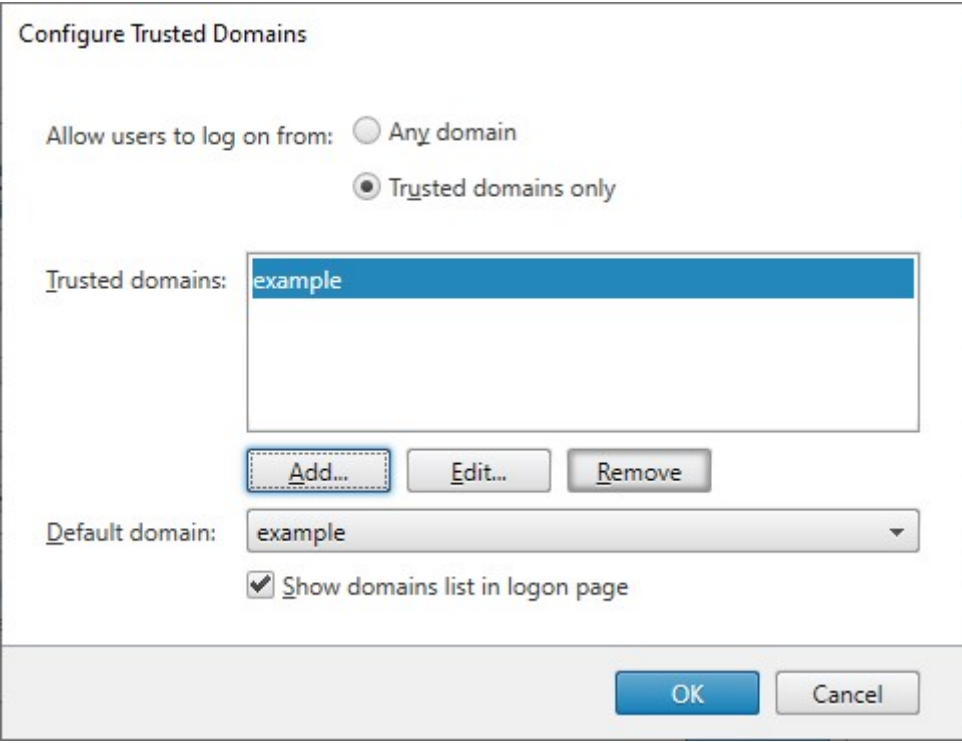
## Configure trusted user domains

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 username 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 username 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.

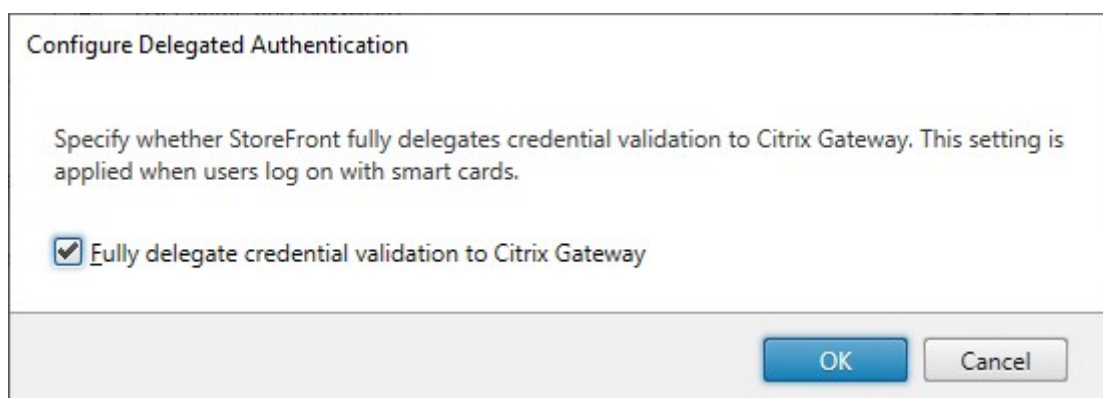


The image shows a 'Configure Trusted Domains' dialog box. It has two radio buttons for 'Allow users to log on from:'. The first is 'Any domain' (unselected). The second is 'Trusted domains only' (selected). Below this is a list box labeled 'Trusted domains:' containing the text 'example'. Below the list box are three buttons: 'Add...' (highlighted with a dashed border), 'Edit...', and 'Remove'. Below these buttons is a dropdown menu labeled 'Default domain:' with 'example' selected. Below the dropdown is a checked checkbox labeled 'Show domains list in logon page'. At the bottom right are 'OK' and 'Cancel' buttons.

## Delegated authentication

By default StoreFront validates the username and password it receives from the Citrix Gateway. If your Citrix Gateway does not use Active Directory credentials via LDAP as a factor, e.g. when using SAML or smart cards, you must configure StoreFront to trust the validation done by the gateway. In this case, it is important that you enter a callback URL when configuring the gateway so StoreFront can verify the request came from the Citrix 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**.



## PowerShell

To configure the store to delegate authentication to the Citrix Gateway using [PowerShell](#), run cmdlet [Set-STFCitrixAGBasicOptions](#).

- To delegate authentication to the gateway set [CredentialValidationMode](#) to [Auto](#).
- For StoreFront to validate the credentials, set [CredentialValidationMode](#) to [Password](#)

## Password validation

You can choose whether StoreFront validates the credentials itself or asks the delivery controller to validate credentials. For more information, see [Username and password authentication - password validation](#).

If **Fully delegate credential validation to citrix gateway** is selected then the setting to validate passwords using the Delivery Controller has no effect. In this case, StoreFront must be able to look up the user in Active Directory so the StoreFront server's domain must always have a trust relationship with the user's domain.

## 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

You can configure StoreFront to allow users to change their passwords after logging on. This functionality is only available when the gateway uses LDAP authentication and when the user access the store through a browser, not locally installed Citrix Workspace app.

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

To modify change password options using [PowerShell](#), run 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 Active Directory credentials

When the gateway is configured with LDAP authentication, it passes the credentials through to StoreFront so that it can single sign-on to VDAs. No additional configuration is required.

### Using Federated Authentication Service

For gateway authentication methods other than LDAP, StoreFront does not have access to the user's credentials so single sign-on is not available by default. You can use [Federated Authentication Service](#) to provide single sign on.

### Using Entra ID

When the gateway is configured to use Entra ID authentication via OIDC, you can enable Entra ID single sign-on. This requires CU1 or higher. For more information, see [Configure VDA Entra ID single sign-on](#).

## Manage websites

November 5, 2025

When you create a store, a website is created for it automatically which users can access through either through a browser or through Citrix Workspace app. You must have at least one website. 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.

**View websites**

To view the websites for a store:

- 1. From the management console, select the **Stores** node in the left pane.
- 2. Select the store you wish to configure.
- 3. In the **Actions** pane, select **Manage websites**.

Manage websites - Store

You can configure one or more websites for 'Store', each with its own URL, appearance, and configuration. These can be accessed through a browser, and the default website can be access using Citrix Workspace app.

Websites:

| Website URL                                    | Store authenticated |
|------------------------------------------------|---------------------|
| https://storefront.example.com/Citrix/StoreWeb | Yes                 |

Add...

Configure...

Remove

Close

From the **Manage websites** screen, you can perform the following actions:

| Action              | 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.                                                   |

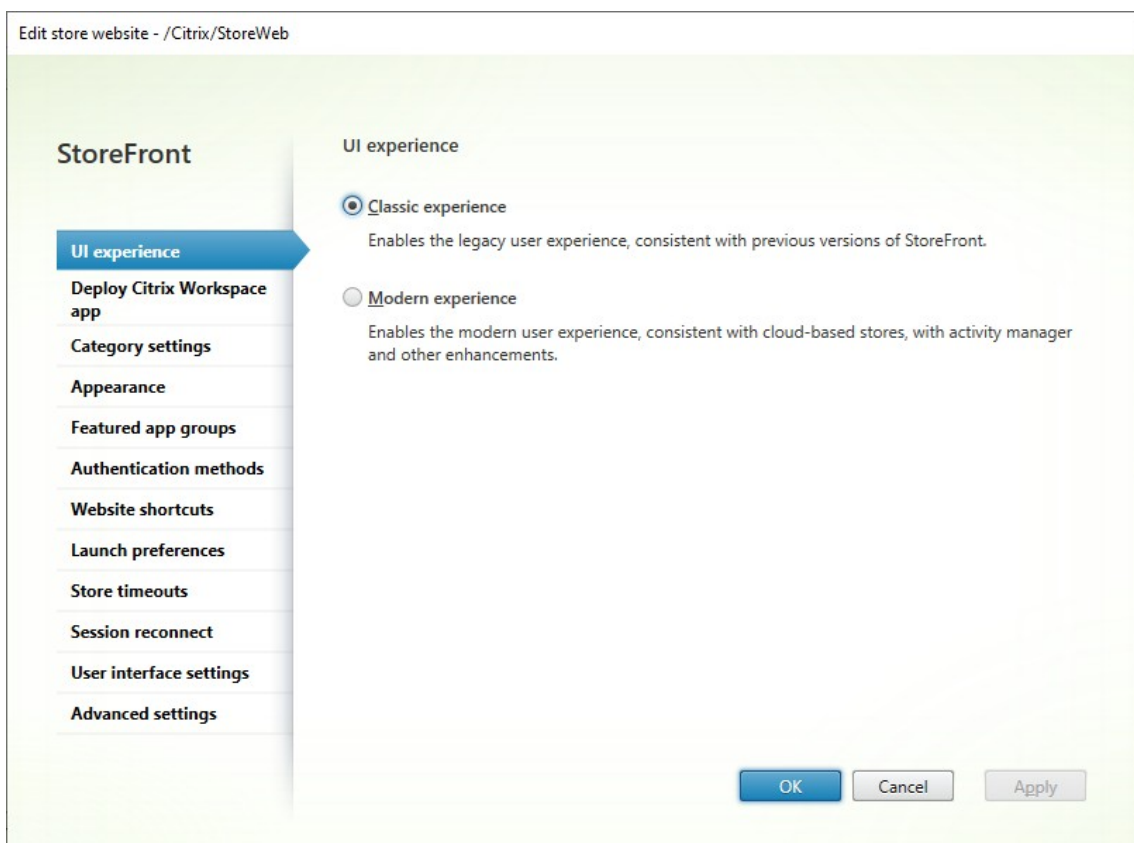
## PowerShell

To get a list of websites, use cmdlet [Get-STFWebReceiverService](#).

## Configure a website

To configure a website:

1. Select a web site and press **Configure...**



2. Modify the settings on the appropriate tabs.

- [UI Experience](#)
- [Deploy Citrix Receiver/Workspace app](#)
- [Category Settings](#)
- [Customize Appearance](#)
- [Featured App Groups](#)
- [Authentication Methods](#)
- [Website Shortcuts](#)
- [Launch preferences](#)
- [Session Settings](#)

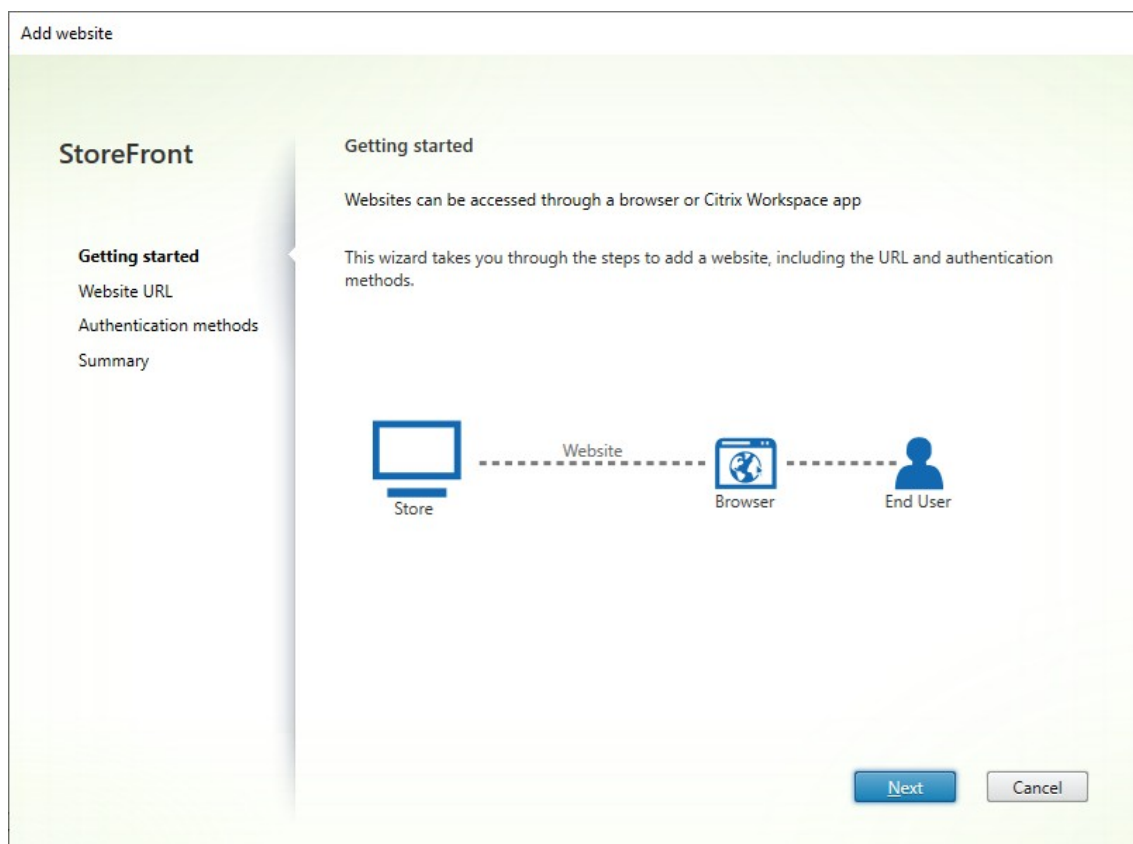
- [Workspace Control](#)
- [Client Interface Settings](#)
- [Pinned links](#)
- [Custom announcements](#)
- [Dialog after log in](#)
- [Advanced Settings](#)

3. Once you have finished your changes, click **OK**.
4. To configure [App Protection](#) you must use PowerShell. Ensure you close StoreFront management console before running PowerShell commands.

## Create a website

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](#).

1. Select **Add....**



2. On the **Getting started** tab, select **Next**.

3. Type the desired **Web Site Path**, choose if you want to this to be the default website for the base URL and select **Next**.

Add website

**StoreFront**

- ✓ Getting started
- Website URL**
- Authentication methods
- Summary

**Website URL**

Choose the URL used to access the Store.

Base URL:

Website path:

☐ Set this website as the default for this deployment  
If selected, when a web browser goes to the deployment's base URL, it is redirected to this website.

4. Tick or untick the desired [authentication methods](#). Some methods are only available if they have been configured for the store. Press **Next**.

Add website

**StoreFront**

- ✓ Getting started
- ✓ Website URL
- Authentication methods**
- Summary

**Authentication methods**

Select the authentication methods which users use to authenticate and access resources. The authentication methods are specific to the website. ⓘ

| Method                                                                     | Status                                                                                                                                                                      |
|----------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> Active Directory username and password | Selected                                                                                                                                                                    |
| <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 Citrix Workspace app for Windows must have the single sign-on component installed. |
| <input type="checkbox"/> Smart card                                        | Disabled                                                                                                                                                                    |
| <input checked="" type="checkbox"/> Pass-through from Citrix Gateway       | Selected                                                                                                                                                                    |

Back Create Cancel

- When the site has been created, click **Finish**.
- Select the newly created site and press **Edit** to configure your web site as required, see Configure Websites.

## PowerShell

To create a website using [PowerShell](#), run cmdlet `Add-STFWebReceiverService`.

## Remove a website

- 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 websites** in the **Actions** pane.
- Select a site and click **Remove**. When you remove a site, users can no longer use that webpage to access the store.

## PowerShell

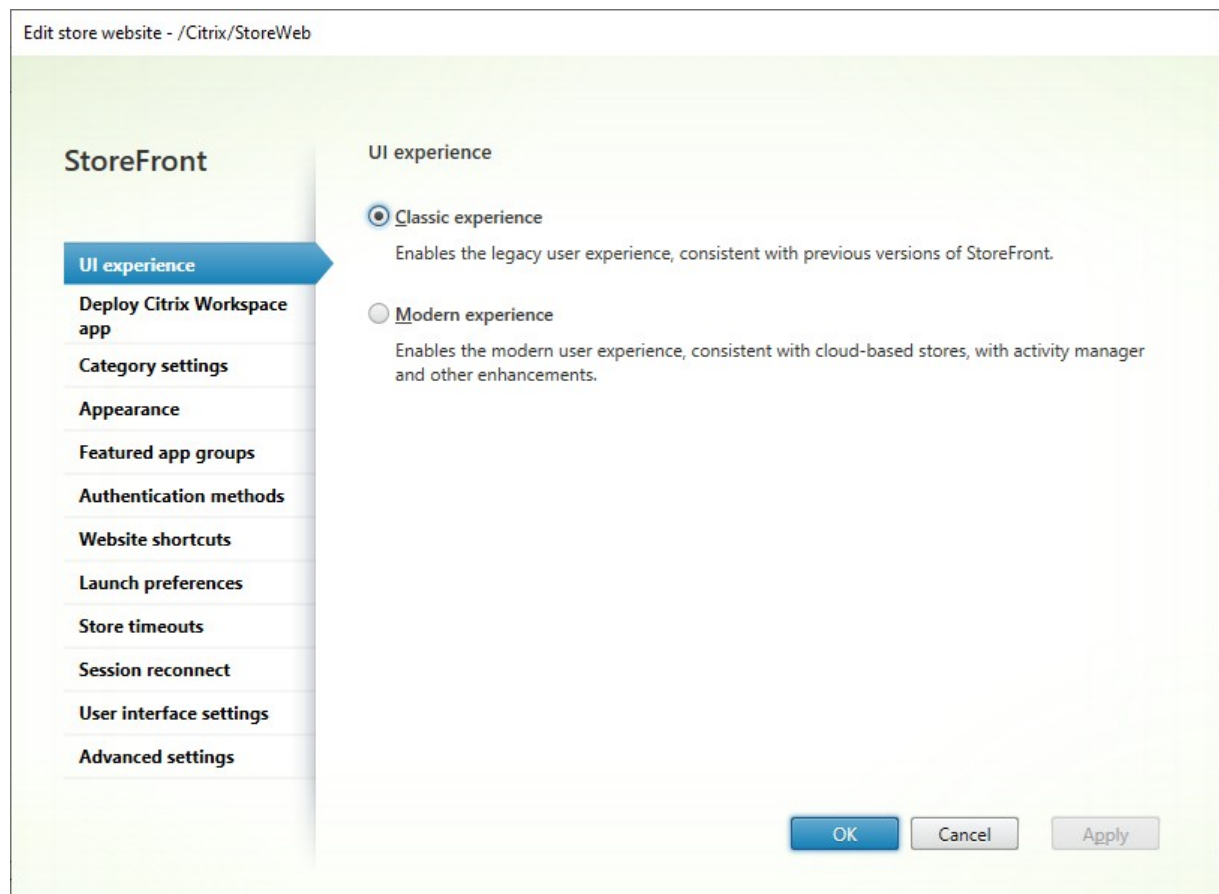
To remove a website using [PowerShell](#), run cmdlet `Remove-STFWebReceiverService`.

## UI Experience

November 14, 2025

On the UI experience tab, you can choose a UI experience for your end-users. You can choose between:

- **Classic experience** - For more information, see [Classic experience](#).
- **Modern experience** - For more information, see [Modern experience](#).



If you use a Citrix Gateway for remote access, you can choose a theme to match the selected experience. For more information, see [NetScaler documentation](#).

## PowerShell

To get the UI experience using PowerShell, call cmdlet `Get-STFWebReceiverService` and view the `WebReceiver.WebUIExperience` property.

For example:

```
1 (Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb").WebReceiver
 .WebUIExperience
```

`WebUIExperience` takes the following values:

- `ReceiverForWeb` - Classic experience
- `Workspace` - Modern experience

To change the UI experience using PowerShell, call cmdlet `Set-STFWebReceiverService` with parameter `WebUIExperience`.

For example to use the classic experience:

```
1 $rfw=Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"
2 Set-STFWebReceiverService -WebReceiverService $rfw -WebUIExperience
 Workspace
```

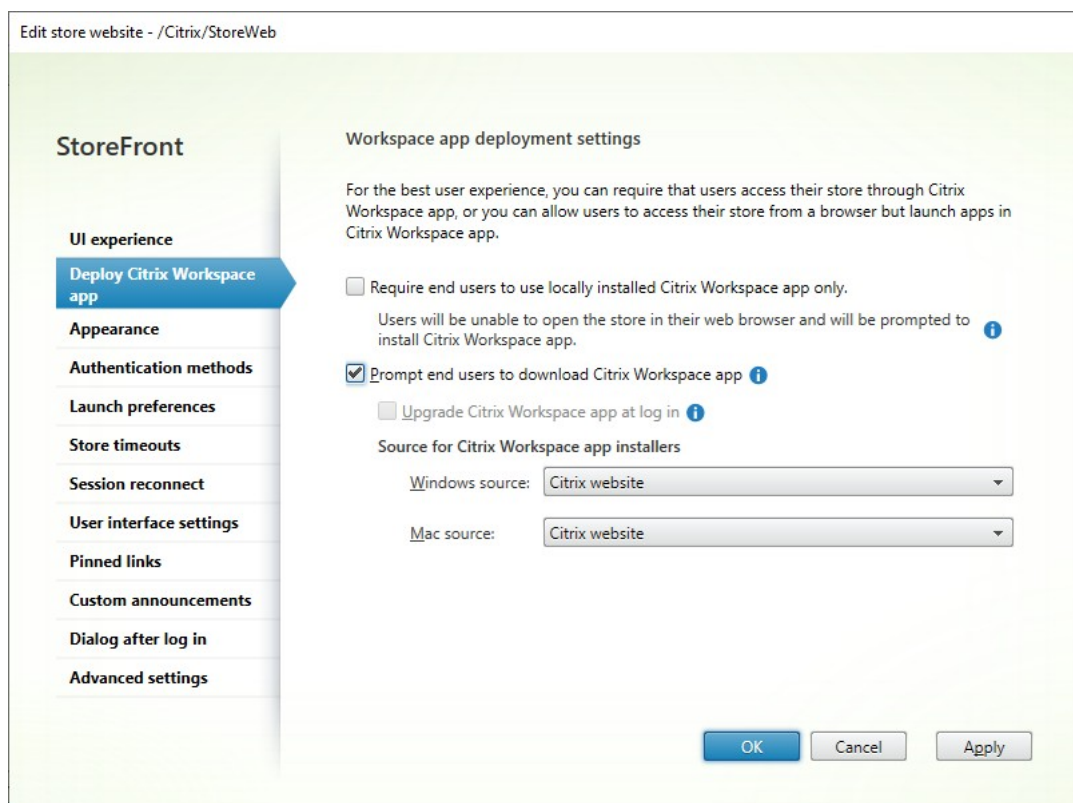
## Citrix Workspace app deployment

November 5, 2025

By default, when a user first opens a store in their web browser on Windows, macOS, or Linux, StoreFront 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. Once it is installed, users can either open the locally installed Citrix Workspace app and connect it to the store, or continue in their browser but connect to virtual apps and desktops in their locally installed Citrix Workspace app HDX client.

Alternatively, users who cannot install Citrix Workspace app locally can use a web browser to both access the store and to connect to virtual apps and desktops.





To modify deployment options, go to [Edit store website](#) and select the **Deploy Citrix Workspace app** tab.

## Require use of Citrix Workspace™ app

Administrators can enforce the use of the native Citrix Workspace app, eliminating the option for users to connect to the store using their web browser. This feature is designed for customers who want to leverage the full benefits of Citrix Workspace app. Citrix Workspace app offers advantages such as built-in App Protection service, avoids browser version compatibility issues, enhanced security and telemetry for monitoring and troubleshooting. For more information see [User access options](#).

This functionality can be enabled in the management console when using the modern experience. It is available via a plug-in when using either the classic experience or a Citrix Gateway.

## Supported platforms

Automatically configuring Citrix Workspace app requires the following versions.

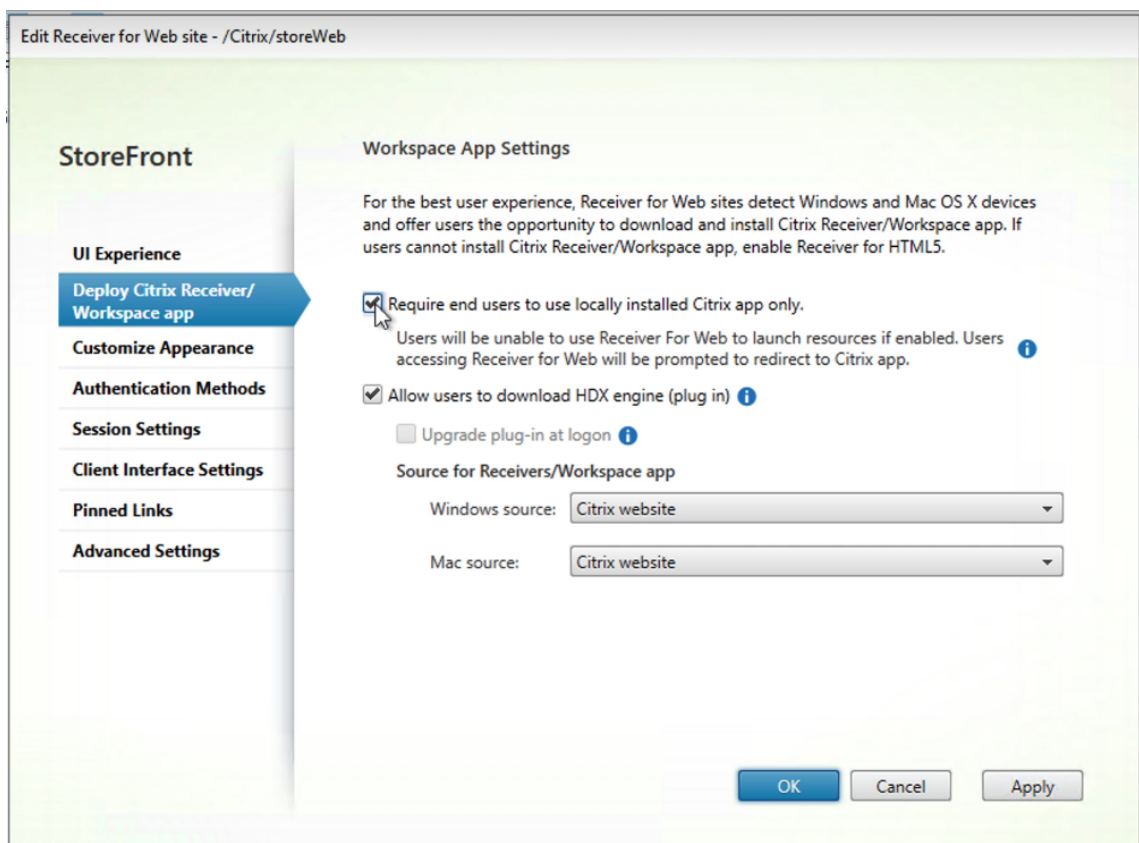
- Citrix Workspace app for Windows 24.9.0 or later
- Citrix Workspace app for Mac 24.5.0 or later
- Citrix Workspace app for Android 24.9.0 or later

- Citrix Workspace app for iOS 24.9.0 or later

### Configure on StoreFront using modern experience

Administrators can follow these steps to require the use of Citrix Workspace app on user devices connecting to StoreFront:

1. Select the **Stores** node in the left pane, and in the **Actions** pane, click **Manage websites**.
2. Click **Configure > Deploy Citrix Workspace app**.



3. Select the option **Require end users to use locally installed Citrix Workspace app only**.
4. Click **OK**.

### Configure using classic experience

1. Download the plug-in from [Citrix Downloads](#).
2. Extract the zip file and citrix-ui-plugin.tar.gz to any directory on the StoreFront server. It contains Powershell files, Javascript files, and config files.

3. Open the plugin.config file in a text editor. Configure as follows:

If you want to enable the native app mandate feature keep the key-value pair as follows: `<param name="requireNativeAppUse" value="true"/>`

If you want to disable the native app mandate feature keep the key-value pair as follows: `<param name="requireNativeAppUse" value="false"/>`

4. Open PowerShell as an administrator.
5. Navigate to the extracted folder.
6. Run `./CitrixPluginInstaller.ps1 -VirtualPath /Citrix/<store web name>`.
7. Repeat for each server in the StoreFront server group.
8. Validate that it has installed correctly by opening a web browser and navigating to the store website.

### Configure using a Citrix Gateway

If users access their store through a Citrix Gateway then you can install a plug-in on the gateway to require use of Citrix Workspace app. For more information, see [Require Citrix Workspace app through a gateway](#).

### User experience

For more information about the end user experience for this feature, see [End user experience](#).

### Allow users to download Citrix Workspace app

#### Note:

If you have not required users to open the store in Citrix Workspace app, and you have configured [Launch preferences](#) to always open resources in a web browser, these settings do not apply.

If you select **Allow users to download Citrix Workspace app**, the first time a user logs on to a device on Windows or Mac, they are given the option to download the app.

### Upgrade Workspace app on logon

If you select **Upgrade Citrix Workspace app at log in**, users are offered 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)**.

### PowerShell

To configure these settings using [Powershell](#), run cmdlet [Set-STFWebReceiverPluginAssistant](#).

### Progressive Web App (Preview)

In cases where users are not able to install Citrix Workspace app, the Progressive Web App (PWA) feature allows you to install the store website so that it can be launched from your start menu or desktop, similar to a native app. This is available only in the classic experience.

### Prerequisites

To use the web client as a Progressive Web App, ensure that you have the following:

- Users must access StoreFront over HTTPS.
- The [Launch option](#) must be set to **Always use Receiver for HTML5**.
- Use Google Chrome or Microsoft Edge browser on Windows, Mac, or Linux.
- The feature is off by default and must be turned on.

### Known limitations

- When you set single tab mode on the StoreFront deployment, it does not apply to PWA launches.
- Hybrid scenarios during session-shared app launches are not supported. For example, launching an app from the PWA and then trying to launch a session-shared app in the browser does not work.
- Switching from the PWA session window to the browser window does not work.

## Enable Progressive Web App

This feature is disabled by default. Admins can enable the functionality as follows:

1. From the **Edit store website** window go to the Launch preferences tab and set the [Launch options](#) to **Open in a web browser**.
2. Save settings and close the management console.
3. Run the PowerShell command Set-STFWebReceiverUserInterface

```
1 $receiver = Get-STFWebReceiverService
2 Set-STFWebReceiverUserInterface -WebReceiverService $receiver -
 ProgressiveWebAppEnabled $true
```

## User experience

For more information on how users can install the app, see [Installing as a progressive web app \(preview\)](#).

## Category Settings

November 5, 2025

### Note:

This functionality is only available using the [classic experience](#).

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:



Application category (optional):

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 store website](#) and select the **Category 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

### Category Settings

Use these settings to configure categories.

Category view

☐ Expanded

All sub-categories and apps under a selected top-level category display on one page.

☒ Collapsed

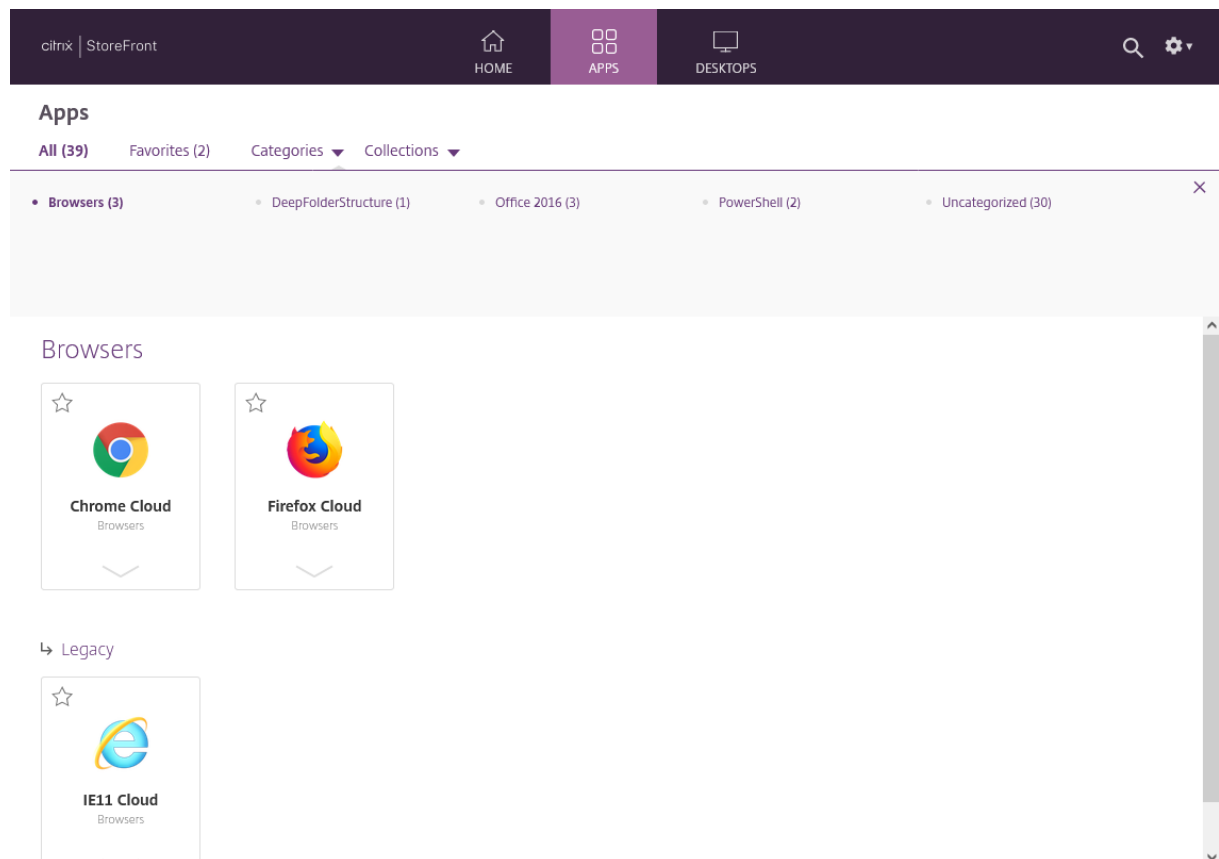
Only the immediate contents (sub-categories and apps) of the selected category or sub-category are displayed.

☐ Move uncategorized apps into an "Uncategorized" folder.

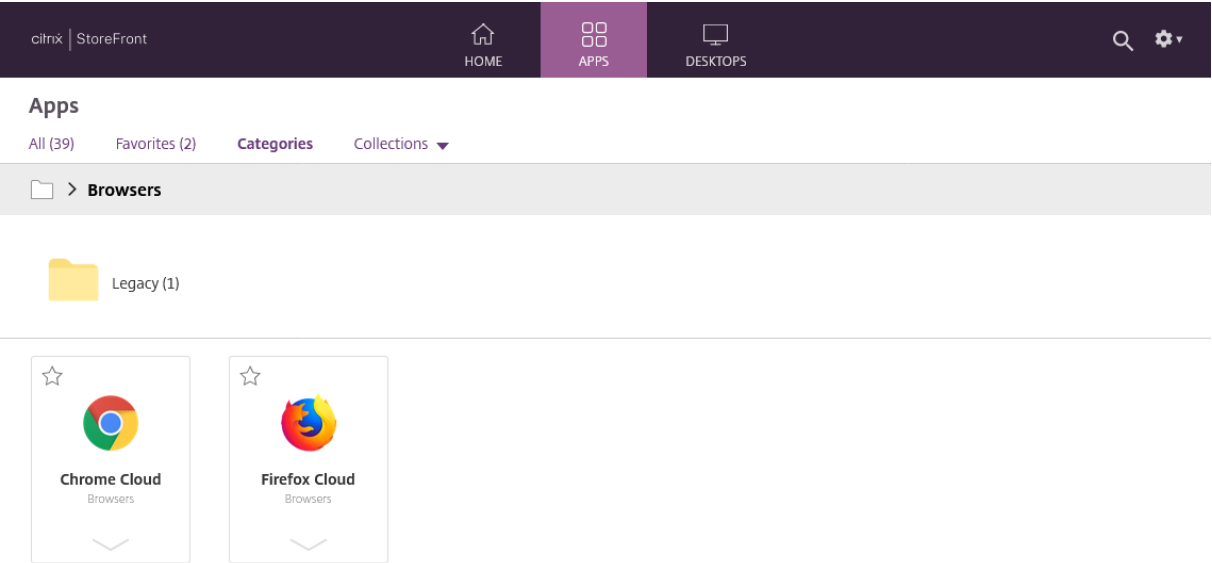
## Category view

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:

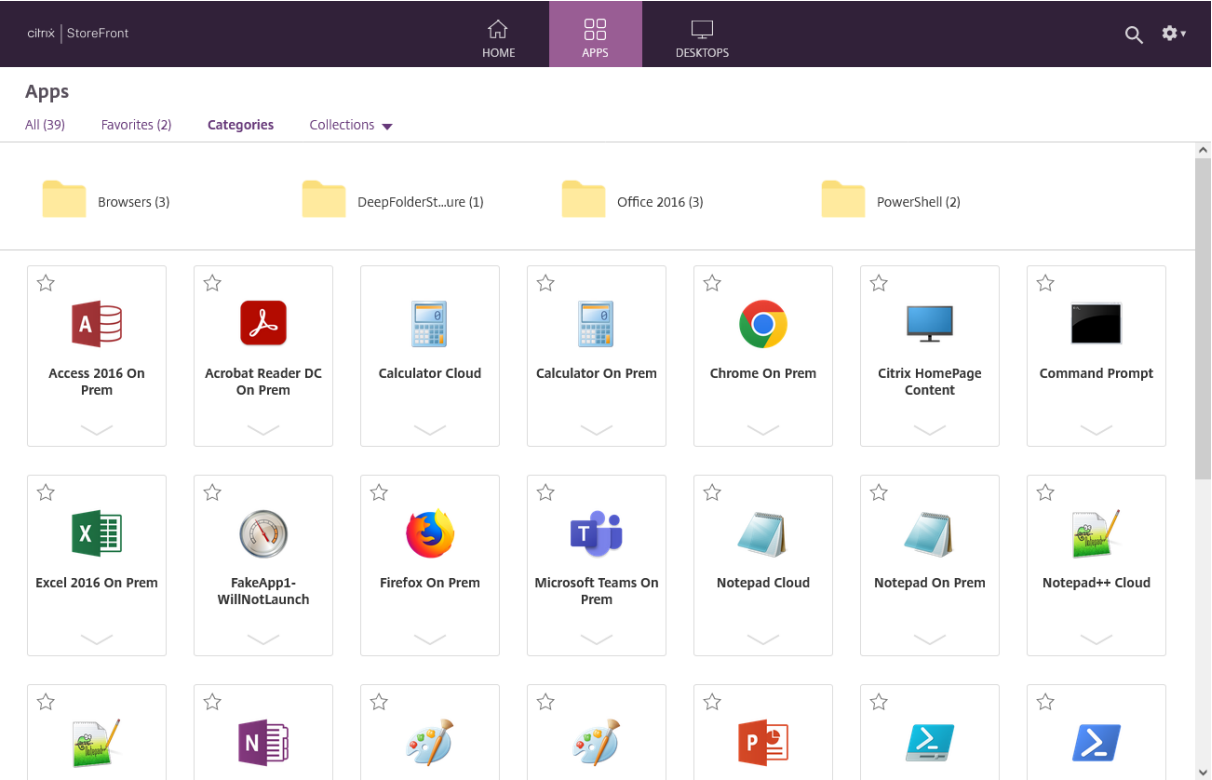


In the collapsed view, StoreFront initially displays a list of top level categories, and optionally all uncategorized apps. When the user clicks a category, StoreFront displays only the immediate contents (subcategories and apps) of the selected category. The user can click each subcategory to expand the contents.



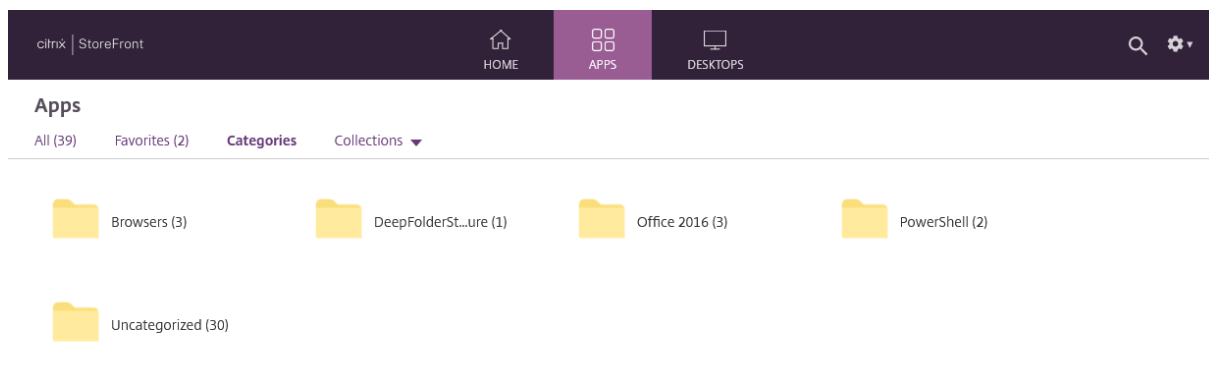
Uncategorized apps

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.



## Hide categories view

To hide the **Categories** view, on the Advanced settings tab, clear [Enable folder view](#).

## Configure category settings PowerShell

To use PowerShell to enable or disable category view call cmdlet [Set-STFWebReceiverUserInterface](#) with parameter [EnableAppsFolderView](#).

To use PowerShell to change the category view call cmdlet [Set-STFWebReceiverUserInterface](#) with parameter [CategoryViewCollapsed](#).

## Appearance

November 5, 2025

You can modify the logo and colors used within your store website.

### Edit logo and colors

To customize the appearance, go to [Edit store website](#) and select the **Customize Appearance** tab. You can modify the following:

- **Logon branding logo** - The logo displayed on the log on screen. It is not displayed when logging in through a Citrix Gateway or using Citrix Workspace app. 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 color for icons in the navigation section at the top of the page.
- **Accent color** - The color used to indicate which item has focus and for buttons and links.

The defaults vary depending on whether you use the classic or modern experience but any customizations apply to both.

### Edit logo and colors using PowerShell

Using [PowerShell](#), run 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

Using [PowerShell](#), run cmdlet [Clear-STFWebReceiverSiteStyle](#).

## Customization using Javascript and CSS

When using the classic experience, you can further customize the website using the [StoreFront Client UI Customization API](#). This does not apply when using the modern experience.

## Featured app groups

November 5, 2025

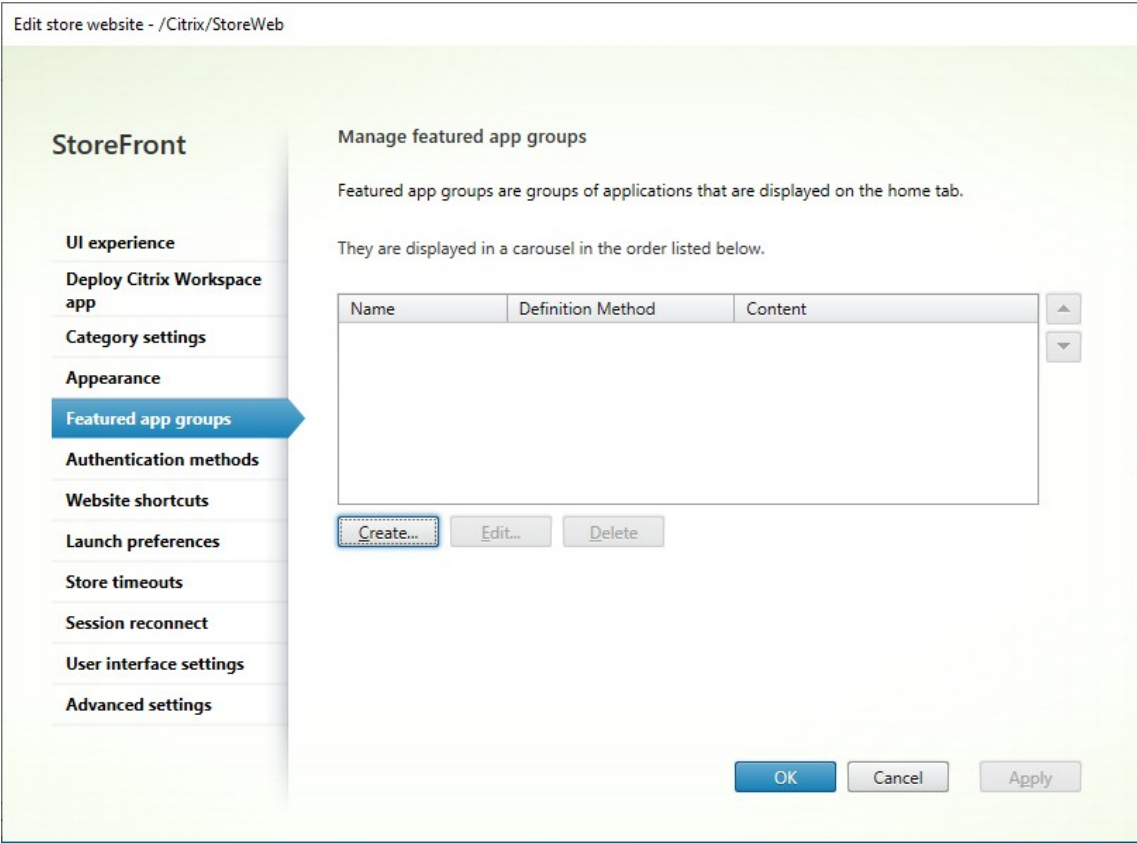
### Note:

This functionality is only available using the [unified experience](#).

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 store website](#) 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.                                                                                                    |

| Option            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 <b>Exc</b> does not match anything. |

Create Featured App Group

Name:

Description:  
(Optional)

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

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

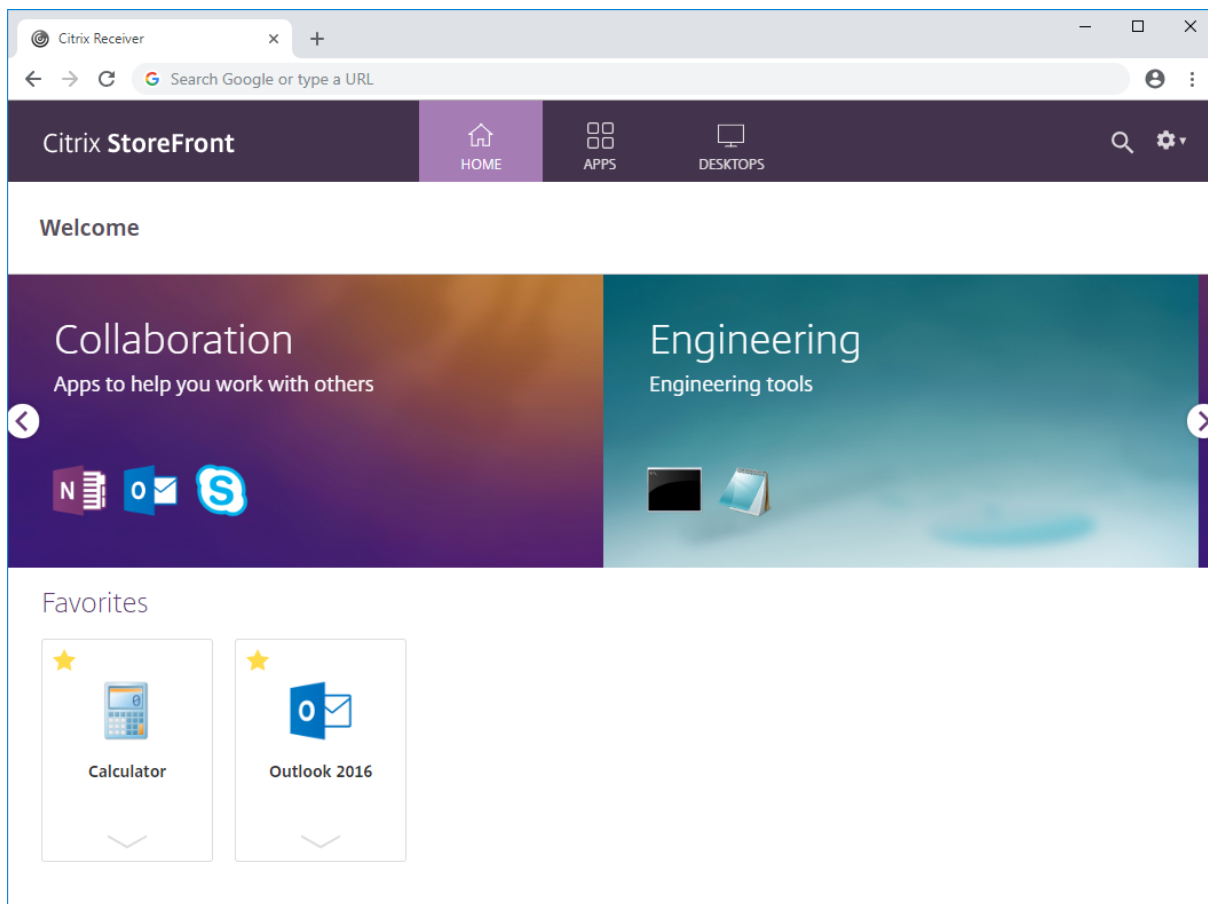
Cancel

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 PowerShell

To add a feature app group with [PowerShell](#), run cmdlet [New-STFWebReceiverFeaturedAppGroup](#).

### Edit featured app group

In the [Edit store website](#) screen, select the **Featured App Groups** tab. Select the group that you want to edit and click **Edit...**

### Edit featured app group using PowerShell

To modify a feature app group with [PowerShell](#), run cmdlet [Set-STFWebReceiverFeaturedAppGroup](#).

## Delete featured app group

In the [Edit store website](#) 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

Using [PowerShell](#) 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

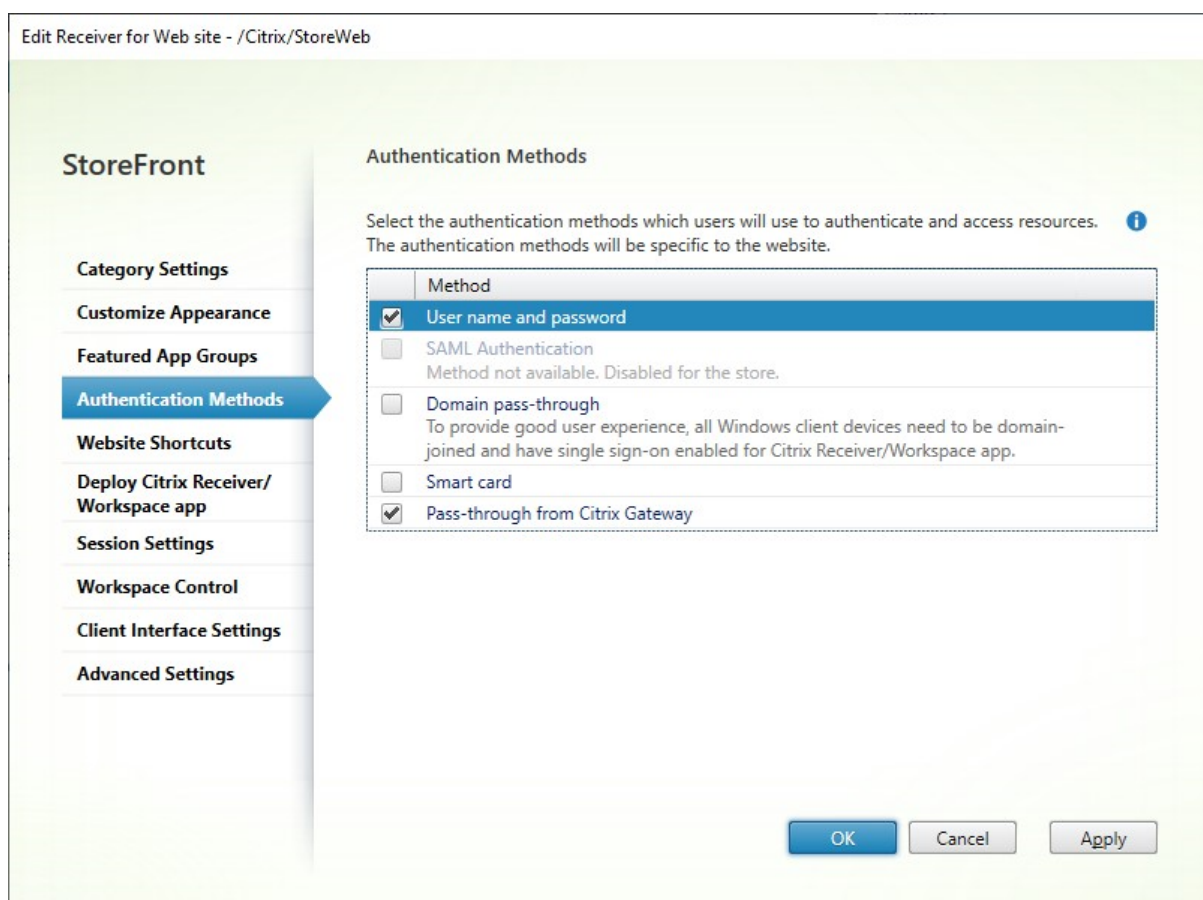
November 5, 2025

To configure the authentication methods available for a store, see [Configure Authentication](#). You can override some of these settings for a particular website. These overrides only apply when users open the store in a web browser. Locally installed Citrix Workspace app uses the settings from the store rather than the website.

### 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 when using a web browser, go to [Edit store website](#) and select the **Authentication methods** tab.



- Select the **Active Directory username and password** check box to all users to authenticate by entering their username and password. See [Username 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, to avoid users needing to authenticate a second time at StoreFront. See [Pass-through from Citrix Gateway](#).

If you select multiple authentication methods then the default authentication method for users logging in directly to StoreFront™ is determined according to the following order of precedence:

1. Domain pass-through
2. Smart card



3. SAML
4. Username and password

The user can choose to switch to a different authentication method. An exception is that if you configure both SAML and username and password authentication then users are not able to switch to Username and password authentication.

When users log out, they can choose whether to remember the authentication method for next time.

## Configure using PowerShell

To configure the available authentication methods using the [PowerShell](#), run the cmdlet [Set-STFWebReceiverAuthenticationMethods](#).

## Website shortcuts

November 5, 2025

### Note:

This functionality is only available using the [classic experience](#).

Use website shortcuts to provide users with rapid access to desktops and applications from trusted websites hosted on the internal network. You can generate URLs for resources and embed these links on your websites. Users click a link and are redirected to the store website, where they log on if they have not already done so. The website automatically starts the resource.

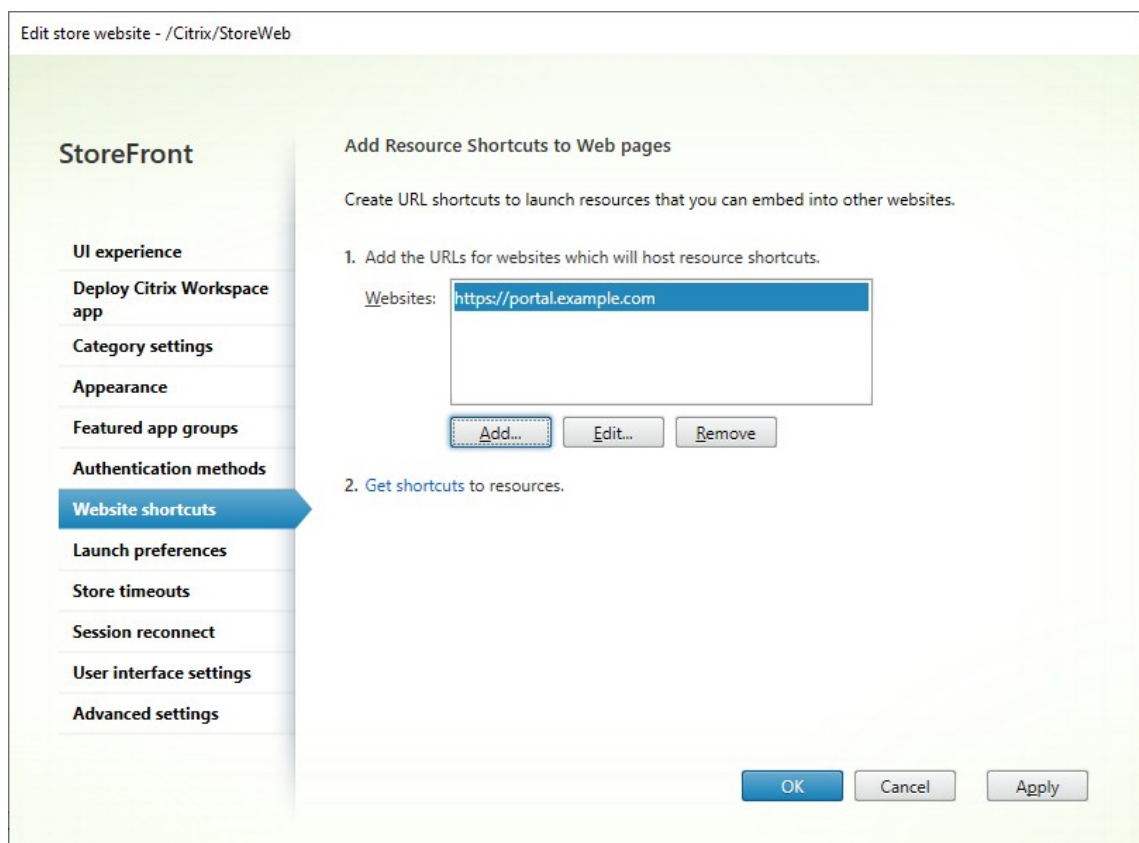
Before you can generate resource shortcuts, you must add the URLs of host websites to the *trusted URLs* list, using the Citrix StoreFront management console or using PowerShell.

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, on Advanced settings, clear [prompt for untrusted shortcuts](#).

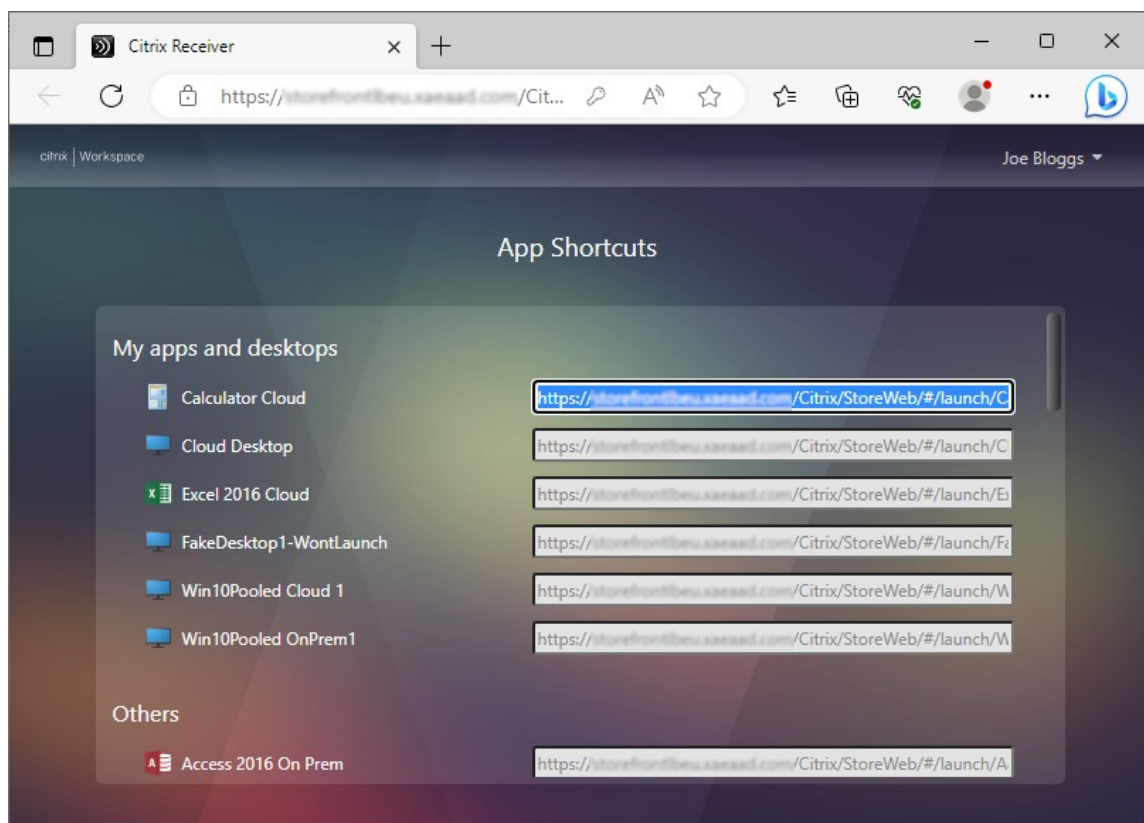
For security reasons, Internet Explorer users may be prompted to confirm that they want to start resources accessed through shortcuts. Instruct your users to add the StoreFront server FQDN the Local intranet or Trusted sites zones in Internet Explorer to avoid this extra step.

## Add trusted websites using the management console

1. On the [Edit store website](#) 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.



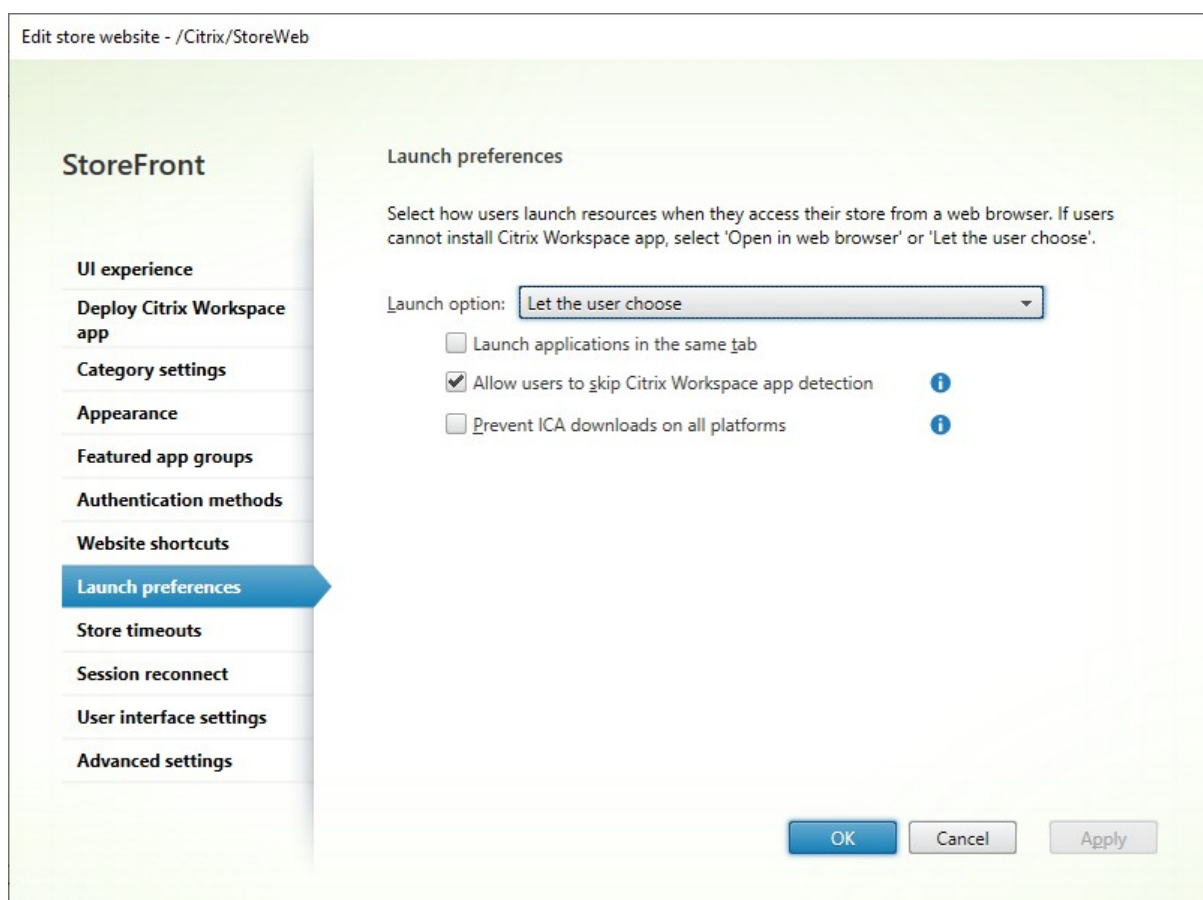
## Add trusted websites using PowerShell

To add trusted URLs using [PowerShell](#), run cmdlet [Set-STFWebReceiverApplicationShortcuts](#).

## Launch Preferences

November 12, 2025

From **Launch Preferences**, you can choose which launch options are made available to the users when they open their store in a web browser. These settings do not apply when using Citrix Workspace app. For more information about launch options, see [User access options](#).



To modify launch options, go to [Edit store website](#) and select the **Launch preferences** tab.

## Launch option

You can choose from one of the following options:

- Select **Open in a web browser** 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 **Let the user choose** 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 **Open in Citrix Workspace app** 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 **Open in a web browser** or **Let the user choose**, by default, resources launched in the browser open a new browser tab. If you want your resources to open in the same tab, replacing the store, select **Launch applications in the same tab**.

## Allow users to skip Citrix Workspace™ app detection

When end users open a store in their browser for the first time, 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 select the **Skip detection** 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 session reconnect.

The downloaded `.ica` file may pose a security risk. Citrix recommends that you clear **Allow users to skip Citrix Workspace app detection**.

## 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 ChromeOS, ChromeOS users must either select **Use web browser** if available, or they must add their store to their locally installed Citrix Workspace app.

### Important:

This option should not be selected if **Allow users to skip Citrix Workspace app detection** is also selected.

## Citrix web extension

By default, when a user first logs in using a web browser, or goes to **Account settings** and chooses **Change launch method**, it checks whether **Citrix web extension** is installed. If it is found, it uses it to detect Citrix Workspace app and to launch virtual apps and desktops. This provides the best and most secure experience by avoiding browser prompts and downloading ICA files. The detection process takes up to 6 seconds (2 attempts with 3s timeouts), to allow for situations where the webpage is slow to load e.g. due to low bandwidth low performance devices. Therefore if Citrix web extension is not detected then first time users may experience a 6s delay. This does not apply when using the modern experience or web browsers other than Chrome and Edge. You can configure whether the website uses Citrix web extension and if so what timeouts it uses.

To view the current configuration, use [PowerShell](#) cmdlet [Get-STFWebReceiverPluginAssistant](#). For example:

```
1 $receiver = Get-STFWebReceiverService "/Citrix/StoreWeb"
2 Get-STFWebReceiverPluginAssistant -WebReceiverService $receiver
```

To modify the configuration, use cmdlet [Set-STFWebReceiverPluginAssistant](#) with parameters [BrowserExtensionEnabled](#), [BrowserExtensionTimeout](#) and [BrowserExtensionRetries](#). For example to disable Citrix web extensions:

```
1 $receiver = Get-STFWebReceiverService "/Citrix/StoreWeb"
2 Set-STFWebReceiverPluginAssistant -WebReceiverService $receiver -
 BrowserExtensionEnabled $False
```

Or to reduce the timeout to 2s with only one attempt:

```
1 $receiver = Get-STFWebReceiverService "/Citrix/StoreWeb"
2 Set-STFWebReceiverPluginAssistant -WebReceiverService $receiver -
 BrowserExtensionTimeout 2000 -BrowserExtensionRetries 1
```

Reducing the timeout from the default may cause the website to fail to detect Citrix web extensions.

## PowerShell

To configure these settings using [Powershell](#), run cmdlet [Set-STFWebReceiverPluginAssistant](#).

To configure Prevent ICA Downloads, run cmdlet [Set-STFWebReceiverUserInterface](#) with parameter [PreventIcaDownloads](#).

## Store timeouts

November 5, 2025

To modify store timeouts, go to the [Edit store website](#) screen, select the **Store timeouts** tab.

The screenshot shows the 'Edit store website - /Citrix/StoreWeb' window. On the left is a navigation pane with the following items: 'StoreFront', 'UI experience', 'Deploy Citrix Workspace app', 'Category settings', 'Appearance', 'Featured app groups', 'Authentication methods', 'Website shortcuts', 'Launch preferences', 'Store timeouts' (highlighted with a blue arrow), 'Session reconnect', 'User interface settings', and 'Advanced settings'. The main area is titled 'Store timeouts' and contains the instruction 'Configure when inactive users are logged off, and other timeouts.' There are four settings, each with an information icon (i):  
1. 'Internal server communication attempts:' with a text box containing '1'.  
2. 'Internal communication timeout duration:' with a spinner box set to '3' labeled 'Minutes' and another spinner box set to '0' labeled 'Seconds'.  
3. 'Inactivity timeout for web browser:' with a spinner box set to '0' labeled 'Hour' and another spinner box set to '20' labeled 'Minutes'.  
4. 'Log in screen timeout for web browser:' with a spinner box set to '5' labeled 'Minutes'.  
At the bottom right are three buttons: 'OK' (blue), 'Cancel' (gray), and 'Apply' (gray).

### Internal 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.

### Internal 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.

### Inactivity timeout for web browser

While accessing a StoreFront store through a web browser, after the specified period of inactivity, the session times out and user is logged out. Refreshing the web page or performing an action on a resource extends the session. User actions that do not result in network activity, such as navigating between tabs, do not extend the session.

The timeout is enforced on both the client and the server. Shortly before the session expires, the UI prompts the user to extend the session. One minute before the session timeout, the UI notifies StoreFront and, if applicable, Citrix Gateway to log off. This is to allow the client to cleanly log off before the server timeout expires. If the session timeout is set to 1 minute then the client logs off after 30s. This does not affect locally installed Citrix Workspace app.

If you modify the session timeout so that it is greater than the Gateway session timeout you must increase the gateway session timeout accordingly. If you modify the session timeout so that it is greater than the Authentication token lifetime or Maximum token lifetime, these are automatically increased to match the session timeout.

## PowerShell

To configure the timeout use cmdlet [Set-STFWebReceiverService](#) with parameter `-SessionStateTimeout`. 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
```

## Sign in timeout

When on the log in screen in a web browser, after a period of time the log in times out and a message is displayed to the user. The user can press **Log On** to return to the log on screen.

## 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 locally installed Citrix Workspace apps. The value is not display on the management console.

To view the current value use [Get-STFWebReceiverAuthenticationMethods](#) and check the `TokenLifeTime` property. For example:

```
1 $rfweb=Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"
2 $rfauth = Get-STFWebReceiverAuthenticationMethods -WebReceiverService
 $rfweb
3 $rfauth.TokenLifeTime.ToString()
```

To set the timeout using PowerShell, use cmdlet [Set-STFWebReceiverAuthenticationMethods](#) with parameter `TokenLifeTime`. For example:

```
1 $rfweb=Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"
2 $rfauth = Get-STFWebReceiverAuthenticationMethods -WebReceiverService
 $rfweb
```



```
3 Set-STFWebReceiverAuthenticationMethods -WebReceiverService $rfweb -
TokenLifeTime "07:00:00"
```

If you increase the session timeout to be more than 20 hours, you must also increase the Maximum token lifetime of Authentication Service.

## Citrix Gateway timeouts

For more information on gateway timeouts see [Gateway documentation](#).

### Session time-out

The session time-out applies if there is no network activity for the specified length of time. Refreshing the web page or performing an action on a resource extends the session. User actions that do not result in network activity, such as navigating between tabs, do not extend the session.

For web browser access you should set the Citrix Gateway **Session time-out** to a slightly higher value than the StoreFront **Session timeout**. This is to ensure that when the StoreFront session times out and it notifies the gateway, the gateway is able to cleanly sign out before its own session expires.

Locally installed Citrix Workspace app does not apply an inactivity timeout when connected to a StoreFront store. Therefore, the gateway is the only place that you need to apply an inactivity timeout. The app periodically refreshes the list of resources. For it to take effect, the session time-out must be lower than the app's refresh period. By default the app's refresh period is 60 minutes. To change this, see [CTX221465](#).

### Forced time-out

On the Citrix Gateway you may set a **Forced time-out** to disconnect the session after a given time regardless of the user's activity.

## Maximum token lifetime of Authentication Service

The Authentication Service issues tokens that are used when connecting to a store. By default the token expires after 20 hours which causes the user to be logged out.

If the user authenticated by a Citrix Gateway, then when the StoreFront token expires, StoreFront issues a challenge to the Citrix Gateway. If the gateway's session is still active then it supplies the credentials to log back in to StoreFront. If you wish to prevent this then you must configure the gateway's **Forced time-out** to be the same as the maximum token lifetime.

Normally when using the store in a web browser, the inactivity timeout causes the session to be logged out before the token expires so the token lifetime is mainly relevant to locally installed Citrix Workspace app.

To view the maximum token lifetime run the following PowerShell:

```
1 $store = Get-STFStoreService -VirtualPath "[store path]"
2 $auth = Get-STFAuthenticationService -StoreService $store
3 $relyingParty = $auth.ProducerService.RelyingParties | Where-Object {
4 $_.Id -eq $auth.ProducerService.Id }
5
6 $relyingParty.MaxLifetime.ToString()
```

Replacing `[store path]` with the appropriate store path.

To configure the maximum token lifetime run the following PowerShell:

```
1 $store = Get-STFStoreService -VirtualPath "[store path]"
2 $auth = Get-STFAuthenticationService -StoreService $store
3 $relyingParty = $auth.ProducerService.RelyingParties | Where-Object {
4 $_.Id -eq $auth.ProducerService.Id }
5
6 $relyingParty.MaxLifetime = "[max lifetime]"
7 Save-STFService -Service $auth
```

Replacing `[store path]` with the appropriate store path and `[max lifetime]` with the desired timeout. For values up to a day use the format `hh:mm:ss`. For values over a day use the format `d. hh:mm:ss`.

## Session reconnect

November 5, 2025

As users move between devices, session reconnect 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

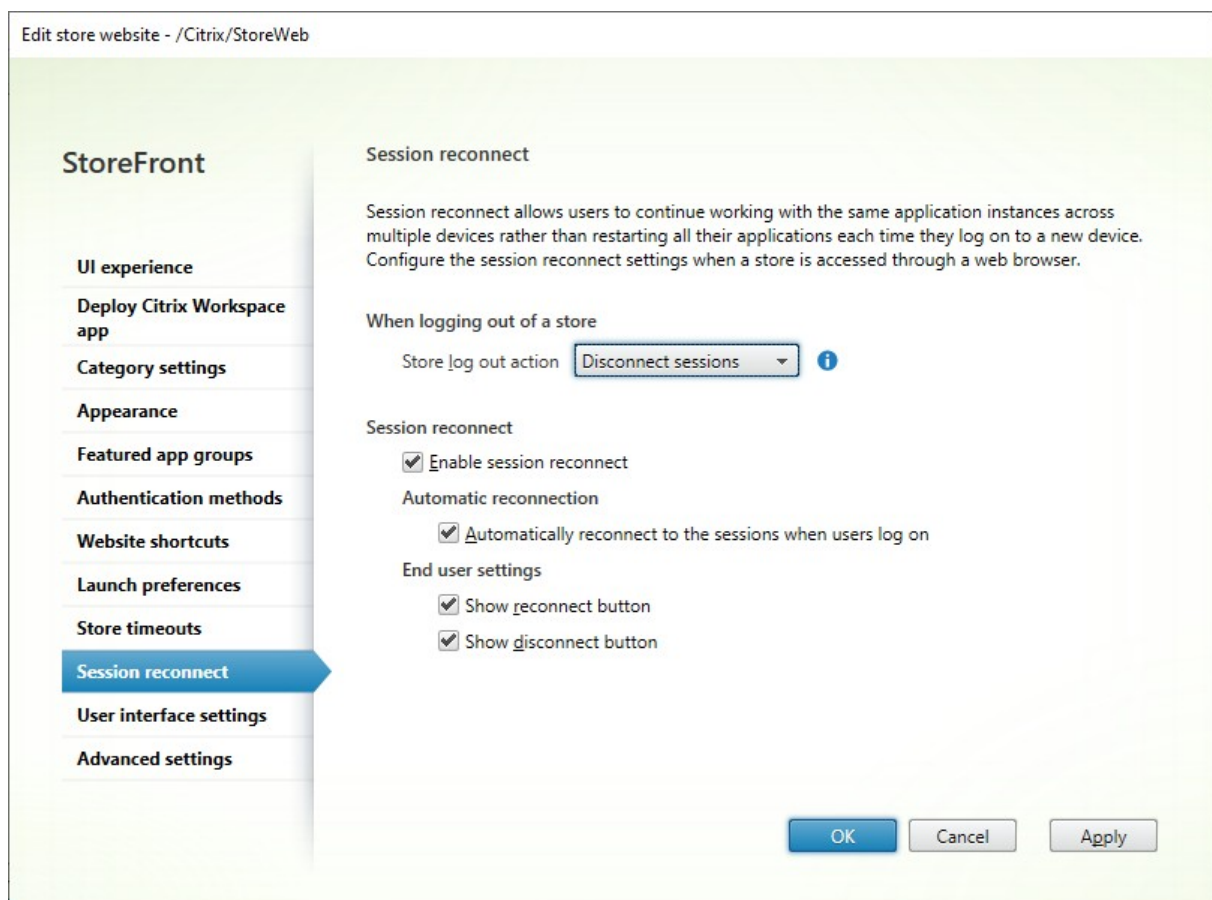
the case of accessing a store through a web browser, the same browser must be used to log on, start the applications, and log off.

## **Configure Session reconnect in a web browser**

The session reconnect settings within StoreFront management console only apply when accessing the store through a web browser. This is subject to the following requirements and restrictions:

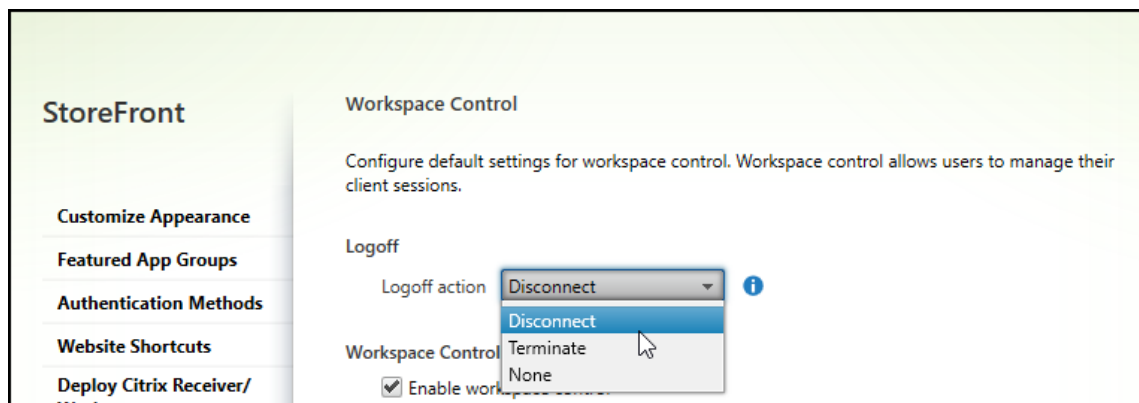
- Session reconnect is not available when the web browser is running within a hosted desktops or application.
- For users accessing websites from Windows devices, session reconnect is only enabled if the site can detect that Citrix Workspace app for Windows is installed on users' devices or if resources open with the web browser.
- 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 session reconnect configuration.
- Due to browser limitations, [Citrix Workspace launcher](#) can only be used to reconnect one app. To reconnect to multiple apps, users should install [Citrix web extensions](#).
- 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 from the web client.
- Session reconnect is not available when resources open within the same browser tab. To configure this, see [Citrix Workspace app deployment](#).

To modify session reconnect settings when a store is accessed through a web browser, select **Session reconnect** on the [Edit store website](#) screen.



Configure settings for session reconnect as follows:

- Specify the **Logoff action**. The log off actions are as follows:
  - **Disconnect sessions:** When you log off from the website, the app and desktop sessions are automatically disconnected from the client device.
  - **Log off sessions:** When you log off the site, app and desktop sessions are automatically logged off on the server.
  - **None:** When you log off from the site, app and desktop sessions remain running.



- **Automatically reconnect to the sessions when users logon** - when the user logs, all disconnected sessions are reconnected on the local device.

## End user settings

When using the classic experience, you can allow users to disconnect and reconnect sessions using the following settings:

- **Show reconnect button** - displays a **Reconnect** button that reconnects all disconnected sessions on the current device.
- **Show disconnect button** - displays a **Disconnect** button that reconnects all disconnected sessions on the current device.

These settings have no effect on the modern experience. Instead use **Activity manager** to disconnect and reconnect sessions.

## Configure Session reconnect using PowerShell

To configure session reconnect using [PowerShell](#), run cmdlet [Set-STFWebReceiverUserInterface](#).

## Configure Session reconnect on Workspace app for Windows

To configure Session reconnect on Workspace for Windows, see [Manage workspace control reconnect](#).

## Configure Session reconnect on Workspace app for Mac

To configure Session reconnect Workspace app for Mac, see [Configure workspace control settings](#).

## Disable Session reconnect across all apps

You can disable session reconnect in StoreFront across Workspace apps, regardless of how they are configured. For more information, see [Allow session reconnect](#).

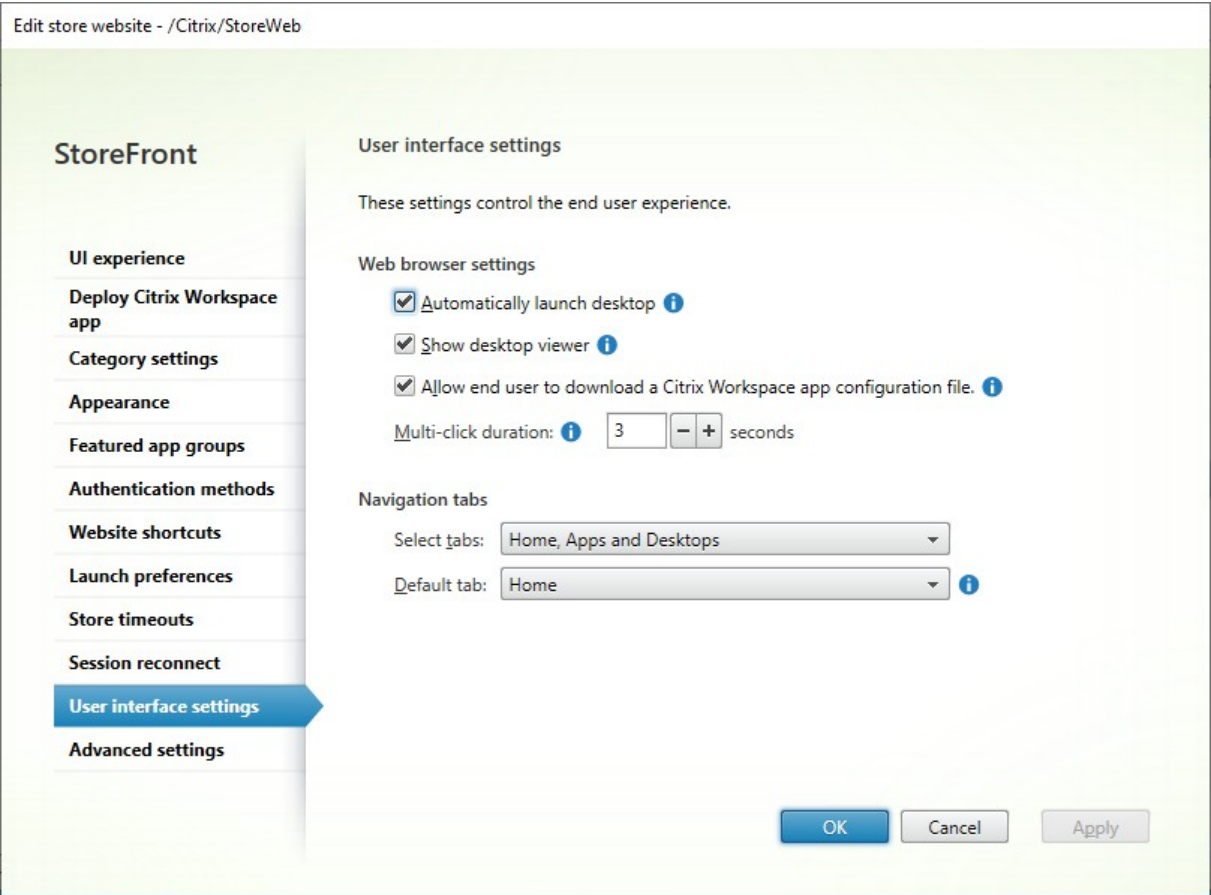
## User interface settings

November 5, 2025

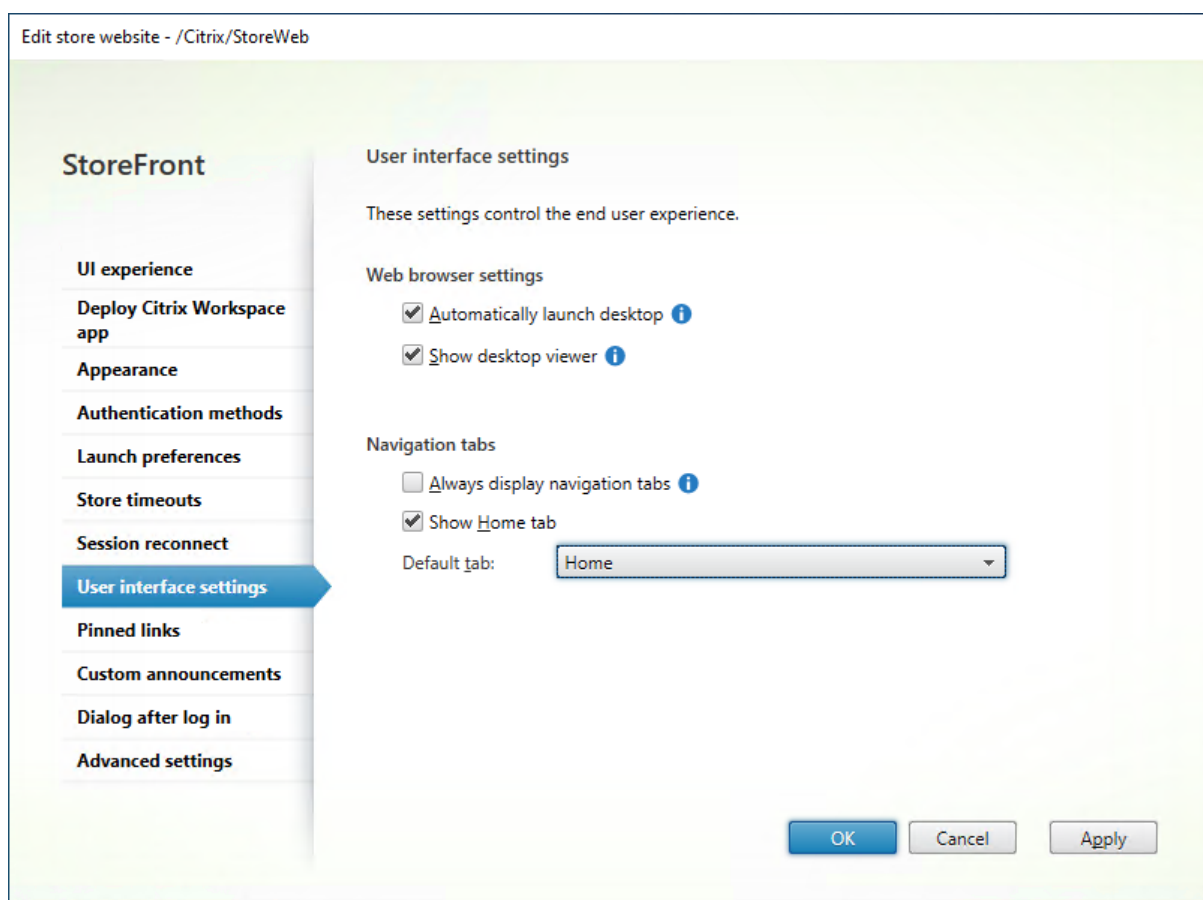
To modify user interface settings, open the [Edit store website](#) screen and the **User interface settings** tab.

The settings available depend on which [UI experience](#) is selected.

For the classic experience:



For the modern experience:



## 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 [PowerShell](#) to change auto launch desktop setting, run cmdlet [Set-STFWebReceiverUserInterface](#) with parameter [AutoLaunchDesktop](#).

This setting applies when launching resources from a web browser. It does not apply when launching resources from locally installed Citrix Workspace™ apps.

To use [PowerShell](#) to change this option call cmdlet [Set-STFWebReceiverUserInterface](#) with parameter [AutoLaunchDesktop](#).

## 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. The desktop viewer provides the best user experience and is enabled by default.

This setting only applies when [hybrid launching](#) resources from a web browser, using the Windows, Linux and other locally installed HDX clients. When a user launches resources in their web browser using the HTML5 HDX client it always shows the toolbar regardless of this setting.

To use [PowerShell](#) to change this option call cmdlet [Set-STFWebReceiverResourcesService](#) with parameter [ShowDesktopViewer](#).

## **Allow end user to download a Citrix Workspace app configuration file**

If selected, when accessing the store using a web browser, users can download a provisioning file that configures Citrix Workspace app 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 [PowerShell](#) to change this option call cmdlet [Set-STFWebReceiverUserInterface](#) with parameter [ReceiverConfigurationEnabled](#).

## **Multi-click duration**

Prevent users from launching the same application multiple times in the configured duration. This only when launching resources from a web browser and not from locally installed Citrix Workspace app.

To use [PowerShell](#) to change the multi-click duration, run cmdlet [Set-STFWebReceiverUserInterface](#) with parameter [MultiClickTimeout](#).

This setting only applies when launching resources from a web browser. It does not apply to locally installed Citrix Workspace apps.

## **Navigation tabs**

The settings available depend on which [UI experience](#) is selected.

### **Modern experience**

**Always display navigation tabs** By default, if there are fewer than 20 resources, the UI displays a simple view where all the resources are on one screen without tabs. Administrators can select the Always display navigation tabs option, effectively disabling the simple view. When selected, users see the navigation tab regardless of the resource count.



**Disable home tab** By default, the UI includes a Home tab (except in simple view) that displays favorite and recent apps and desktops. The Home tab provides quick access to favorites and recently used apps and desktops. Administrators can now clear the Show home tab option to hide it. Favorites are still available from the individual Apps or Desktops tabs.

**Default tab** By default, after logging in, users land on the Home tab. You can change the Default tab so that users land on the **Apps** or **Desktops** tab. If you have selected **Apps**, then, in addition, you can choose whether by default it shows all Apps, apps in a particular category, or uncategorized apps.

## Classic experience

When both desktops and applications are available, the website 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 tabs** drop-down list, select whether to display apps or desktops, or both.

From the **Default tab** view drop-down list, select which tab to display when the user first logs in.

| Option   | Description              |
|----------|--------------------------|
| Home     | Display the Home tab     |
| Apps     | Display the Apps tab     |
| Desktops | Display the Desktops tab |

To use PowerShell to change these options, run cmdlet [Set-STFWebReceiverUserInterface](#) with parameters [ShowAppsView](#), [ShowDesktopsView](#) and [DefaultView](#).

## Pinned links

October 22, 2025

### Note:

This functionality is available only using the [modern experience](#).

Custom URLs on StoreFront™ UI refer to customer-defined hyperlinks that provide quick access to specific websites. This feature functions as a shortcut that helps users to efficiently navigate to websites directly from the StoreFront UI. Important links, such as support websites or company portals, can be

made available to the users without needing them to search for these links. It makes the navigation effortless and faster. This feature is only available on the modern experience.

## Configuration

To add a pinned link:

1. Go to [Edit store website](#) and select the **Pinned Links** tab.

Edit Receiver for Web site - /Citrix/StoreWeb

**StoreFront**

- UI Experience
- Deploy Citrix Receiver/Workspace app
- Customize Appearance
- Authentication Methods
- Launch Preferences
- Session Settings
- Client Interface Settings
- Pinned Links**
- Advanced Settings

**Pinned Links**

Add up to 20 links and pin them to the top of the store for easy access

☒ Enable pinned links

| Icon | Name    | Link                        |
|------|---------|-----------------------------|
|      | Support | https://support.example.com |

Add... Edit... Remove

OK Cancel Apply

2. Click **Add**.

Add Pinned Links

Name:

Link:  
(Required)

Icon:  
(80 x 80 px)

Tooltip Text:

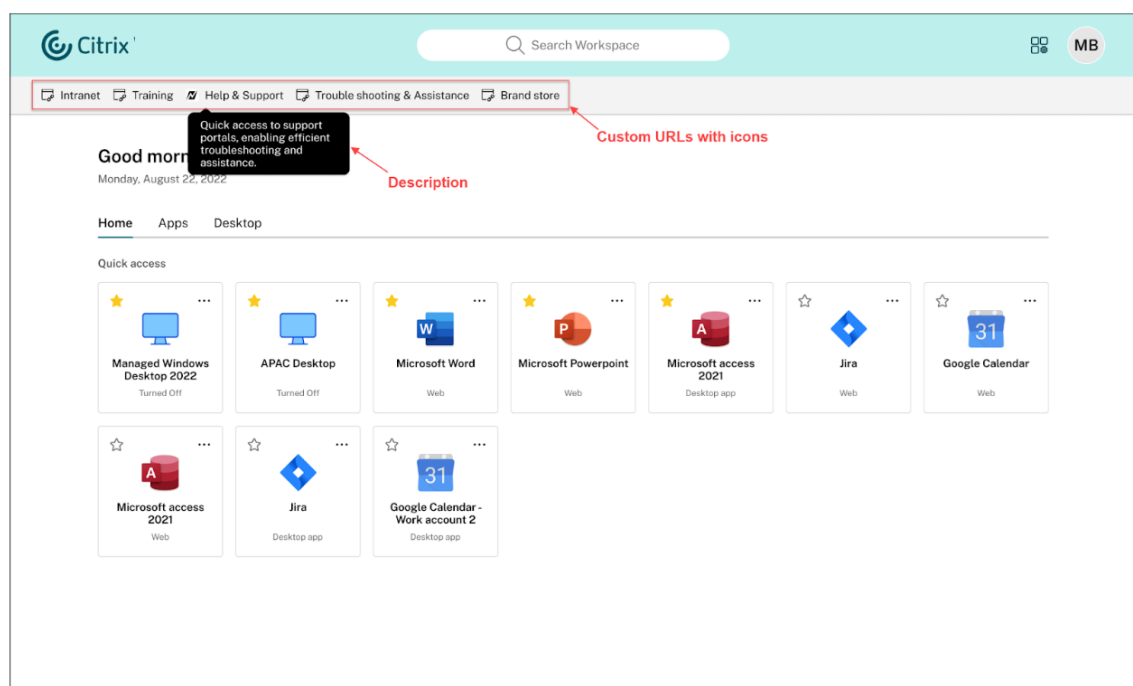
Preview:

Support

FL

3. Enter the name, link, tool tip, and browse for the icon.
4. Preview the updates and click **OK**.

These links appear on top of the store for quick access.



## Custom announcements

October 22, 2025

You can configure a banner that is displayed to the end-users, for instance to notify them of upcoming changes or maintenance windows.

**Note:**

This functionality is available only using the [modern experience](#). If you are using the classic experience then you create a custom announcement using the [StoreFront Client UI Customization API](#). See example [Add a dynamic header](#).

To set or modify a the custom announcement:

1. Go to [Edit store website](#)
2. Select the **Category Settings** tab.
3. Select **Enable custom announcement**.
4. Enter a **Title**.
5. Enter a **Description**.
6. Enter the date and time you wish the custom announcement to start being displayed.
7. Enter the date and time you wish the customer announcement to be hidden.
8. Choose whether to display the announcement at the top or the bottom of the screen.

Edit store website - /Citrix/StoreWeb

StoreFront

UI experience

Deploy Citrix Workspace app

Appearance

Authentication methods

Launch preferences

Store timeouts

Session reconnect

User interface settings

Pinned links

Custom announcements

Dialog after log in

Advanced settings

Custom announcements

Send a custom announcement so end users stay up-to-date on events such as maintenance windows, software updates, or expected outages.

☒ Enable custom announcement

Title:Upcoming maintenance window

Description:This store will be unavailable on 24th April from 22:00 to 23:00

Time period

Start:01 April 2025 00:00:00UTC

End:24 April 2025 22:00:00

Position

☒ Top

☐ Bottom

OK

Cancel

Apply

When users log in, the announcement is displayed permanently at the top or bottom of the screen.

The screenshot shows the Citrix Workspace user interface. At the top, there is a blue header bar with the Citrix Workspace logo, a search bar labeled "Search Workspace", and user profile icons. Below the header, a red-bordered banner displays a custom announcement: "Upcoming maintenance window" followed by "This store will be unavailable on 24th April from 22:00 to 23:00". Below the banner, the main content area shows a greeting "Good afternoon, Joe Bloggs" with the date "Friday, March 14, 2025". There are tabs for "Home", "Apps", and "Desktops". Under the "Home" tab, there is a "Quick access" section with two app tiles: "Calculator Cloud" and "Excel 2016 Cloud", both labeled as "Desktop App". At the bottom of the interface, it says "Powered by Citrix" and "storefront-eu-1".

© 1997–2025 Citrix Systems, Inc. All rights reserved.

216

## Dialog after login

October 22, 2025

You can configure a pop-up dialog that appears after login, which users must accept before interacting with StoreFront. You can use this to inform users about important information such as regulatory information, policy acknowledgments, internal policies, instructional content, security notices, system updates, and legal disclaimers.

**Note:**

This functionality is available only using the [modern experience](#). If you are using the classic experience then you add a similar dialog using the [StoreFront Client UI Customization API](#). See example [Show a disclaimer message before or after sign in](#).

To set or modify the dialog:

1. Go to [Edit store website](#)
2. Select the **Dialog after log in** tab.
3. Select **Enable dialog prompt**.
4. Enter the **Title**, **Description** and **Button text**.
5. Choose how often the message should be displayed. If you choose **Repeat display** then you can choose between **every day**, **every 7 days** and **every 30 days**. If you change the message, the prompt always appears the next time the user logs in.

Edit store website - /Citrix/StoreWeb

## StoreFront

- UI experience
- Deploy Citrix Workspace app
- Appearance
- Authentication methods
- Launch preferences
- Store timeouts
- Session reconnect
- User interface settings
- Pinned links
- Custom announcements
- Dialog after log in**
- Advanced settings

### Dialog after log in

Create a dialog prompt that displays to the user after logging into their store. Include details such as an agreement or policy before accessing the store, organization information, or step-by-step guidance.

☒ Enable dialog prompt

Title:

Description:

Button text:

Display frequency

☒ Display only the first time the user logs into the store

☐ Repeat display

For more information on the end user experience, see [Modern Experience](#).

## App Protection

November 5, 2025

App Protection provides an extra level of security by blocking key logging and screen capture. For more information, see the [App Protection](#) documentation.

### Important:

When accessing a store through a web browser, apps requiring App Protection are hidden by default. StoreFront must be configured to display protected apps. When accessing a store through Citrix Workspace app, no StoreFront configuration is required.

## App Protection for launches from Citrix Workspace app

When users access the store using a [supported version of Citrix Workspace app](#), StoreFront displays all resources requiring App Protection. No additional StoreFront configuration is required.

## App Protection for hybrid launch

When users access a store through a web browser, virtual apps and desktops requiring App Protection are hidden by default. StoreFront 2308 and higher can be configured to display protected resources, unless using ChromeOS, or the user has chosen to launch resources in their web browser, as these do not support App Protection.

### Warning

It is possible to launch apps using older versions of Citrix Workspace app that do not apply App Protection. Therefore before you enable App Protection for hybrid launches, Citrix recommends that you enable [App Protection Posture Check](#) which blocks launching virtual apps and desktops from Citrix Workspace app versions that do not support App Protection.

If launching resources using ICA downloads, the user could edit the ICA file to remove the instruction to apply App Protection. Therefore before you enable App Protection for hybrid launches, Citrix recommends that you enable [Policy Tampering Detection](#).

Versions of StoreFront earlier than 2507 attempted to detect the version of Citrix Workspace app installed using [Citrix web extensions](#) or [Citrix Workspace launcher](#) and only displayed resources with App Protection if the client met certain minimum versions. However it was not possible to guarantee that the version was correctly detected which lead to resources being incorrectly shown or hidden. Therefore this check has been removed.

## Enable App Protection for hybrid launch

To allow StoreFront to display protected apps on supported Citrix Workspace app versions, use the PowerShell cmdlet [Set-STFWebReceiverAppProtection](#).

1. Open a PowerShell console as an administrator.
2. If you have more than one website, find the virtual path of the website you wish to configure. This is the path that appears in the user's web browser, e.g. [/Citrix/StoreWeb](#). You can get a list of all websites and their path using the command [Get-STFWebReceiverService](#).
3. Run the powershell:



```
1 $receiver = Get-STFWebReceiverService -VirtualPath "[virtual path]"
2 Set-STFWebReceiverAppProtection -WebReceiverService $receiver -
 Enabled On
```

Replacing `[virtual path]` with the path found in the first step. `-VirtualPath` can be excluded if there is only one website.

4. If the user has chosen to open resources in their web browser, either through admin configuration or because the user chose **Use web browser**, App Protection is not available. You can optionally configure the store to always launch using locally installed Citrix Workspace app. For more information, see [Citrix Workspace app deployment](#).
5. The first time the user opens a store website, if Citrix web extension is not available then it displays the **Detect Citrix Workspace app** screen. If the user chooses **Skip detection** then StoreFront is unable to determine the app version so does not display protected apps and desktops. Therefore it is recommended that you disable the **Skip detection** option. For more information, see [Allow users to skip Citrix Workspace app detection](#).

### View whether App Protection for hybrid launch is enabled

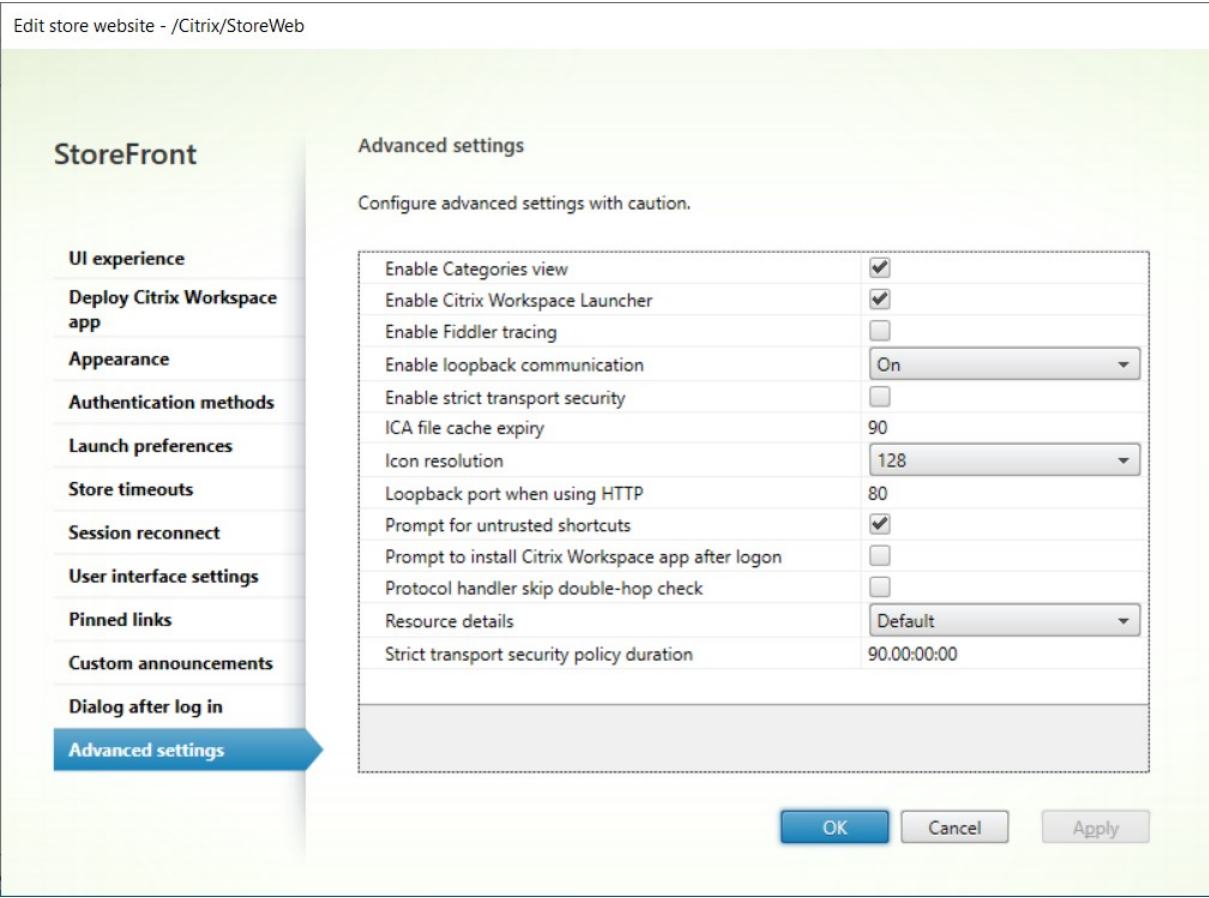
To find out whether App Protection for hybrid launch is available for a store website using [PowerShell](#), run cmdlet [Get-STFWebReceiverAppProtection](#). For example:

```
1 $receiver = Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"
2 Get-STFWebReceiverAppProtection -WebReceiverService $receiver
```

## Advanced settings

November 12, 2025

To modify advanced settings for a website, open the [Edit store website](#) screen and select the **Advanced settings** tab.



### Enable Fiddler tracing

Enables [Fiddler](#) tracing of the traffic between StoreFront services for debugging purposes. Loopback communication must also be disabled. This is off by default and should only be enabled if requested by support. Once you have completed troubleshooting, disable Fiddler tracing.

### Enable Folder view

By default, on the **Apps** tab there is **Categories** view. To hide the **Categories** view, clear **Enable folder view**. Only applies to the classic experience. Has no effect when using the modern experience. For more information on display of categories, see [Category settings](#).

To modify this setting using PowerShell, run cmdlet `Set-STFWebReceiverUserInterface` with paramater `EnableAppsFolderView`.

## Enable loopback communication

Enables direct communication between StoreFront™ services without going via the base URL. Enable when using a load balancer. Can be set to the following values:

| Value                | Description                                                                                                                                                                                                                                                                 |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>On</b>            | The StoreFront web proxy communicates with the store service using the loopback address, ensuring that communication remains on the StoreFront server.                                                                                                                      |
| <b>Off</b>           | The StoreFront web proxy communicates with the store service using the FQDN defined in the base URL. If the base URL is a load balancer then could result in communication being directed via the load balancer to a different StoreFront server, causing requests to fail. |
| <b>On using HTTP</b> | As <b>On</b> but changes the protocol from HTTP to HTTPS. Select this option when using load balancer that terminate HTTPS, connecting to StoreFront over HTTP. To change the port, see <a href="#">Loopback port when using HTTP</a>                                       |

To modify this setting using PowerShell, run cmdlet [Set-STFWebReceiverCommunication](#) with paramater [Loopback](#).

## Enable Citrix Workspace Launcher

Enabled by default. When users open a store from a web browser, this allows the website to use [Citrix Workspace launcher](#) to attempt to detect whether Citrix Workspace app is installed and subsequently to launch resources.

To modify this setting using PowerShell, run cmdlet [Set-STFWebReceiverPluginAssistant](#) with paramater [Enabled](#).

Disabling this option can result in users [downloading ICA files](#) which is not recommended.

## Enable strict transport security

When enabled, adds the [Strict-Transport-Security](#) header to tell browsers to only connect to the website over HTTPS.

To modify this setting using PowerShell, run cmdlet `Set-STFWebReceiverStrictTransportSecurity` with parameter `Enabled`.

There are other ways to enable HSTS. For more information, see [HTTPS](https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security).

### ICA file cache expiry

The number of seconds for which an ICA file is cached in memory on the server. After the client initiates the launch and the ICA file is ready, the client must retrieve the ICA file within this time. Defaults to 90s.

To modify this setting using PowerShell, run cmdlet `Set-STFWebReceiverResourcesService` with parameter `IcaFileCacheExpiry`.

### Icon resolution

The icon file size to request from the server. Note this does not directly equate to the icon size displayed in the UI. The default is 128.

To modify this setting using PowerShell, run cmdlet `Set-STFWebReceiverResourcesService` with parameter `IconSize`.

### Loopback port when using HTTP

When Enable loopback communication is set to **On using HTTP**, this sets the port.

To modify this setting using PowerShell, run cmdlet `Set-STFWebReceiverCommunication` with parameter `LoopbackPortUsingHttp`.

### Prompt for untrusted shortcuts

When launching [website shortcuts](#), by default, if the referrer is not in the list of trusted sites then the user is prompted to confirm. If you disable this then users can launch resource from non-trusted websites.

### Prompt to install Citrix Workspace app after Logon

When a user first goes to the store website, the website attempts to detect Citrix Workspace app and provides the option to download Citrix Workspace app. By default, when accessing StoreFront directly, this occurs before the user logs in. Alternatively you can select **Prompt to install Citrix Workspace**

**app after logon.** This has no effect when users log in via a Citrix Gateway as this always occurs before the user reaches the StoreFront Citrix Workspace app detection screen.

To modify this setting using PowerShell, run cmdlet `Set-STFWebReceiverPluginAssistant` with parameter `ShowAfterLogin`.

## Resource details

Whether to fetch **Default** or **Full** resource details when using the Classic experience. Normally **Default** is sufficient. If you have a JavaScript customizations that uses the `preProcessAppData`, you can use the additional data returned by **Full**. Has no effect when using the modern experience.

## Strict transport security policy duration

If Strict transport security is enabled, the duration for which the strict transport policy is imposed, in format dd.hh:mm:ss. The default is 90 days.

To modify this setting using PowerShell, run cmdlet `Set-STFWebReceiverStrictTransportSecurity` with parameter `PolicyDuration`.

## Configure remote access settings

October 22, 2025

You can 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.
2. 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

3. 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.

4. 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](#).
5. 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.
6. 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](#).

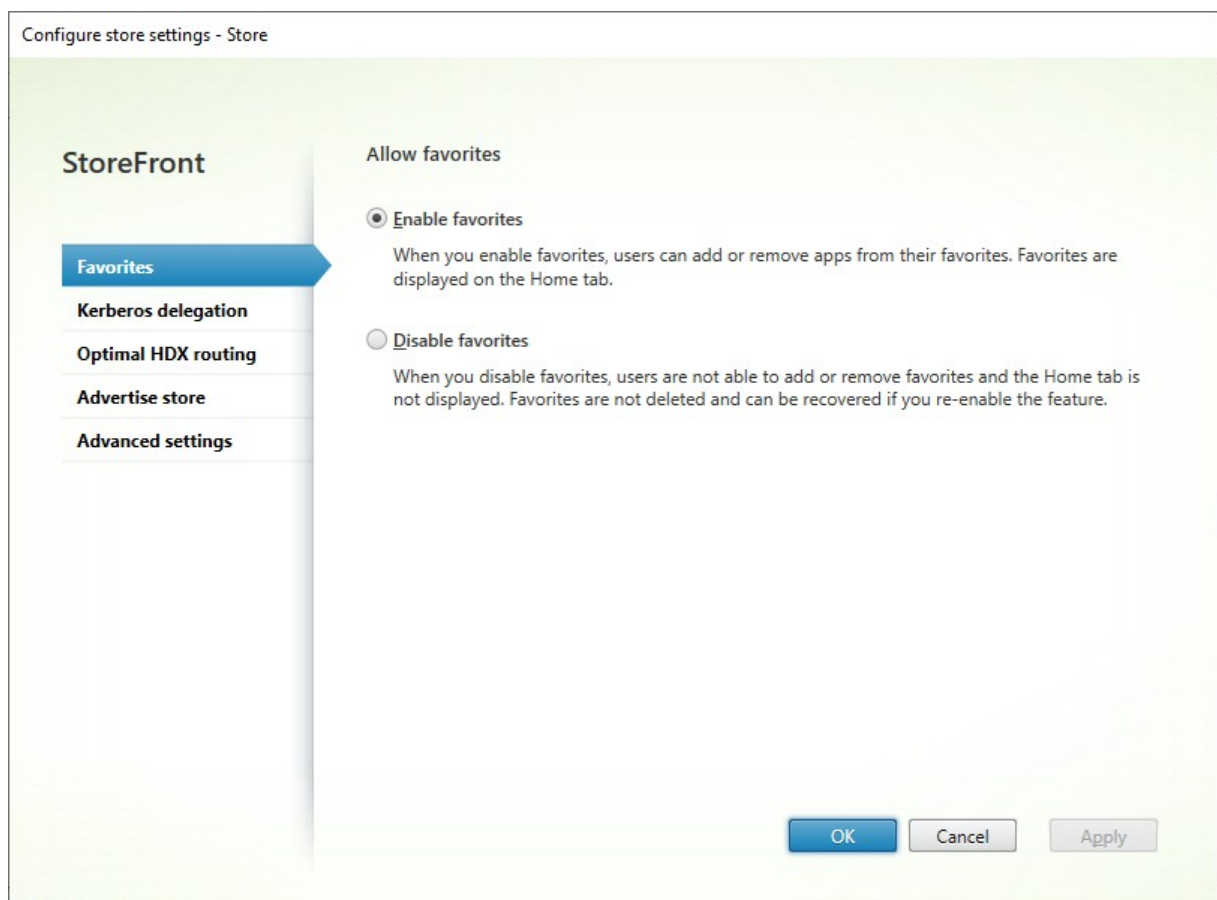
By default StoreFront uses the Gateway through which the user is connected to the store to launch resources. To configure StoreFront to launch resources using an alternative gateway or no gateway, see [Optimal HDX routing](#).

## Configure a Store

October 22, 2025

To modify a store settings:

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.



## Favorites

November 5, 2025

You can allow users to set resources to be favorites. These favorites are displayed on the user's home tab for quick access. If you are using the classic experience and disable favorites then the **Home** tab is hidden.

### Enable or disable favorites

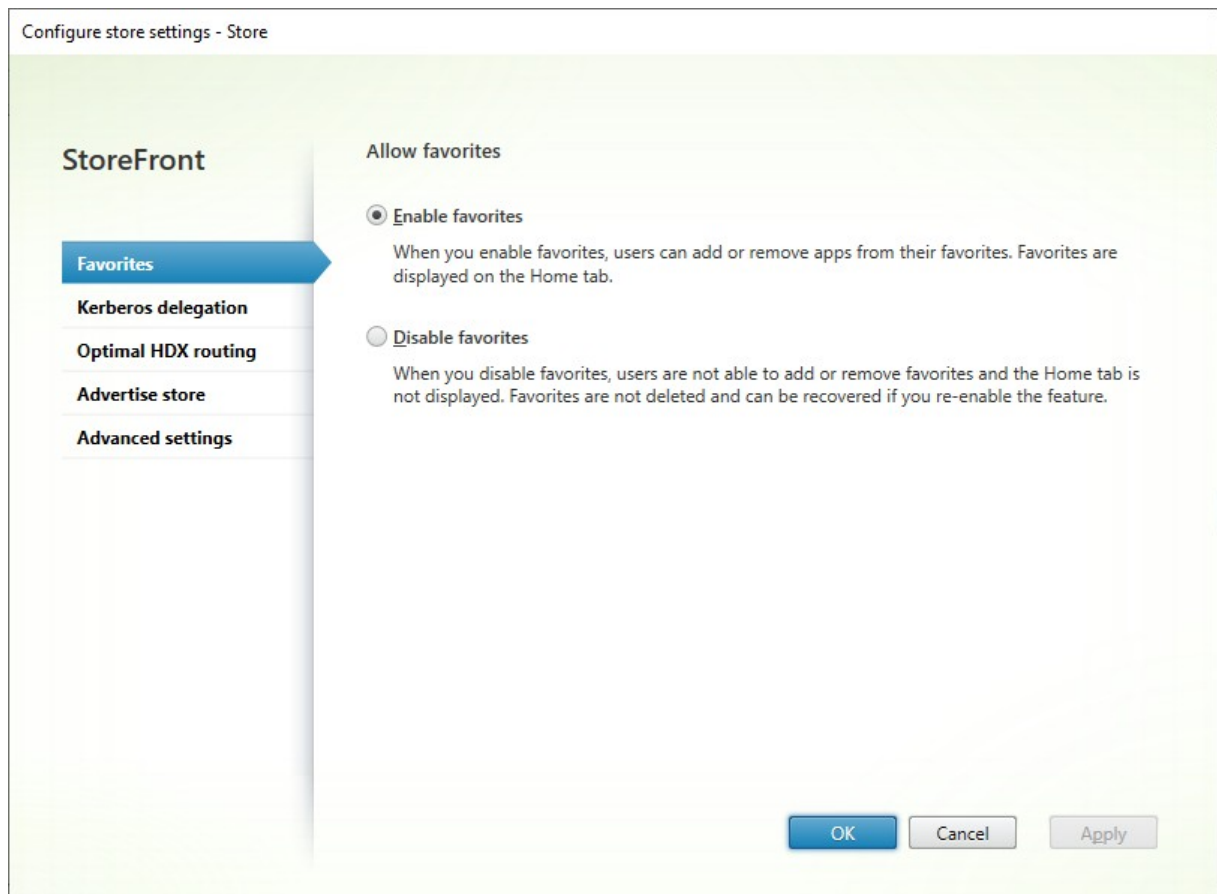
Use the Favorites to do select one of the following options:

- Allow users to create and remove favorites. Users can favorite an app by clicking the star on the app tile. Users can click the star again to un-favorite an app. Favorite apps are displayed on the **Home** tab.
- Disable favorites. 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 favorites 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 favorites** tab to toggle the user favorites feature off or on.
3. Choose **Enable user favorites** to enable favorites.
4. Choose **Disable user favorites** to disable favorites.



Alternatively, you can use the PowerShell cmdlet [Set-STFStoreService](#) with the [LockedDown](#) parameter. For example to disable favorites:

```
1 $StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/<
 yourstore>"
2 Set-STFStoreService -StoreService $StoreObject -LockedDown $True -
 Confirm:$False
```

## Favorites database

By default, favorites are stored in a local database that is replicated between servers in the server group. Alternatively, you can store favorites in an external SQL server database.

To view whether the store is using a local or external database run the PowerShell cmdlet `Get-STFStoreSubscriptionsDatabase`. For example:

```
1 $store = Get-STFStoreService -VirtualPath [store path]
2 Get-STFStoreSubscriptionsDatabase -StoreService $store
```

This returns:

- `UseLocalStorage` - if `True`, favorites are stored in the local database (the default). If `False`, favorites are stored in an external database.
- `DatabaseConnectionString` - if using an external database this contains the connection string. Otherwise it is blank.

For more information, see [Managing the subscriptions database](#).

### Use SQL server database

To use an external SQL server database, run PowerShell cmdlet `Set-STFStoreSubscriptionsDatabase`, specifying the connection string. For more information, see [Store subscription data using Microsoft SQL Server](#).

### Configure two StoreFront stores to share subscriptions datastore

Where different configuration settings are required, it is common for administrators to configure StoreFront with two distinct stores for the same resources; e.g. one for external access to resources using Citrix Gateway and another for internal access using the corporate LAN. If you are using a SQL server database, set both stores to use the same database connection string. When using a local database, StoreFront by default creates a separate database for each store. Therefore a user must favorite the same resource twice, once on each store. You can configure both stores to use the same database so users see the same favorites whichever store they connect to.

#### **Important:**

As the site name forms part of the key for a favorite, you must ensure that sites have exactly the same name in both stores.

E.g. suppose you have stores called “Internal” and “External”. When using a local database, use the following script to configure the “External” store to use the same subscriptions database as the “Internal” store.

```
1 $internalStore=Get-STFStoreService -VirtualPath '/Citrix/Internal'
2 $internalUri = $internalStore.SubscriptionStoreClient.ClientEndpoint.
 Uri.ToString()
3
```

```
4 $externalStore=Get-STFStoreService -VirtualPath '/Citrix/External'
5 $externalStore.SubscriptionStoreClient.ClientEndpoint.Uri = internalUri
6 Save-STFService $externalStore
```

Propagate the configuration to other servers in the server group.

To check which local database a store is using, run following script:

```
1 $store=Get-STFStoreService -VirtualPath '/Citrix/External'
2 $store.SubscriptionStoreClient.ClientEndpoint.Uri.ToString()
```

## Kerberos delegation

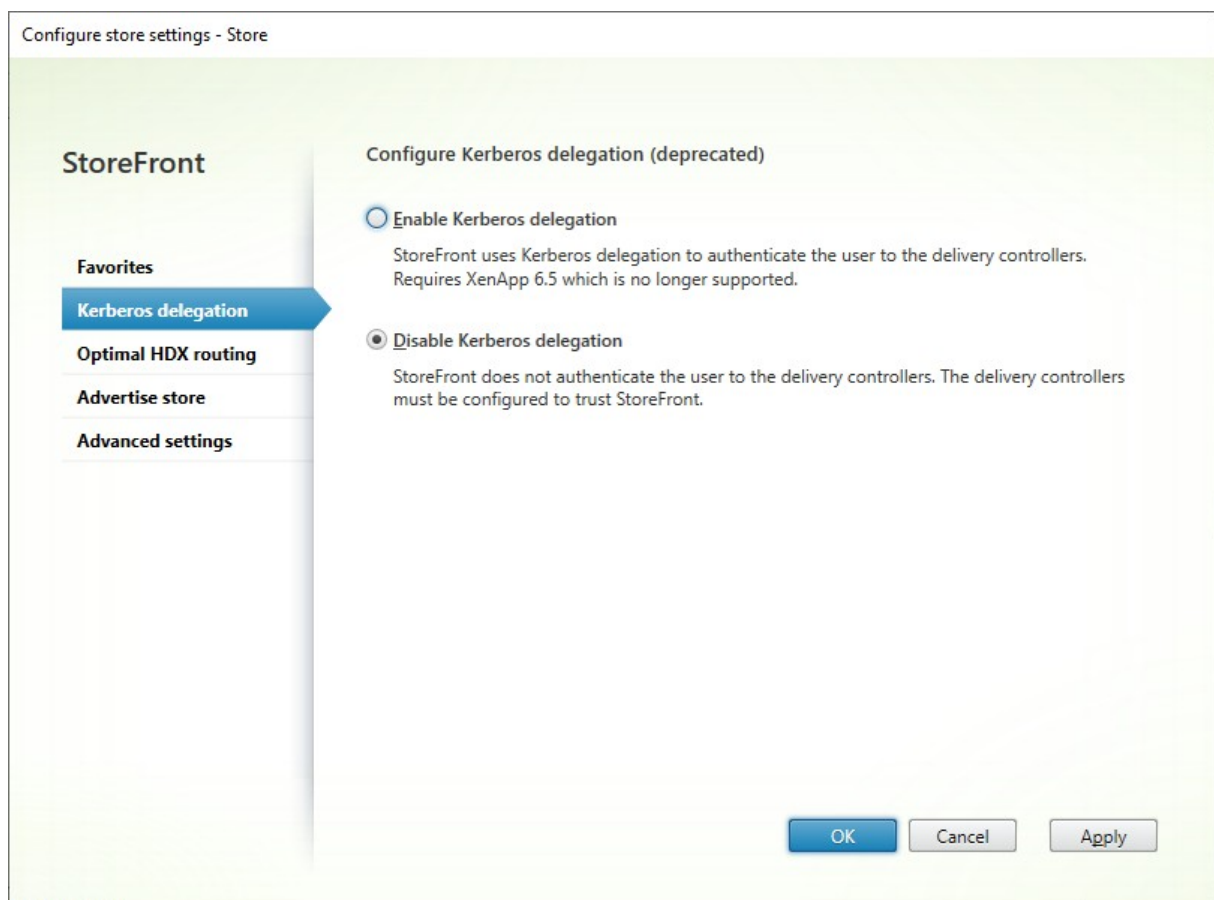
November 5, 2025

### 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

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

## Configure optimal HDX™ routing for a store

November 5, 2025

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 sites or to zones. A zone usually represents a data center in a geographic location. You can map an optimal gateway to more than one zone, but typically you should use a single zone. It is expected that each zone has at least one optimal Citrix Gateway that is used for HDX connections to resources within that zone.

When using Citrix Virtual Apps and Desktops, zones are defined in Studio and any zones defined in StoreFront must exactly match the zone names defined in Studio. For more information, see [Zones](#).

When using Citrix Desktops as a Service, a zone is equivalent to a resource location. Resource locations are defined in Citrix Cloud console and any zones defined in StoreFront must exactly match the resource location name defined in Citrix Cloud console. For more information, see [Set up resource locations](#).

### Example scenario using sites

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 sites in its sites list. UK users access remote resources through their geographically colocated gateway, StoreFront, and sites. If their UK sites 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 site 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

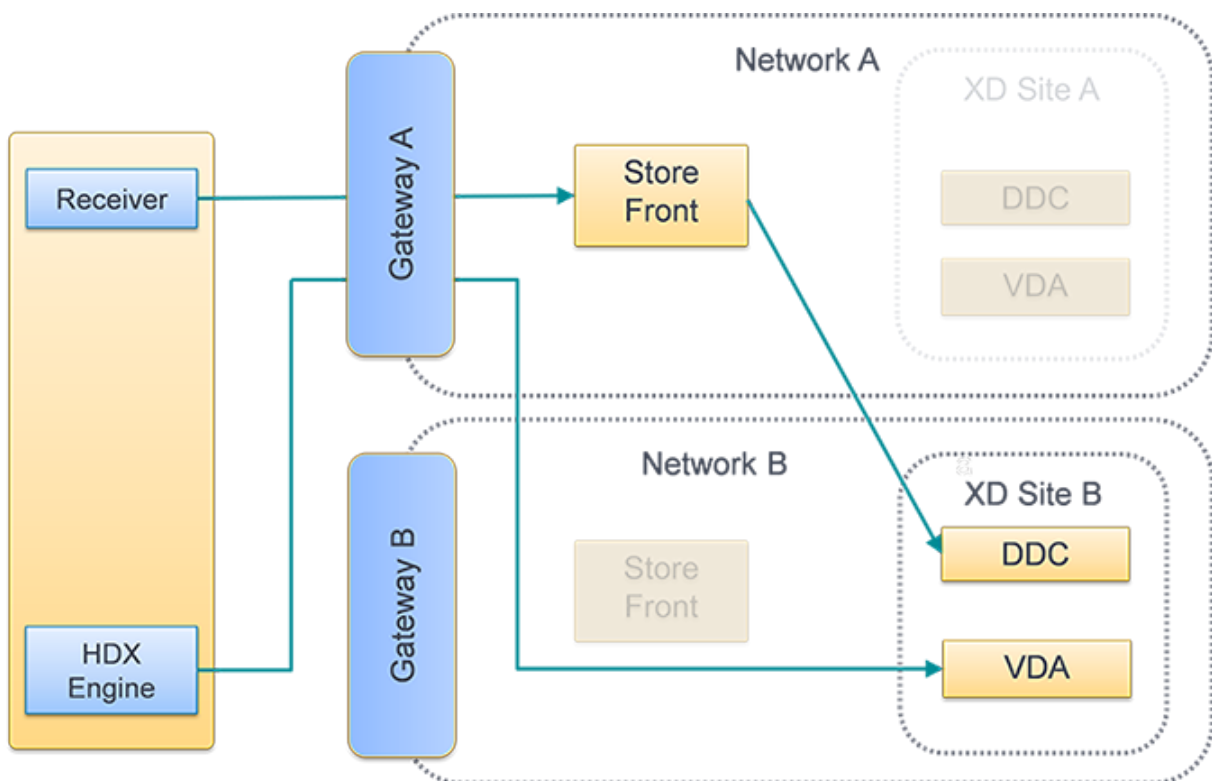
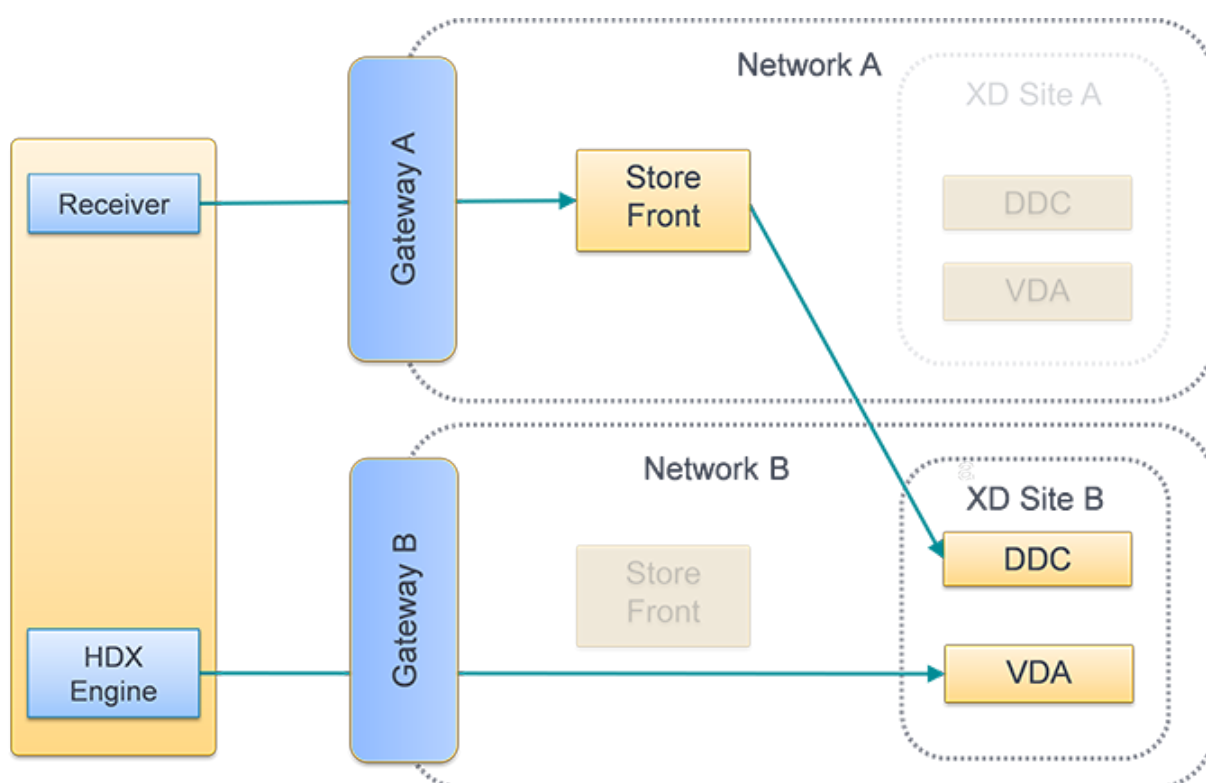
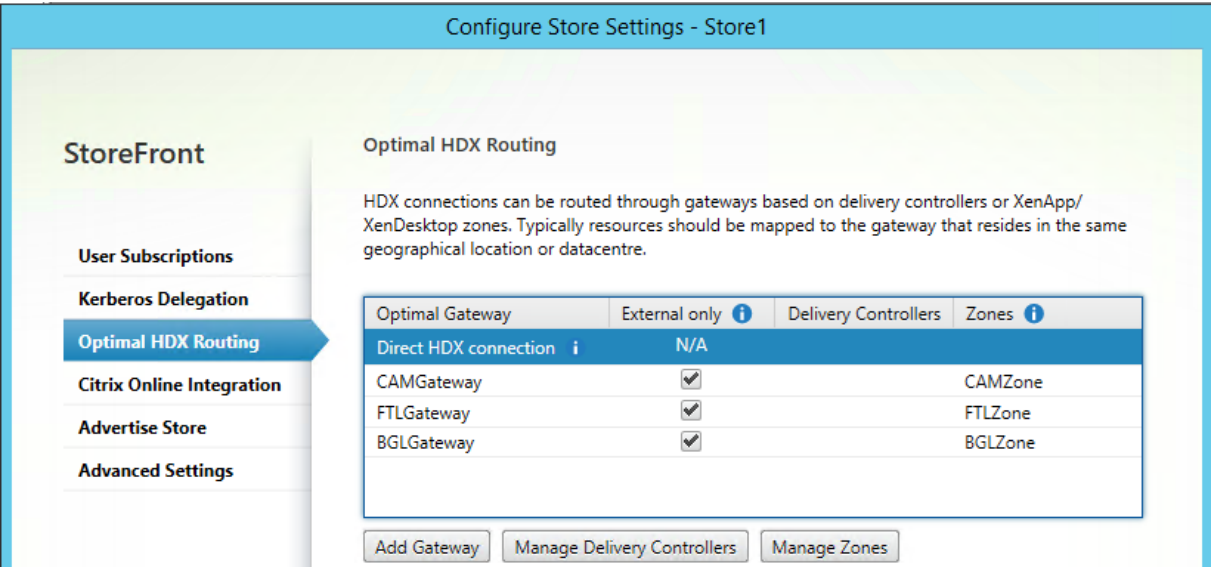


Figure 2. Optimal gateway routing



## 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 sites, click **Manage sites** and tick one or more sites.
  - b) To use the gateway when accessing resources from specific zones, click **Manage Zones** and enter one or more zone.
  - c) By default once you add a site 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 sites 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](#).

**Advertise or hide stores to users**

October 22, 2025

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.

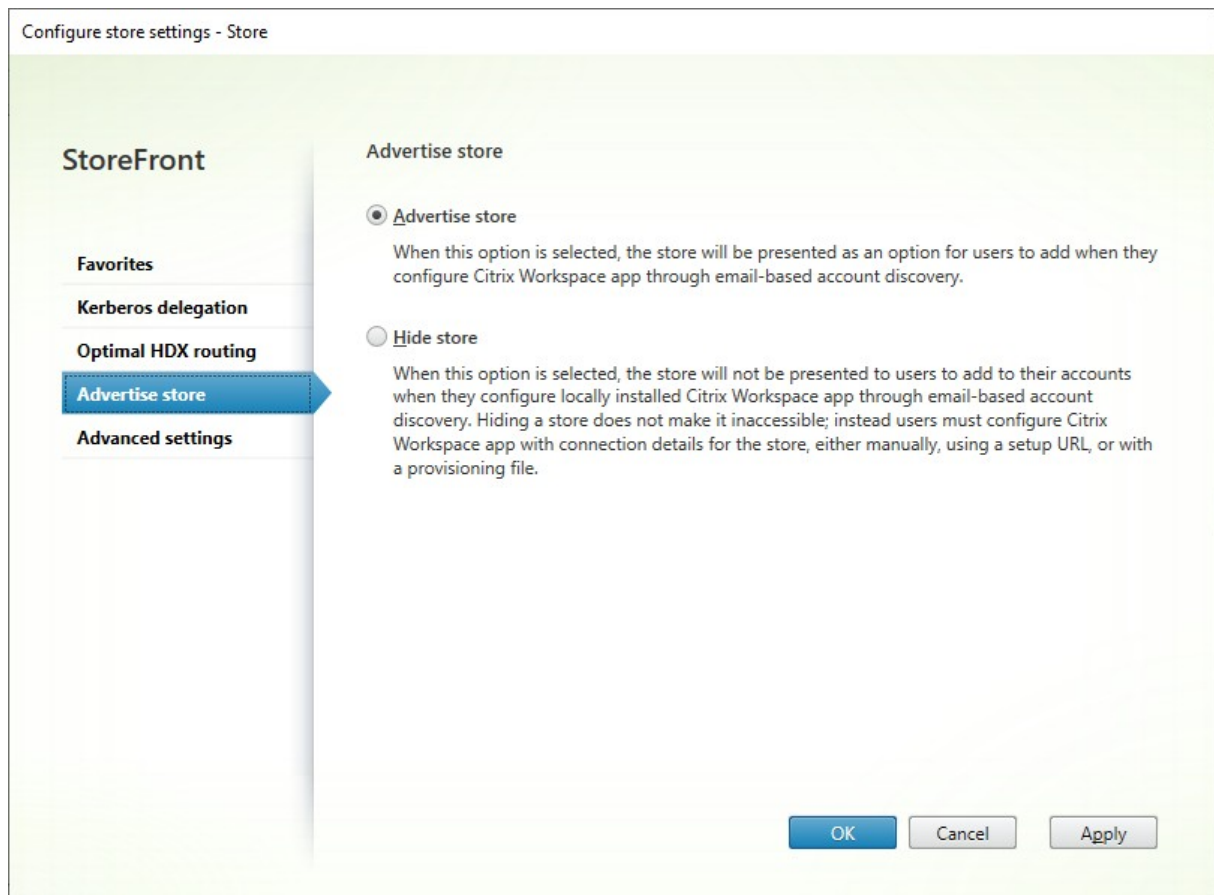
Important:

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**.



## Advanced store settings

November 5, 2025

You can configure most advanced store properties by using the Advanced Settings tab in [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.

| Setting                                  | Value                               |
|------------------------------------------|-------------------------------------|
| Address resolution type                  | DnsPort                             |
| Allow font smoothing                     | <input checked="" type="checkbox"/> |
| Allow session reconnect                  | <input checked="" type="checkbox"/> |
| Allow special folder redirection         | <input type="checkbox"/>            |
| Background health-check polling period   | 00:01:00                            |
| Communication timeout duration           | 30                                  |
| Connection timeout                       | 6                                   |
| Enable enhanced enumeration              | <input checked="" type="checkbox"/> |
| Enable socket pooling                    | <input type="checkbox"/>            |
| Filter resources by excluded keywords    |                                     |
| Filter resources by included keywords    |                                     |
| Filter resources by type                 |                                     |
| Maximum concurrent enumerations          | 0                                   |
| Minimum farms for concurrent enumeration | 3                                   |

At the bottom right are buttons for **OK**, **Cancel**, and **Apply**.

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 site to include all cloud connectors in all resource locations in the server list and enable the advanced health check feature.

Advanced health check is enabled by default. To enable or disable advanced health check, use the PowerShell cmdlet [Set-STFStoreFarmConfiguration](#) with parameter [AdvancedHealthCheck](#). Disabling advanced health check is not recommended as it would reduce resiliency.

## 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. To disable the health check, set the polling period to 00:00:00, this is not recommended. 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

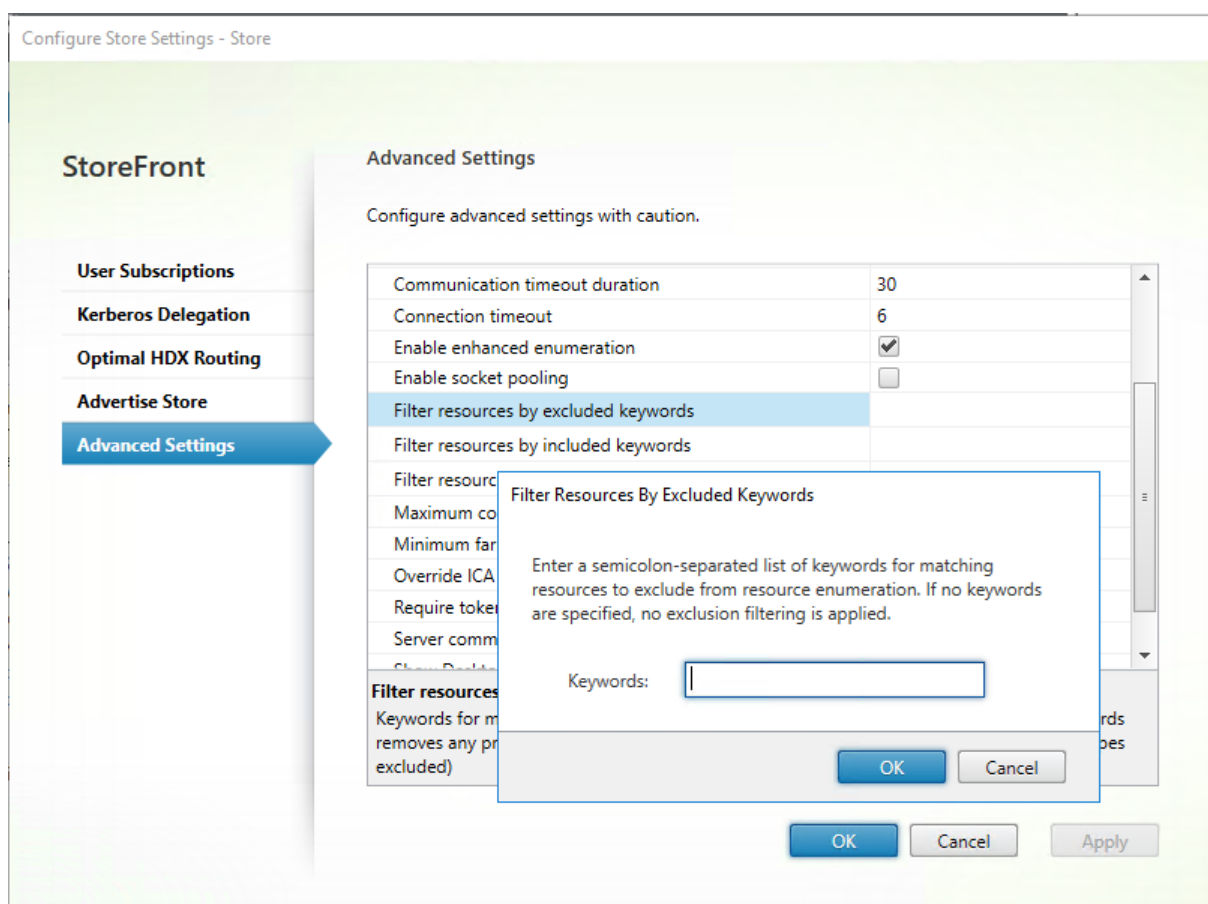
By default, file type association is enabled in stores so that content is seamlessly redirected to users' subscribed applications when they open local files of the appropriate types. To enable disable file type association, use the PowerShell command [Set-STFStoreFarmConfiguration](#). For example:

```
1 $storeService = Get-STFStoreService -VirtualPath '/Citrix/Store'
2 Set-STFStoreFarmConfiguration $storeService -EnableFileTypeAssociation
 $false
```

## 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**.

## Federated Authentication Service Configuration

November 5, 2025

[Federated Authentication Service](#) (FAS) provide single sign-on to VDAs using certificate authentication. This is useful when using authentication methods such as SAML, where StoreFront does not have access to the Active Directory credentials.



## Enable FAS for a Store

Before enabling FAS for a store, you must configure the list of FAS servers using Group policy. For more details see [FAS documentation](#).

To enable FAS for a store, you must use the PowerShell cmdlet [Set-STFStoreLaunchOptions](#) to set the VDA logon data logon provider to [FASLogonDataProvider](#).

For example to enable FAS for a store and select the server at login:

```
1 $store = Get-STFStoreService -VirtualPath [VirtualPath]
2 Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider "
 FASLogonDataProvider"
```

To disable FAS for a store:

```
1 $store = Get-STFStoreService -VirtualPath [VirtualPath]
2 Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
```

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

When using [username and password authentication](#) on a store with FAS enabled, StoreFront always uses FAS rather than the supplied credentials for single sign-on.

## Select FAS server at log in

By default, StoreFront selects the FAS server at launch. You can change this so that StoreFront selects the FAS server at login. This is not normally required but you can enable this if FAS selection is slow to avoid delays at launch. To configure the behavior, run PowerShell cmdlet [Set-STFClaimsFactoryNames](#) with parameter [ClaimsFactoryName](#). To choose the FAS server at login, set it to [FASClaimsFactory](#). To restore the default behavior and choose a FAS server at launch, set it to [standardClaimsFactory](#).

For example to choose a FAS server at log in:

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

## 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
```

## Export store provisioning files for users

October 22, 2025

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 website through a web browser.

To generate a provisioning file containing details for a single store

1. In the StoreFront management console select the **Store** node.
2. Select the store for which you wish to export a provisioning file.
3. From the **Actions** pane, select **Export provisioning file**.
4. Select **Export**.
5. Choose a location to save the file and select **Save**.

Export provisioning file

Distribute this file to your users to automate Citrix Workspace app setup.

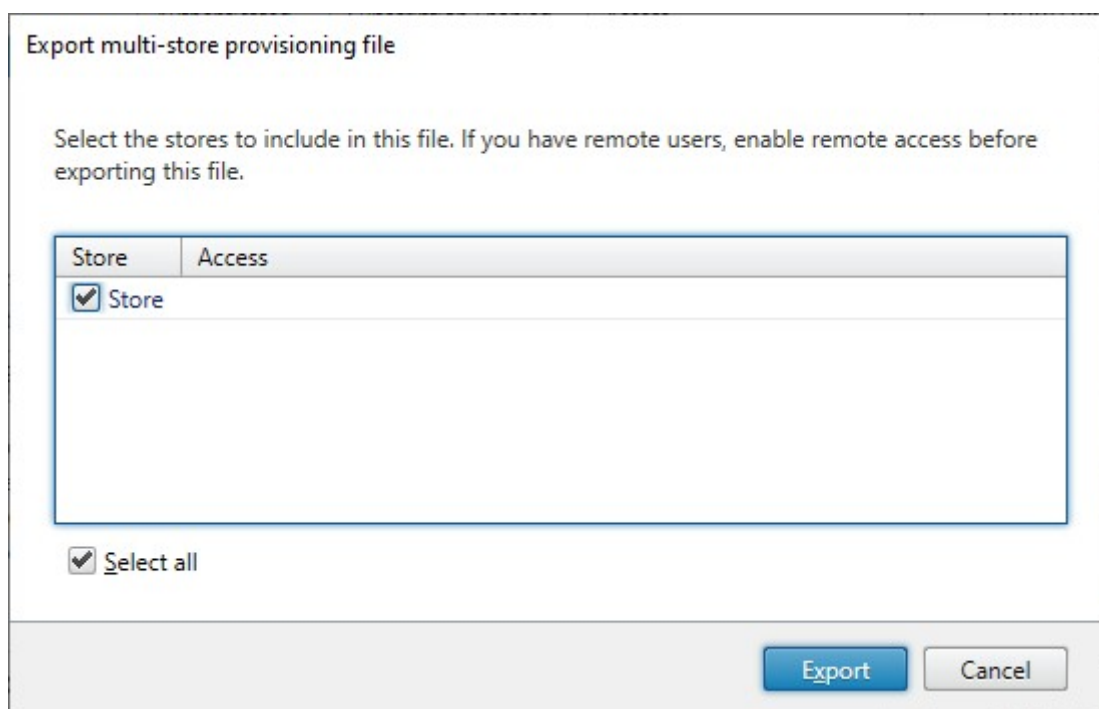
Name: Store  
URL: https://storefront.example.com/Citrix/Store  
Access: Internal and external networks

Details

Export Cancel

To generate a provisioning files for multiple stores:

1. In the StoreFront management console select the **Store** node.
2. In the Actions pane, click **Export multi-store provisioning file**
3. Select the stores to include in the file.
4. Select **Export**.
5. Choose a location to save the file and select **Save**.



## Configure session settings

October 22, 2025

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 particular 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.

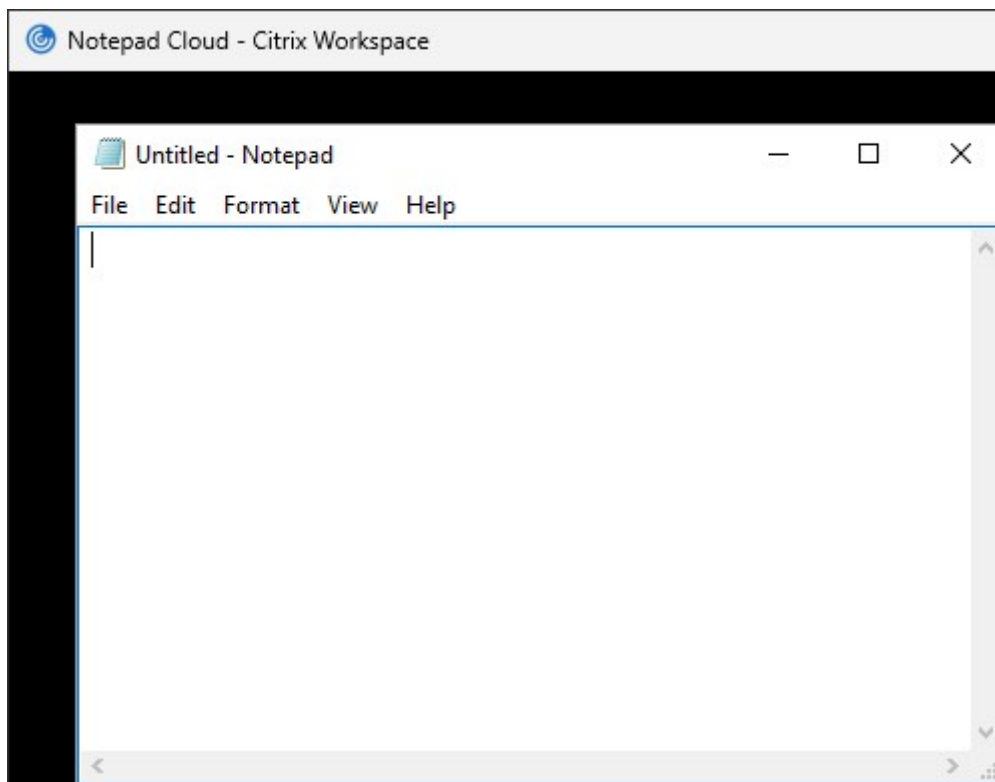
**Example: Launch Notepad in windowed mode**

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
```

**Citrix Workspace™ app configuration**

October 22, 2025

## 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>
```

### 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](#).

## Integrate with Citrix Gateway and NetScaler ADC

October 22, 2025

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                                                                                                                                                          |
|-------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">Import a Citrix Gateway</a>                                                         | Export configuration from your Citrix Gateway and import it into StoreFront                                                                                     |
| <a href="#">Manage Citrix Gateways</a>                                                          | Add, remove and edit Citrix Gateway connection settings                                                                                                         |
| <a href="#">Load balancing with NetScaler ADC</a>                                               | Configure NetScaler ADC as a load balancer in front of a StoreFront server group                                                                                |
| <a href="#">Configure NetScaler ADC and StoreFront for Delegated Forms Authentication (DFA)</a> |                                                                                                                                                                 |
| <a href="#">Authenticate using different domains</a>                                            | Configure StoreFront and Citrix Gateway so that users first authenticate with the gateway on one domain, then authenticate to StoreFront on a different domain. |
| <a href="#">Configure beacon points</a>                                                         | Configure beacon URLs that Citrix Workspace app can use to determine whether it is inside or outside your corporate network.                                    |
| <a href="#">Create a single FQDN used internally and externally</a>                             | 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.     |
| <a href="#">Require Citrix Workspace app when connecting through a gateway</a>                  |                                                                                                                                                                 |

---

## Configure Citrix Gateways

November 5, 2025

Use Citrix Gateways to provide authentication and remote access to StoreFront and your Virtual Delivery Agents (VDAs). Citrix Gateways run on a hardware or software NetScaler ADCs. The Citrix Gateway

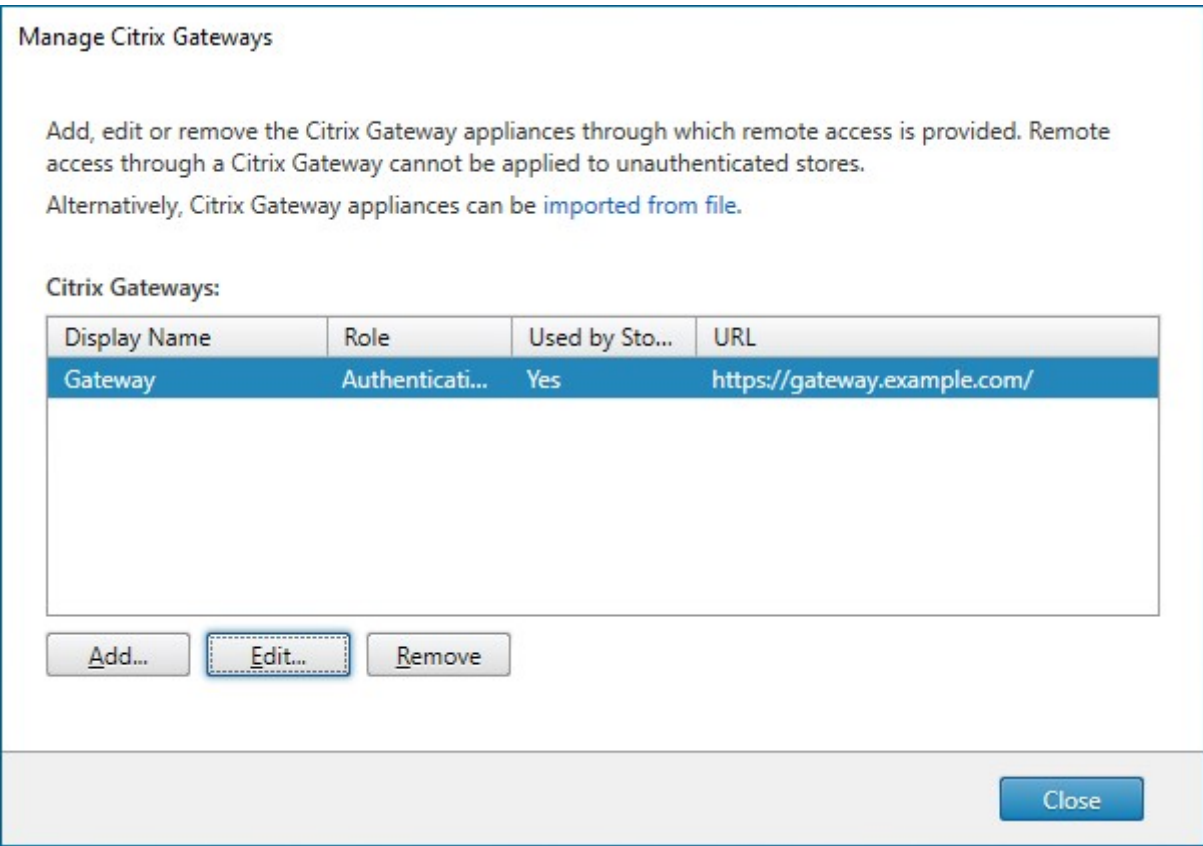
Service is managed by Citrix and can be used for HDX routing but not authentication or remote access to StoreFront.

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.



### PowerShell

To get a list of gateways and their configuration call [Get-STFRoamingGateway](#).

## Add Citrix Gateway appliance

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, 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.

- Set the **Gateway type** to **Citrix Gateway appliance**.
- 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 simplify 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"
```

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. This option prevents <a href="#">Citrix Workspace launcher</a> from working. Therefore, if you need to use hybrid launches, choose <b>Authentication and HDX routing</b> even when the gateway will only be used for authentication. |
| 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**

**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:

Gateway type:

Usage or role:

Citrix Gateway URL:

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 Citrix Workspace app detection and access to VDAs.

- Enter one or more Secure Ticket Authority server URL.
  - If you are using Citrix Virtual Apps and Desktops™ then you can use the delivery controllers as STA servers.
  - If you are using Citrix Desktop as a Service then you can use your cloud connectors as STA servers. These either proxy requests to the Citrix Cloud™ Ticketing Authority, or when in LHC mode generate their own tickets. In the future this will change so that they always generate their own tickets for improved resiliency.
  - It is recommended that you use at least 2 STA servers for redundancy.
  - When using Cloud Connectors as STA servers, it is recommended that you include all cloud connectors in at least one resource location. Firstly, within a resource location, Citrix Cloud ensures that only one cloud connector is upgraded at a time so including all connectors ensures that there is always at least one connector not being upgraded. Secondly, if the resource location goes into LHC mode then only the single Cloud Connector designated as the “elected broker” can issue STA tickets. As you cannot know

in advance which connector this will be, include all Cloud Connectors in the resource location.

- Ensure that all STA servers listed in StoreFront are also listed as STA servers in the Citrix Gateway virtual server. If any servers are missing from the Citrix Gateway, this can cause launches to fail. Today when using Cloud Connectors as STAs this may not be apparent in normal use as any connector can be used to redeem tickets from the Citrix Cloud Ticking Authority. However Local Host Cache mode the connector generates its own tickets and in the future this will become the default behavior.
- The Delivery Controller or Cloud Connector may be configured so that StoreFront must include a security key. It is not possible to add security keys using the GUI; see the later step for adding them using PowerShell.
- Select **Load balance multiple STA servers** to distribute requests between the STA servers. If cleared 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 **Enable session reliability**.
- If you configured multiple STAs, optionally select **Request tickets from two STAs, where available**.

When **Request tickets from two STAs, where available** 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 'Secure Ticket Authority (STA)' tab selected. The left sidebar shows 'StoreFront' with 'General Settings' checked, and 'Secure Ticket Authority' selected under 'Authentication Settings'. The main area contains the following configuration options:

- Secure Ticket Authority (STA)**: 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.
- Secure Ticket Authority URLs**: A list box containing two URLs: `https://ddc1.example.com/scripts/ctxsta.dll` and `https://ddc2.example.com/scripts/ctxsta.dll`. There are 'Add...', 'Edit...', and 'Remove' buttons below the list.
- ☐ **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**

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: (optional) 10.1.0.18

Logon type: Domain

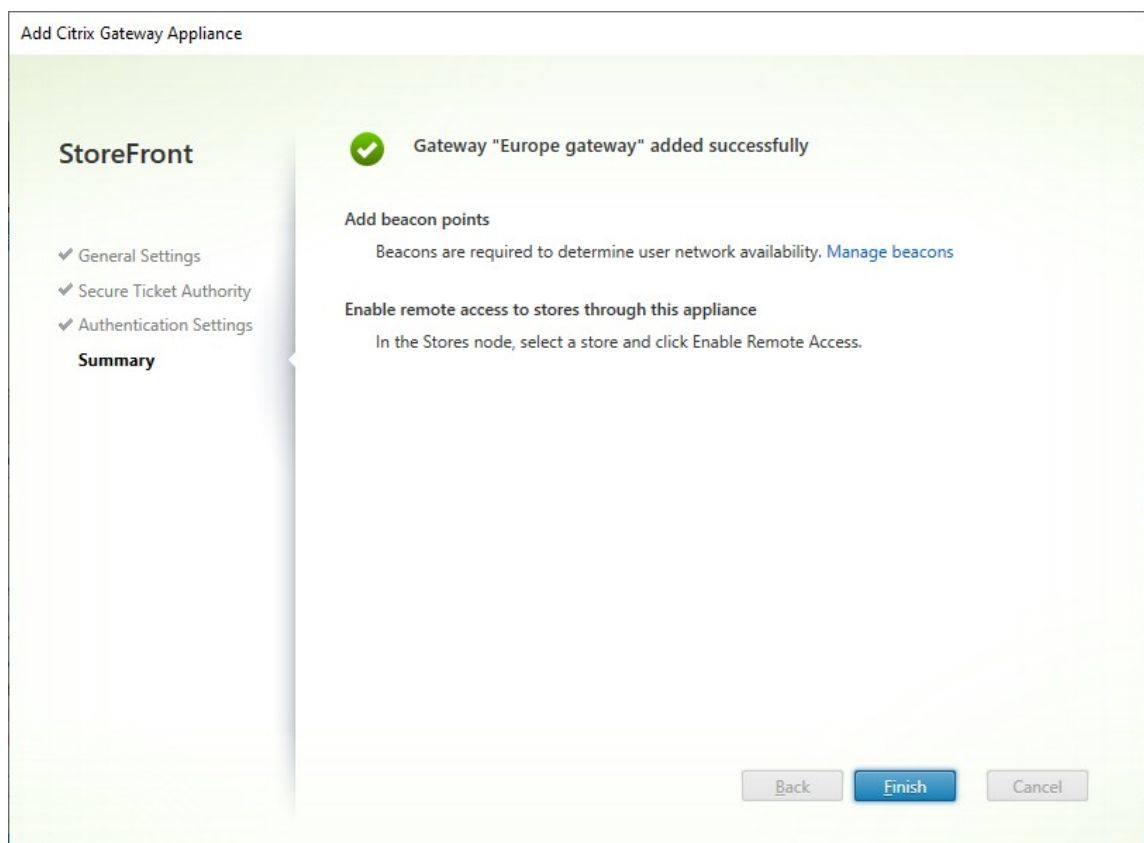
Smart card fallback: None

Callback URL: (optional) https://callback.example.com /CitrixAuthService/AuthService.asmx

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. If you have configured [Security keys](#) (recommended) then you must close the management console and configure them using PowerShell. For example:

```
1 $gateway = Get-STFRoamingGateway -Name [Gateway name]
2 $sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL] -
 StaValidationEnabled $true -StaValidationSecret [secret]
3 $sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL] -
 StaValidationEnabled $true -StaValidationSecret [secret]
4 Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
 $sta1,$sta2
```

8. To enable users to access your stores through the Gateway, configure [remote user access](#).
9. By default StoreFront uses the gateway that authenticated the user for HDX routing to their resources. You can optionally configure StoreFront to use the gateway when accessing particular resources using [Optimal HDX routing](#).

## PowerShell

To add a gateway using PowerShell run cmdlet [New-STFRoamingGateway](#).

## Add Citrix Gateway Service

If you have enabled the [Citrix Gateway Service for StoreFront](#) in Citrix Cloud then you must configure it as a gateway within StoreFront.

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, 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.
  - Set the **Gateway type** to **Citrix Gateway Service**. This causes the **Usage or role** to be set to **HDX™ routing only** and disables the **Citrix Gateway URL**.
  - Optionally enter a **Citrix Gateway Service URL**. If the URL is left blank then it uses the default commercial URL <https://global.g.nssvc.net> which chooses the optimal point of presence for the user's location. If you wish to use a specific gateway region, for example for a particular region, then you can enter its URL here. For a list of available gateway service URLs, see [Citrix Gateway Service documentation](#).
  - If you have entered a **Citrix Gateway Service URL** then you must also enter the corresponding **Citrix Gateway Service URL (STA Connector Mode)**. This specifies the gateway service URL to use when the cloud connector is unable to reach Citrix Cloud so issues its own STA tickets. If the URL is left blank then it uses the default URL <https://global-s.g.nssvc.net>.

**Add Citrix Gateway**

**StoreFront**

**General settings**

Cloud Connectors

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:

Gateway type:

Usage or role:

Citrix Gateway Service URL (optional):

Citrix Gateway Service URL (STA Connector Mode) (optional):

For a list of available Citrix Gateway Service URLs, see [documentation](#)

**Next** **Cancel**

3. Fill out the settings on the **Cloud Connectors** tab.

Cloud connectors allow StoreFront to reach Citrix Cloud to look up Gateway configuration and to reach the cloud ticketing authority to request session tickets.

- Enter at least one Cloud Connector server URL.

StoreFront calls these cloud connectors to retrieve STA tickets which Citrix Workspace app can use to authenticate requests through the . In normal operation the Cloud Connectors proxy requests to the Citrix Cloud Ticketing Authority, or when in LHC mode generate their own tickets. In the future this will change so that they always generate their own tickets for improved resiliency.

- It is recommended that you include multiple cloud connectors in the same resource location as only one Cloud Connector is upgraded at a time in each resource location, ensuring at least Cloud Connector is always available. For further redundancy add Cloud Connectors in multiple resource locations.
- Ensure that all Cloud Connectors listed in StoreFront are also listed as STA servers in the Citrix Gateway virtual server. If any servers are missing from the Citrix Gateway, this can cause launches to fail. Today, this may not be apparent in normal use as any connector can be used to redeem tickets from the Citrix Cloud Ticking Authority. However Local Host Cache mode the connector generates its own tickets and in the future



this will become the default behavior.

- The Cloud Connector may be configured so that StoreFront must include a security key. It is not possible to add security keys using the GUI; see the later step for adding them using PowerShell.
- Select **Load balance multiple servers** to distribute requests between the servers. If cleared then StoreFront will try the servers in the order in which they are listed.
- If StoreFront cannot reach a server then it avoids using that server for a period of time. By default this is 1 hour but you can customize this value.
- Always select **Enable session reliability**.

Currently Citrix Gateway Service requires session reliability. This may change in a future release.

- Do not select **Request tickets from two cloud connectors, where available**.

There is currently no benefit in selecting **Request tickets from two cloud connectors, where available**. This may change in the future.

Add Citrix Gateway Appliance

**StoreFront**

- ✓ General Settings
- Cloud Connectors**
- Summary

**Cloud Connectors**

StoreFront uses cloud connectors to reach the cloud ticketing authority and Citrix Gateway Service configuration service. Enter the FQDN of atleast one cloud connector. Add multiple connectors for resiliency.

Cloud Connector URLs ⓘ

☒ Load balance multiple servers

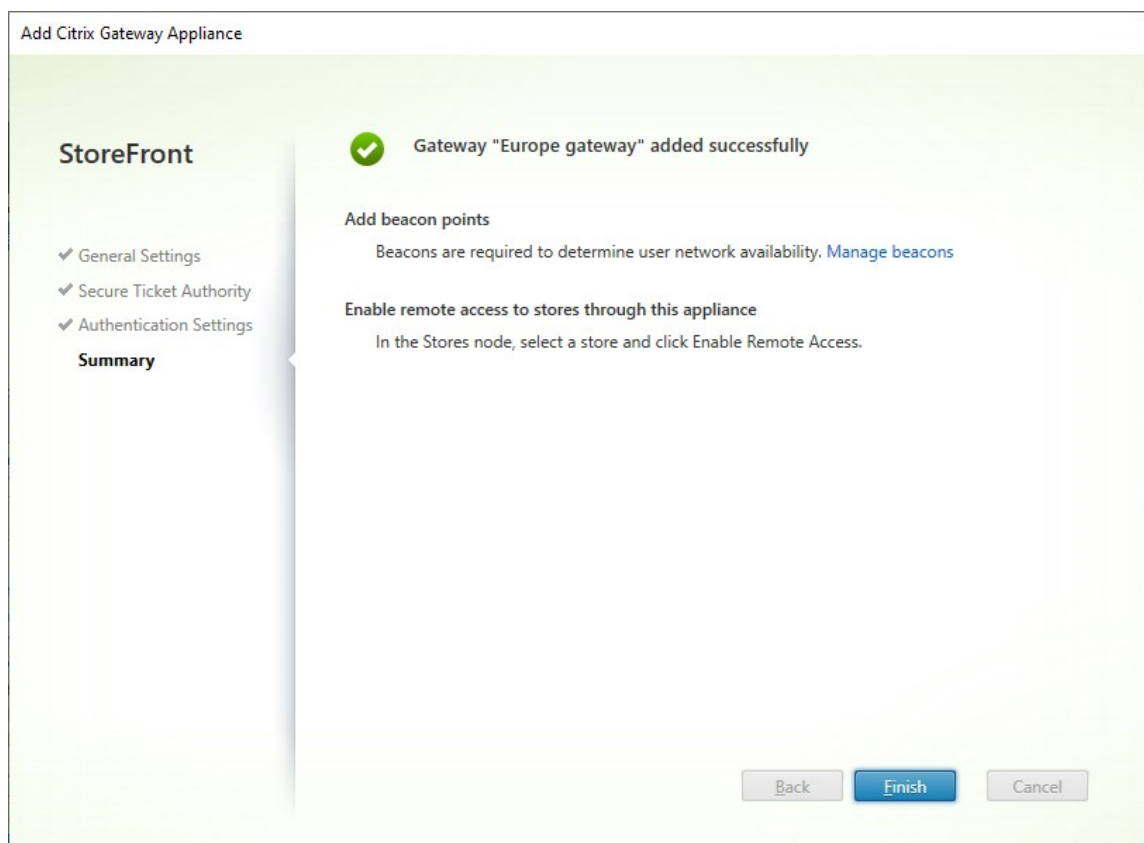
Bypass failed connector for:  hours  minutes  seconds

☒ Enable session reliability ⓘ

☐ Request tickets from two cloud connectors, where available ⓘ

Once you have completed filling out the settings select **Next**

4. Select **Create** to apply the configuration.



5. Once the deployment has been applied, select **Finish**.
6. If you have configured [Security keys](#) (recommended) then you must close the management console and configure them using PowerShell. For example:

```
1 $gateway = Get-STFRoamingGateway -Name [Gateway name]
2 $sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL] -
 StaValidationEnabled $true -StaValidationSecret [secret]
3 $sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL] -
 StaValidationEnabled $true -StaValidationSecret [secret]
4 Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
 $sta1,$sta2
```

7. By default StoreFront uses the same gateway to access resources as was used to authenticate, hence the Citrix Gateway service is never used. You must use [Optimal HDX routing](#) to configure when StoreFront should use Citrix Gateway Service.

## PowerShell

To add a gateway using [PowerShell](#), run cmdlet [New-STFRoamingGateway](#), setting `-IsCloudGateway $true`.

## 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 appliance

2. Press **Save** to save your changes.

## PowerShell

To modify gateway configuration using [PowerShell](#), run 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

To remove the gateway using [PowerShell](#), run cmdlet [Remove-STFRoamingGateway](#).

## Import a Citrix Gateway

October 22, 2025

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 websites 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.

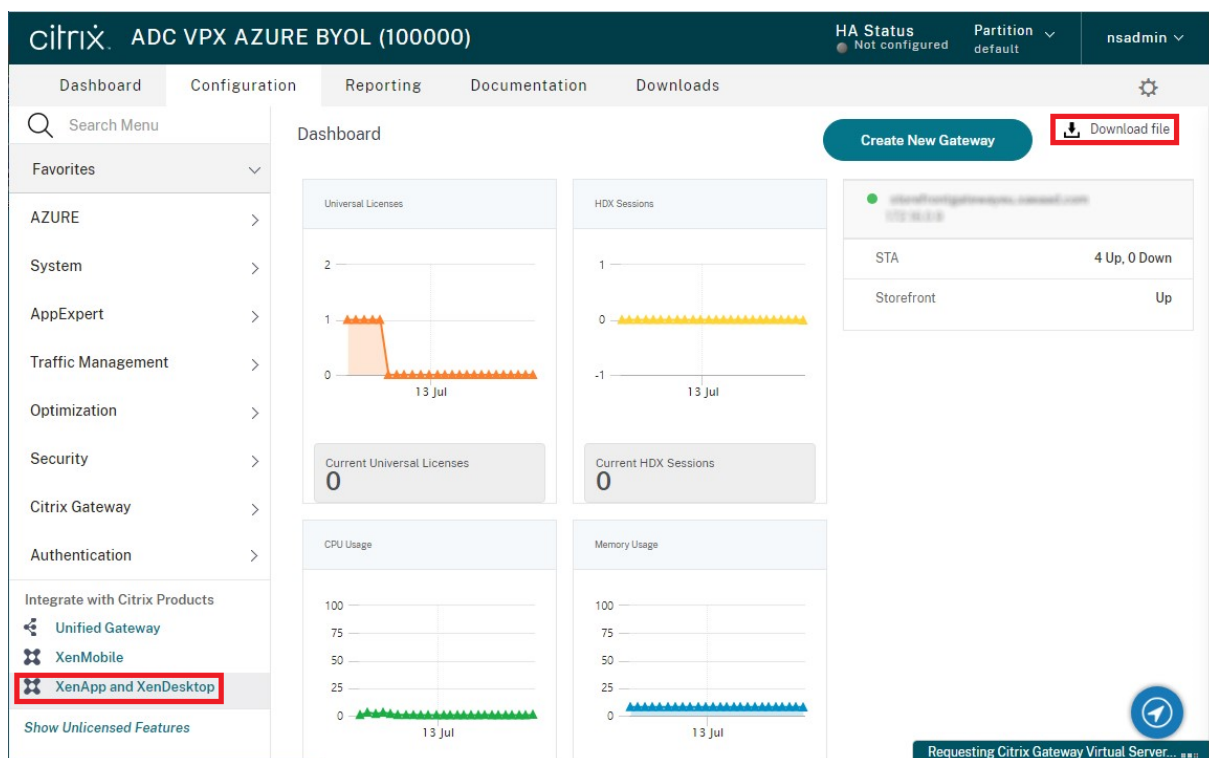
The callback URL and port combination you use is usually the same as the gateway URL and port combination, as long as StoreFront can resolve this URL.

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.

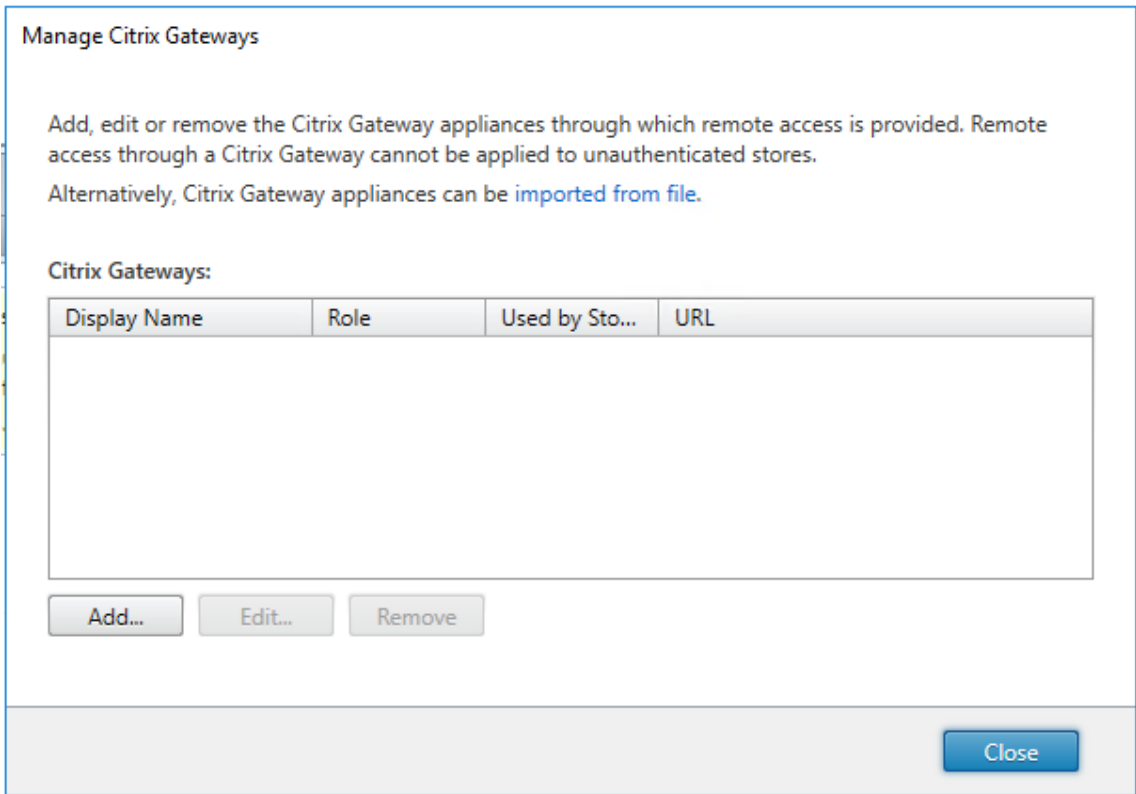
## Import a Citrix Gateway using the console

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.

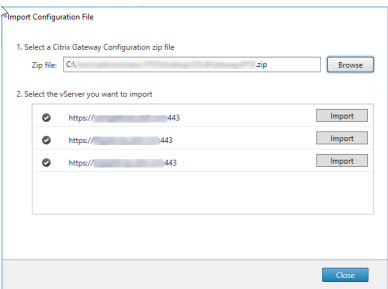
Important:

Citrix does not support manual editing of the configuration file exported from Citrix Gateway.

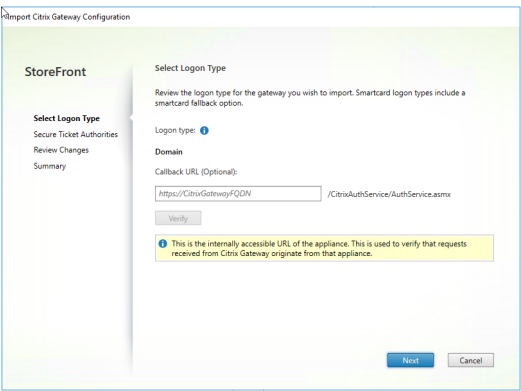
1. Select **Stores** in the left pane of the Citrix StoreFront management console, and in the **Actions** pane, click **Manage Citrix Gateways**.
2. On the Manage Citrix Gateways screen, click the **imported from file** link.



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.

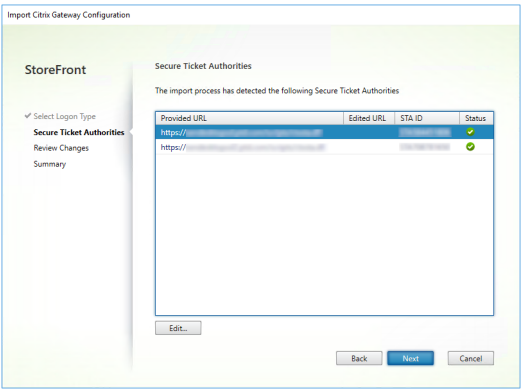


| Logon type in console                  | LogonType in JSON file | Callback URL required |
|----------------------------------------|------------------------|-----------------------|
| Domain                                 | Domain                 | No                    |
| Domain and security token              | 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                   |

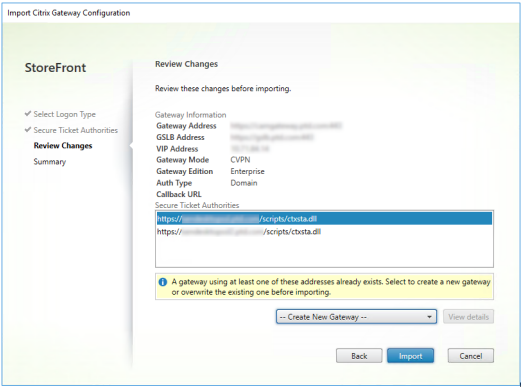
If a callback URL is required, StoreFront will autofill Callback URL based on the gateway URL found in the ZIP file. You can change this to any valid URL that points back to the correct Citrix Gateway VIP. For GSLB gateways, unique callback URLs are required for each of the gateways you import.

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            |
| STA URL and STA ID                        | Yes            |



| Gateway Setting | Can be updated |
|-----------------|----------------|
| 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"
```

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 }
```

### 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"
```

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
```

### 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
```

### 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
```

## Load balancing with NetScaler® ADC

October 22, 2025

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.

### 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
```

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>

```
1 <ArrayOfServiceStatus xmlns="http://schemas.datacontract.org
 /2004/07/Citrix.DeliveryServices.ServiceMonitor.Contract" xmlns
 :i="http://www.w3.org/2001/XMLSchema-instance">
2 <ServiceStatus>
3 <name>Citrix Peer Resolution Service</name>
4 <status>running</status>
5 </ServiceStatus>
6 <ServiceStatus>
7 <name>CitrixConfigurationReplication</name>
8 <status>running</status>
9 </ServiceStatus>
10 <ServiceStatus>
11 <name>CitrixCredentialWallet</name>
12 <status>running</status>
13 </ServiceStatus>
14 <ServiceStatus>
15 <name>CitrixDefaultDomainService</name>
16 <status>running</status>
17 </ServiceStatus>
18 <ServiceStatus>
```

```
19 <name>CitrixSubscriptionsStore</name>
20 <status>running</status>
21 </ServiceStatus>
22 <ServiceStatus>
23 <name>NetTcpPortSharing</name>
24 <status>running</status>
25 </ServiceStatus>
26 <ServiceStatus>
27 <name>WAS</name>
28 <status>running</status>
29 </ServiceStatus>
30 <ServiceStatus>
31 <name>W3SVC</name>
32 <status>running</status>
33 </ServiceStatus>
34 </ArrayOfServiceStatus>
```

## Configure NetScaler Load Balancer

### Install Root certificate

If your StoreFront servers use a certificate signed by an internal authority then you must install the root certificate on to the NetScaler. This is required so that NetScaler trusts the StoreFront server's certificate.

1. Log on to the NetScaler ADC appliance management GUI.
2. Select **Traffic Management > SSL > Certificates > CA Certificates**.
3. Click **Install**.
4. On the **Install CA Certificate** page, enter a Certificate-Key Pair Name, click **Choose File** and browse for the certificate file.
5. Click **Install**.

### Install the server certificate

To enable HTTPS you need a certificate whose Subject alternate name includes the FQDN of the load balancer. You can sign the certificate with an enterprise or public certificate authority.

You must have separate certificate and key files in PEM format. If you have a certificate containing the private key in PKCS12 format then you can use [openssl](#) to convert the file. E.g.:

```
1 openssl pkcs12 -in cert.pfx -clcerts -nokeys -out cert.cer
2 openssl pkcs12 -in cert.pfx -nocerts -out storefrontlbeu.key
```

A prompt appears to enter the existing password and a new PEM passphrase.

To install the certificate:

1. Log on to the NetScaler ADC appliance management GUI.
2. Select **Traffic Management > SSL > Certificates > CA Certificates**.
3. Click **Install**.
4. On the **Install CA Certificate** page:
  - a) Enter a **Certificate-Key Pair Name**.
  - b) Under **Certificate File Name**, click **Choose File** and browse for the certificate file.
  - c) Under **Key File Name**, click **Choose File** and browse for the key file.
  - d) Under **Password** enter the passphrase.
  - e) Click **Install**.
5. Click **Link** to link the certificate to the root certificate.

## ← Install Certificate<sup>?</sup>

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

Q

Click here to search or you can enter Key : Value format

i

| <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 Monitor

Name\*

StoreFront

i

Type\*

STOREFRONT

>

i

Basic Parameters

Interval

5

Second

▼

Response Time-out

2

Second

▼

Store Name

☒ StoreFront Account Service

☒ Check Backend Services 

i

☒ Secure

▶ Advanced Parameters

Create

Close

### 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

i

Note: The port number is mandatory only for DNS servers of query type A (domain name of the IP address)

Port

443

i

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

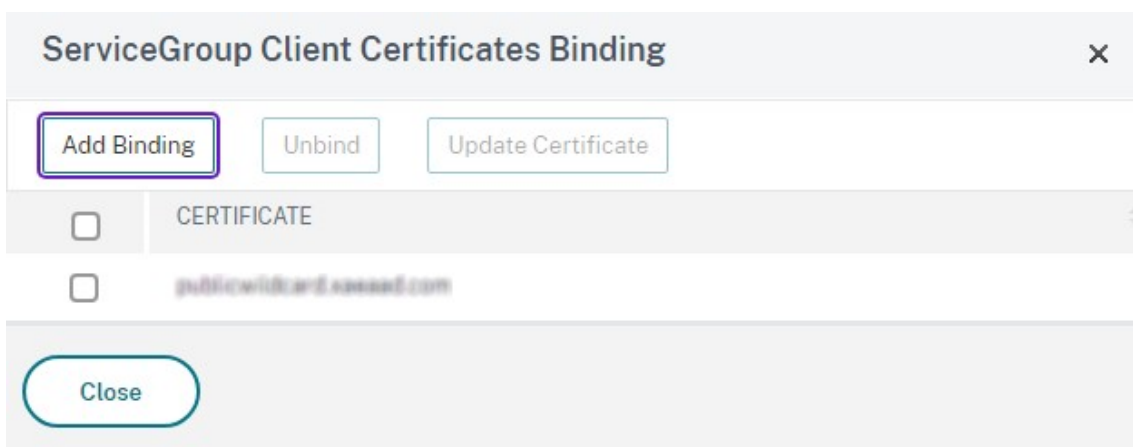
Edit Monitor

| <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\*

 ⓘ

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)\*

2

Cookie Name

NSC\_SFPersistence

Backup Persistence

Backup Persistence\*

NONE

Backup Time-out (mins)

2

IPv4 Netmask

255 . 255 . 255 . 255

IPv6 Mask Length

128

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 behavior. 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 scheme (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 also changes 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**.

|                          | MONITOR NAME       | WEIGHT | STATE |
|--------------------------|--------------------|--------|-------|
| <input type="checkbox"/> | StoreFront-SubSync | 1      | ✓     |

### 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". The "Basic Settings" tab is active. It contains several input fields: "Name\*" with the value "StorefrontSubSyncLb", "Protocol\*" with a dropdown set to "TCP", "IP Address Type\*" with a dropdown set to "IP Address", "IP Address\*" with the value "172 . 16 . 0 . 11", and "Port\*" with the value "808". Each field has an information icon (i) to its right. At the bottom of the settings area is a "More" link with a right-pointing arrow. Below the settings area are two buttons: "OK" and "Cancel".

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)

October 22, 2025

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-
DSDFA Server
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

```

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

```

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>

```

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

```

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

October 22, 2025

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

**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<br>Can be enabled / disabled separately on Receiver for Web sites |          |
| <input type="checkbox"/> Smart card<br>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:

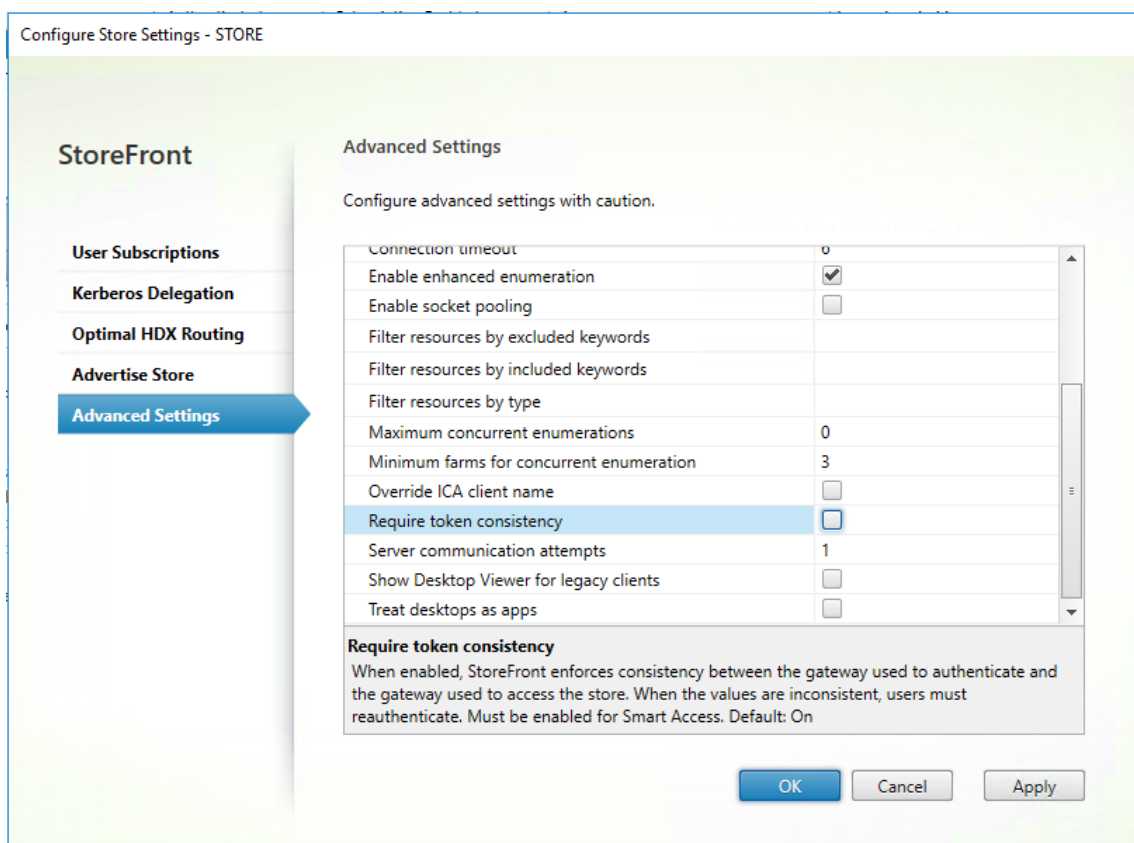
ProductionGateway ▼

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.

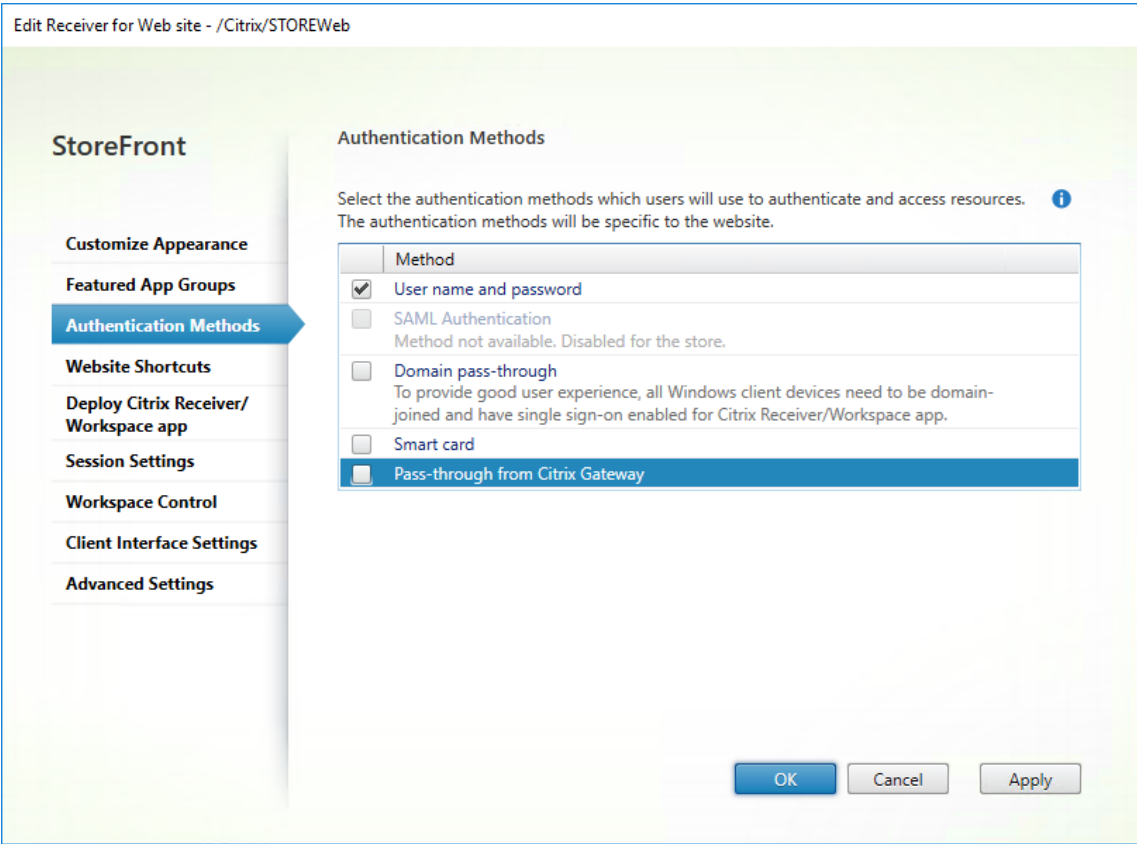
## Disable pass-through from Citrix Gateway for the website

### 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.

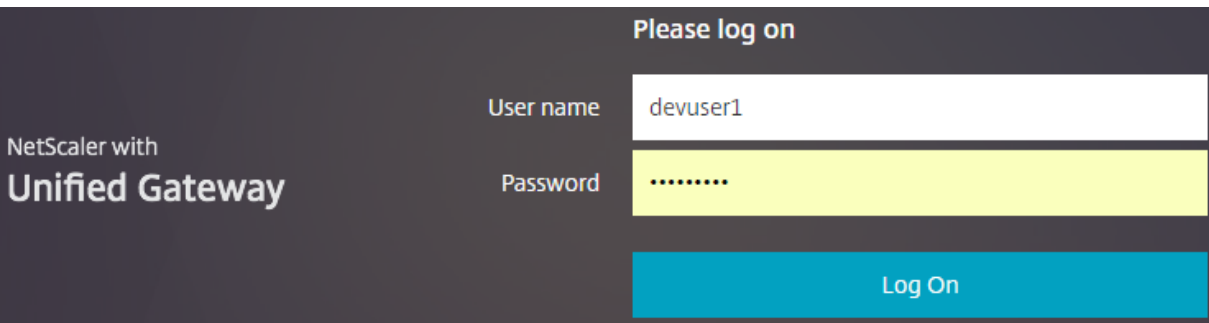
1. Select the **Stores** node in the left pane of the Citrix StoreFront management console.
2. Select the **store** that you want to modify.
3. In the **Actions** pane, click **Manage websites**.
4. In Authentication Methods, clear **Pass-through from Citrix Gateway**.

5. Click **OK**.

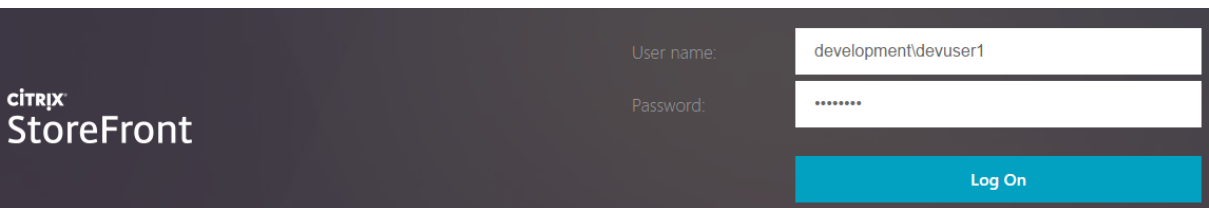


### Log on to Gateway using a `production.com` user and credentials

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 username 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 **Username 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

**CITRIX**  
**StoreFront**

User name:

Password:

Domain:

**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></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></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"/> <a href="#">Advanced Settings</a>                           |                   |          |                        |

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

November 5, 2025

**Important:**

- <http://ping.citrix.com> is no longer available and should not be used.
- Do not use third party websites that you do not own as an external beacon. Instead use websites controlled by your organization.

- The internal and external beacon URLs should be fully qualified domain names (FQDN) like (<http://example.com>) and not the abbreviated NetBIOS name (<http://example>).

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 the browser based HDX client. Citrix Workspace app for Windows 2503 and higher only uses the internal beacon, not external beacons. Older versions and Citrix Workspace app on other platforms use both internal and external beacons.

**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:

External beacons:

- <http://ping.example.com>
- <https://gateway.example.com>

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>. This is no longer available must be replaced with your own beacon.
  - 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 the internet. These must respond to HTTP HEAD requests. 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 by logging in using a web browser and going to account settings. Otherwise, you can [export a provisioning file](#) for the store and make this file available to your users.

## PowerShell

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

October 22, 2025

You can create a single fully qualified domain name (FQDN) that can access a store directly from within your corporate network and remotely through a Citrix Gateway.

For example you could use the following URLs:

- <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. When inside your network this resolves 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, or 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.

## Require Citrix Workspace™ app when connecting through a gateway

October 22, 2025

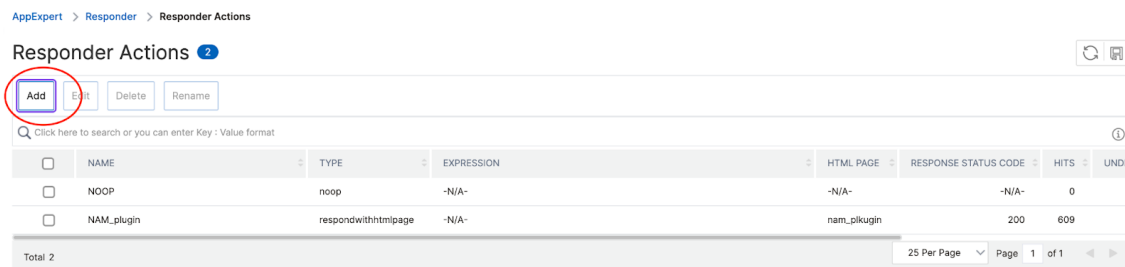
You can require users to use Citrix Workspace app when connecting through a gateway by using a plug-in.

To deploy the plug-in to your gateway:

1. Download the plugin from [Citrix Downloads](#).
2. Extract the zip file and citrix-gateway-plugin.tar.gz. It consists consists of an HTML file and a JavaScript file.
3. Copy the files to the NetScaler gateway under `/var/netscaler/gui/vpn/init`
4. Configure using the Management GUI or Configure using the CLI

### Configure using the Management GUI

1. Sign in to the Netscaler® admin GUI.
2. Create a responder action and click Add.



3. Configure the responder action:

**Type:** Respond with HTML page

**Add:** Enter path `/vpn/init/native-app-mandate.html`

4. Create a responder policy.

AppExpert > Responder > Responder Policies

### Responder Policies 1

Add Edit Delete Show Bindings Policy Manager Statistics Rename

Click here to search or you can enter Key : Value format

| <input checked="" type="checkbox"/> | NAME              | EXPRESSION                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> | NAM_Plugin_policy | HTTP.REQ.IS_VALID && HTTP.REQ.URL.ENDSWITH(".js").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("CWAWEVIEW").NOT && HTTP.REQ.HEADER("X-Requested-With").CONTAINS("com.citrix.Receiver").NOT && HTTP.REQ.HEADER("X-Requested-With").CONTAINS("XMLHttpRequest").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("AuthManager").NOT |

Total 1

25 Per Page Page 1 of 1

5. Configure the responder policy:

**Action:** The name of the action you created above.

**Expression:** `HTTP.REQ.IS_VALID && HTTP.REQ.URL.ENDSWITH(".js").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("CWAWEVIEW").NOT && HTTP.REQ.HEADER("X-Requested-With").CONTAINS("com.citrix.Receiver").NOT && HTTP.REQ.HEADER("X-Requested-With").CONTAINS("XMLHttpRequest").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("AuthManager").NOT`

Configure Responder Policy

Name

NAM\_Plugin\_policy

Action\*

NAM\_plugin

Add

Edit

Log Action

Add

Edit

AppFlow Action

Add

Edit

Undefined-Result Action\*

-Global undefined-result action-

Expression\*

Select

Select

Select

Expression Editor

HTTP.REQ.IS\_VALID && HTTP.REQ.URL.ENDSWITH(".js").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("CWAWEVIEW").NOT && HTTP.REQ.HEADER("X-Requested-With").CONTAINS("com.citrix.Receiver").NOT && HTTP.REQ.HEADER("X-Requested-With").CONTAINS("XMLHttpRequest").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("AuthManager").NOT

Evaluate

6. Navigate to the virtual server where you want to bind the responder policy.

### VPN Virtual Server Responder Policy Binding

Add Binding Unbind Regenerate Priorities No action

Click here to search or you can en

| <input type="checkbox"/> | PRIORITY | POLICY NAME       | EXPRESSION                                                                                                                                                                                                                                                                                                                                                                                     |
|--------------------------|----------|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <input type="checkbox"/> | 100      | NAM_Plugin_policy | HTTP.REQ.IS_VALID && HTTP.REQ.URL.ENDSWITH(".js").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("CWAWEVIEW").NOT && HTTP.REQ.HEADER("X-Requested-With").CONTAINS("com.citrix.Receiver").NOT && HTTP.REQ.HEADER("X-Requested-With").CONTAINS("XMLHttpRequest").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("AuthManager").NOT |

Close

## 7. Bind the policy you created.

VPN Virtual Server Responder Policy Binding > Policy Binding

### Policy Binding

Policy Name

NAM\_Plugin\_policy

► More

### Binding Details

Priority\*

100 ⓘ

Goto Expression\*

END ▼

**Bind** **Close**

Name of a policy to bind to the virtual server.

MaxLength = 127

8. To verify it is configured correctly, open the gateway URL to confirm that it displays the **Citrix Workspace app required** screen. Add the Netscaler URL to Citrix Workspace app and confirm that it does not display the **Citrix Workspace app required** screen.

## Configure using the CLI

To configure the require Citrix Workspace app feature using the CLI, perform the following:

1. Create a responder action with an HTML file (you can edit the configuration in GUI)

```
1 add responder action respond_with_html_act respondwithhtmlpage
 sample_page -responseStatusCode 200
```

2. Create a responder policy to handle requests from a web browser, not Citrix Workspace app.

```
1 add responder policy respond_with_html_pol "HTTP.REQ.IS_VALID &&
 HTTP.REQ.URL.ENDSWITH(".js").NOT && HTTP.REQ.HEADER("User-Agent")
 .CONTAINS("CitrixReceiver").NOT && HTTP.REQ.HEADER("User-Agent")
 .CONTAINS("CWAWebView").NOT && HTTP.REQ.HEADER("X-Requested-With")
 .CONTAINS("com.citrix.Receiver").NOT && HTTP.REQ.HEADER("X-Requested-With")
 .CONTAINS("XMLHttpRequest").NOT && HTTP.REQ.HEADER("User-Agent")
 .CONTAINS("AuthManager").NOT"
 respond_with_html_act
```

3. Bind the policy to the VPN vserver

```
1 bind vpn vserver vpn_vs -policy respond_with_html_pol -priority
 100 -gotoPriorityExpression END -type AAA_REQUEST
```

## Entra ID authentication via OIDC and single sign-on to VDA

December 12, 2025

### StoreFront Entra ID integration with NetScaler Gateway

This article describes how to set up remote StoreFront access using a NetScaler Gateway virtual server with AAA Entra ID and OIDC. This configuration provides Microsoft Entra ID SSO for users who use Citrix Workspace app or a web browser.

#### Prerequisites

- NetScaler
- StoreFront 2507 CU1 or higher
- Microsoft Entra ID and account with one of the following permissions:
  - Cloud Application Administrator
  - Application Administrator
  - Global Administrator
- DaaS subscription with connectors
- Published desktops and/or apps
- For launches from a web browser into Citrix Workspace app, to enable SSO to VDAs, [Citrix web extension](#).

#### Azure application registration

**Create a Microsoft Azure Entra ID application** An App Registration in Microsoft Entra ID defines your application so that Entra ID recognizes it—in this case, NetScaler OIDC. This registration also manages the application's authentication and authorization requests. Because OAuth requires a trusted Identity Provider (IdP) to authenticate users and issue tokens, registering your app tells Entra ID: "This application uses you as its IdP for OAuth flows."

1. Sign in to the Azure portal for the Entra ID tenant that you use for NetScaler or StoreFront authentication.
2. Go to **Microsoft Entra ID resource > Manage > App registrations**, then select **New registration**.
3. Name the application, for example, NetScaler StoreFront Authentication.

4. Under **Supported account types**, select **Accounts in this organizational directory only**.
5. Under **Redirect URI**, select **Web** for the type of application you want to create. Enter the URI where the access token is sent. Use the format <NetScaler Virtual Server URL>/oauth/login, for example <https://netscalerentra.customer.com/oauth/login>.

### Register an application ...

#### \* Name

The user-facing display name for this application (this can be changed later).

NetScaler StoreFront Authentication ✓

#### Supported account types

Who can use this application or access this API?

- ☒ Accounts in this organizational directory only (StoreFront Essentials Test CP1 only - Single tenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)
- ☐ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- ☐ Personal Microsoft accounts only

[Help me choose...](#)

#### Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web ▼

<https://netscaler-entra.citrix.com/oauth/login> ✓

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from [Enterprise applications](#).

## Create client secret

To create client secret:

1. After you register the application, go to **Manage > Certificates & Secrets**.
2. Select **Client secrets**, and then select **New client secret**.  
Your app uses these credentials to securely communicate with the IdP and request tokens.
3. Provide a description of the secret and a duration.
4. After you create the secret, record the secret value because you need it later in the setup process and it's only visible during this stage of creation.

## Configure application permissions

To configure app permissions:

1. Go to **Manage > App registrations**, then select your application.
2. Select **Manage > API Permissions**.
3. The **User.Read** permission is already added by default.
4. Add **openid** and **profile**.
5. Select **Grant admin consent for <tenant name>** and accept.

“Grant admin consent for” in API permissions in Microsoft Entra ID means that an administrator gives approval, on behalf of all users in the organization, for an application to access specific resources or APIs with the requested permissions.

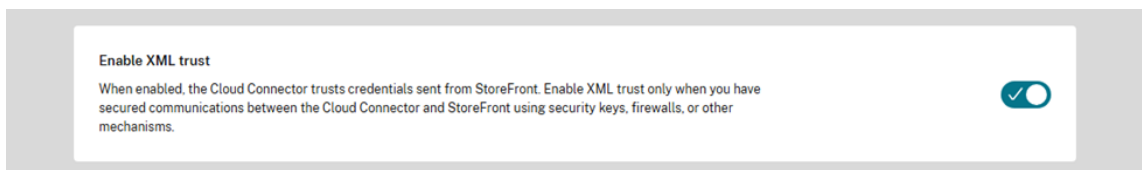
```
1 ! [Azure grant permission] (/en-us/storefront/2507-ltsr/media/integrate-with-citrix-gateway-and-citrix-adc/azure-grant-permission.png)
```

## Configure Citrix DaaS

**Configure XML trust and optional service keys** XML trust for Citrix DaaS (Desktop as a Service) allows StoreFront to pass the relevant Microsoft Entra ID user credentials. You need XML trust if you use authentication methods like pass-through authentication, smart cards, SAML (Single Sign-On), or OIDC that don't rely on a password.

1. Sign in to Citrix Cloud and go to the DaaS console.
2. Go to **Settings**.
3. Turn on **XML trust**.





4. (Optional step) For added security you can enable security keys between DaaS and StoreFront. For more information, see [Manage security keys](#) in the Citrix DaaS™ documentation.

## Configure Citrix NetScaler

**Configure NetScaler Gateway with StoreFront** Complete steps 1, 2, and 4 from [Integrate NetScaler Gateway with StoreFront](#).

1. Create a [session policy for web browser-based access](#).
2. Create a [session policy for Citrix Workspace app-based access](#).
  - a. Setting up a CWA session also requires a profile, so you must include the following steps that are missing in the document for the CWA session.

- 1 i. In the **\*\*Session Policies\*\*** tab, click **\*\*Add\*\***. The session policy is required **for** NetScaler to differentiate between the web browser-based and Citrix Workspace app-based connections. This policy is applied to web browser-based connections.
- 2 ii. In **\*\*Name\*\***, assign a name to session policy.
- 3 iii. In **\*\*Profile\*\***, select the session profile that you created.
- 4 iv. Click the **\*\*Advanced Policy\*\*** option and enter the following syntax under **\*\*Expression\*\***:
 

```
5 ``HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver")``
```
- 8 v. Click **\*\*Create\*\***.

3. See Configure Authentication ICA Proxy virtual server in the upcoming sections.
4. [Create a NetScaler Gateway virtual server](#).
  - a. The ICA Proxy virtual server name is required for the additional Entra ID configuration described as follows.

## Configure authentication

Create the OAuth action and policy to set up the Authentication virtual server as an OIDC Relying Party for Microsoft Entra ID. This configuration tells the ADC how to redirect users to an external OAuth IdP (like Microsoft Entra ID) for sign-in and how to handle the OAuth tokens received after authentication. It specifies endpoints, client credentials, scopes, and how the ADC extracts user information from tokens.

You need the client secret from the previous steps and the Microsoft Entra ID authentication endpoints. You can find the authentication endpoints in the Azure portal by going to your App Registration Overview and clicking the **Endpoints** tab.

### Create authentication virtual server

The authentication virtual server handles authentication for users before they access backend resources (like StoreFront, web apps, VPN, and so on).

Run these commands on the NetScaler command line with line breaks removed (breaks are added for readability).

```
1 add authentication vserver EntraId_Authentication_VirtualServer SSL <IP
 Address> 443
2 -state ENABLED
3 -authentication ON
4 -td 0 -appflowLog ENABLED
5 -noDefaultBindings NO
6 bind ssl vserver EntraId_Authentication_VirtualServer
7 -certkeyName <Certificate Key Name>
```

### Create OAuth action

The OAuth action specifies how NetScaler ADC interacts with an OAuth IdP (like Microsoft Entra ID, Okta, or Google). This action allows ADC to redirect users to the IdP for sign-in and handle the OAuth token returned. It facilitates single sign-on (SSO) for applications published through Citrix Gateway.

You need the Client ID and Client secret from the previous steps.

```
1 add authentication OAuthAction EntraId_Oauth_Server
2 -authorizationEndpoint "https://login.microsoftonline.com/<TenantId>/
 oauth2/v2.0/authorize?prompt=login"
3 -tokenEndpoint "https://login.microsoftonline.com/<TenantId>/oauth2/
 v2.0/token"
4 -clientId <ClientId>
5 -clientSecret <ClientSecret>
6 -Attribute1 email
7 -Attribute2 family_name
8 -Attribute3 given_name
9 -Attribute4 upn
10 -CertEndpoint "https://login.microsoftonline.com/<TenantId>/discovery
 /v2.0/keys"
11 -userNameField oid
12 -allowedAlgorithms HS256 RS256 RS512
13 -PKCE ENABLED
14 -tokenEndpointAuthMethod client_secret_post
15 -OAuthType GENERIC
16 -grantType CODE
```

```
17 -refreshInterval 1440
```

The `authorizationEndpoint` includes the query string parameter `prompt=login` so that users are forced to reauthenticate when they attempt to access StoreFront through the NetScaler.

**Create OAuth policy** Create a policy used to trigger the preceding OAuth Action

```
1 add authentication Policy EntraId_Authentication_Policy
2 -rule true
3 -action EntraId_Oauth_Server
```

**Bind the authentication policy to the virtual server**

```
1 bind authentication vserver EntraId_Authentication_VirtualServer
2 -policy EntraId_Authentication_Policy
3 -priority 100
4 -gotoPriorityExpression END
```

**Add authentication profile to Auth virtual server**

```
1 add authentication authnProfile EntraId_Auth_Profile
2 -authnVsName EntraId_Authentication_VirtualServer
3 -AuthenticationLevel 0
```

**Bind AAA authentication server to StoreFront virtual server** Bind the configured AAA authentication server to your ICA Proxy virtual server. When you bind at the StoreFront virtual server level, authentication occurs directly when users access the StoreFront endpoint.

Running this command replaces the existing authentication profile bound to the ICA Proxy/StoreFront virtual server with `EntraId_Auth_Profile`. It doesn't remove other unrelated bindings, but it does override whatever authentication profile was previously in use.

Consider backing up the existing ICA Proxy virtual server configuration before you run this command so that you can revert the changes if necessary.

```
1 set vpn vserver <StoreFront ICA Proxy vServer>
2 -authentication ON
3 -authnProfile EntraId_Auth_Profile
```

## Entra ID token injection configuration for SSO

When you pass the Entra ID token, users authenticated through Azure AD/OAuth on NetScaler Gateway don't need to enter credentials again at StoreFront. The rewrite rule takes the Entra ID token received at NetScaler Gateway and inserts it into the authentication HTTPS requests sent to StoreFront. StoreFront recognizes and validates the token, then signs in the user based on its claims.

The NetScaler rewrite policy requires that you enable the feature.

```
1 enable ns feature Rewrite
2 add rewrite action EntraId_Oauth_Insert_AccessToken_Header
 insert_http_header X-Citrix-OIDC-Access-Token "AAA.USER.ATTRIBUTE(\"
 accesstoken\")"
3 -comment "A rewrite policy to add the OAUTH access_token to
 subsequent user authentication requests"
4 add rewrite policy EntraId_Oauth_Insert_AccessToken_Policy "HTTP.REQ.
 URL.TO_LOWER.ENDSWITH(\"gatewayauth/login\") || HTTP.REQ.URL.
 TO_LOWER.ENDSWITH(\"citrixagbasic/authenticate\")"
 EntraId_Oauth_Insert_AccessToken_Header
5 -comment "A rewrite policy to add the OAUTH access_token to
 subsequent user authentication requests"
6 bind vpn vserver <StoreFront ICA Proxy vServer>
7 -policy EntraId_Oauth_Insert_AccessToken_Policy
8 -priority 100
9 -gotoPriorityExpression END
10 -type REQUEST
```

## Configure NetScaler content switcher

You have two options for configuring content switching.

You need a NetScaler content switching policy to route requests to the unauthenticated [/Citrix/<StoreWeb>/Tickets/RedeemStoreTicket](#) endpoint on the StoreFront server. This ensures that the Microsoft Entra ID SSO flow completes successfully, because requests to this URL originate from the Citrix Entra ID client page and must be specially routed.

**Add backend server for content switching** Replace storefront.fqdn.com with the FQDN that you use as the StoreFront host base URL.

This service represents the backend StoreFront server, accessible through HTTP on port 80. You can use it in load balancing or other traffic management configurations on NetScaler.

```
1 add server storefront1 storefront.fqdn.com
2 add service srv_storefront1 HTTP 80
```

The SSL backend service represents a backend server accessible through HTTPS on port 443. NetScaler can use this service for load balancing, content switching, or other traffic management. Change the private IP address `srv_ssl IP Address` to represent your network.

```
1 add service srv_ssl <srv_ssl IP Address> SSL 443
```

**HTTP load balancing virtual server** You have two options here: forward requests to StoreFront on port 80 HTTP or port 443 (SSL).

Create a server that listens on all IPs/ports with no persistence. Use this in a content switching setup where the virtual server itself doesn't need a dedicated IP/port.

```
1 add lb vserver lb_vs HTTP 0.0.0.0 0 -persistenceType NONE -cltTimeout 180
```

Create an SSL load balancing virtual server on a specific IP and port with no persistence. This sets up an SSL virtual server to handle HTTPS traffic on IP, load balancing requests among backend services without session persistence. Update the private IP address to represent your network.

```
1 add lb vserver lb_ssl SSL <lb_ssl Ip Address> 443 -persistenceType NONE -cltTimeout 180
```

**Bind service to load balancing virtual server where the protocol type is HTTP** Bind the server `storefront.fqdn.com` represented by `srv` to a load balancer. At this point, you can bind multiple StoreFront servers that are used for the final step of the Microsoft Entra ID single sign-on.

```
1 bind lb vserver lb_vs srv
```

**Bind SSL service to load balancing virtual server where the protocol type is HTTPS** This enables the `lb_ssl` virtual server to route incoming SSL (HTTPS) traffic to the backend server or service defined as `srv_ssl`. Without this binding, the virtual server has no backend servers to send client requests to.

```
1 bind lb vserver lb_ssl srv_ssl
```

**Create SSL content switching virtual server** Create an SSL content switching virtual server to handle client requests.

This content switching virtual server listens for HTTPS traffic on port 443 and routes requests to the appropriate backend services or load balancers.

**Note:**

Content Switching isn't enabled by default on NetScaler and you must explicitly configure it.

```
1 enable feature CS
2 add cs vserver cs_vs SSL <cs_vs Ip Address> 443 -cltTimeout 180 -
 persistenceType NONE
3 bind ssl vserver cs_vs -certkeyName <Certificate Name>
```

**Define content switching action (VPN)** Define a content switching action to redirect matching traffic to the ICA Proxy virtual server. Create the action with the name `cs_vpn_vs`, configured to route

matching requests to the target virtual server. The exact virtual server name varies depending on what was specified in the earlier StoreFront virtual server configuration steps.

```
1 add cs action cs_vpn_vs -targetVserver <StoreFront ICA Proxy vServer>
```

**Define content switching action (LB)** Define a content switching action to redirect matching traffic to the ICA Proxy virtual server. Create the action with the name `cs_vpn_vs`, configured to route matching requests to the target virtual server. The exact virtual server name varies depending on what was specified in the earlier StoreFront virtual server configuration steps.

If the backend server is configured to communicate over the HTTPS protocol

```
1 add cs action cs_lb_vs -targetLBVserver lb_ssl
```

Or if the backend server is configured to communicate over the HTTP protocol

```
1 add cs action cs_lb_vs -targetLBVserver lb_vs
```

**Create content switching policy** Create a content switching policy for load balancing based on a URL containing a StoreFront ticket redemption path. Replace “StoreEntraWeb” with the name of the StoreFront website from the StoreFront virtual server web policy.

This policy matches requests when the URL contains `/Citrix/StoreEntraWeb/Tickets/RedeemStoreTicket`.

Action: Routes those matching requests to the content switching action `cs_lb_vs` (which, in turn, sends them to the appropriate backend, such as a load balancing virtual server). This ensures that requests for the StoreFront Entra ID ticket redemption endpoint are properly routed to the backend StoreFront virtual server.

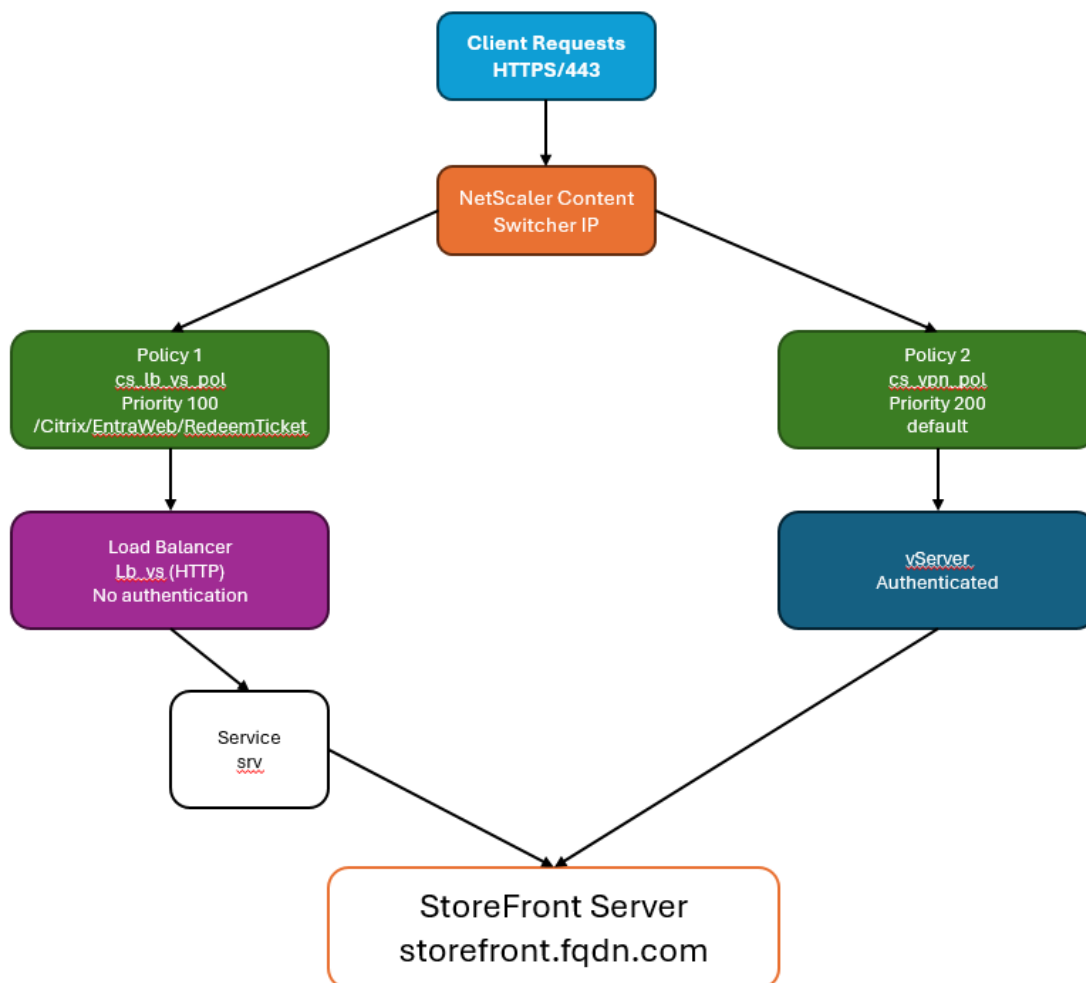
```
1 add cs policy cs_lb_vs_pol -rule "HTTP.REQ.URL.CONTAINS(\"/Citrix/StoreEntraWeb/Tickets/RedeemStoreTicket\")" -action cs_lb_vs
```

**Catch-all policy** Create a catch-all content switching policy to send all other StoreFront traffic to VPN virtual server.

```
1 add cs policy cs_vpn_pol -rule TRUE -action cs_vpn_vs
```

**Bind content switching policies** Bind content switching policies to content switching virtual server with explicit priorities. This binds different content switching policies to `cs_vs`, which allows it to evaluate incoming requests and route them according to the rule above.

```
1 bind cs vserver cs_vs -policyName cs_lb_vs_pol -priority 100
2 bind cs vserver cs_vs -policyName cs_vpn_pol -priority 110
```



## Configure StoreFront

### Configure Citrix Gateway

1. [Add a NetScaler Gateway instance on StoreFront.](#)

- a. [Configure Citrix Gateways.](#)

1 Set up the gateway as though it does domain authentication and ensure that you specify a working callback URL because it isn't optional when you use Entra ID with StoreFront.

2. Configure the gateway for remote access for the Store aggregating the Citrix DaaS resources.
  - a. [Configure remote access settings.](#)
3. Enable and configure Entra ID authentication from NetScaler Gateway.  
Replace the Tenant ID with the ID from your Entra ID tenant.

```
1 $store = Get-STFStoreService /Citrix/EntraStore
2 $authenticationService = Get-STFAuthenticationService -Store $store
3 Set-STFEntraIdSettings -AuthenticationService $authenticationService -
 TenantId "<Your tenant id>" -Enabled $true
```

**Configure VDA Entra ID single sign-on** Single sign-on enables users to authenticate once when they sign in to the Citrix Gateway—and then access their virtual desktops and applications without having to re-enter their credentials to the VDA.

```
1 $store = Get-STFStoreService /Citrix/EntraStore
2 Set-STFStoreLaunchOptions -StoreService $store -EntraIdSsoEnabled $true
```

### Considerations for enabling or disabling Entra ID SSO

1. Only enable single sign-on if you configure the Azure Entra ID Enterprise Application and update StoreFront with the tenant. If you enable this setting for stores currently using Entra ID with SAML without these settings, it potentially breaks existing single sign-on if you're using FAS.
2. If you enable the setting for existing stores using Entra ID with SAML where the VDAs don't currently have SSO, launch might be delayed and or you might see errors related to Entra ID authentication settings.

## End user experience

October 22, 2025

End users can view the stores either in a web browser or Citrix Workspace app. See [End user access](#).

StoreFront provides the following user experiences:

### Modern experience

The modern user experience is consistent with Citrix Workspace. It incorporates Activity Manager for managing your sessions and improved searching.

The modern experience has the following limitations:

- It is not possible to create embedded URL shortcuts that lead you directly to your app or desktop.



- It is not possible to perform deep customizations using JavaScript and css with the StoreFront™ Client UI Customization API. However many customizations can be done using the management console, avoiding the need for JavaScript or css.

For more information, see [Modern experience](#)

## **Classic experience**

This is the default user experience consistent with previous versions of StoreFront. You can customize the user interface using JavaScript and CSS.

For more information, see [Classic experience](#)

## **Citrix Gateway cVPN**

If users access StoreFront through a Citrix Gateway configured for [clientless VPN \(CVPN\)](#) then it provides its own user interface instead of displaying the interface from StoreFront. In this case some UI configuration settings within StoreFront do not apply.

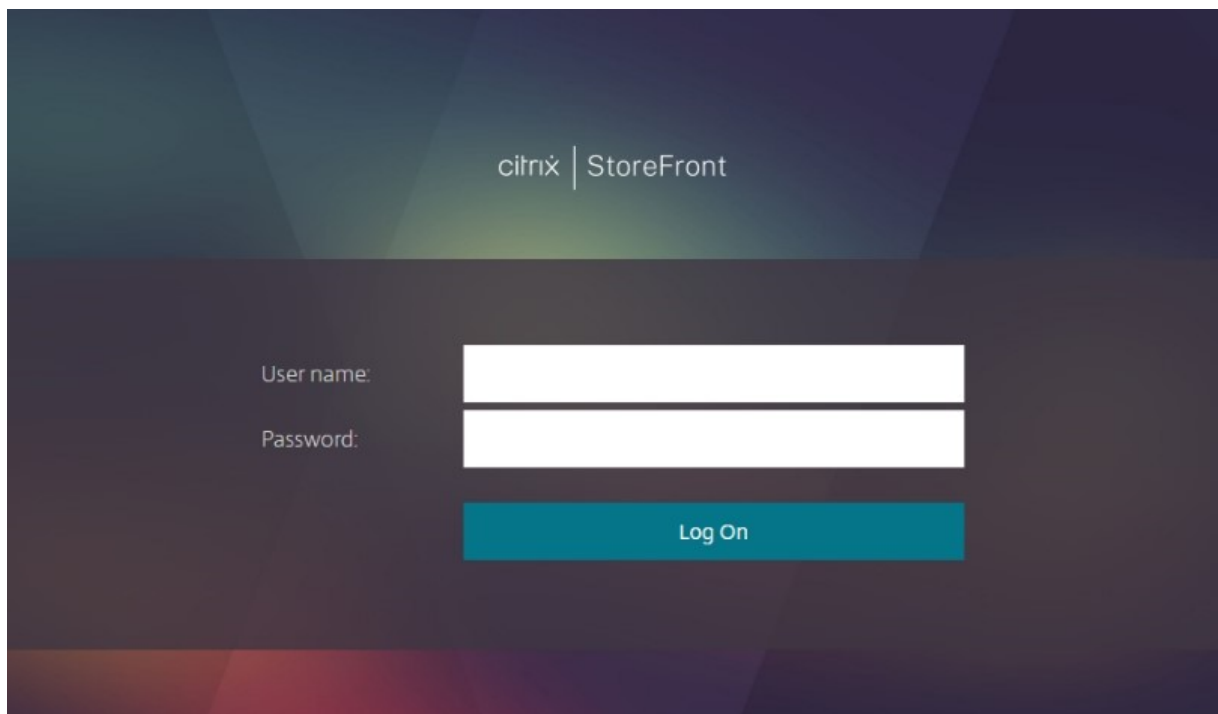
## **Classic experience**

November 12, 2025

This section describes how users can access and interact with their stores using the classic experience.

### **Log On**

Depending on the [authentication methods](#) configured and whether single sign-on is enabled, users might be required to log in.



If multiple authentication methods are available then the user can choose to switch to a different authentication method.

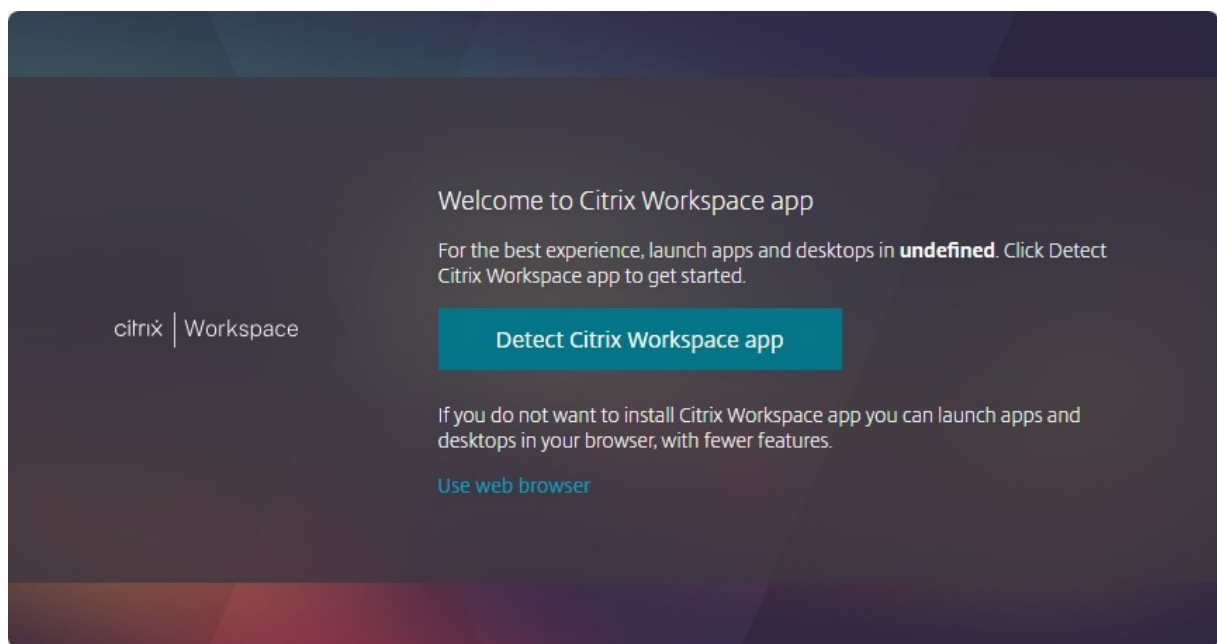
### Citrix Workspace app detection

#### Note:

This section only applies when accessing the store through a web browser, and the [launch option](#) is set to **Open in Citrix Workspace app** or **Let the user choose**. This step may occur before or after log on depending on configuration.

If Citrix Web Extension is installed and has detected Citrix Workspace app, or Citrix Workspace launcher is [disabled](#), then it skips this step. Users can instead change the launch preference from the Advanced settings.

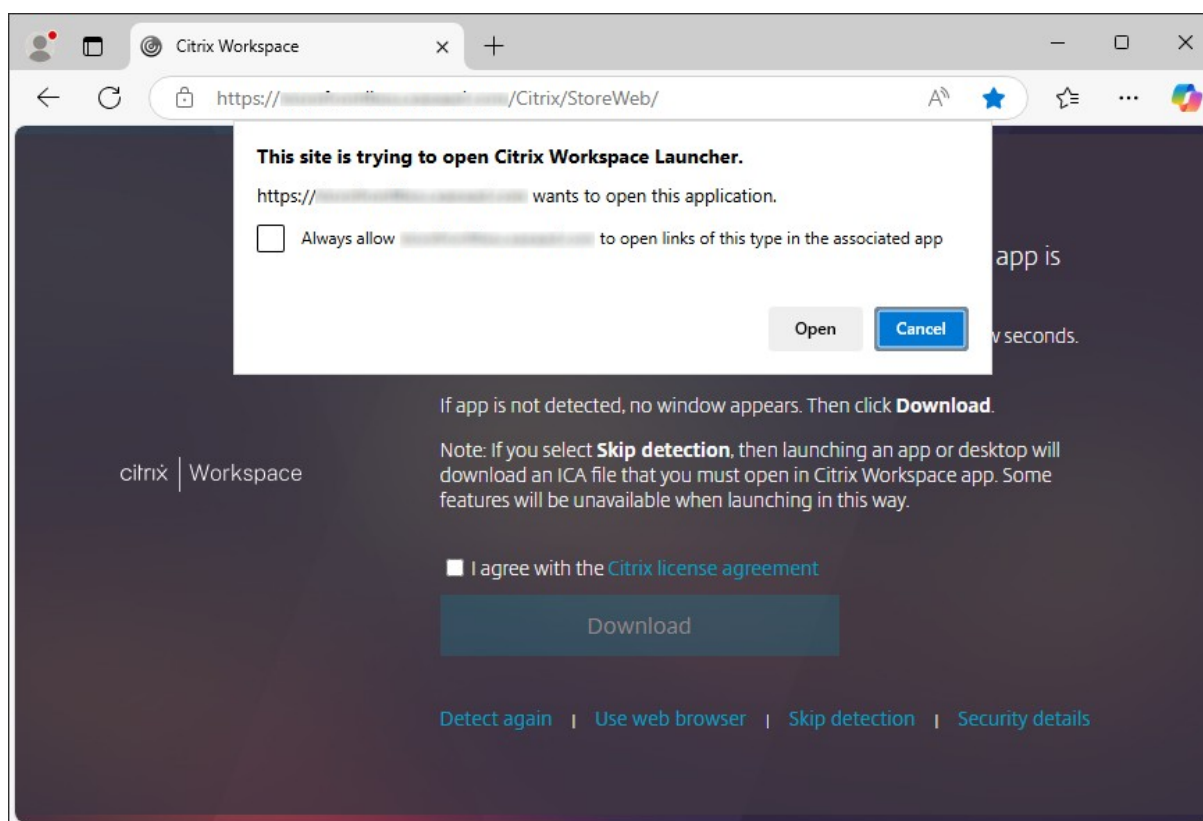
When accessing the store through a web browser for the first time or after clearing their cookies, the user sees the **Welcome to Citrix Workspace app** screen.



They can either:

- Select **Detect Citrix Workspace app** to launch resources in the locally installed Citrix Workspace app. This is recommended for the best experience.
- Select **Use web browser** to always launch resources within the browser. This option is only available if [launch option](#) is set to **Let the user choose**.

When the user selects **Detect Citrix Workspace app**, it attempts to open **Citrix Workspace Launcher** which is a component of Citrix Workspace app. If Citrix Workspace app is installed then their browser pops up a window asking to run the **Citrix Workspace Launcher**. They should select **Open Citrix Workspace Launcher**, **Open link**, **Open**, or **Always open** (depending on the browser). It is recommended they also select **Always allow domain to open links of this type in the associated app** (or similar depending on the browser) to avoid this window appearing every time they launch a resource.



If a locally installed Citrix Workspace app is detected then after a few seconds it continues to the next screen. When the user subsequently launches a resource it either uses Citrix web extensions or Citrix Workspace Launcher, depending on which was detected, to open the resource in the locally installed Citrix Workspace app.

If Citrix Workspace app is not installed, or the user cancels the launcher then depending on configuration they have the following options:

- **Download** - Downloads Citrix Workspace app from the Citrix website or from the StoreFront server. To hide this option, see [Allow users to download Citrix Workspace app](#).
- **Detect again** - Attempts to detect the locally installed Citrix Workspace app again.
- **Use web browser** - Skips Workspace app detection and always opens resources in the web browser. To show this option, set the [Launch option](#) to **Let the user choose**.
- **Skip detection** - users can use this option if they have a legacy version of Citrix Receiver installed that does not support the Citrix Workspace Launcher or Citrix web extensions. If they select this option, when they launch a virtual app or desktop then their browser downloads a file **launch.ica** that they can open with Citrix Receiver. This option results in reduced functionality and security so is recommended that administrators [disable this option](#).

## Home tab

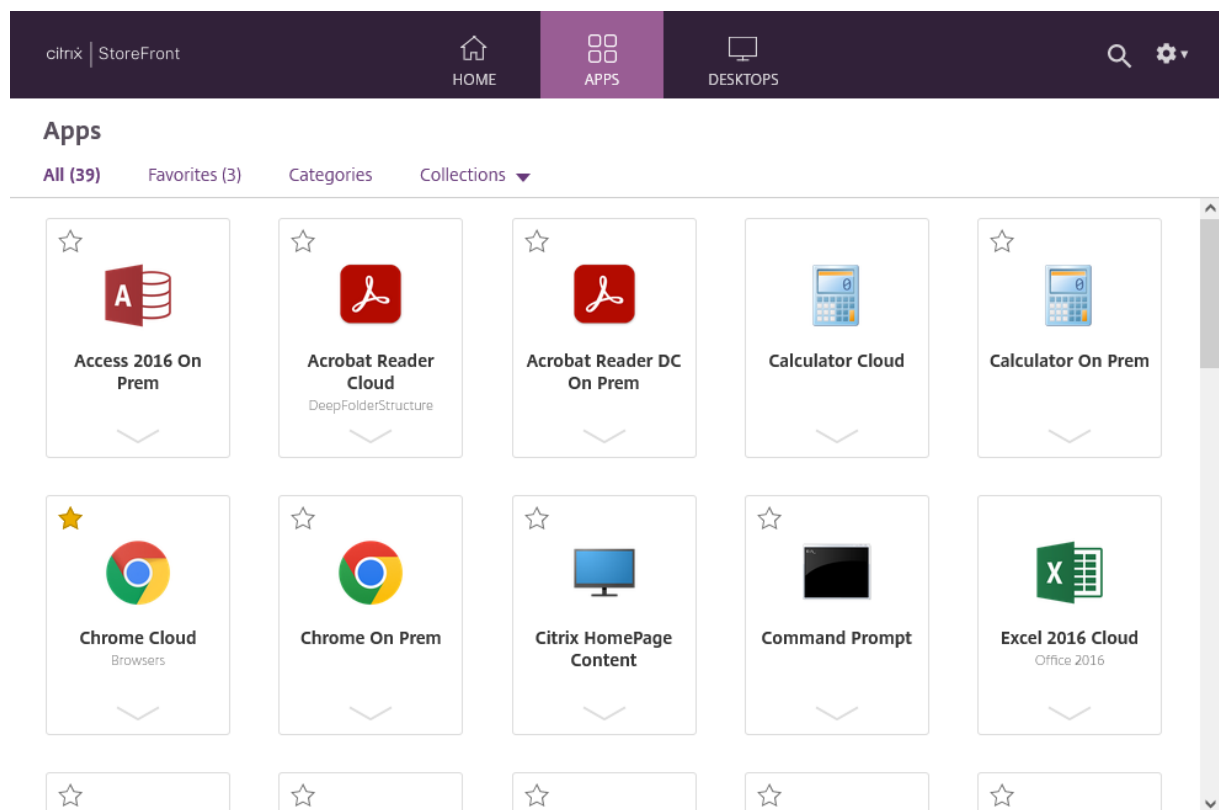
The **Home** tab displays any featured app groups along with any favorite or mandatory apps and desktops. The **Home** tab is only shown if favorites are enabled for the store.



## 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:

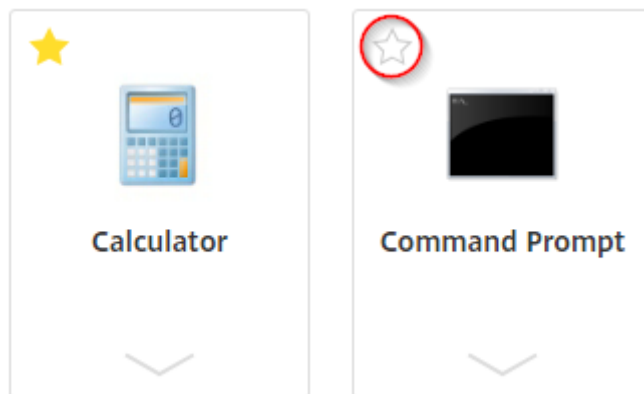
- **All** - Displays all desktops.
- **Favorites** - Displays the user's favorite desktops.

## App and desktop tiles

Click on an icon to launch the app or desktop.

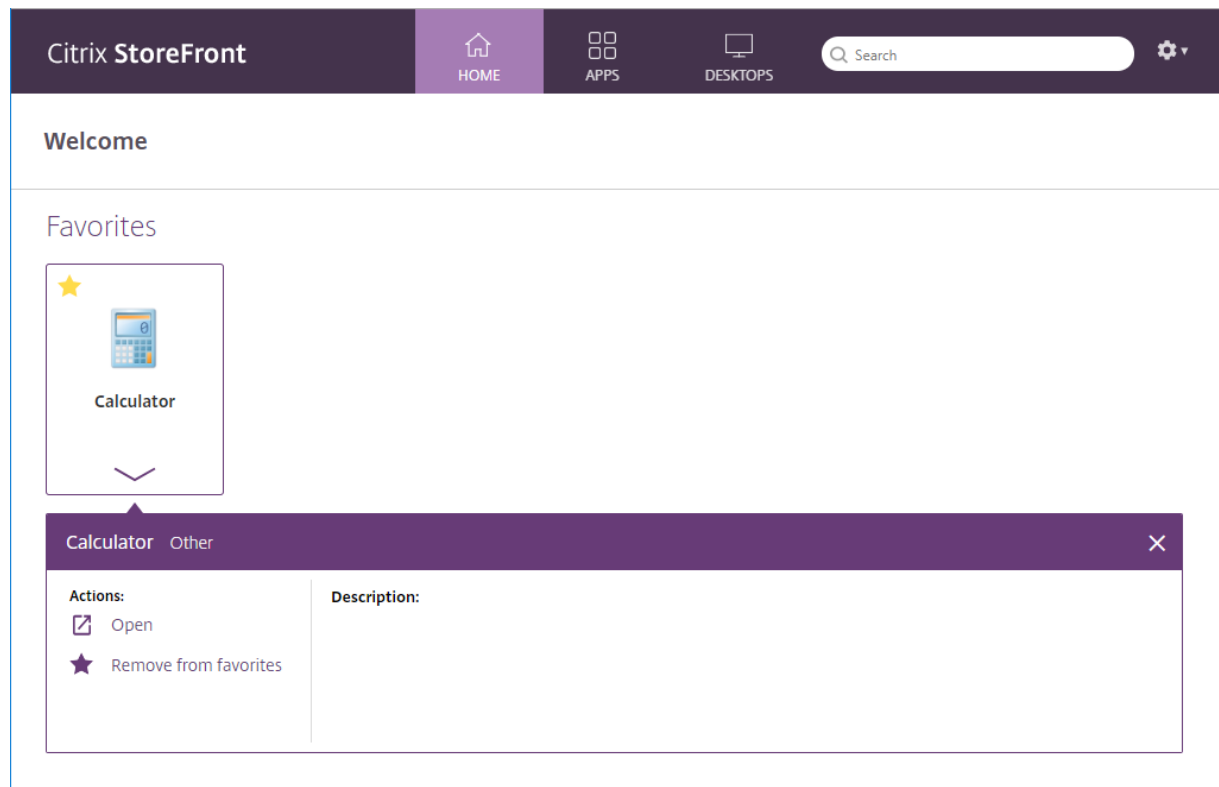
## Favorites

If [favorites are enabled](#) then the user can select star on a resource's tile to make it a favorite:



### View details and actions

The user 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 makes the app or desktop a 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 being a favorite.

- **Restart** - For assigned desktops where restart is available, this restarts the desktop.

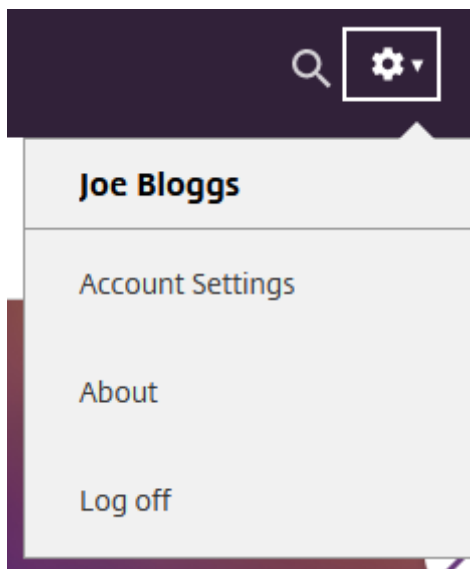
## Search

Users can select the magnifying glass icon to bring up the search box. Search across all apps, desktops, and categories:



## Settings menu

The settings menu is available only when accessing the store through a web browser.

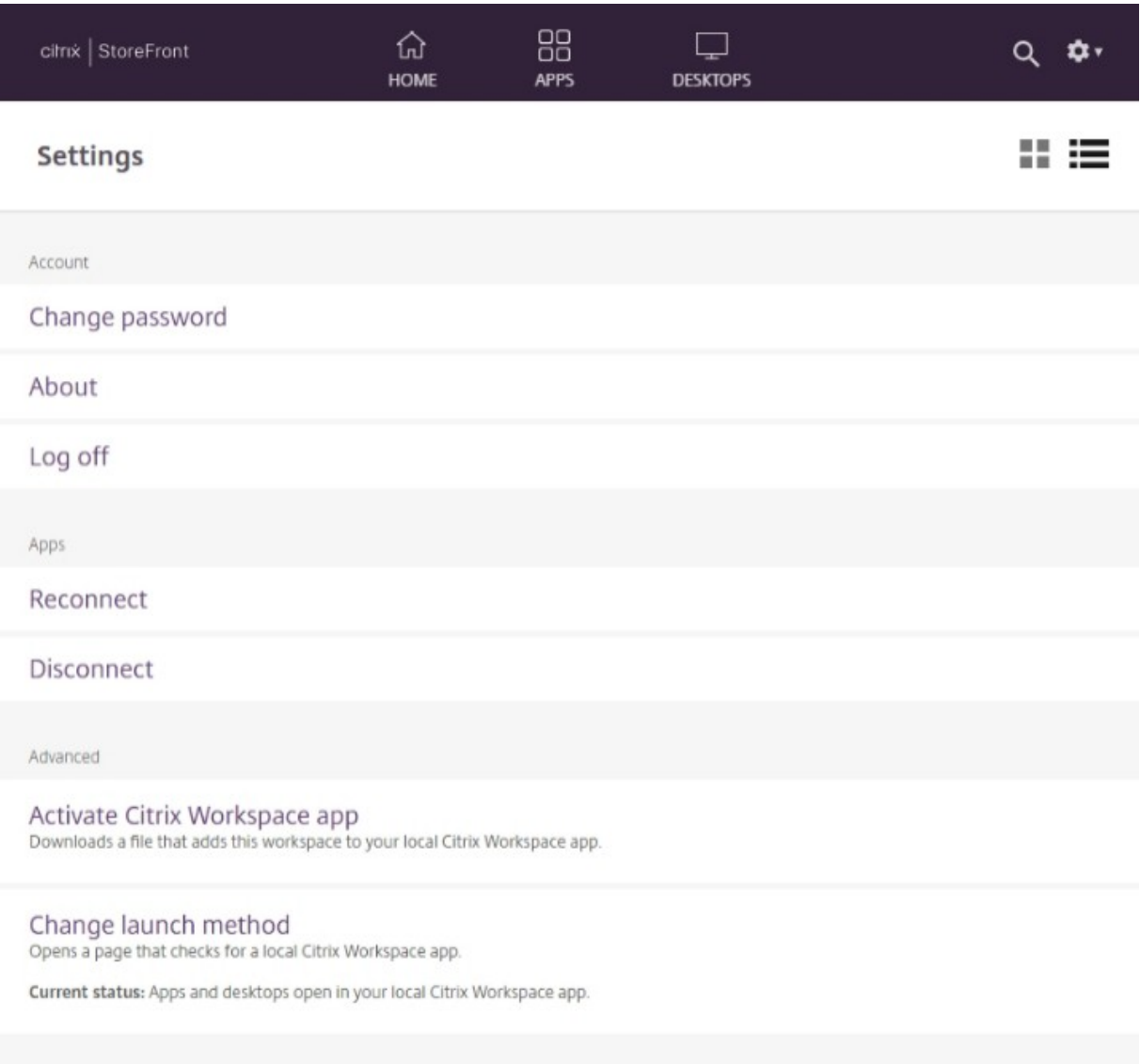


The settings menu has the following options:

- **Account Settings** - opens the settings page.
- **About** - Displays information about the application.
- **Log off** - Logs off the website.



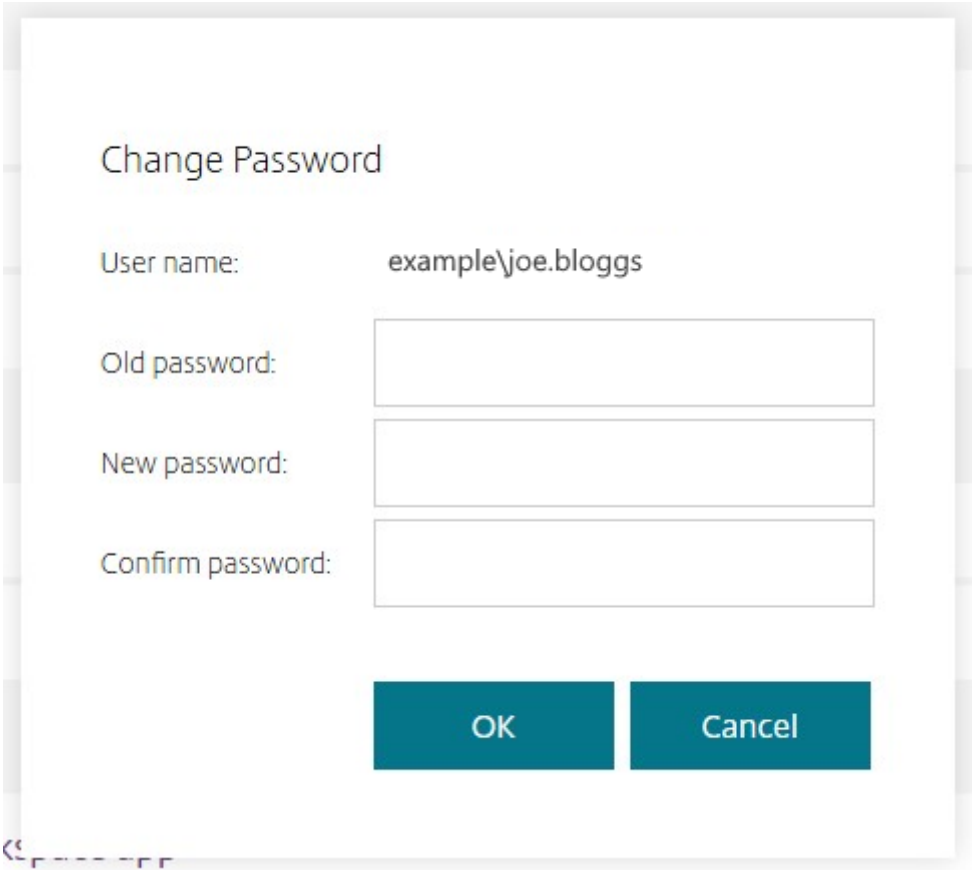
Settings



The account settings page may have the following sections.

Account

**Change password.** Only when using Username and password authentication. To configure whether this option is displayed, see [Username and password](#).

A screenshot of a 'Change Password' dialog box. The dialog has a title bar at the top. Below the title, the text 'Change Password' is displayed. There are four input fields: 'User name:' with the value 'example\joe.bloggs', 'Old password:', 'New password:', and 'Confirm password:'. Each of the last three fields is represented by an empty rectangular box. At the bottom of the dialog, there are two buttons: 'OK' and 'Cancel', both with a teal background and white text.

Change Password

User name: example\joe.bloggs

Old password:

New password:

Confirm password:

OK Cancel

**About.** Provides links to third party notices.

**Log off.** Log off the user.

## Apps

**Connect.** Resumes any disconnected sessions. To configure whether this option is displayed, see [Workspace Control](#).

**Disconnect.** Disconnects all of the current sessions and logs off. To configure whether this option is displayed, see [Workspace Control](#).

## Advanced

**Activate Citrix Workspace app.** Downloads a file that adds this store to the local Citrix Workspace app. To configure whether this option is displayed, see [User interface settings](#).

**Change launch method.** 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 the user off the store. If they are connected to any resources then depending [configuration](#), it will either:

- Terminate the resources.
- Disconnect from the resources
- Leave the resources connected.

## Installing as a Progressive Web App (Preview)

If the admin has enabled [Progressive Web App](#) then users can install the store website as a Progressive Web App.

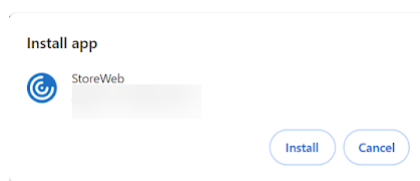
### Install Progressive Web App using Google Chrome

Users can install the store website as follows:

1. Open the store in the Google Chrome browser.
2. Select the following icon in the toolbar:



The option to install PWA appears.



3. Select **Install** to add the store to the desktop and Start menu:



If the user has have multiple StoreFront™ stores, they can install each store website separately. Each installation will generate a shortcut named `<Store website name>`, which can be renamed as required.

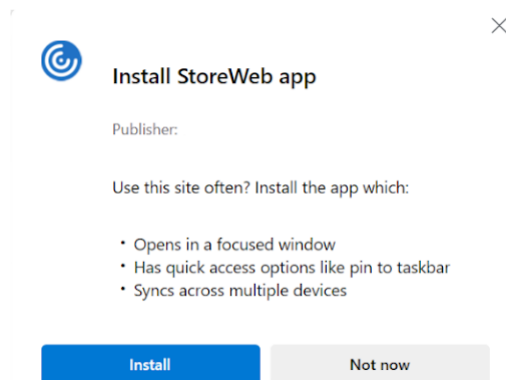
### Install Progressive Web App using Microsoft Edge

Users can install the store website as follows:

1. Open the store in the Microsoft Edge browser.
2. Select the following icon in the toolbar:



The option to install appears.



3. Select **Install** to add the store to the desktop and Start menu:



If the user has have multiple StoreFront stores, they can install each store website separately. Each installation will generate a shortcut named <Store website name>, which can be renamed as required.

## Modern experience

October 23, 2025

This section describes how users can access and interact with their stores using the modern experience. The modern experience is not enabled by default. To enable it, see [UI experience](#).

### Citrix Workspace app required screen

If the user opens the store in web browser but the store is configured to require Citrix Workspace app then the user is directed to install and configure Citrix Workspace app. For more information, see [Require Citrix Workspace app](#).

## Citrix Workspace app detection

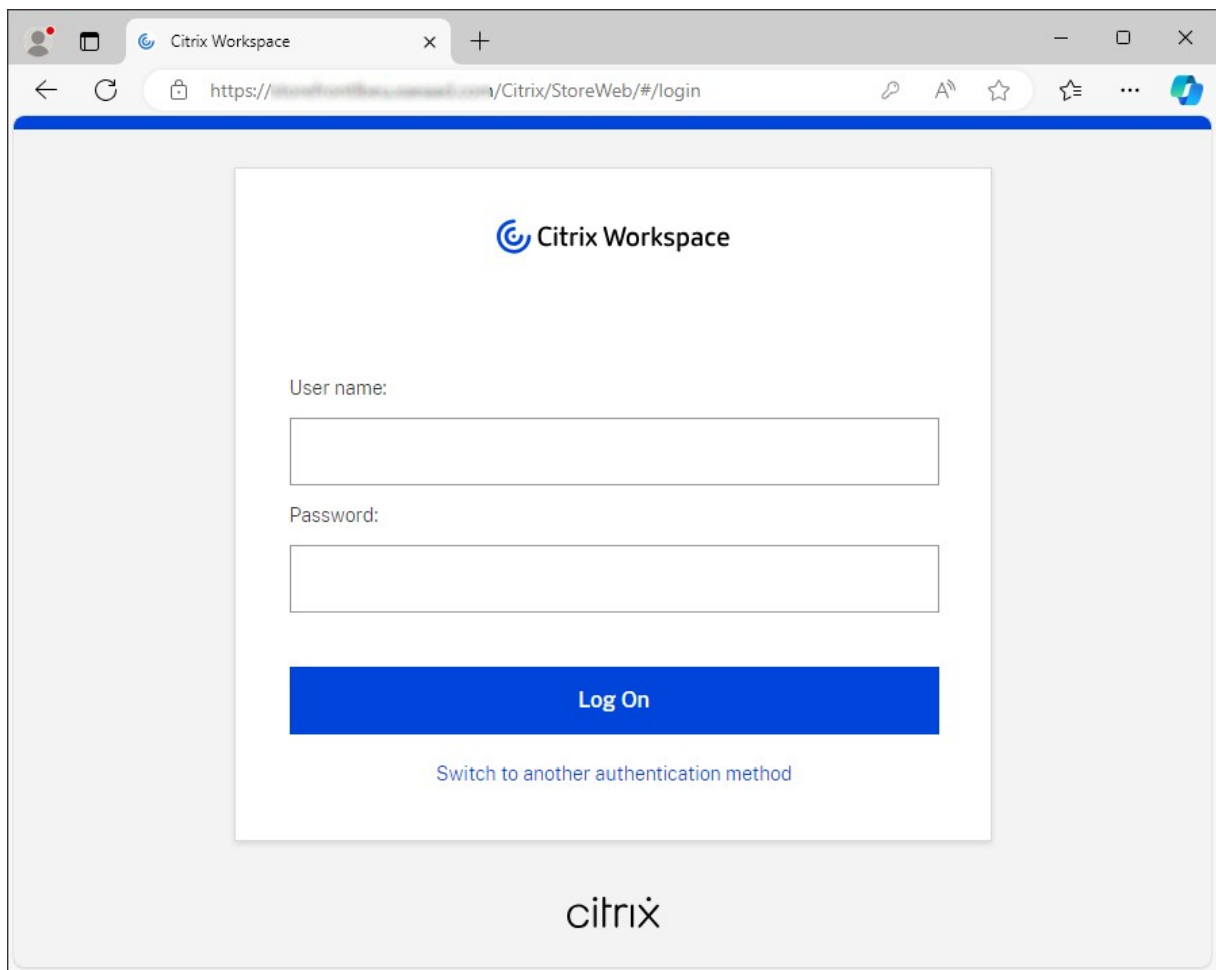
The first time the user opens the store in a web browser, or after clearing cookies, the web page may display the **Welcome to Citrix Workspace app** screen, which prompts the user to detect Citrix Workspace app. This step may occur before or after log in depending on configuration. For more information, see [Citrix Workspace app detection](#) screen.

When users authenticate at the NetScaler Gateway this screen is displayed after authentication. When users authenticate directly to Storefront, normally this screen is displayed before authentication, unless you have configured [prompt to install Citrix Workspace app after login](#).

If Citrix Web Extension is installed and has detected Citrix Workspace app then it skips this step and defaults to launching in Citrix Workspace app. Users can change the launch method from the Settings page.

## Authentication

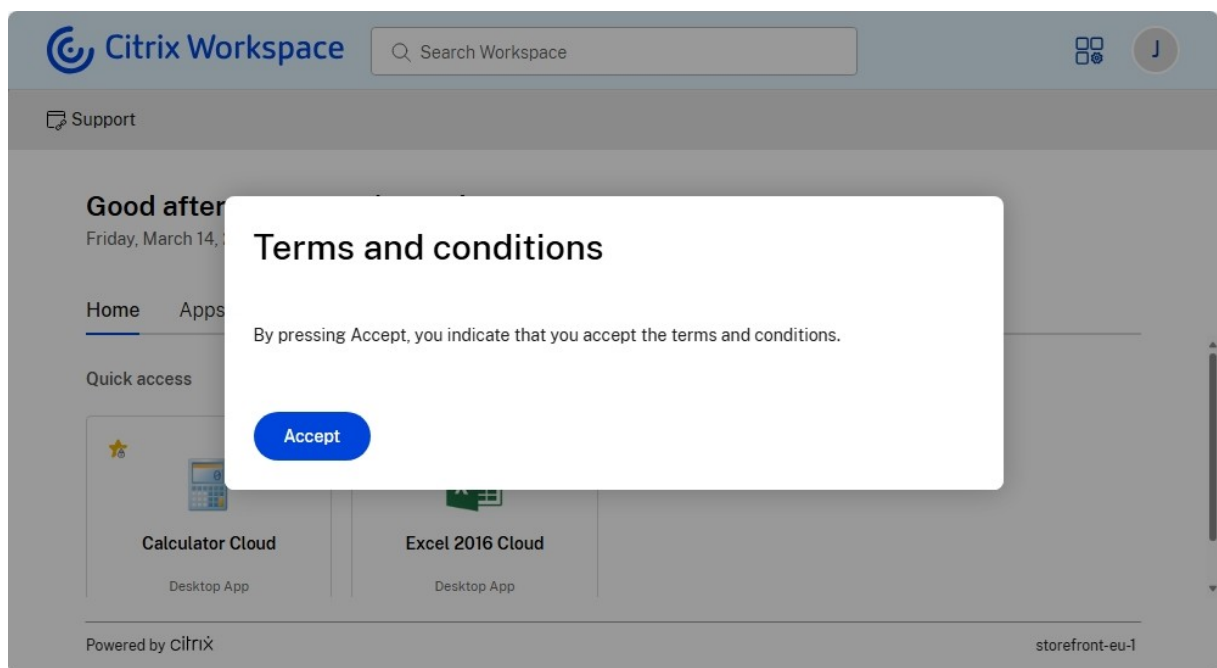
Depending on the [authentication methods](#) configured and whether single sign-on is enabled, users might be required to log in.



The screenshot shows a web browser window with the title 'Citrix Workspace'. The address bar displays the URL 'https://[redacted]/Citrix/StoreWeb/#/login'. The main content area features the Citrix Workspace logo at the top. Below the logo, there are two input fields: 'User name:' and 'Password:'. A blue 'Log On' button is positioned below the password field. Underneath the button is a link that says 'Switch to another authentication method'. The Citrix logo is also visible at the bottom center of the page.

If multiple authentication methods are available then the user can choose to switch to a different authentication method.

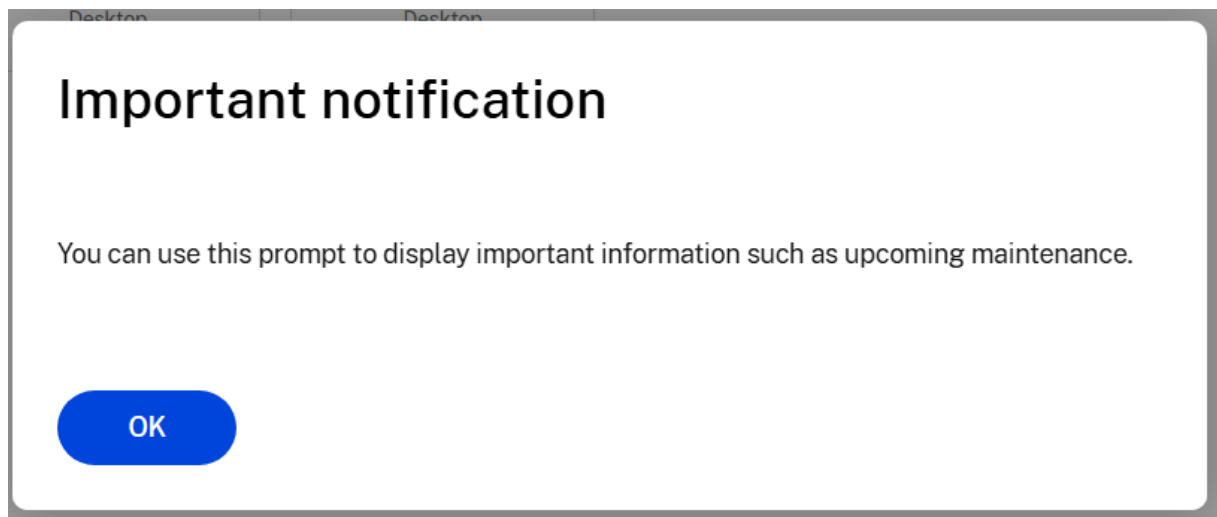
After logging in, if [configured](#), users may see a message they must accept to proceed.



For more information on how to configure this, see [Dialog after login](#).

### After log in dialog

A dialog may be displayed to the user. For more information, see [Configure a custom dialog to be displayed after log in](#).



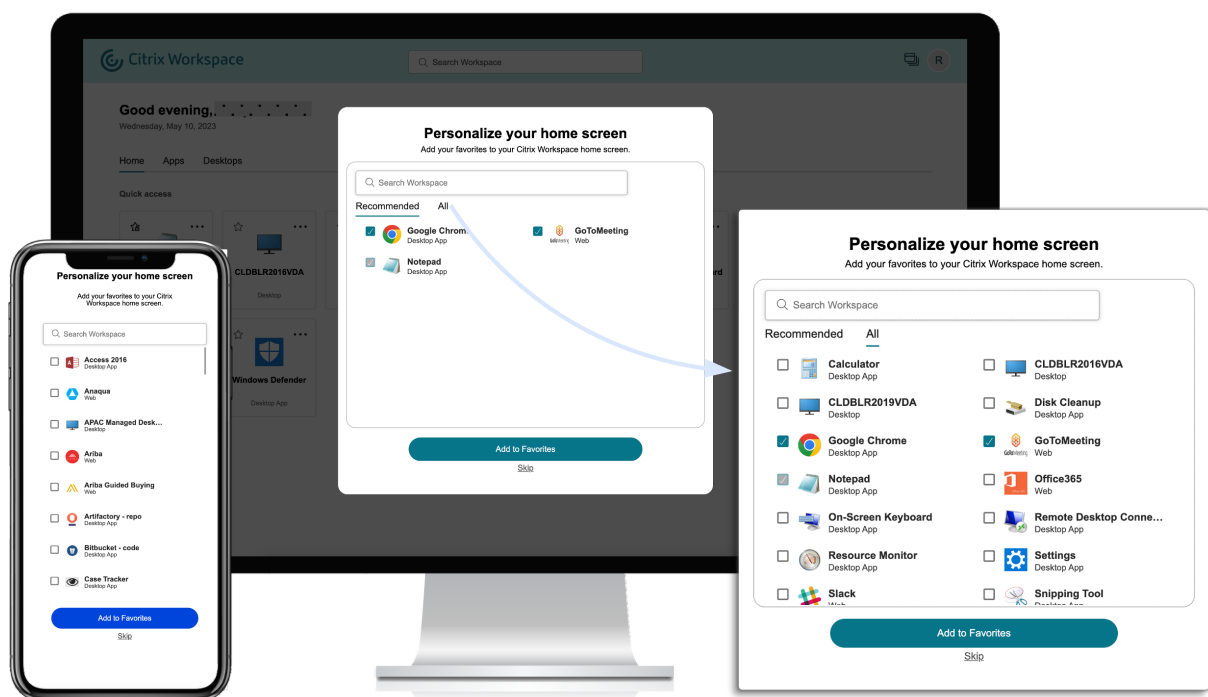
The user must press accept the message before accessing their resources. You can configure how frequently the message is displayed.

## First-time user experience

When accessing the UI, for the first time, users are prompted with a pop-up where they can favorite multiple apps in one easy single step.

The first-time user experience is activated when users have more than 20 apps, and haven't added any of them to Favorites. The experience is supported on all browsers and native clients (Mac, Windows, Linux, and ChromeOS), and mobile devices (iOS and Android). You're able to see it the first time you sign in.

The recommended or mandatory apps appear on the **Recommended** tab of the first-time user screen, as set by admins on the DaaS console for Citrix Virtual Apps and Desktops™, and on the Secure Private access console for Web and SaaS apps. Mandatory apps are selected by default and check disabled. **Recommended** and auto-favorite apps are selected by default and check enabled for users. End users can also select other apps to subscribe to, or add to Favorites from all tabs. All selected apps are automatically added to Favorites, and reflected on the home page.



## Limitations

- The **Personalization** screen appears once per device and browser, and every time for incognito mode unless users mark a favorite.



- If the admin removes the mandatory or recommended tag from the apps, the apps in **Favorites** won't have any impact.
- If the end-user has not added any apps to **Favorites**, the **Personalization** screen appears each time the workspace app is opened.

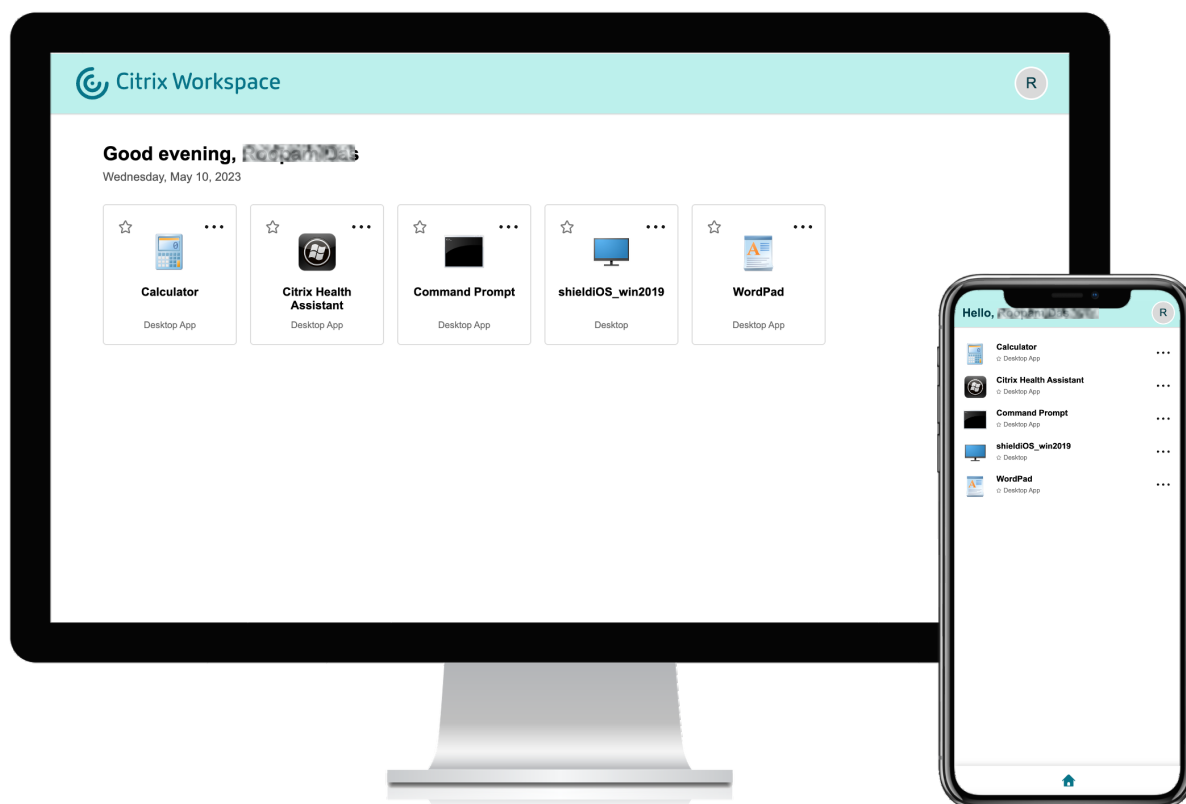
To avoid this:

- End users can add one or more apps to **Favorites**. This prevents the personalization screen from appearing every time they start the app.
- Administrators can add one or more apps to Favorites. For more information, see [Citrix Virtual Apps and Desktops configuration](#).

## Navigation tabs

### Simple view

If users have fewer than 20 resources, by default, they land on the screen with Simple View that doesn't have any tabs or categories. All the apps and desktops appear on the same page. On this screen, their favorites show up first, followed by all the other apps in an alphabetical order.



You can configure the store to [Always display navigation tabs](#), which disables simple view.

### **Full view**

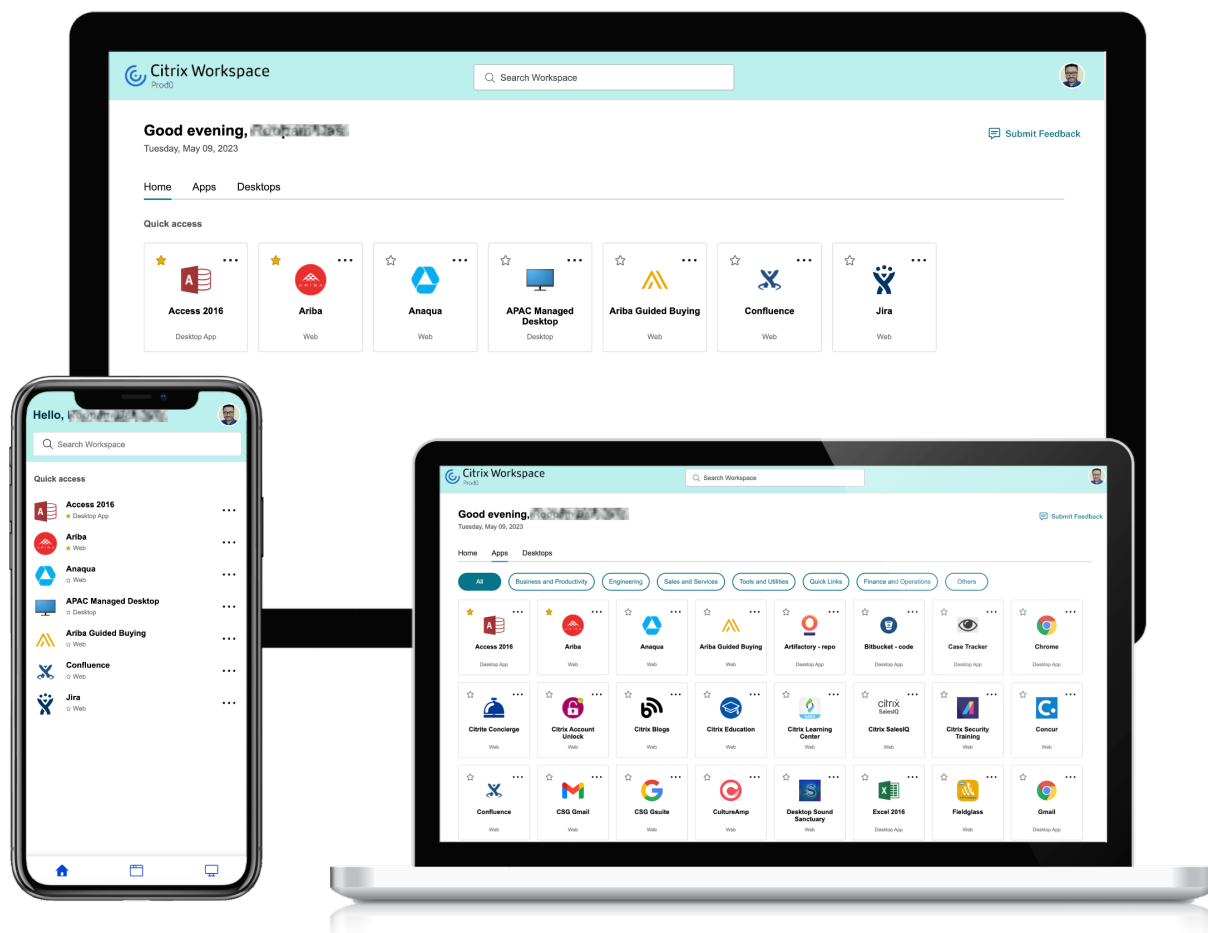
If users have more than 20 resources, or the store website is configured to Always display navigation tabs, then up to three tabs are displayed - **Home**, **Apps** and **Desktops**. By default when a user logs in they land on the **Home** tab if it exists, otherwise the **Apps** tab. You can [configure](#) whether the home tab appears and the default tab.

### **Home tab**

On the home tab, mandatory and favorite apps appear first, followed by the five most recently used apps. The star icons for the **Mandatory** apps are locked, and users can't remove them from Favorites.

### **Apps tab**

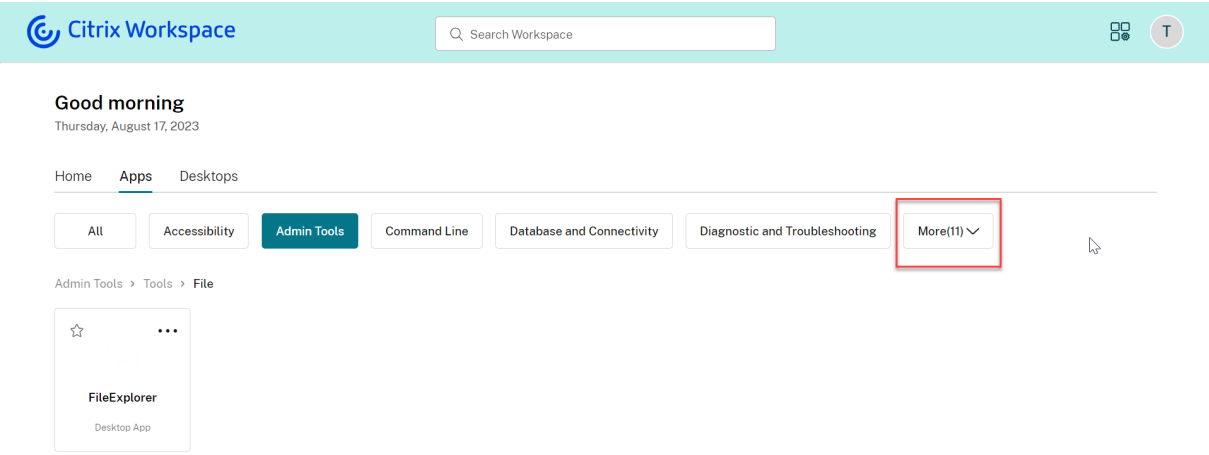
On the **Apps** tab, favorites appear first, followed by all the other apps in an alphabetical order. If the admin has created categories and attached the apps to them, then the various categories appear, and users can select the category of the apps that they want to view.



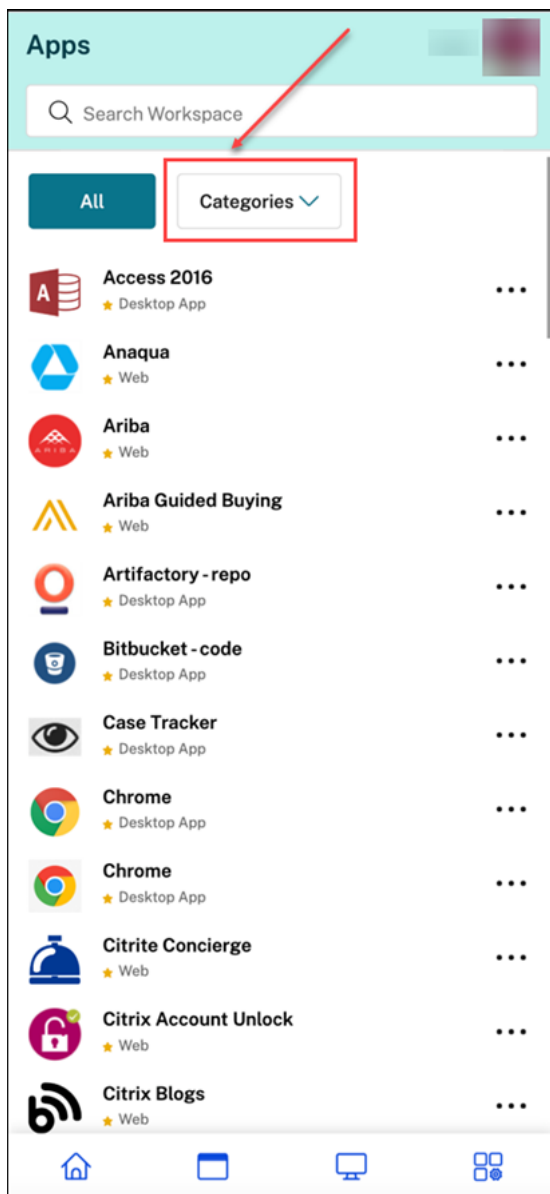
For each application you can define a category. The category represents the folder structure that appears on the screen for end users. For example, consider an app for which the folder is defined as [Optimisation tools/Cleaning](#). Now, to access this app, end users must go to Optimisation tools > Cleaning, where Optimisation tools is a category and Cleaning is it's sub-category. For more information about configuring categories, see [Applications](#).

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.

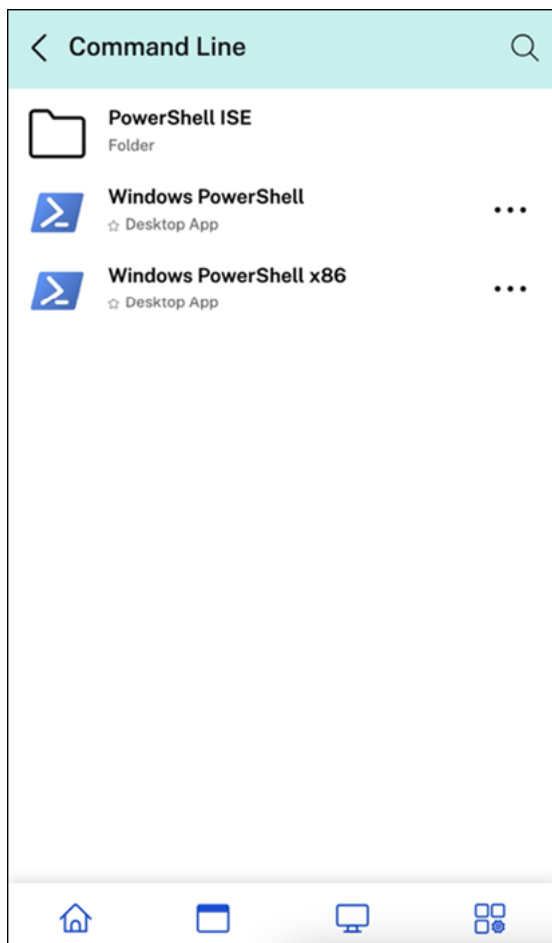
The navigation breadcrumbs are also displayed to the users.



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



Select the relevant category, a list of available sub-categories and applications is displayed based on the configuration made by the admin.



## Desktops tab

The **Desktops** tab displays all available virtual desktops.

## Favorite and mandatory apps

By default, users can create and remove favorites by selecting the star icon on the tile.

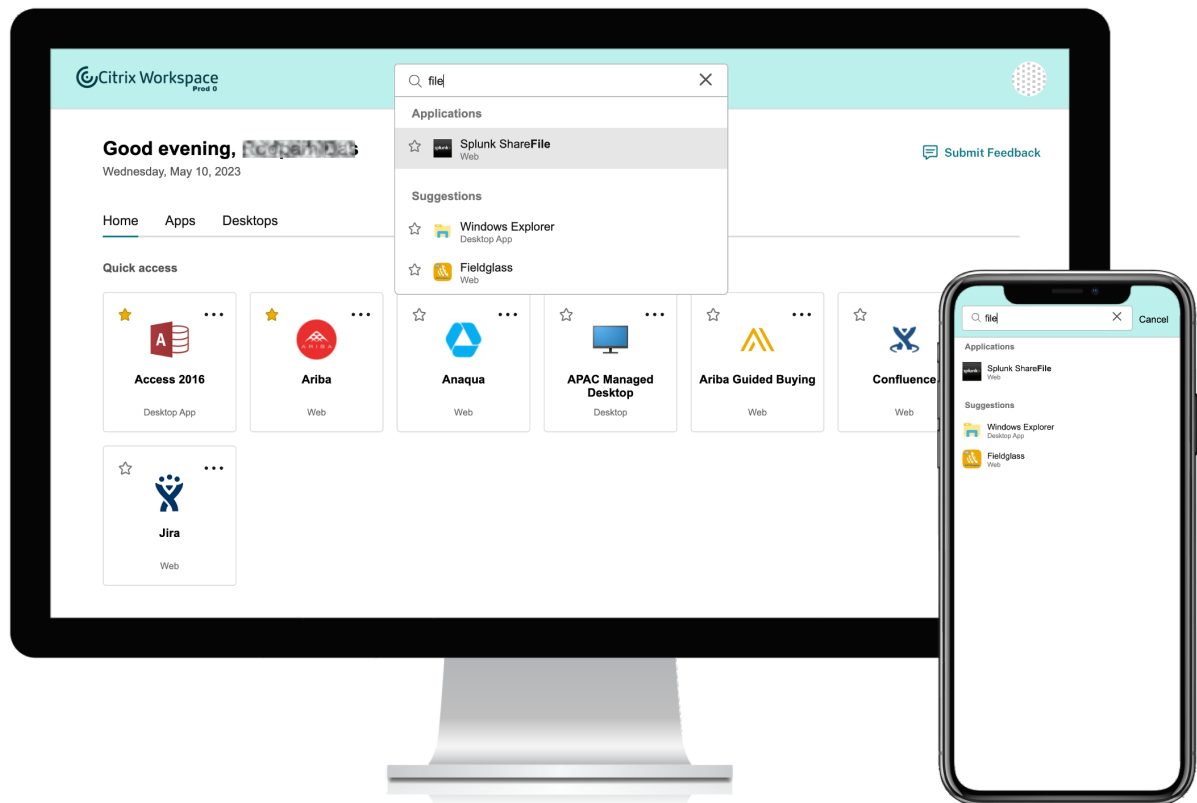
Administrators can also configure the following using keywords [keywords](#):

- **auto** - apps are automatically created as favorites but they can be removed by the user.
- **mandatory** - apps are always favorites and cannot be removed by the user.

To disable favorites see [Enable or disable favorites](#). If favorites are disabled, all apps appear on the **Home** tab.

## Search for apps and desktops

Users can enter search terms to search for apps and desktops by name and category. Favorites appear at the top of the list.



## Activity Manager

Users can manage their sessions using [Activity manager](#).

## App and desktop tiles

The tile displays the application name and name as configured within Studio. Users can click the tile to launch the application.

For assigned desktops, in addition the power state is displayed. For more information, see [Power status](#).

## Tile actions

The **More** options menu (ellipsis icon) on the tile provides users with access to relevant actions. The options presented are context-sensitive.

These actions might include:

- **Open Desktop** or **Open App** - Launch or reconnect to the app or desktop. If the desktop is powered off or in hibernation then this first powers on the desktop before launching the session.
- **Add to favorites** - Adds to favorites so it appears on the **Home** tab. This has the same effect as clicking the **Star**. Only enabled if favorites is enabled.
- **Show Details** - Opens a pop-up window containing the description of the app or desktop.
- For assigned desktops, additional power management actions may be available. For more information, see [Power actions](#).

## Settings

Users access **Account Settings** from a menu that appears when they select their profile icon in the upper-right corner of the UI.

### Settings

Advanced

### Advanced

#### Change Password

[Change Password](#)

#### Apps and Desktops Launch Preference

##### Current Method:

Apps and desktops will launch in your **Citrix Workspace app** on your device (Recommended).

[Verify connection](#)

#### Download Workspace Configuration

Add the workspace URL and other configuration details to the Workspace app on your device.



You must have Citrix Workspace installed to use the configuration file. [Download Workspace app](#)

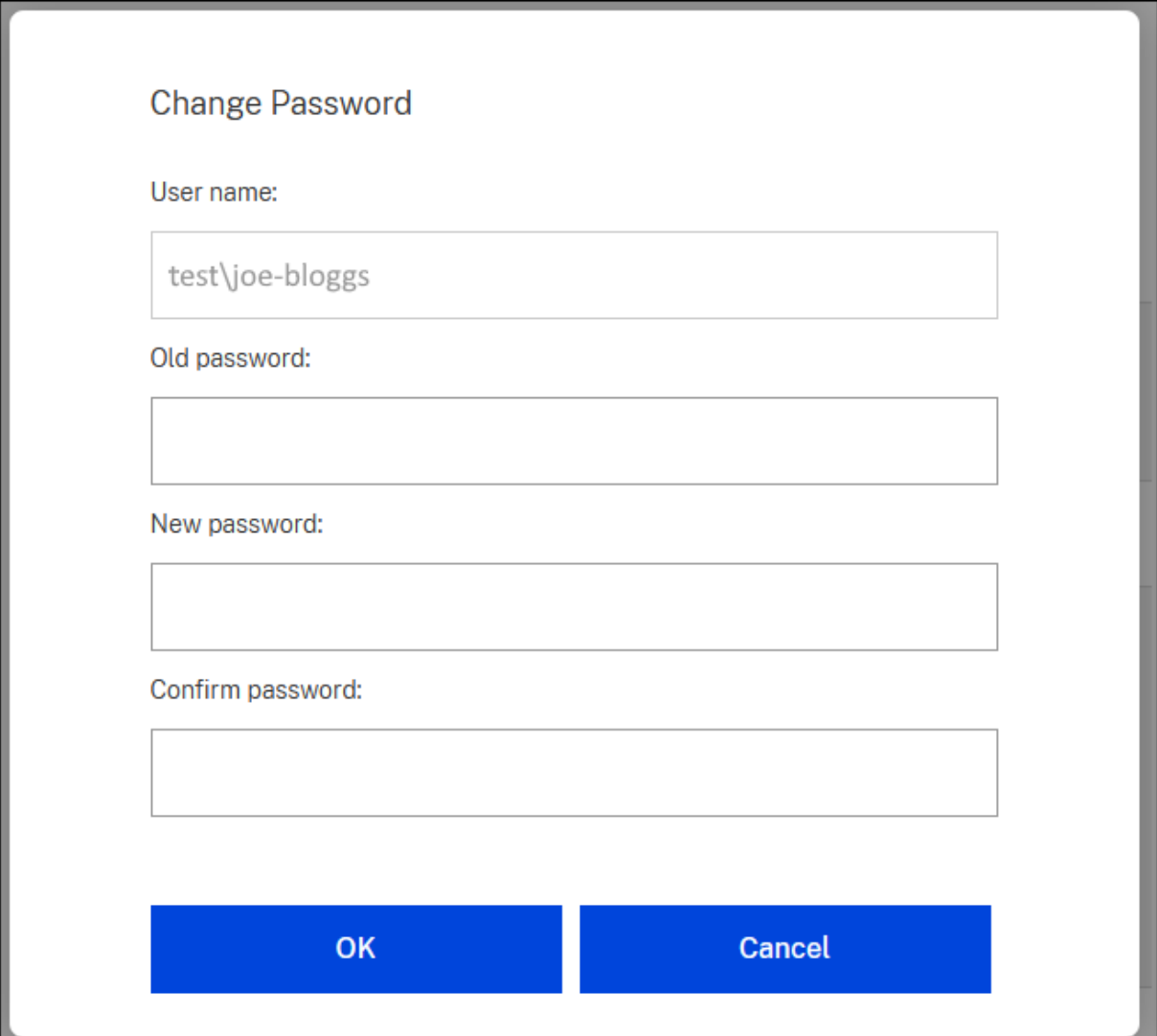
[Download configuration file](#)

Download and open the file, then click **Add** to update the Workspace app.



## Change Password

If users logged in using username and password authentication and StoreFront is configured to [allow users to change their password at any time](#) then users see an option to **Change Password**. If the user selects this screen a window appears where they can enter their old and new password:

A screenshot of a 'Change Password' dialog box. The dialog has a title bar at the top. Below the title, the text 'Change Password' is displayed. There are four input fields: 'User name:' with the text 'test\joe-bloggs', 'Old password:', 'New password:', and 'Confirm password:'. At the bottom, there are two blue buttons labeled 'OK' and 'Cancel'.

## Apps and Desktops Launch Preference

When using a web browser, this displays whether apps launch in the web browser, or in Citrix Workspace app, or by downloading and ICA file that the user can open in Citrix Workspace app.

The user can select **Verify connection** to open the Citrix Workspace app detection screen.

## Download Workspace Configuration

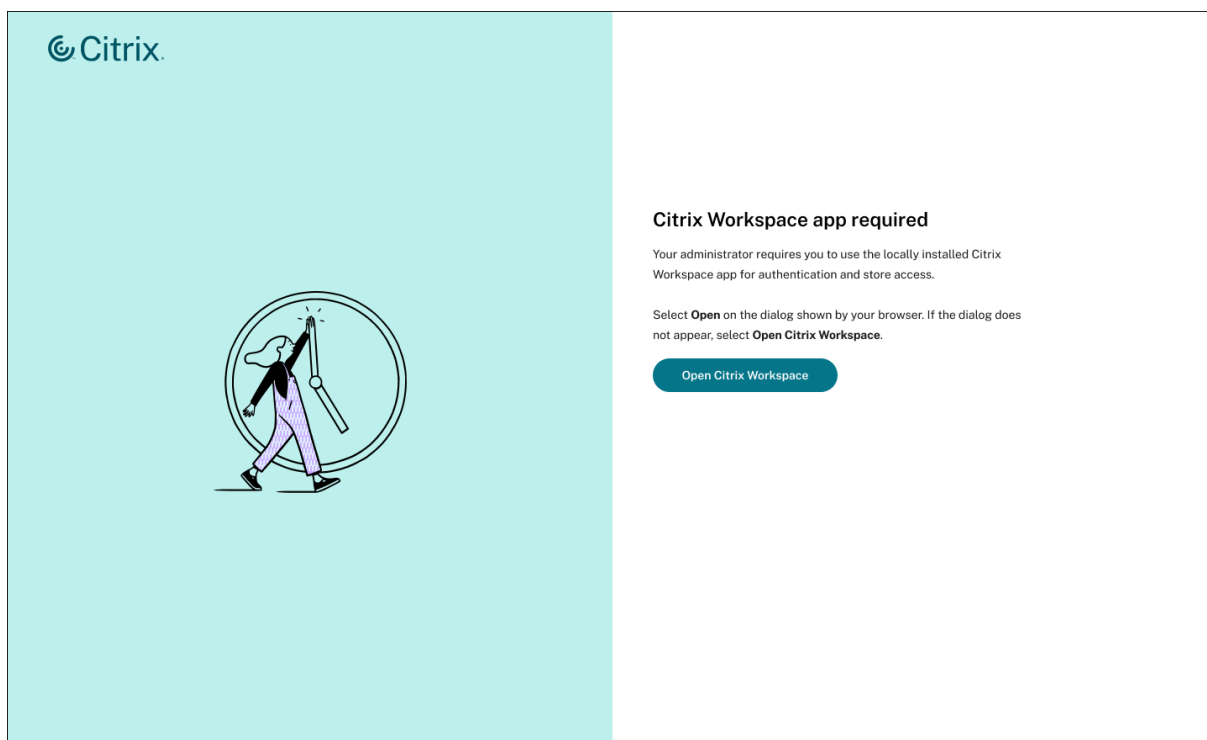
When using a web browser, users can download a file that configures Citrix Workspace app to connect to the store. To enable this, see [Allow end user to download a Citrix Workspace app configuration file](#)

## Require Citrix Workspace app

October 22, 2025

Once administrators have enabled [Require Citrix Workspace app](#), end users can't use the Citrix Workspace web client in browsers.

When users try to access web client by entering a store URL in a browser, they see the following webpage that prompts to open the native app.



1. Click **Open Citrix Workspace**.

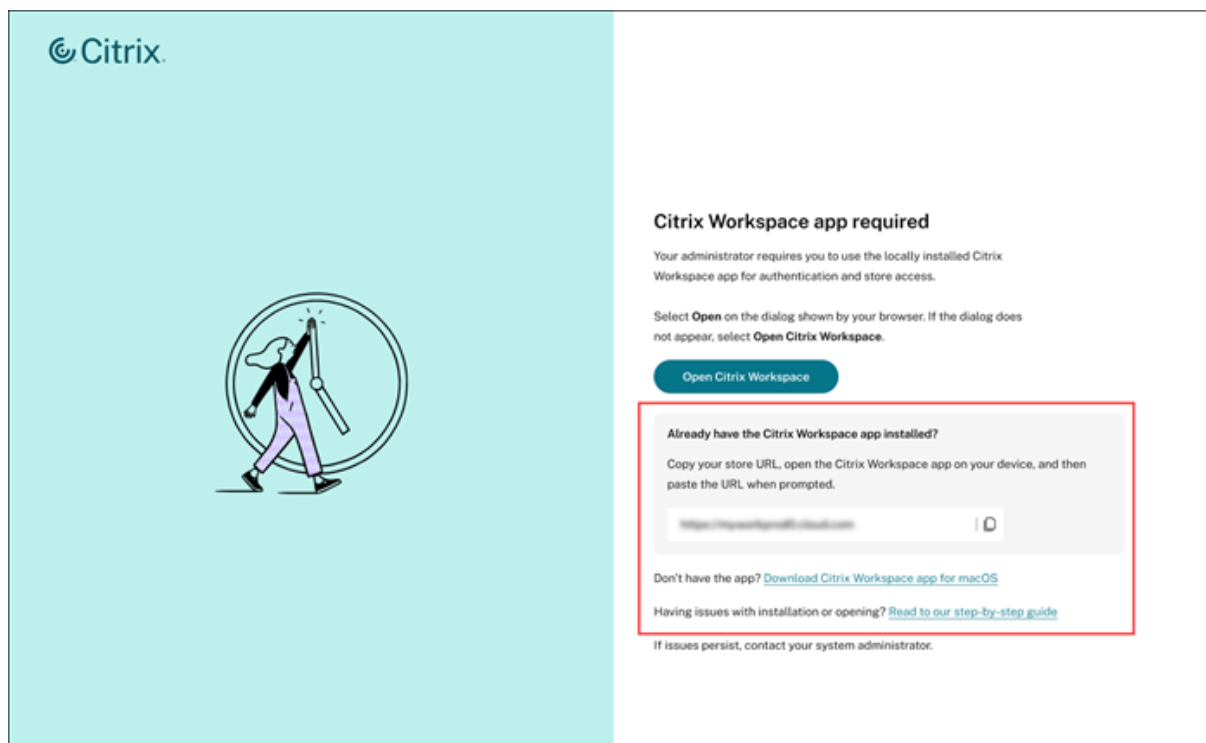
The client detection process starts, checking whether Citrix Workspace app is installed locally on the user device.

The **Open Citrix Workspace Launcher** prompt appears asking users to open the native app.

2. Click **Open Citrix Workspace app**.

If a user doesn't see the prompt or doesn't click **Open Citrix Workspace app** on the prompt within 5 seconds, the webpage provides the following extra options to continue:

- The store URL to copy and add manually in the native Citrix Workspace app.
- A download link to install Citrix Workspace app. To configure the download links, see [Citrix Workspace app deployment](#).
- The link to the end-user guide, which provides step-by-step instructions for installing and opening Citrix Workspace app.



#### Note:

If a user is using the Safari browser on an iPad, the browser can't differentiate it from a Mac desktop. Therefore, the user has to click the **I am on iPad** link to proceed with automatic store addition.

Automatic store addition is not supported on Linux and ChromeOS. As a result, the **Open Citrix Workspace Launcher** prompt doesn't appear on these devices. In such cases, users need to manually add the store url in the native app. For more information, see [Manual store addition](#).

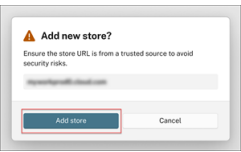
### Automatic store addition

On supported versions of Citrix Workspace app, it automatically adds the store. The minimum versions are as follows:

| Operating system | Compatible version |
|------------------|--------------------|
| Windows          | 24.9.0 or later    |
| Mac              | 24.5.0 or later    |
| Android and iOS  | 24.9.0 or later    |

**Note:**

Automatic store addition is not supported on Linux and ChromeOS platforms and has version requirement on Windows and Mac platforms. In such cases, users need to manually add the store url in the native app. For more information, see Manual store addition.

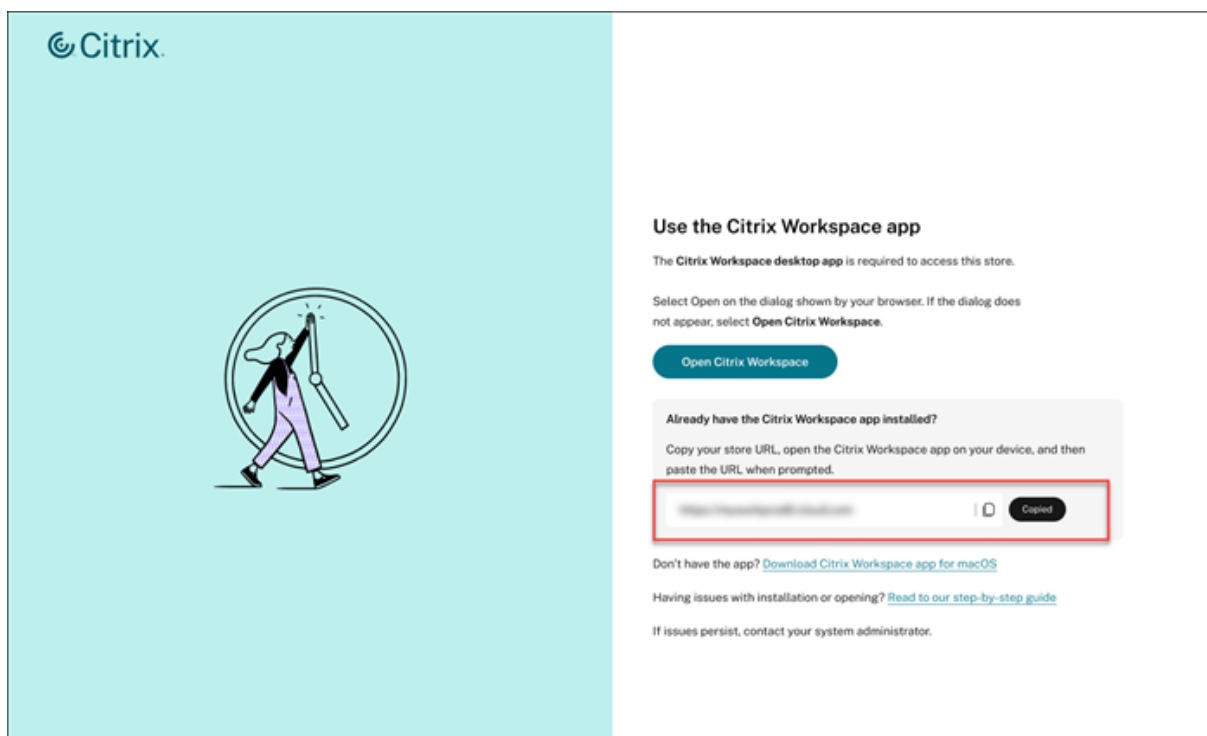


Click **Add store**.

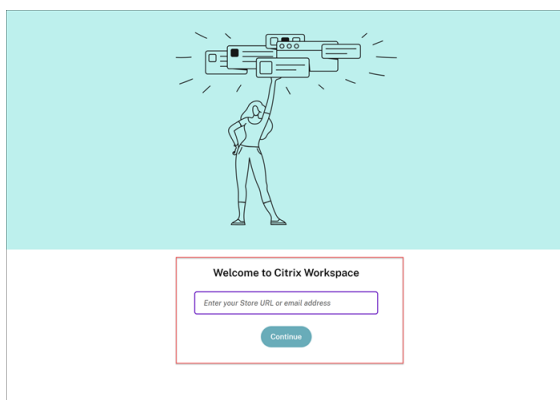
Once clicked, the native app automatically captures the store URL entered in the browser and displays the authentication page for the user to sign in. After the successful authentication, the user can see the home page of the native Citrix Workspace app.

**Manual store addition**

Users can manually add a store to Citrix Workspace app if the native app doesn't automatically capture the store URL when they click the **Add store** option.



1. Copy the store URL from the native mandate webpage, and paste it into the **Welcome to Citrix Workspace** page.



2. Click **Continue**.

After submitting a valid store URL, Citrix Workspace app displays the authentication page for the user to sign in. After the successful authentication, the user can see the home page of the native Citrix Workspace app.

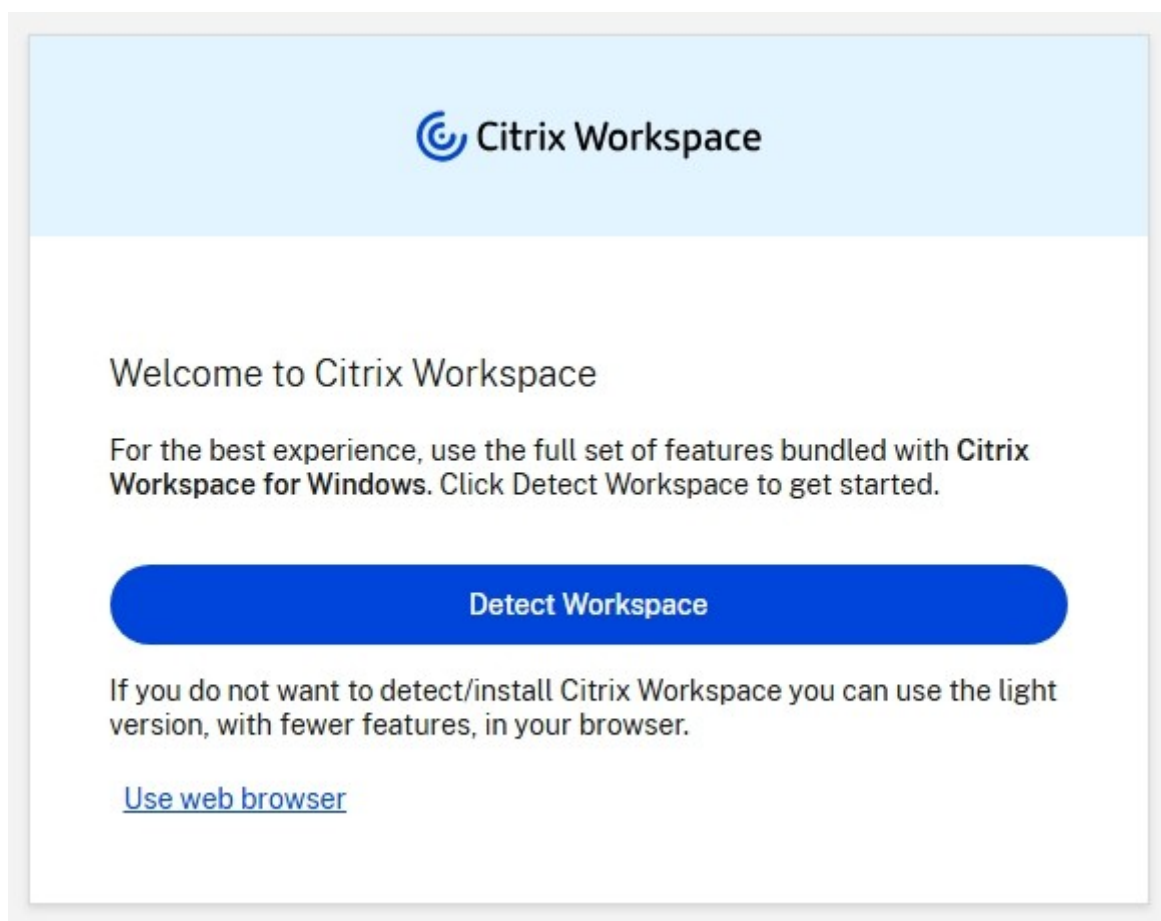
## Citrix Workspace app detection

October 22, 2025

## Welcome to Citrix Workspace screen

When accessing the store through a web browser, the website may display the **Welcome to Citrix Workspace** screen. This applies when:

- The user opens the store in their web browser for the first time, or after clearing site data from the web browser.
- [launch preference](#) is set to **Open in Citrix Workspace app** or **Let the user choose**.
- If Citrix Web Extension is not installed, or has not detected Citrix Workspace app. If Citrix Web Extension detects Citrix Workspace app then it skips this step and defaults to launching in Citrix Workspace app.
- The device's operating system supports [Citrix Workspace launcher](#).

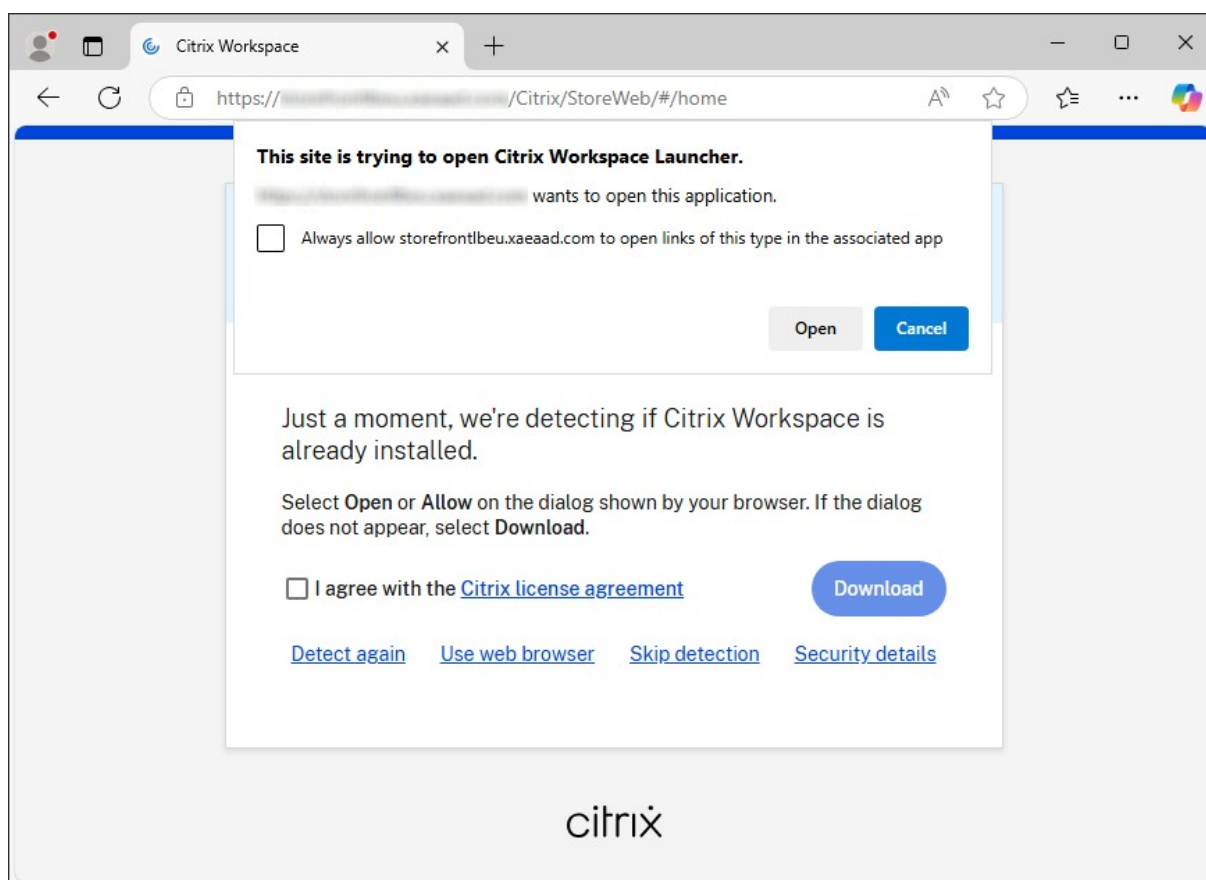


Users can either:

- Select **Detect Citrix Workspace app** if they wish to launch resources in the locally installed Citrix Workspace app. This is recommended for the best experience.
- Select **Use web browser** to always launch resources within the browser. This option is only available if [launch preference](#) is set to **Let the user choose**.

## Citrix Workspace app detection screen

When the user selects **Detect Citrix Workspace app**, the website displays the Citrix Workspace app detection screen. This attempts to open **Citrix Workspace Launcher** which is a component of Citrix Workspace app. If Citrix Workspace app is installed then your browser displays a message asking to run the **Citrix Workspace Launcher**. Click **Open Citrix Workspace Launcher** or **Open link** (depending on the browser). It is recommend that they also select **Always allow domain to open links of this type in the associated app** (or similar depending on the browser) to avoid this message appearing every time they launch a resource.



The user can also reach this from the [setting screen](#).

If a locally installed Citrix Workspace app is detected then after a few seconds it continues to the next screen. When the user subsequently launches a resource it uses Citrix Workspace Launcher to open resources in the locally installed Citrix Workspace app.

If Citrix Workspace app is not installed, or the user cancels Citrix Workspace launcher then they might have the following options:

- **Download** - Downloads Citrix Workspace app from the Citrix website. To configure this option, see [Citrix Workspace app deployment](#).
- **Detect again** - Attempts to detect the locally installed Citrix Workspace app again.

- **Use web browser** - Skips Workspace app detection and always opens resources in the web browser. This option is only available if [launch preference](#) is set to **Let the user choose**.
- **Skip detection** - Users can use this option if they have a legacy version of Citrix Receiver installed that does not support the Citrix Workspace Launcher or Citrix web extensions. If they select this option, when they launch a virtual app or desktop then their browser downloads a [.ica](#) file that they can open with Citrix Workspace app. This option results in reduced functionality and security so is recommended that administrators [disable this option](#).

## Activity Manager

October 22, 2025

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 on the go.

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 desktop and at the bottom of their screen on mobile devices.

### Note:

If you are unable to view the Activity Manager icon in a darker banner theme, consider changing and testing the color selected in the **Banner text and icon color** setting. The icon might not be visible clearly due to a low contrast between the banner and the Activity Manager icon. For more information, see [Appearance](#).

## Prerequisites

Activity Manager feature requires Citrix Desktops as a Service or Citrix Virtual Apps™ and Desktops 2311 and later. If you use an earlier version of Citrix Virtual Apps and Desktops then Activity Manager does not display any sessions so it is recommended that hide Activity Manager.

To hide the Activity Manager button run the PowerShell:

```
Add-STFFeatureState -Name "Citrix.StoreFront.ActivityManager"-IsEnabled $false
```

To re-enable the Activity Manager button run the PowerShell:

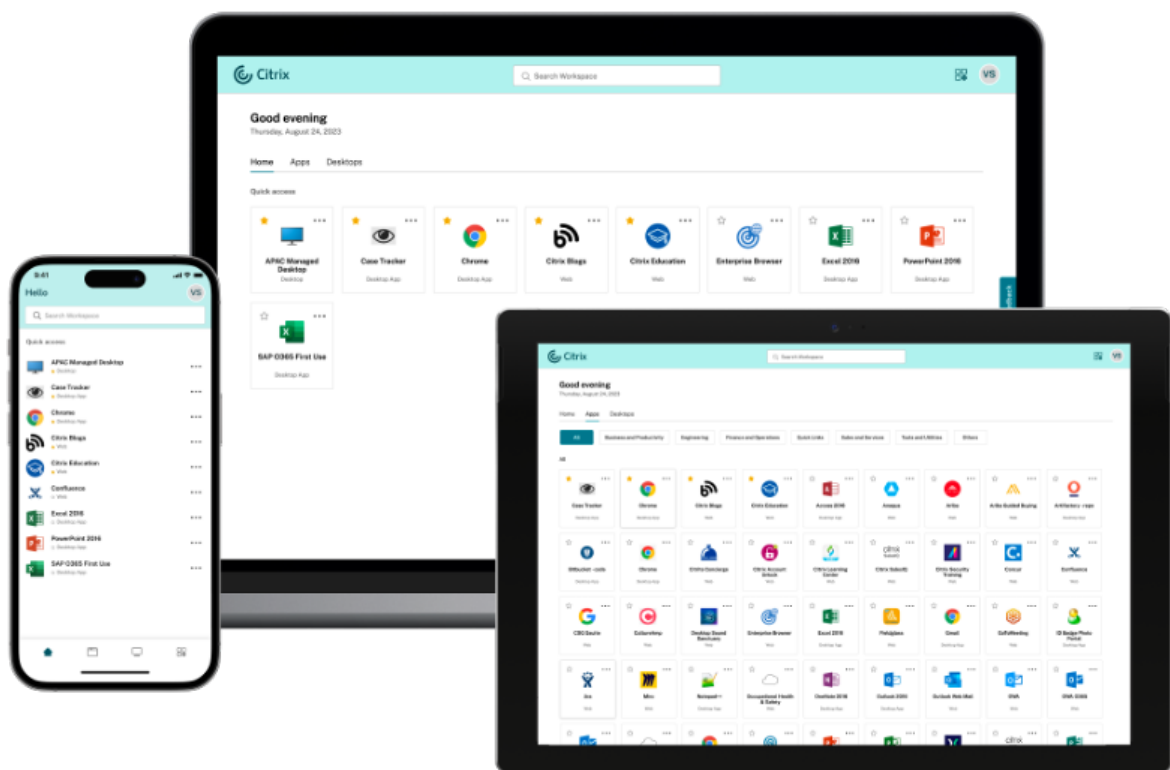


```
Add-STFFeatureState -Name "Citrix.StoreFront.ActivityManager"-IsEnabled $true
```

## Using Activity Manager

Active apps and desktops are grouped as follows on Activity Manager.

- A list of apps and desktops that are active on current device are grouped under **On this device**.
- A list of apps and desktops that are active on other devices are grouped under **Running Remotely**.



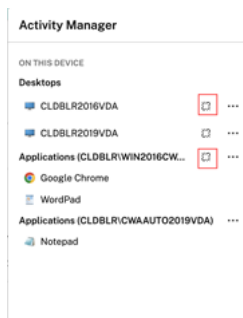
Users can perform the following actions on an app or desktop by clicking the respective ellipsis(...) button.

- **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 sessions are closed, and any unsaved files are lost.
- **Shut Down:** Closes your disconnected desktops.
- **Force shutdown:** Forcefully powers off your desktop in case of a technical issue.
- **Restart:** Shuts down your desktop and start it again.

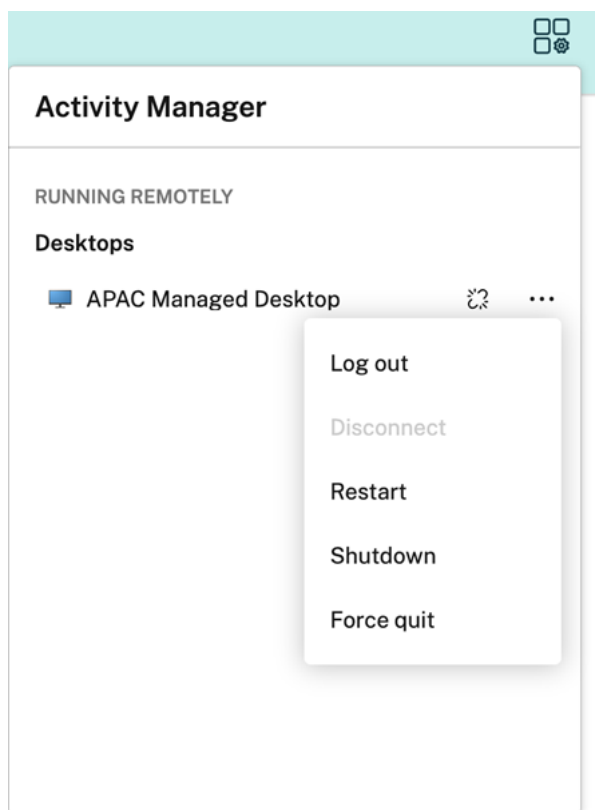
- **Hibernate:** Saves the current state and powers off the machine.
- **Resume:** Starts and restores the state of a machine in hibernation state.

## Disconnected apps and desktops

Activity Manager 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 are displayed 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 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 in case of a technical issue.
- **Restart:** use this option to shutdown and start the disconnected desktop again.

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

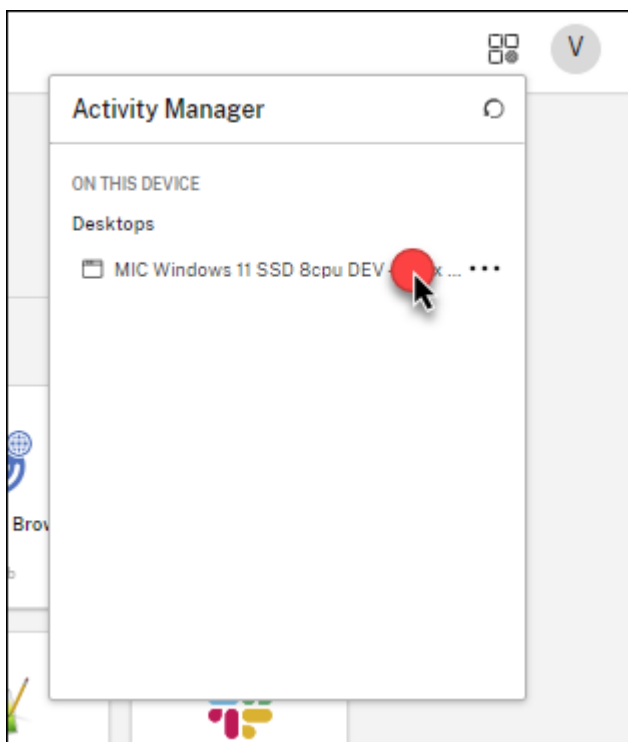
- If the user is signed into Citrix® workspace through a browser, and disconnects a local session, the session is first displayed under **On this device**. However, once the user closes and reopens Activity Manager, the disconnected session is moved under Running Remotely.
- If the user is signed into Citrix Workspace app, and disconnects a local session, the disconnected session disappears from the list. However, once the user closes and reopens Activity Manager again, the disconnected session is moved under **Running Remotely**.

## Reconnect to disconnected apps and desktops

The reconnect feature allows end users to effortlessly reopen their disconnected apps and desktop sessions, ensuring a smooth transition between devices without losing progress. This feature seamlessly restores access to the previous work environment, eliminating the need to search for and re-open apps and desktops.

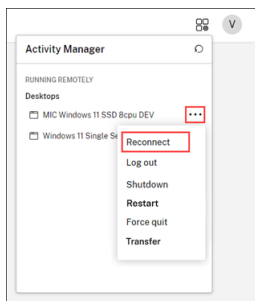
To reconnect to a disconnected app or desktop:

- Open Activity Manager and then click on the resource item.



OR

- Click the ellipsis button (...) and then click **Reconnect**.

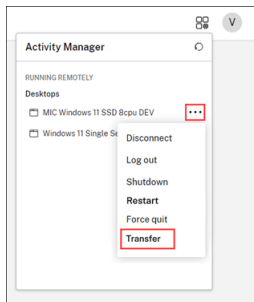


Clicking **Reconnect** reopens the disconnected resource from where you left off.

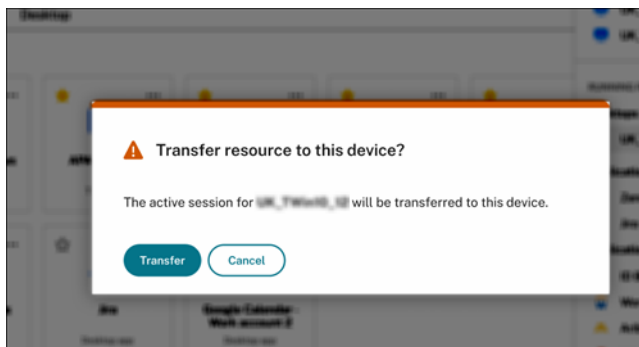
## Transfer your apps and desktops

The transfer feature allows end users to transfer their active apps and desktop from other devices to the current device. To transfer the apps and desktops, follow these steps:

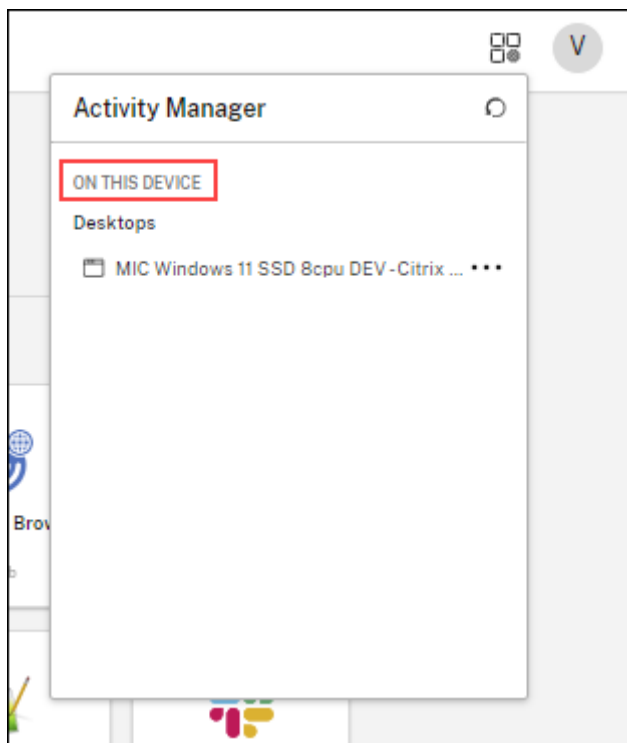
1. Click the ellipsis button (...) and then click **Transfer**.



2. Click **Transfer** on the confirmation dialog box.



Once the resources are transferred to the current device, you can see them listed under the **ON THIS DEVICE** section in the Activity Manager.



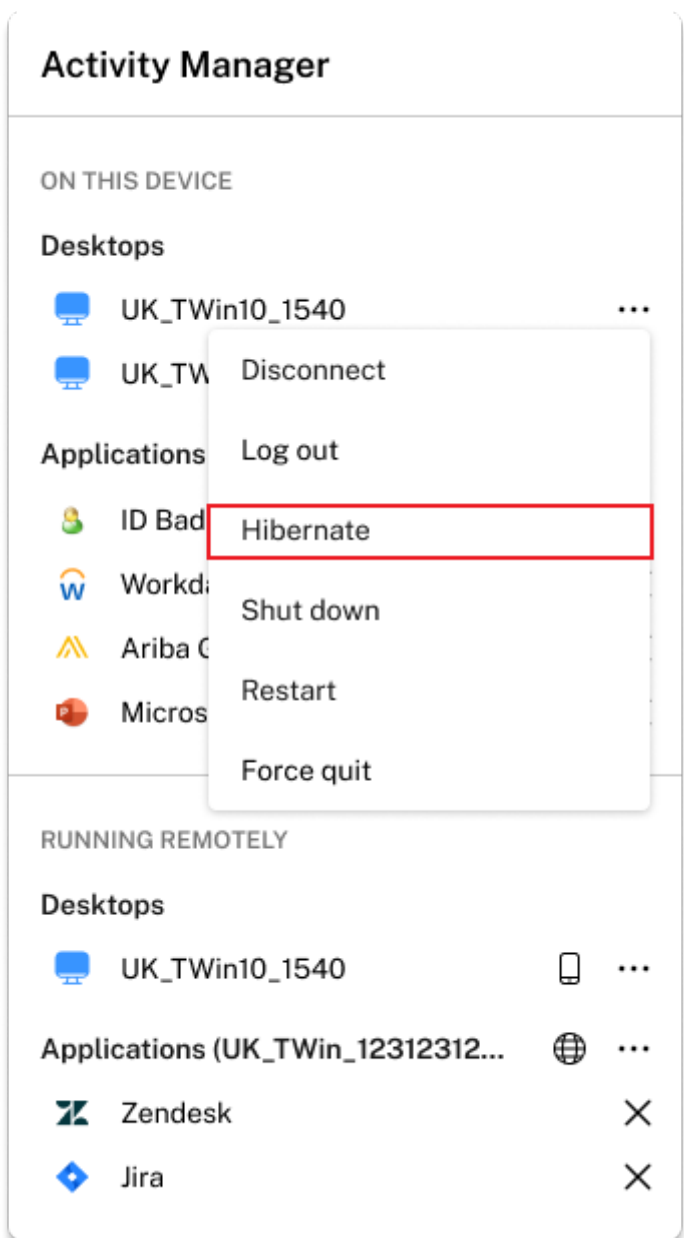
## Hibernate and Resume virtual desktop sessions

The Hibernate and Resume feature allows users to optimize resource utilization by hibernating virtual desktops when not in use and seamlessly resuming them as needed. This not only saves costs and energy but also enhances user workflow with faster session resumption times.

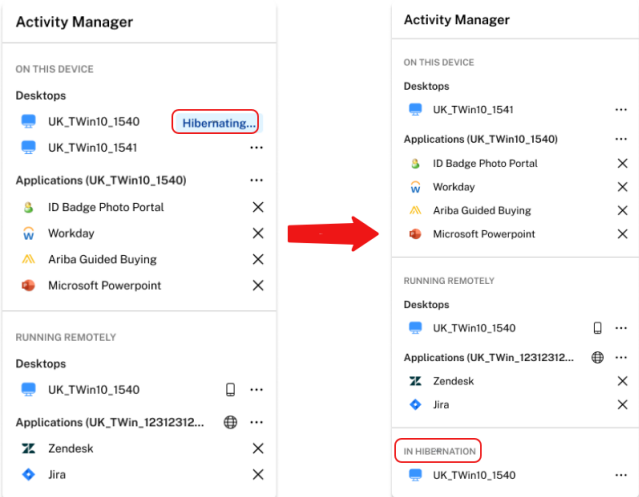
When initiating hibernation, the hypervisor communicates with the guest operating system, triggering a suspend-to-disk action. During this process, the memory (RAM) contents of the virtual desktops are preserved on the OS disk, while the virtual desktop itself is deallocated. Upon subsequent startup, the virtual desktop's RAM contents are restored from the OS disk, ensuring that applications and processes resume seamlessly from their last state.

Hibernation is available for assigned power managed desktops on supported hypervisors. To enable hibernation capability, an administrator needs to follow specific guidelines and enable preview features both in Azure and Citrix DaaS. For more information, see [Create hibernation-capable VMs \(Preview\)](#).

### Hibernate a desktop session:

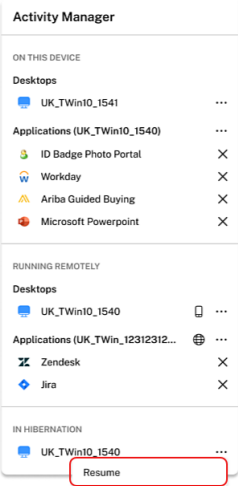


To hibernate a desktop session, users can click the three-dot button (...) and then click the **Hibernate** option. The desktop initiates the hibernation once the users click the **Hibernate** option. Once the desktop is hibernated, the desktop resource moves to the **In Hibernation** section on **Activity Manager**.



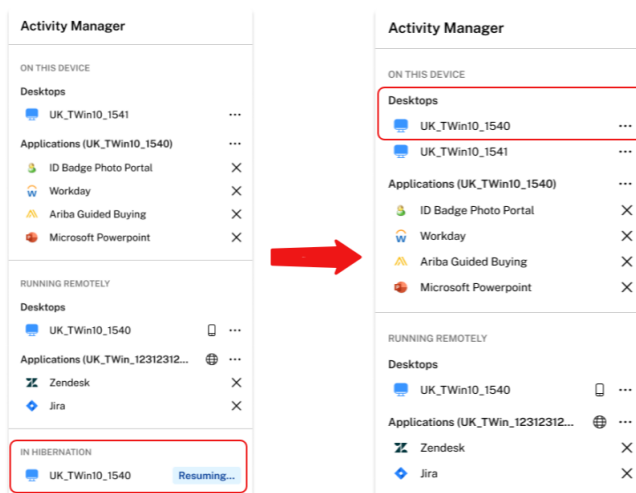
**Resume a hibernated desktop session:**

Hibernated desktop sessions are available under the **In Hibernation** section on **Activity Manager**. To resume the hibernated desktop session, users can click the three-dot button (...), and then click the **Resume** option.



Once users click the **Resume** option, the desktop gets restored.





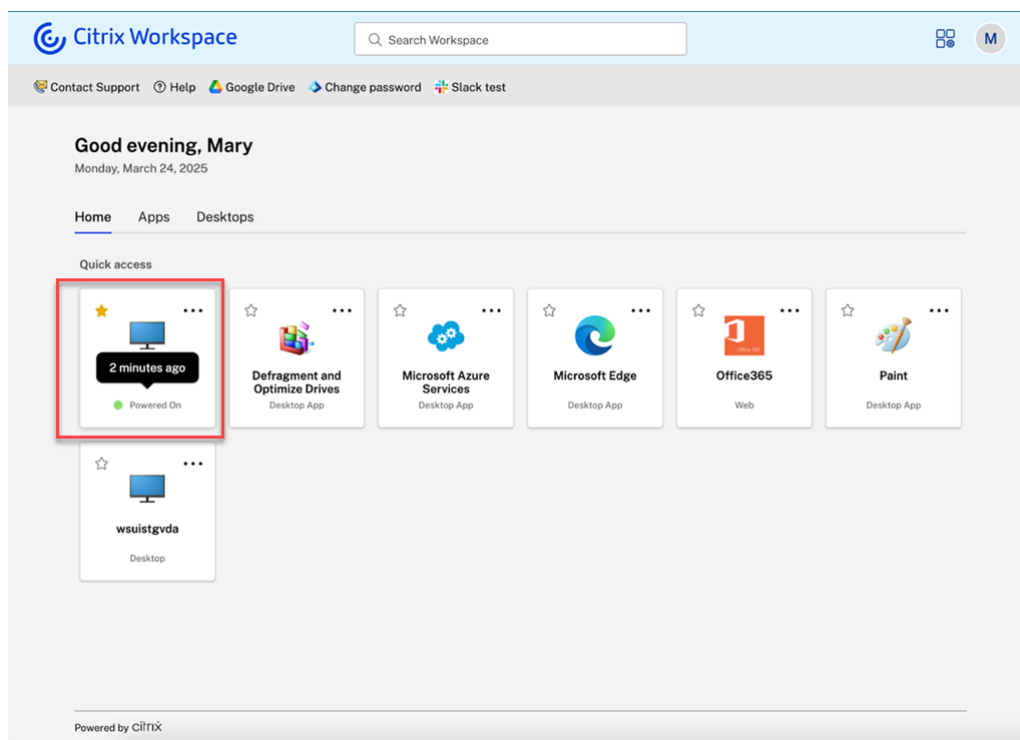
## Assigned desktop power management

October 22, 2025

### Power status

The desktop tile may display the power status if:

- The machine catalog has a single-session OS where the [Desktop Experience](#) is set to **Connect to the same (static) desktop each time the users log in..**
- The machine catalogue must be configured as [power managed](#).
- The machine is published by Citrix DaaS. It is not currently available for desktops published by Citrix Virtual Apps™ and Desktops.
- App protection is not enabled for the desktop.



The following power statuses may be displayed:

- **Powered off:** The machine has been shut down and is not currently running.
- **In hibernation:** The machine is in a hibernation state, where its current session is saved to disk, and the machine is using minimal power.
- **Powering on:** A machine that was in the **Powered Off** or **In hibernation** has been recently started but is not yet ready to use.
- **Powered on:** The desktop is active and running. With dedicated resources, the power state typically remains in a “Powered On” state even if the user disconnects from their session.
- **Shutting down:** The user has initiated a shut down.

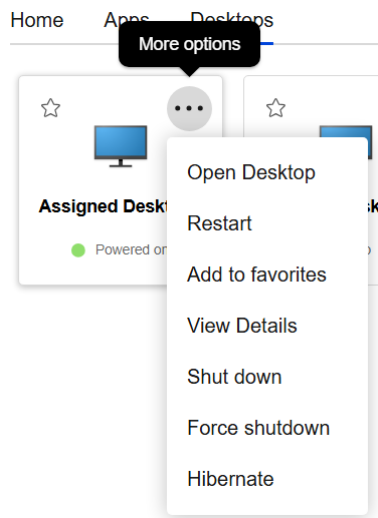
The status is refreshed every two minutes or when the user clicks the ellipsis menu on the desktop tile. When the user hovers over the power state it displays when the last refresh occurred.

### Known issues

- When you launch one of multiple power-managed desktops, Workspace might show inconsistent power statuses for the other desktops until the first desktop completes launching. [WSUI-10870]

## Power actions

The **More** options menu (ellipsis icon) on the tile provides users with access to relevant actions. For power managed assigned machines there are additional actions that depend on the current power state of the resource.



These actions might include:

- **Open App** - Launch or reconnect to the app.
- **Restart** - Initiates a force restart. Only available for assigned power managed desktops.
- **Shut down** - Initiates a graceful shutdown. Only available for assigned power managed desktops.
- **Force shutdown** - Force powers off the machine. Only available for assigned power managed desktops.
- **Hibernate** - Puts the dedicated desktop into a hibernation state. Only available for assigned power managed desktops where hibernation is enabled.
- **Resume** - Wakes the dedicated desktop from a hibernated state. Only available for assigned power managed desktops where hibernation is enabled.

## Secure your StoreFront deployment

October 22, 2025

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

## End user authentication

Normally end users must authenticate either to StoreFront directly, or to a Citrix Gateway in front of StoreFront. For more information on available authentication methods, see [Authentication](#).

## Communication with end-users

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](#).

On your NetScaler Gateway or load balancer virtual server, you can configure which TLS versions are enabled. It is recommended that you disable legacy TLS versions earlier than 1.2.

On StoreFront servers, Windows and IIS determines what TLS versions are allowed for incoming connections. It is recommended that you disable legacy TLS versions older than 1.2. On Windows Server 2025, TLS 1.0 and 1.1 are disabled by default. On Windows Server 2022, you can configure IIS to disable TLS 1.0 and 1.1 for client connections, see [Securing StoreFront with HTTPS](#). On all Windows server versions, you can disable TLS 1.0 and 1.1 using Group Policy or Windows registry settings, see [Microsoft documentation](#).

Older versions of Citrix Receiver cannot connect using TLS 1.2, see [CTX232266](#) for more details.

## Communication with Delivery Controllers

Citrix recommends using the HTTPS protocol to secure data passing between StoreFront and your Citrix Virtual Apps and Desktops delivery controllers. For more information, see [Enable HTTPS on Delivery Controllers](#). To configure StoreFront to use HTTPS, see [Add sites for Citrix Virtual Apps and Desktops](#) and [Add Citrix Gateway appliance](#). In case the certificates are compromised, you can use [Certificate Revocation List \(CRL\) checking](#). StoreFront uses TLS 1.2 or higher to communicate with delivery controllers.

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

## Communication with Cloud Connectors

Citrix recommends using the HTTPS protocol to secure data passing between StoreFront and your Cloud Connectors. See [HTTPS Configuration](#). To configure StoreFront, see [Add sites for Citrix Desktops as a Service](#) and [Add Citrix Gateway appliance](#). In case the certificates are compromised, you can use [Certificate Revocation List \(CRL\) checking](#). StoreFront uses TLS 1.2 or higher to communicate with Cloud Connectors.

It is recommended that you configure DaaS and StoreFront to ensure that only trusted StoreFront servers can communicate with the Cloud Connectors. For more information, see [Manage security keys](#).

## Communication with Federated Authentication Service

For information on communication between StoreFront and Federated Authentication Service (FAS) servers, see [Federated Authentication Service - Security and network configuration](#).

## 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. However, ASP.NET requires the ISAPI Windows feature. 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.

### Default IIS landing page

You can delete files `iisstart.htm`, `welcome.png` from `c:\inetpub\wwwroot`.

### 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](#). In Windows Server 2025 and higher, NTLMv1 has been removed so NTLMv2 is always used.

## **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.

## StoreFront security separation

If you deploy any web applications on your StoreFront server 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 downloads

ICA files contain the information to connect to VDAs and often to single sign onto them without further authentication. Therefore ensure that ICA files are protected. For hybrid launches, depending on configuration, ICA files may be downloaded to the user's device. It is recommended that you disable ICA downloads. For more information, see [Launch preferences](#).

## 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](#).

## App protection

You can use [App Protection](#) to prevent screen capture and screen loggers. For hybrid launches, App Protection is disabled by default. To enable it see [App Protection](#).

## 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, the content security policy blocks scripts from other servers. When writing customizations, place scripts in the website [custom](#) folder. 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. In addition the HTML page includes a <code>meta</code> tag containing a <code>content-security-policy</code> that restricts script sources to mitigate against XSS attacks.                    |
| <code>X-Content-Type-Options</code>  | <code>nosniff</code>                | This avoid MIME type sniffing.                                                                                                                                                                                                                                                                                   |
| <code>X-Frame-Options</code>         | <code>deny</code>                   | 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> |
| <code>X-XSS-Protection</code>        | <code>1; mode=block</code>          | 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                                                                               |
|--------------------------------|-------------------------------------------------------------------------------------------|
| <code>ASP.NET_SessionId</code> | Tracks the user's session including authentication status. Has <code>HttpOnly</code> set. |

| Cookie                       | Description                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <a href="#">CtxsAuthId</a>   | To prevent session fixation attacks, StoreFront in addition tracks whether the user is authenticated using this cookie. It has <a href="#">HttpOnly</a> set.                                                                                                                                                                                                                        |
| <a href="#">CsrfToken</a>    | Used to prevent cross-site request forgery via the standard <a href="#">Cookie-to-header token</a> 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 <a href="#">HttpOnly</a> not set so the client JavaScript can read it. |
| <a href="#">CtxsDeviceId</a> | Identifies the device. Has <a href="#">HttpOnly</a> 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.

If the client connects over HTTPS then it sets the [secure](#) attribute when creating or updating cookies.

## 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.


## Securing StoreFront with HTTPS

October 22, 2025

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 have secure connections between the gateway, load balancer and StoreFront using HTTPS. When using a NetScaler load balancer, for certificate requirements, see the link [Server certificate support matrix on the ADC appliance](#).

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

 StoreFront using HTTP not HTTPS.

## Create or import certificate

- Ensure that the StoreFront [base URL](#) is included in the DNS field as Common Name or Subject Alternative Name (SANs). When using a load balancer in front of your StoreFront servers, it is recommended that you include both the server FQDN and the load balancer FQDN as SANs. This allows you to connect directly to a specific StoreFront server for troubleshooting.
- Sign the certificate using an enterprise root CA for your organization or a public CA.
- If users access StoreFront via a load balancer or gateway, then the certificate only needs to be trusted by the load balancer or gateway. If users connect directly to the StoreFront server then the clients must trust the certificate.

You must create or import a certificate into the **Personal** certificate store within Windows. To view installed certificate:

1. Open **IIS Information Services (IIS) Manager**.
2. In the **Connections** pane, select the server.
3. Open **Server Certificates**.

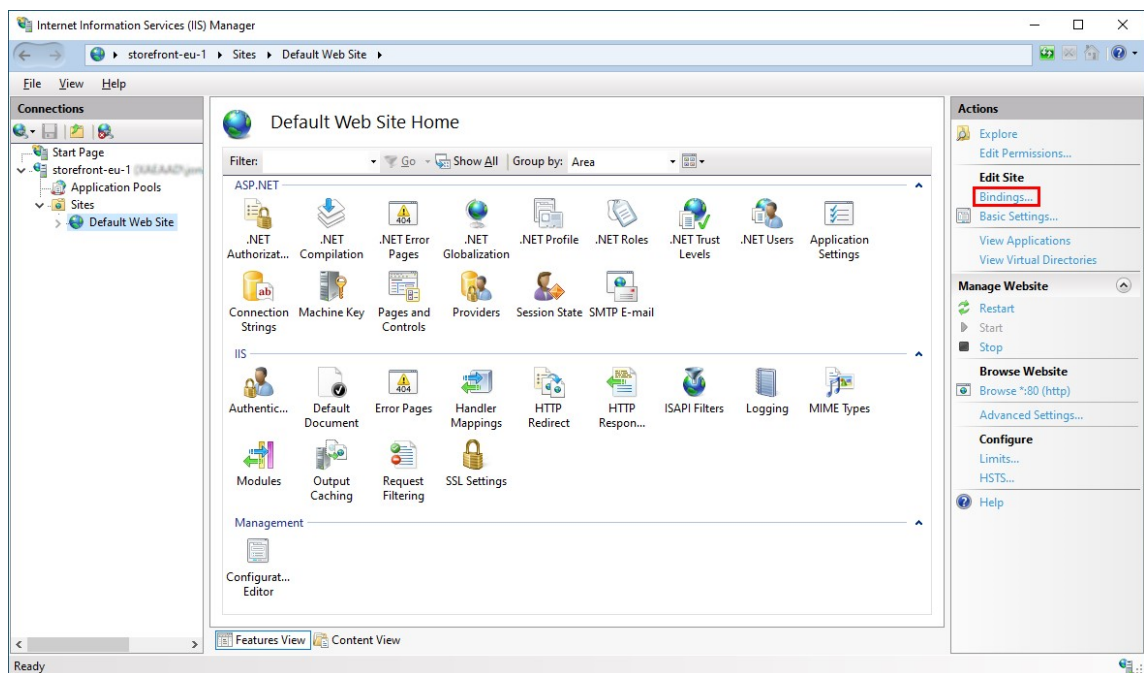
For more information on managing certificates, see [Manage certificates](#).

## Configure IIS for HTTPS

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



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



3. In the bindings window click **Add...**
4. In the **Type** drop down select **https**
5. 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](#).
6. Select the certificate previously imported. Press OK

**Add Site Binding**

Type: **https** IP address: **All Unassigned** Port: **443**

Host name:

☐ Require Server Name Indication

☐ Disable TLS 1.3 over TCP ☐ Disable QUIC

☒ Disable Legacy TLS ☐ Disable HTTP/2

☐ Disable OCSP Stapling

SSL certificate: **self-signed.crt** **Select...** **View...**

**OK** **Cancel**

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

**Site Bindings**

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

**Add...** **Edit...** **Remove** **Browse**

**Close**

8. Update the [base url](#) to use the https protocol.

## 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 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.

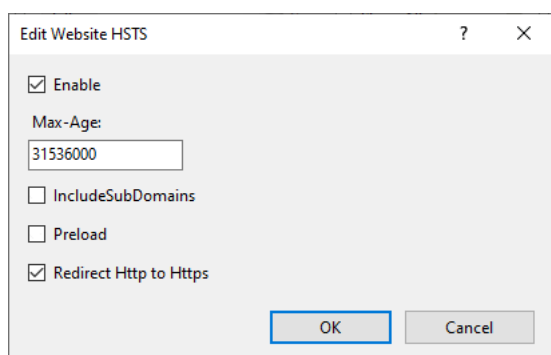
### Note:

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 might not be desired.

There are a number of options for enabling HSTS.

**Option 1 - IIS** On Windows Server 2019 and above you can configure HSTS in IIS.

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. Select **Enable**.
5. Enter a max age, e.g. 31536000 for one year.
6. Optionally select **Redirect HTTP to HTTPS**.
7. Press **OK**



**Option 2 - StoreFront™ management console** For each store website:

1. Select the store and click **Manage websites**.
2. Select the website and click **Configure...**
3. Go to the **Advanced Settings** tab
4. Select **Enable strict transport security**.
5. Update **Strict transport security policy duration** to the required value.
6. Click **OK**.

**Option 3 - NetScaler® load balancer** If you are using a NetScaler load balancer in front of your StoreFront servers then you can configure HSTS on the virtual server. For more information, see [NetScaler documentation](#).

## Certificate Revocation List (CRL) checking

November 5, 2025

### 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

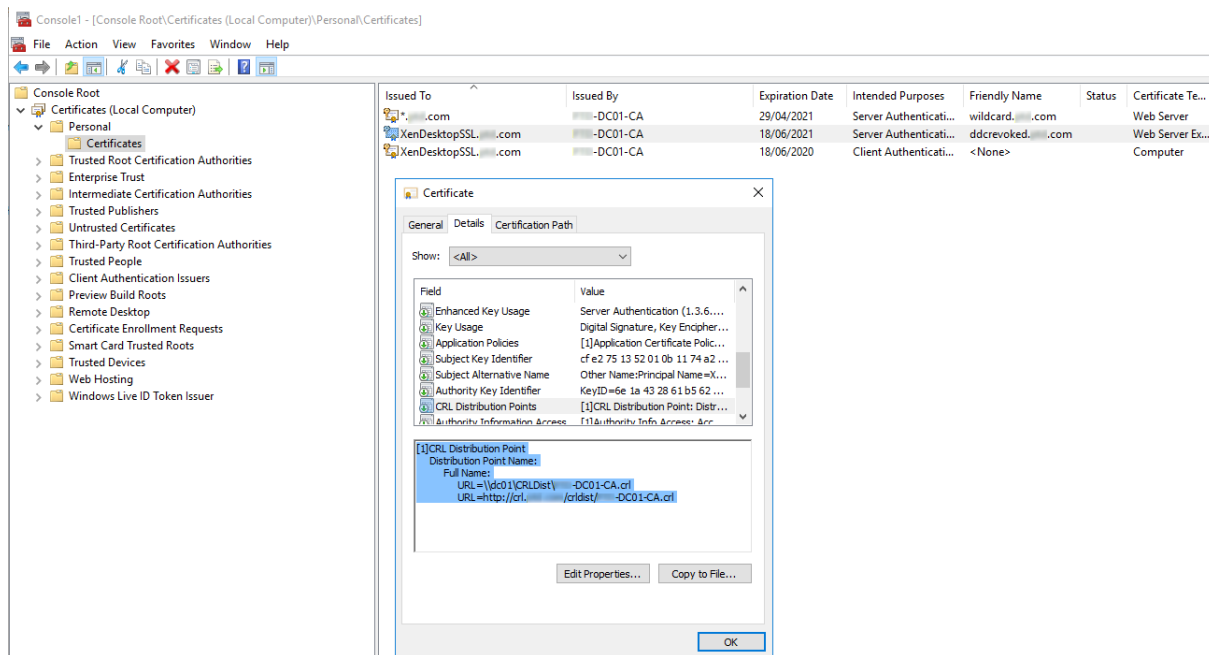
#### Note:

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 CLR are not supported.

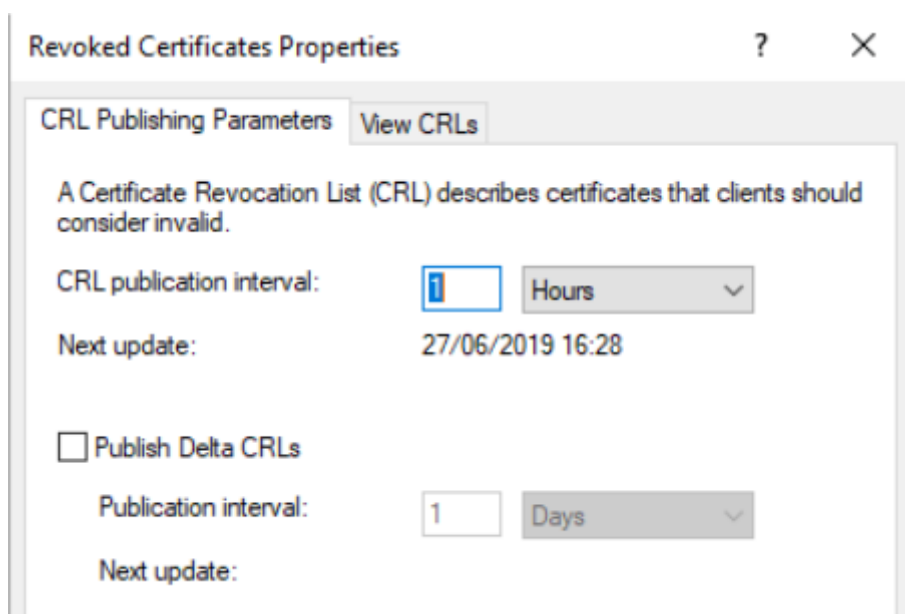
## CRL Distribution Points (CDP) extensions

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.

**View certificate revocation policy**

To view the policy setting using [PowerShell](#), run cmdlet `Get-STFStoreFarmConfiguration` and in the resulting object, view property `CertRevocationPolicy`. For example:

```
1 $store=Get-STFStoreService -VirtualPath '/Citrix/Store'
2 (Get-STFStoreFarmConfiguration -StoreService $store).
 CertRevocationPolicy
```

**Configure certificate revocation policy**

To set the certificate revocation policy for a store using [PowerShell](#), run cmdlet `Set-STFStoreFarmConfiguration` with parameter `-CertRevocationPolicy`.

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. |

For example:

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

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.



## Using locally imported CRLs on the StoreFront server

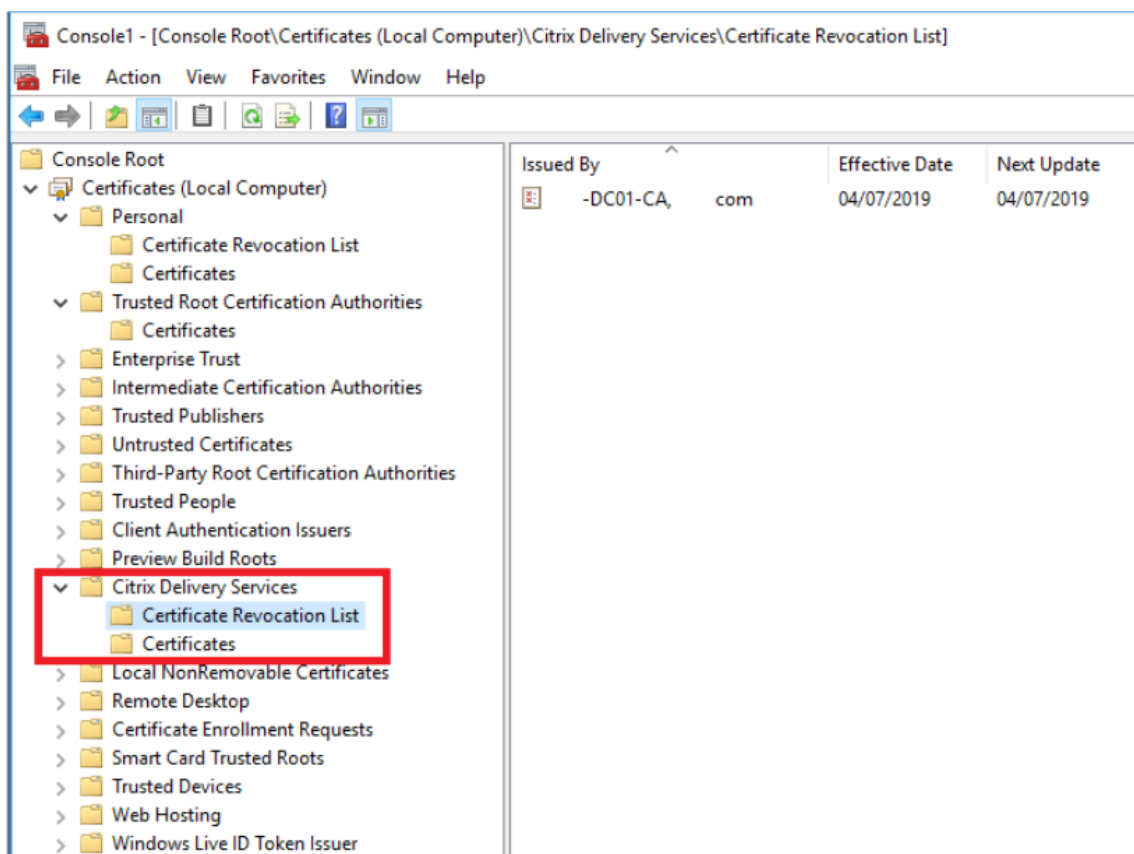
Using locally imported CRLs is supported, but Citrix® does not recommend it because:

- 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 behavior 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"
```

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
```

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. Confirm that you have set the correct certificate revocation mode.

```
1 $AuthObject = Get-STFAuthenticationService -SiteID 1 -VirtualPath
 $AuthVirtualPath
2 $AuthObject.FarmsConfiguration.CertRevocationPolicy
```

## 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.
```

### 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)
```

## ICA® file signing

November 5, 2025

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. To enable ICA file signing, you must install a certificate and configure the store to use that certificate. Signing the ICA file has no effect unless you also configure Citrix Workspace app for Windows to require a certificate, for more information 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. On your StoreFront server, open **Manage computer certificates**.
2. Add your certificate to the **Citrix Delivery Services** certificate store.
3. Open the certificate, go to the **Details** tab and record the thumbprint.
4. Enable signing for a store using the [Set-STFStoreService](#) PowerShell cmdlet:

```
1 $storeService = Get-STFStoreService
2 Set-STFStoreService $storeService -IcaFileSigning $true -
 IcaFileSigningCertificateThumbprint [certificatethumbprint]
```

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.

## Logs and Analytics

October 22, 2025

StoreFront generates a number of log files and telemetry. See the following topics.

| Topic                                | Description                                                                          |
|--------------------------------------|--------------------------------------------------------------------------------------|
| <a href="#">Log files</a>            | StoreFront creates various different log files for diagnostic purposes.              |
| <a href="#">Event logs</a>           | StoreFront writes significant events and errors to the Windows event log.            |
| <a href="#">Performance counters</a> | StoreFront records performance counters that you can view using Performance Monitor. |

| Topic                                          | Description                                                                           |
|------------------------------------------------|---------------------------------------------------------------------------------------|
| <a href="#">Telemetry</a>                      | StoreFront sends information on your configuration to Citrix Cloud.                   |
| <a href="#">Citrix Workspace app analytics</a> | Configure Citrix Workspace app to send data to Citrix Analytics                       |
| <a href="#">Citrix Scout</a>                   | Run Citrix Scout to collect log files and other system information to send to support |

## Log files

November 5, 2025

### 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.

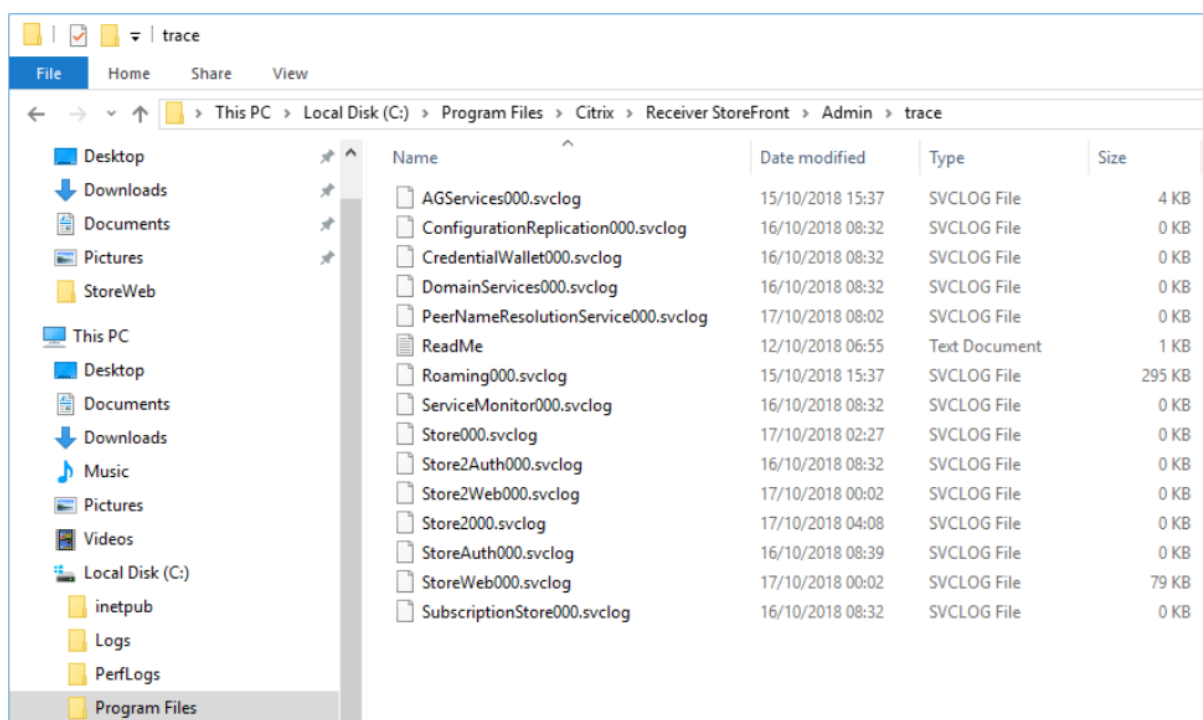
- `Citrix-DeliveryServicesRoleManager-*.log`—Created when StoreFront is installed interactively.
- `Citrix-DeliveryServicesSetupConsole-*.log`—Created when StoreFront is installed silently and when StoreFront is uninstalled, either interactively or silently.
- `CitrixMsi-CitrixStoreFront-x64-*.log`—Created when StoreFront is installed and uninstalled, either interactively or silently.

### 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.

To customize logging using [PowerShell](#), run cmdlet `Set-STFDiagnostics`.

- 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.
- To change the level of detail logged use parameter `-TraceLevel`. Allowed values are `Off`, `Error`, `Warning`, `Info`, or `Verbose`.
- To set the logging parameters for all services, use parameter `-All`. You can customize logging for an individual service using `-Service [Service name]`

## Verbose logging

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
```

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
```

## IIS log files

By default IIS writes a log of each request to %SystemDrive%\inetpub\logs\LogFiles. For more information, see [Microsoft documentation](#).

## Event Log

October 22, 2025

StoreFront supports Windows event logging for the authentication service, stores, and websites. 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 websites.

## 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 store-name 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 the 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.

## Performance counters

October 22, 2025

StoreFront writes a number of performance counters. To view the counter values:

1. From the **Start** menu, open **Performance Monitor**. This can be found under the **Windows Administrative Tools** folder.
2. In the tree view, select **Monitoring Tools > Performance Monitor**.
3. Select the + button (**Add**) on the toolbar.
4. Choose the counters you wish to view. They can be found under categories starting **Citrix®**.

## Telemetry

October 22, 2025

StoreFront sends telemetry on your Storefront Configuration and log in events to Citrix Cloud. This is sent via either a local on-prem DDC and license server or via Cloud connectors to DaaS. For more information, see [Citrix Virtual Apps and Desktops documentation](#).

## StoreFront™ configuration

### Usage

### Headers

| Field   | Description                                               | Example                              |
|---------|-----------------------------------------------------------|--------------------------------------|
| ver     | The version of the license usage event                    | 1.0                                  |
| id      | The unique identifier of the usage event                  | d4ce7919-5d80-44de-a8fa-102923fe0ead |
| type    | The event type used by CAS to identify cloud usage events | Configuration                        |
| st      | The timestamp when the event is generated in Broker       | 2011-08-12T20:17:46.384Z             |
| prod    | The originating product and deployment of the usage event | OnPrem.StoreFront                    |
| prodVer | The StoreFront version                                    | 3.30.0.0                             |

### Payload

| Field             | Description                                                                                               | Example                                      |
|-------------------|-----------------------------------------------------------------------------------------------------------|----------------------------------------------|
| serverName        | The hostname of the service StoreFront is running on                                                      | storefront-01.storefront.local               |
| deploymentId      | The unique identifier of the deployment of StoreFront                                                     | f47ac10b-58cc-4372-a567-0e02b2c3d479         |
| installedWithCVAD | Indicates whether StoreFront was installed alongside CVAD                                                 | false                                        |
| cpuCores          | The total number of CPU cores                                                                             | 4                                            |
| cpuModel          | The CPU running StoreFront                                                                                | 12th Gen Intel(R) Core(TM) i7-1255U 1.70 GHz |
| ramGb             | The total amount of RAM in GB                                                                             | 16                                           |
| numServersInGroup | The number of servers in the server group                                                                 | 3                                            |
| stores            | The StoreFront Store configuration JSON blob. An array of Store objects. <b>Some values are scrambled</b> | Example                                      |
| rfWebSites        | The StoreFront website configuration JSON blob. An array of RFWeb Config objects                          | Example                                      |

| Field          | Description                                                                            | Example |
|----------------|----------------------------------------------------------------------------------------|---------|
| gateways       | The gateway configuration objects as JSON blob. An array of gateway objects            | Example |
| authServices   | The Auth service configuration objects as JSON blob. An array of auth services objects | Example |
| IsPiiScrambled |                                                                                        | true    |

**Example of field stores**

```

1 [{
2
3 "BaseUrl": "baseUrl",
4 "StorePath": "/",
5 "EnabledFeatures": 21 bit bitmap,
6 "ResourceTypeFilteringEnabled": "disabled|Citrix.MPS.
7 Application;Citrix.MPS.Desktop",
8 "DefaultRfWebSite": "/Citrix/StoreWeb",
9 "GatewaysUsed": [
10 "gatewayId"
11],
12 "VdaLogonDataProvider": "",
13 "ResourceFeeds": [
14 {
15 "FeedName": "<resourceFeedName>|scrambled",
16 "Type": "CVAD",
17 "LoadBalancingEnabled": true,
18 }
19],
20 "AdvancedAggregation": {
21 "Enabled": true,
22 "GroupingCount": 1,
23 "ControllersPushIdenticalResources": true,
24 "LoadBalanced": true,
25 "AnyPrimaryFarms": true,
26 "AnyBackupFarms": true,
27 }
28 }
29]
30
31 }
32]

```

If no Stores are found, it is an empty array [].

**Example of field rfWebSites**

```

1 [{
2
3 "SiteId": "siteId",
4 "BaseUrl": "baseUrl",
5 "StorePath": "storePath",
6 "UiExperienced": 0,
7 "EnabledFeatures": 9 bit,
8 "AuthMethodsEnabled": [
9 "ad"
10],
11 "CanUsersDownloadApps": {
12
13 "Enabled": true,
14 "Windows": "exe",
15 "MacOS": "dmg"
16 }
17 ,
18 "WorkspaceControl": {
19
20 "Enabled": true,
21 "LogoffAction": 0,
22 "AutoReconnectAtLogon": true,
23 "ShowReconnectButton": true,
24 "ShowDisconnectButton": true
25 }
26 ,
27 "MultiClickTimeout": 1,
28 "UiViews": [
29 "apps",
30 "desktops"
31],
32 "DefaultTab": 0,
33 }
34]

```

If no rfWebSites are found, it is an empty array [].

#### Example of field gateways

```

1 [{
2
3 "GatewayId": "gatewayId",
4 "IsCloudGateway": true,
5 "LoadBalancingSTAEnabled": true,
6 "SessionReliabilityEnabled": true,
7 "RequestTicketsFromTwoSTA": true,
8 "Version": "1234",
9 "LogonType": "domain",
10 "SmartCardFallbackEnabled": true
11 }
12]

```

If no gateways are found, it is an empty array [].

Example of field authServices

```
1 [{
2
3 "SiteId": "SiteId",
4 "Store": "StoreAuth",
5 "AuthMethodsEnabled": [
6 "ad"
7],
8 "PasswordChangeWhenExpired": 0,
9 "PasswordRemindersForm": 1,
10 "DelegateCredentialValidationToCitrix": true,
11 "ValidatePasswordsOnDeliveryControllers": true
12 }
13]
```

If no auth services found, it is an empty array [].

Storefront Login

Usage

Headers

| Field   | Description                                               | Example                              |
|---------|-----------------------------------------------------------|--------------------------------------|
| ver     | The version of the license usage event                    | 1.0                                  |
| id      | The unique identifier of the usage event                  | d4ce7919-5d80-44de-a8fa-102923fe0ead |
| type    | The event type used by CAS to identify cloud usage events | Login                                |
| st      | The timestamp when the event is generated in Broker       | 2011-08-12T20:17:46.384Z             |
| prod    | The originating product and deployment of the usage event | OnPrem.StoreFront                    |
| prodVer | The StoreFront version                                    | 3.30.0.0                             |

Payload

| Field | Description                                                       | Example                                                                                                          |
|-------|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------|
| user  | The user that initiated the launch. <b>The value is scrambled</b> | fullName: C648FE671A44B3F7<br><b>(always scrambled)</b><br>samName:C758LH671A44B3F7<br><b>(always scrambled)</b> |

| Field            | Description                                                                        | Example                                                                         |
|------------------|------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| serverName       | The hostname of the service StoreFront is running on                               | storefront-01.storefront.local                                                  |
| loginMethodRfWeb | Not used                                                                           |                                                                                 |
| loginMethodAuth  | The method the user used to login to StoreFront                                    | 0                                                                               |
| gatewayURL       | The URL of the Netscaler Gateway used during login                                 | netScaler-gateway.com                                                           |
| enabledFeatures  | A bitmask of enabled features                                                      | 12                                                                              |
| userAgent        | The UserAgent of the client used to login                                          | CitrixReceiver/22.11.0.19<br>Linux/5.17.15 X1Class<br>CWACapable CWA/22.11.0.19 |
| baseUrl          | The base url of the store that the user logged in to                               | storefront-dev.storefront.dev                                                   |
| storePath        | The store path that the user logged in to                                          | /Citrix/StoreWeb                                                                |
| apiUsed          | Indicates if the client is using the Store API, Web API, or PNAgent API            | 0                                                                               |
| deviceId         | The name of the device used to log into StoreFront. <b>The values is scrambled</b> | john-doe                                                                        |
| transactionId    | Identifier used to group related events                                            | 773aba9e-5b91-4ef9-8782-c4afb75698e7                                            |

## Citrix Workspace app analytics

October 22, 2025

If you have Citrix Analytics, you can configure StoreFront so that Citrix Workspace app sends 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 [Onboard 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:**

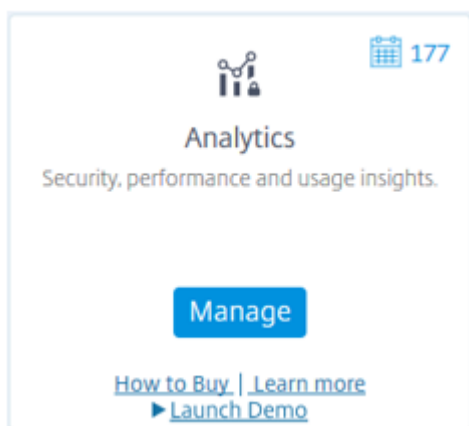
Your StoreFront deployment must be able to contact Citrix API Services. See [Analytics network requirements](#).

## 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 }
```

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
```

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

```

CustomerId :
EnablementService : https://
CwsServiceKey :

EnablementServiceStatus : https://
InstanceId :
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

```

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
```

## 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:

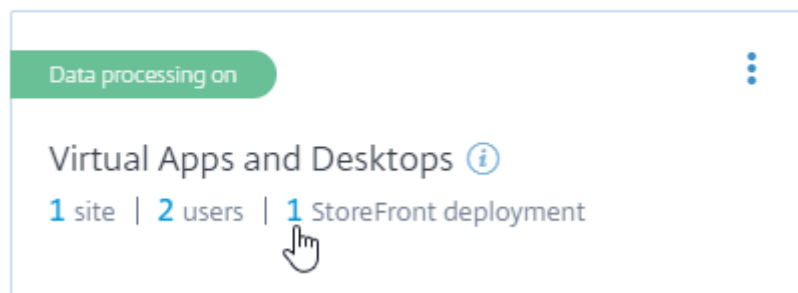
```
Publish-STFServerGroupConfiguration
```

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
```

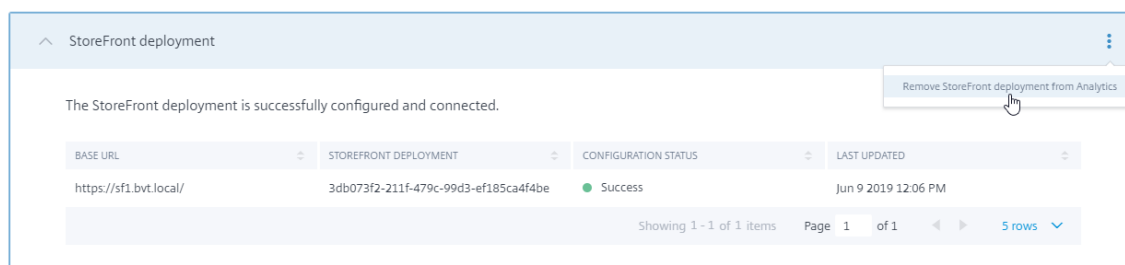
5. Log on to monitor (<https://citrix.cloud.com/>) using an administrator account.
6. Select a monitor customer.
7. Open the Citrix Analytics service management console by clicking **Manage**.
8. In the Citrix Analytics service management console, select **Settings > Data Sources**.
9. In the Virtual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

```

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

```

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>

```

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>

```

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>
```

4. Import the Citrix Analytics data as described in [Import Citrix Analytics data into your StoreFront deployment](#).

## Deprecation notices

September 7, 2025

The announcements in this article are intended to give you advanced notice of platforms, Citrix products, and features that are being phased out so that you can make timely business decisions. Citrix monitors customer use and feedback to determine when they are withdrawn. Announcements can change in subsequent releases and might not include every deprecated feature or functionality. For details about product lifecycle support, see the [Product Lifecycle Support Policy](#) article. For information about the Long Term Service Release (LTSR) servicing option, see <https://support.citrix.com/article/CTX205549>.

### Deprecations

Deprecated items are not removed immediately. Citrix® continues to support them, but they will be removed in a future release.

| Item                                     | Deprecation announced in version | Alternative                                                                                     |
|------------------------------------------|----------------------------------|-------------------------------------------------------------------------------------------------|
| XenApp® Services (also known as PNAgent) | 2308                             | Within workspace app, connect to stores using the store URL rather than the XenApp Services URL |

## Removals

Removed items are either removed, or are no longer supported.

| Item                                                                           | Deprecation announced in version | Removed in version | Alternative                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------------|----------------------------------|--------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Citrix Customer Experience Improvement Program                                 | 2507                             | 2507               |                                                                                                                                                                                                                                    |
| Windows Server 2016                                                            | 2402                             | 2407               | Install StoreFront on Windows server 2019 or higher                                                                                                                                                                                |
| Support for Microsoft .NET Framework versions earlier than 4.8.0.              | 2407                             | 2407               | Upgrade to .NET Framework version 4.8.0 or later. (The installer automatically installs .NET Framework 4.8.0 if it is not already installed.)                                                                                      |
| Internet Explorer 11 for connecting to resources using Workspace app for HTML5 | 2308                             | 2308               | Either use a supported web browser or install Citrix Workspace™ app for Windows. It is still possible to use Internet Explorer 11 to access your store but to launch resources Citrix Workspace app for Windows must be installed. |

| Item                                                                                                                          | Deprecation<br>announced in version |  | Removed in version | Alternative                                                                                                                                   |
|-------------------------------------------------------------------------------------------------------------------------------|-------------------------------------|--|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| XenApp 6.5 sites.                                                                                                             | 2308                                |  | 2308               | Upgrade to the latest Citrix Virtual Apps and Desktops.                                                                                       |
| Support for Self-service password reset (SSPR)                                                                                | 2203                                |  | 2203               | -                                                                                                                                             |
| Support for TLS 1.0, and TLS 1.1 protocols between Citrix Virtual Apps and Desktops and Citrix Workspace app.                 | 3.14                                |  | 2203               | Upgrade Citrix Receivers to a Citrix Workspace app that supports TLS 1.2                                                                      |
| Installing StoreFront on Windows Server 2012 R2                                                                               | 2203                                |  | 2203               | Install StoreFront on a supported operating system.                                                                                           |
| Support for Microsoft .NET Framework versions earlier than 4.7.2.                                                             | 2203                                |  | 2203               | Upgrade to .NET Framework version 4.7.2 or later. (The installer automatically installs .NET Framework 4.7.2 if it is not already installed.) |
| Removal of Delivery Controller options for the following end-of-life products: VDI-in-a-Box, and XenMobile (9.0 and earlier). | 1903                                |  | 1903               | —                                                                                                                                             |
| Internet Explorer 9 and 10                                                                                                    | 1903                                |  | 1903               | —                                                                                                                                             |
| Support for users to access desktops on Desktop Appliance sites                                                               | 1811                                |  | 1912               | Use <a href="#">Desktop Lock</a> for non-domain-joined use cases.                                                                             |

| Item                                                                                               | Deprecation          |                    | Alternative                                                                         |
|----------------------------------------------------------------------------------------------------|----------------------|--------------------|-------------------------------------------------------------------------------------|
|                                                                                                    | announced in version | Removed in version |                                                                                     |
| Citrix classic experience (“green bubbles” user interface)                                         | 3.12                 | 1903               | Use the Unified UI                                                                  |
| Installing StoreFront on Windows Server 2012 and Windows Server 2008 R2 (including Service Packs). | 3.12 LTSR            | 3.15               | Install components on a supported operating system.                                 |
| Citrix Online Integration (Goto product) integration                                               | 3.11                 | 3.12               | —                                                                                   |
| In-place upgrades from StoreFront 2.0, 2.1, 2.5, and 2.5.2                                         | 3.9                  | 1818               | Upgrade from one of these versions to 3.12 and then to a more recent latest version |
| Installing StoreFront on 32-bit (x86) machines.                                                    | 3.8                  | 3.13               | Install on a supported x64 operating system.                                        |

For information about deprecations in Citrix Workspace app for HTML5 see the [Deprecation](#) page.

## Third Party Notices

October 22, 2025

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).

### **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.

### **Microsoft.IdentityModel.JsonWebTokens**

Copyright © Microsoft Corporation. Licensed under the MIT license.

### **Microsoft.IdentityModel.Logging**

Copyright © Microsoft Corporation. Licensed under the MIT license.

### **Microsoft.IdentityModel.Tokens**

Copyright © Microsoft Corporation. Licensed under the MIT license.

### **ManagedEsent Release 1.9.4**

Copyright © Microsoft Corporation.

Licensed under the Microsoft Public License (MS-PL).

### **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**

jScrollPane - v2.0.0beta11 - 2011-07-04

Copyright (c) 2010 Kelvin Luck

Dual licensed under the MIT and GPL licenses.

### **jquery.contextmenu.js**

jQuery Plugin for Context Menus

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](mailto: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 Copyright (c) 2006-2014 Microsoft

MS-PL license

### **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).

For more features, controls, and fast professional support, pick up the Plus Edition at [http://xceed.com/wpf\\_toolkit](http://xceed.com/wpf_toolkit)

Stay informed: follow @datagrid on Twitter.

### **WiX Toolset**

Copyright (c) .NET Foundation and contributors. Microsoft Reciprocal License (Ms-RL)

### **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 v3.7.1**

(c) OpenJS Foundation and other contributors

Released under the MIT license

<https://jquery.org/license>

### **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.

### **Microsoft.WebApi.Collection**

The MIT License (MIT)

Copyright (c) Microsoft Corporation

### **Polly**

Copyright (c) 2015-2024, App vNext

Licensed under the BSD 3-Clause License

### **Polly.Core**

Copyright (c) 2015-2024, App vNext

Licensed under the BSD 3-Clause License

### **Microsoft.Security.Crypto**

The MIT License (MIT)

Copyright (c) Microsoft Corporation

### **Microsoft .NET 8**

The MIT License (MIT)

Copyright (c) .NET Foundation and Contributors

## 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.
```

### 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 "Legal Entity" shall mean the union of the acting entity and all  
17 other entities that control, are controlled by, or are under common  
18 control with that entity. For the purposes of **this** definition,  
19 "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  
of  
the copyright owner. For the purposes of **this** definition, "submitted  
"  
means any form of electronic, verbal, or written communication sent  
to the Licensor or its representatives, including but not limited to  
communication on electronic mailing lists, source code control  
systems,  
and issue tracking systems that are managed by, or on behalf of, the  
Licensor **for** the purpose of discussing and improving the Work, but

60 excluding communication that is conspicuously marked or otherwise  
61 designated in writing by the copyright owner as "Not a Contribution."  
62  
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  
145        7. Disclaimer of Warranty. Unless required by applicable law or  
146        agreed to in writing, Licensor provides the Work (and each  
147        Contributor provides its Contributions) on an "**AS IS**" BASIS,  
148        WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or  
149        implied, including, without limitation, any warranties or conditions  
150        of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A  
151        PARTICULAR PURPOSE. You are solely responsible **for** determining the  
152        appropriateness of using or redistributing the Work and assume any  
153        risks associated with Your exercise of permissions under **this**  
154        License.  
155  
156        8. Limitation of Liability. In no event and under no legal theory,  
157        whether in tort (including negligence), contract, or otherwise,  
158        unless required by applicable law (such as deliberate and grossly  
159        negligent acts) or agreed to in writing, shall any Contributor be  
160        liable to You **for** damages, including any direct, indirect, special,  
161        incidental, or consequential damages of any character arising as a  
162        result of **this** License or out of the use or inability to use the  
163        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

## Microsoft Public License (MS-PL)

1 This license governs use of the accompanying software. If you use the  
software, you accept **this** license. If you **do** not accept the license,  
**do** not use the software.  
2  
3 1. Definitions  
4 The terms “reproduce,” “reproduction,” “derivative works,” and  
“distribution” have the  
5 same meaning here as under U.S. copyright law.  
6  
7 A “contribution” is the original software, or any additions or  
changes to the software.  
8  
9 A “contributor” is any person that distributes its contribution  
under **this** license.  
10  
11 “Licensed patents” are a contributor’s patent claims that read  
directly on its contribution.  
12  
13 2. Grant of Rights  
14  
15 (A) Copyright Grant- Subject to the terms of **this** license, including  
the license conditions and limitations in section 3, each  
contributor grants you a non-exclusive, worldwide, royalty-free  
copyright license to reproduce its contribution, prepare  
derivative works of its contribution, and distribute its  
contribution or any derivative works that you create.  
16  
17 (B) Patent Grant- Subject to the terms of **this** license, including  
the license conditions and limitations in section 3, each  
contributor grants you a non-exclusive, worldwide, royalty-free  
license under its licensed patents to make, have made, use, sell,  
offer **for** sale, **import**, and/or otherwise dispose of its

contribution in the software or derivative works of the contribution in the software.

1 3. Conditions and Limitations

2

3 (A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

4

5 (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.

6

7 (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.

8

9 (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.

10

11 (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.

### BSD 3-Clause License

1 Redistribution and use in source and binary forms, with or without  
2 modification, are permitted provided that the following conditions are met:

3

4 1. Redistributions of source code must retain the above copyright notice, **this**  
5 list of conditions and the following disclaimer.

6

7 2. Redistributions in binary form must reproduce the above copyright notice,  
8 **this** list of conditions and the following disclaimer in the documentation  
9 and/or other materials provided with the distribution.

10

11 3. Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from  
12 **this** software without specific prior written permission.

13  
14

15 THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS  
IS"  
16 AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO,  
THE  
17 IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR  
PURPOSE ARE  
18 DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE  
LIABLE  
19 FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR  
CONSEQUENTIAL  
20 DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS  
OR  
21 SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)  
HOWEVER  
22 CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT  
LIABILITY,  
23 OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF  
THE USE  
24 OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

### Microsoft Reciprocal License (Ms-RL)

1 This license governs use of the accompanying software. If you use the  
software, you accept **this** license. If you **do** not accept the license,  
**do** not use the software.  
2  
3 1. Definitions  
4 The terms "reproduce," "reproduction," "derivative works," and "  
distribution" have the same meaning here as under U.S. copyright law  
.  
5 A "contribution" is the original software, or any additions or changes  
to the software.  
6  
7 A "contributor" is any person that distributes its contribution under  
**this** license.  
8  
9 "Licensed patents" are a contributor's patent claims that read directly  
on its contribution.  
10  
11 2. Grant of Rights  
12 (A) Copyright Grant- Subject to the terms of this license, including  
the license conditions and limitations in section 3, each  
contributor grants you a non-exclusive, worldwide, royalty-free  
copyright license to reproduce its contribution, prepare derivative  
works of its contribution, and distribute its contribution or any  
derivative works that you create.  
13 (B) Patent Grant- Subject to the terms of this license, including the  
license conditions and limitations in section 3, each contributor  
grants you a non-exclusive, worldwide, royalty-free license under  
its licensed patents to make, have made, use, sell, offer for sale,  
import, and/or otherwise dispose of its contribution in the software



or derivative works of the contribution in the software.

14 3. Conditions and Limitations

- 15 (A) Reciprocal Grants- For any file you distribute that contains code from the software (in source code or binary format), you must provide recipients the source code to that file along with a copy of this license, which license will govern that file. You may license other files that are entirely your own work and do not contain code from the software under any terms you choose.
- 16 (B) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.
- 17 (C) 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.
- 18 (D) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.
- 19 (E) 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.
- 20 (F) 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.



© 2025 Cloud Software Group, Inc. All rights reserved. This document is subject to U.S. and international copyright laws and treaties. No part of this document may be reproduced in any form without the written authorization of Cloud Software Group, Inc. This and other products of Cloud Software Group may be covered by registered patents. For details, please refer to the Virtual Patent Marking document located at <https://www.cloud.com/legal>. Citrix, the Citrix logo, NetScaler, and the NetScaler logo and other marks appearing herein are either registered trademarks or trademarks of Cloud Software Group, Inc. and/or its subsidiaries in the United States and/or other countries. Other marks are the property of their respective owner(s) and are mentioned for identification purposes only. Please refer to Cloud SG's Trademark Guidelines and Third Party Trademark Notices (<https://www.cloud.com/legal>) for more information.