Citrix® StoreFront 2607 LTSR

Copyright © 1997–2026. Citrix Systems, Inc. All Rights Reserved.

Contents

StoreFront 2607 LTSR Overview 25
- Get started 25
- What's new 25
- Earlier releases 25
- Support lifecycle 26

What's new in 2607 (initial release) 27
- System requirements 27
- Detailed desktop tile 27
- Admin-Configurable Granular Power Actions for Persistent Desktops 28
- Launch failure troubleshooting 28
- “Ready” power state 29
- New options in three dots menu 29
- Configuration FAS in the StoreFront management console 29
- Support for users with Entra ID identities 30
- Entra ID single sign-on to VDAs 31
- Launch timing telemetry included in ICA file 31
- Support for Windows Server Core 31
- Log improvements 32
- Command line install location change in behavior 32
- Citrix Workspace app for HTML5 HDX Client 32
- Fixed issues 32
- Known issues 34

Get started 35
- Prerequisites 35
- Deploy StoreFront 35
- Optimize your deployment 35

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Plan your StoreFront deployment 36
Active Directory 36
StoreFront server groups 36
Citrix Gateway for remote access 37
Global Server Load Balancer 37
User access 39
System requirements 39
StoreFront server requirements 39
Software 39
Hardware 41
Network 42
Active directory 42
Storing subscription data using Microsoft SQL Server 43
Infrastructure requirements 43
Citrix Virtual Apps and Desktops™ 43
Citrix Gateway 43
User device requirements 44
Citrix Workspace app 44
Web browsers 44
Legacy devices 45
Smart card requirements 45
Using Citrix Workspace app with smart cards 45
Citrix Analytics service requirements 46
Configure resources 46
Keywords 47
Smart Access Tags 48
Install StoreFront 48
Before installing 48

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Install StoreFront 49

To install StoreFront at a command prompt 50

.Net Framework 4.8 reboot step with Windows Server 2019 51

Installing as part of Citrix Virtual Apps and Desktops™ 52

Installation logs 52

Configure StoreFront 52

Create a new deployment 53

Create a new deployment using PowerShell 54

Multiple Internet Information Services (IIS) websites 54

End user access 55

Citrix Workspace™ app 55

Beacons 56

Require use of Citrix Workspace app 56

Add Store to Citrix Workspace App 56

Global App Config Service 57

Web browser 58

Requirements for opening resources in your browser 59

Hybrid Launch 59

Citrix web extensions 59

Citrix Workspace launcher 60

Internet Explorer 62

ICA file downloads 62

Resource shortcuts 62

XenApp Services URLs 63

Important considerations 63

Manage Deployment 65

StoreFront Management console 66

StoreFront PowerShell modules 67

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Get started 68
Virtual Path 68
Site ID 69
Example scripts 69
Create a simple deployment 69
Example: Create a remote access deployment 75
Example: Create a remote access deployment with optimal launch Gateway 79
Configure the base URL 82
Configure server groups 83
View server group 83
Add a server to a server group 84
Remove servers from a server group 85
Propagate local changes to a server group 85
Manage the subscriptions database 86
Managing favorites data 87
Syncing favorites between server groups 87
Manage subscriptions data 87
Purge subscription data 87
Export subscription data 89
Restore subscription data 89
Restoring Data on a Single StoreFront Server 90
Restoring Data on a StoreFront Server Group 90
Import subscription data 91
Subscription data file details 91
Example 92
Store Subscription Counters 93
View the Subscription Counters using PowerShell 93
Store subscription data using Microsoft SQL Server 94

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Introduction 94
Configure the StoreFront server's local security group on the SQL Server 100
Configure the subscription database schema within Microsoft SQL Server for each store 106
Configure the SQL Server Connection String for each StoreFront store 108
Migrate existing data from ESENT into Microsoft SQL Server 110
Update or delete existing subscription records using T-SQL 115
Subscriptions synchronization 118
Upgrade StoreFront 121
Supported upgrade paths 121
Good to know 122
Get ready to upgrade 122
Upgrade a single StoreFront server 123
Upgrade a StoreFront server group during scheduled maintenance downtime 123
Upgrade a StoreFront server group without scheduled downtime 124
Troubleshoot upgrade issues 125
Export and import the StoreFront configuration 126
Scenarios where configuration export and import can be used 126
Things to consider when exporting and importing a StoreFront configuration 127
PowerShell cmdlets 127
Export-STFConfiguration 127
Import-STFConfiguration 128
Unprotect-STFConfigurationBackup 129
Configuration export and import examples 129
Import the StoreFront cmdlets into the current PowerShell session 129
Single server scenarios 130
Server group scenarios 132
Create an encrypted backup of your server configuration 134
Default website for deployment 136

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Reset a server to factory defaults 137
Uninstall StoreFront 137
To manually remove StoreFront 138
Installation logs 138
Manage stores 139
View Stores 139
Create a store 140
Configure store 140
Export provisioning files 141
Delete a store 141
Create store 142
PowerShell 147
Manage sites 148
View sites 148
View sites using PowerShell 148
Add site 148
Add sites for Citrix Virtual Apps and Desktops™ 148
Add Citrix Desktops as a Service site 151
Add Citrix Secure Private Access site 154
Edit a site 155
Edit a site using PowerShell 155
Delete a site 155
Delete a site using PowerShell 155
Health check and server bypass behavior 156
To change the bypass parameters 156
Map users to sites 157
Map users to resources using PowerShell 161
Multi-Site Aggregation 162

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Advanced configurations using PowerShell 168

Zone preference 170

Set Citrix Workspace™ app website 171

Authentication 172

Authentication methods 172

Select authentication methods 172

Select authentication methods using PowerShell 173

Authentication method settings 173

Shared authentication service settings 174

Install or uninstall authentication methods 174

Single sign-on to VDAs 174

Active Directory username and password authentication 174

Configure trusted user domains 175

Enable users to change their passwords 176

Password validation 180

Single sign-on to VDAs 182

Customize the logon screen 182

Prevent Citrix Workspace app for Windows from caching passwords and usernames 183

Remote access via Citrix Gateway 184

SAML authentication 184

StoreFront SAML Endpoints 185

Configure using Metadata exchange 186

Configure Identity Provider 187

Configure Service Provider 189

Testing 189

Configure Delivery Controller™ to trust StoreFront 190

Single sign-on to VDAs 190

Known issues 190

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Entra ID SAML authentication 192
Domain pass-through authentication 195
StoreFront Configuration 195
Configure Delivery Controller™ to trust StoreFront 196
Web browser configuration 196
Single sign-on to VDAs 197
Smart card authentication 197
Prerequisites 198
Configure StoreFront 198
Configure Delivery Controller™ to trust StoreFront 199
Remote access via Citrix Gateway 199
Single sign-on to VDAs 199
Important considerations 200
Pass-through from Citrix Gateway 201
Supported Citrix Gateway authentication methods 202
Enable Gateway pass-through 203
Configure trusted user domains 203
Delegated authentication 204
Password validation 206
Allow users to change expired passwords at logon 206
Allow users to change passwords after logon 207
Configure Delivery Controller™ to trust StoreFront 207
Entra ID using OIDC 208
Single sign-on to VDAs 209
Manage websites 209
View websites 210
PowerShell 210
Configure a website 211

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create a website 212
PowerShell 214
Remove a website 214
PowerShell 214
UI Experience 215
PowerShell 215
Citrix Workspace app deployment 216
Require use of Citrix Workspace™ app 217
Allow users to download Citrix Workspace app 219
PowerShell 220
Progressive Web App (Preview) 220
Category Settings 221
Category view 222
Uncategorized apps 224
Hide categories view 224
Configure category settings PowerShell 225
Appearance 225
Edit logo and colors 225
Reset appearance to default 226
Customization using Javascript and CSS 226
Featured app groups 227
Create featured app group 227
Edit featured app group 230
Edit featured app group using PowerShell 230
Delete featured app group 230
Delete featured app group using the PowerShell 231
Authentication methods 231
Configure using PowerShell 232

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Website shortcuts 233
Add trusted websites using the management console 233
Add trusted websites using PowerShell 235
Launch Preferences 235
Launch option 236
Citrix® web extension 237
PowerShell 238
Store timeouts 238
Internal server communication attempts 239
Internal communication timeout duration 239
Inactivity timeout for web browser 239
Sign in timeout 240
Authentication token lifetime 240
Citrix Gateway timeouts 241
Maximum token lifetime of Authentication Service 241
Session reconnect 243
Configure Session reconnect in a web browser 243
End user settings 245
Configure Session reconnect on Workspace app for Windows 245
Configure Session reconnect on Workspace app for Mac 245
Disable Session reconnect across all apps 245
User interface settings 246
Auto launch desktop 247
Show Desktop Viewer 247
Allow end user to download a Citrix Workspace app configuration file 248
Multi-click duration 248
Navigation tabs 248
Detailed Desktop tile 249

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Display Personalize your home screen for first time users 249
Show Activity manager 250
Pinned links 251
Configuration 251
Custom announcements 252
Dialog after login 254
App Protection 255
App Protection for launches from Citrix Workspace app 255
App Protection for hybrid launch 256
Advanced settings 257
Enable Fiddler tracing 258
Enable Folder view 258
Enable loopback communication 258
Enable Citrix Workspace Launcher 259
Enable strict transport security 260
ICA file cache expiry 260
Icon resolution 260
Loopback port when using HTTP 260
Prompt for untrusted shortcuts 261
Prompt to install Citrix Workspace app after Logon 261
Resource details 261
Strict transport security policy duration 261
Configure remote access settings 261
Configure a Store 263
Favorites 264
Enable or disable favorites 264
Favorites database 266
Configure two StoreFront stores to share subscriptions datastore 266

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Kerberos delegation 267
PowerShell 268
Configure optimal HDX™ routing for a store 269
Example scenario using sites 269
Example scenario using zones 270
Configure Optimal HDX routing 271
Use PowerShell to configure optimal Citrix Gateway routing for a store 273
Advertise or hide stores to users 273
Advanced store settings 274
Address resolution type 275
Allow font smoothing 276
Allow session reconnect 276
Allow special folder redirection 276
Advanced health check 276
Background health check polling period 277
Communication time-out duration 277
Connection timeout 277
Enable enhanced enumeration 277
Enable socket pooling 278
File type association 278
Filter resources by excluded keywords 278
Filter resources by included keywords 279
Filter resources by type 280
Maximum concurrent enumerations 280
Minimum farms for concurrent enumeration 280
Override ICA® client name 280
Require token consistency 281
Server communication attempts 281

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Show Desktop Viewer for legacy clients 281
Treat desktops as apps 281
Federated Authentication Service Configuration 281
Configure FAS using management console 282
Entra ID single sign-on to VDAs 284
Prerequisites 284
Configure using management console 285
Configuration using PowerShell 286
Export store provisioning files for users 286
Configure session settings 287
Example: Launch Notepad in windowed mode 288
Citrix Workspace™ app configuration 289
Global App Config service 289
Store account settings 289
Workspace app website 290
Integrate with Citrix Gateway and NetScaler ADC 291
Configure Citrix Gateways 292
View Gateways 292
PowerShell 293
Add Citrix Gateway appliance 293
PowerShell 300
Add Citrix Gateway Service 300
PowerShell 304
Edit Citrix Gateway 304
PowerShell 304
Remove Citrix Gateway 304
PowerShell 304
Import a Citrix Gateway 304

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Requirements 304
Export configuration from Citrix Gateway 305
Import a Citrix Gateway using the console 306
Import multiple Citrix Gateways using PowerShell 312
Read-STFNetScalerConfiguration 312
Import-STFNetScalerConfiguration without specifying a CallbackURL 315
Import-STFNetScalerConfiguration specifying your own CallbackURL 315
Import-STFNetScalerConfiguration override the authentication method stored in the import file and specify your own CallbackURL 316
Load balancing with NetScaler® ADC 316
Create DNS records for the StoreFront server group load balancer 317
Configure StoreFront Servers 317
Optionally Configure Citrix Service monitor for HTTPS 317
Configure NetScaler Load Balancer 320
Install Root certificate 320
Install the server certificate 320
Add individual StoreFront server nodes to the NetScaler ADC appliance load balancer 322
Define a StoreFront monitor to check the status of all StoreFront nodes in the server group 322
Create a service group containing all of the StoreFront servers 323
Create a load balancing virtual server for user traffic 325
Configure StoreFront Loopback 328
Configure NetScaler ADC load balancer for subscription synchronization between server groups 329
Configure a service group for subscription synchronization 329
Create a load balancing virtual server for subscription synchronization 329
Configure StoreFront to pull subscription data via load balancer 330
Configure Citrix Gateway and StoreFront for Delegated Forms Authentication (DFA) 331

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Installation recommendations 331
StoreFront cluster installation considerations 331
Enable Delegated Forms Authentication 331
Uninstall StoreFront 334
Authenticate using different domains 334
Set up a test environment 335
`production.com` domain 335
`development.com` domain 335
Configure a Citrix Gateway for the store 335
Enable pass-through from Citrix Gateway 337
Configure the store for remote access using the Gateway 338
Disable token consistency 339
Disable pass-through from Citrix Gateway for the website 340
Log on to Gateway using a `production.com` user and credentials 341
Add a trusted domain drop-down list in StoreFront (optional) 342
NetScaler® session action policy 343
Configure beacon points 345
PowerShell 347
Create a single FQDN used internally and externally 348
Server Group base URL 348
StoreFront beacons for locally installed Citrix Workspace app 348
External DNS 348
Internal DNS 348
Require Citrix Workspace™ app when connecting through a gateway 349
Configure using the Management GUI 349
Configure using the CLI 351
Citrix Gateway OIDC Entra ID authentication 352

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Prerequisites 352
Create a Microsoft Azure Entra ID application 352
Create client secret 353
Configure application permissions 354
Configure Citrix DaaS to enable XML trust 355
Configure NetScaler authentication profile 355
Create authentication virtual server 355
Create OAuth policy and action 356
Bind the authentication policy to the virtual server 357
Create authentication profile 357
Create VPN Virtual Server and bind the authentication profile 357
Entra ID token injection configuration for SSO to StoreFront 358
Configure Citrix Gateway within StoreFront 359
End user experience 360
Modern experience 360
Classic experience 360
Citrix Gateway cVPN 360
Classic experience 361
Log On 361
Citrix Workspace app detection 361
Home tab 364
Apps tab 364
Desktops tab 365
App and desktop tiles 365
Favorites 365
View details and actions 366
Search 367
Settings menu 367

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Settings 368
Account 368
Apps 369
Advanced 369
Log off 370
Installing as a Progressive Web App (Preview) 370
Install Progressive Web App using Google Chrome 370
Install Progressive Web App using Microsoft Edge 371
Modern experience 371
Citrix Workspace app required screen 372
Citrix Workspace app detection 372
Authentication 372
After log in dialog 374
First-time user experience 374
Limitations 375
Navigation tabs 376
Simple view 376
Full view 376
Home tab 377
Apps tab 377
Desktops tab 380
Favorite and mandatory apps 380
Search for apps and desktops 381
Activity Manager 381
App tiles 381
Desktop tiles 382
Settings 383
Change Password 384

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Apps and Desktops Launch Preference 384
Download Workspace Configuration 385
Require Citrix Workspace app 385
Automatic store addition 386
Manual store addition 387
Citrix Workspace app detection 389
Welcome to Citrix Workspace screen 389
Citrix Workspace app detection screen 390
Activity Manager 391
Prerequisites 391
Using Activity Manager 392
Disconnected apps and desktops 393
Reconnect to disconnected apps and desktops 395
Transfer your apps and desktops 396
Hibernate and Resume virtual desktop sessions 397
Assigned desktop power management 401
Power status 401
Power actions 403
Secure your StoreFront deployment 405
End user authentication 405
Communication with end-users 405
Communication with Delivery Controllers 406
Communication with Cloud Connectors 406
Communication with Federated Authentication Service 406
Remote access 406
Microsoft Internet Information Services (IIS) hardening 407
Filename extensions 407
Verbs 408

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Non-Ascii characters in URLs 408
MIME Types 408
Remove X-Powered-By Header 408
Remove Server header with IIS version 409
Move the StoreFront website to a separate partition 409
IIS features 409
Handler Mappings 409
ISAPI filters 409
.NET Authorization Rules 409
Retail mode 410
Application Pools 410
Default IIS landing page 410
Required settings 410
Services 410
User rights assignment 411
Configure group memberships 412
NTLM 413
Certificates in StoreFront 413
Server certificates 413
Token management certificates 413
Citrix Delivery Services certificates 413
Code signing certificates 414
StoreFront security separation 414
ICA downloads 414
ICA file signing 414
App protection 415
User change password 415
Customizations 415

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Security Headers 415
Cookies 416
Additional security information 417
Securing StoreFront with HTTPS 417
Create or import certificate 418
Configure IIS for HTTPS 418
HSTS 421
Certificate Revocation List (CRL) checking 423
Introduction 423
CRL Distribution Points (CDP) extensions 423
CRL publishing interval 424
Client CRL caching 424
StoreFront’s access to certificate revocation lists (CRLs) 425
View certificate revocation policy 425
Configure certificate revocation policy 425
Using locally imported CRLs on the StoreFront server 427
To use locally imported CLRs 427
To add the CRL to the Citrix Delivery Services certificate store via PowerShell or the command line 428
XML authentication using delivery controllers 429
To delegate user authentication to delivery controllers 429
Configure an XML authentication service for certificate revocation checking 429
Windows Event Viewer errors to expect 430
Example Error: Store cannot contact a delivery controller with a revoked certificate 431
Example Error: From Receiver for Web if user cannot log in due to failing XML authentication 431
ICA® file signing 432
Logs and Analytics 434

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Log files 434
Installation Logs 434
PowerShell and management console logs 435
Diagnostics logging 435
Verbose logging 436
IIS log files 437
Event Log 437
Log throttling 437
Performance counters 437
Telemetry 438
StoreFront configuration 438
Usage 438
Storefront Login 444
Usage 444
Citrix Workspace app analytics 446
Download the configuration file from Citrix Analytics 447
Example configuration file 448
Import Citrix Analytics data into your StoreFront deployment 448
Propagate Citrix Analytics data to a StoreFront server group 449
Check StoreFront server group ID 449
Stop sending data to Citrix Analytics from StoreFront 450
Configure StoreFront to use a web proxy to contact monitor and register with Citrix Analytics 452
Method 1: Set the store proxy configuration via PowerShell for one or more stores (recommended) 452
Method 2: Manually add a `<system.net>` section to the store web.config file 458
Deprecation notices 460
Deprecations 460
Removals 460

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Third Party Notices 464
Castle Windsor 3.3.0 464
Microsoft Unity Application Block (Unity) 2.1 464
Microsoft Patterns and Practices: Prism 2.2 464
Microsoft patterns & practices: Common Service Locator 1.0 464
Microsoft .Net Reference Source 465
ManagedEsent Release 1.9.4 465
jQuery UI - v1.10.4 - 2014-03-12 465
jQuery JavaScript Library v1.12.4 465
jQuery jScrollPane v2.0.0beta11 465
jquery.contextmenu.js 466
jQuery plugin for Hammer.JS - v1.0.0 - 2014-01-02 466
jQuery MouseWheel 466
Extended WPF Toolkit 3.8.2 466
WiX Toolset 466
CLR Security 466
Stack Exchange Redis 1.1 467
Newtonsoft JSON 467
jQuery JavaScript Library v3.7.1 467
jQuery UI - v1.13.2 - 2022-07-14 467
Hammer.JS - v2.0.4 - 2014-09-28 467
VelocityJS.org (1.5.0) 467
slick.js - 1.8.0 468
jQuery UI Touch Punch 0.2.3 468
Polly 468
Polly.Core 468
Microsoft.Security.Crypto 468
Microsoft .NET 10 468

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CoreWCF 1.8 468
Azure SDK for .NET 469
AspNetWebStack 469
Microsoft Graph SDK 469
Microsoft Graph Core SDK 469
AspNet Logging 469
Microsoft AzureAD IdentityModel Extensions for .NET 469
Microsoft .NET Kiota 469
Microsoft.Web.Infrastructure 1.0 469
Std-UriTemplate 470
Microsoft .NET Maintenance Packages 470
APPENDIX: Referenced Licenses 470
MIT License 470
Apache License, Version 2.0 471
Microsoft Public License (MS-PL) 479
BSD 3-Clause License 481
Microsoft Reciprocal License (Ms-RL) 482
StoreFront Document History 485

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StoreFront 2607 LTSR Overview

StoreFront aggregates applications and desktops from Citrix Virtual Apps and Desktops sites and Citrix DaaS, along with web and SaaS apps from Secure Private access, into a single easy to use store for users.

StoreFront is deployed to servers on your network. For the Citrix managed service, see Citrix® StoreFront Cloud.

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

- The authentication methods users use to log on.
- The list of sites that StoreFront queries to enumerate the resources available to the user.
- The appearance of the store.
- Whether a 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.

Get started

To plan your deployment, install StoreFront, and create your first deployment, see Get started.

What's new

To learn about new features, enhancements, fixed issues, and known issues, see What's new in this release.

Earlier releases

Documentation for other currently available releases is located here.

For steps to upgrade from an earlier release, see Upgrade.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Support lifecycle

The product lifecycle strategy for StoreFront Current Releases (CR) and Long Term Service Releases (LTSR) is described in Lifecycle Milestones. For more information about the product lifecycle and FAQs, see CTX200356.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

What's new in 2607 (initial release)

StoreFront 2607 LTSR includes the following new features and enhancements since StoreFront 2507 LTSR:

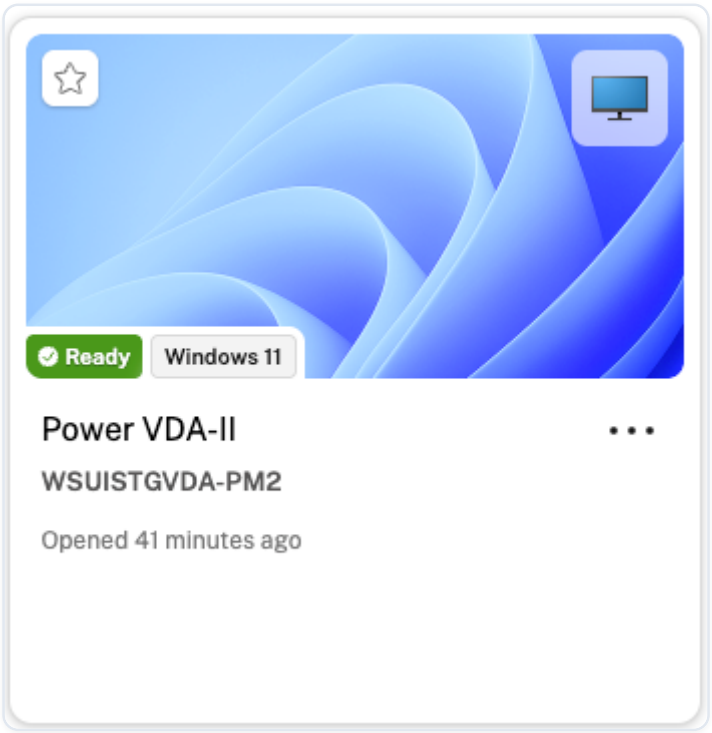
System requirements

StoreFront 2607 LTSR requires .NET 10. If it is not already installed then the installer automatically installs .NET 10.

For more information, see System requirements

Detailed desktop tile

When using the modern experience, you can enable display of a detailed desktop tile.



The tile contains the following information:

- A thumbnail image, making it easier to identify and distinguish between multiple desktops at a glance.
- The operating system running on the desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The power status, which may include new states **Under maintenance**, **Unavailable** and **Active**.
- When you last connected to the desktop. This provides users with a quick security reference — if they notice a connection they don't recognize, they can flag it to their IT team.
- Active session duration if a session is currently running on this desktop.

This feature is disabled by default. To enable it, see detailed desktop tile.

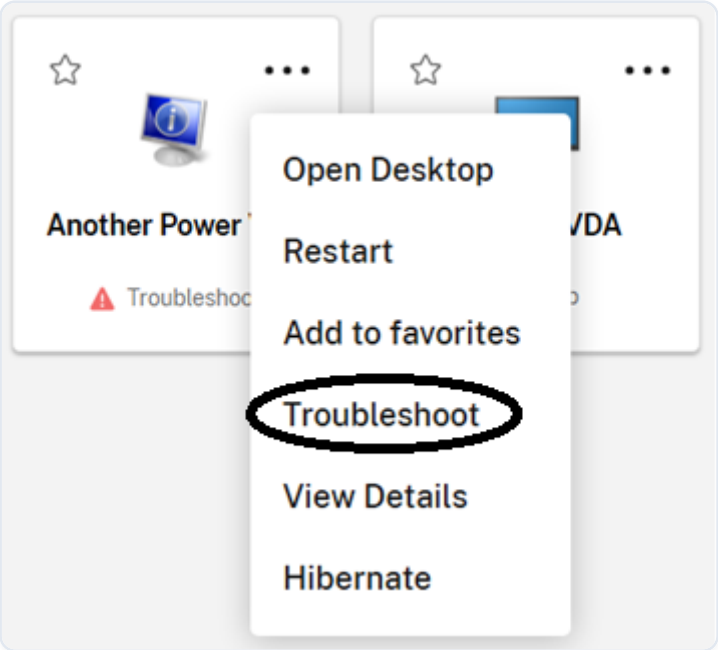
Admin-Configurable Granular Power Actions for Persistent Desktops

Using PowerShell commands, administrators can now configure which power actions are shown to end users for persistent desktops. For more information, see power actions.

Launch failure troubleshooting

When a machine fails to launch, users can now quickly initiate a troubleshooting process directly from the UI. When an error occurs, the machine tile shows text **Troubleshoot**. Clicking the tile initiates the troubleshoot process. Also, the users can also select the **Troubleshoot** option from the three dots menu of the machine to initiate the process.

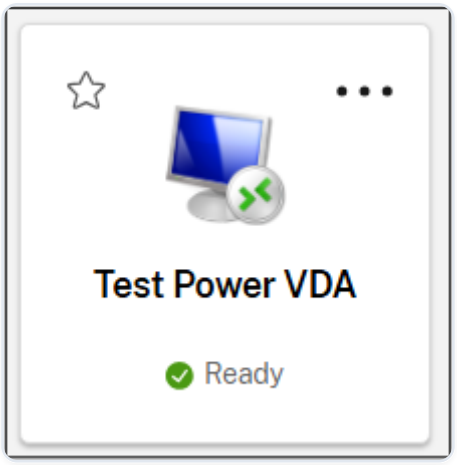
This feature is be available only for desktops and not for published apps and limited to certain types of launch failures.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

“Ready” power state

This release introduces a new power state called **Ready** to improve user launch expectations. The **Ready** state represents a machine that powers on and registers with the system. Machines in the **Ready** state launch faster than machines in **Powered on** or **Powered off** states.



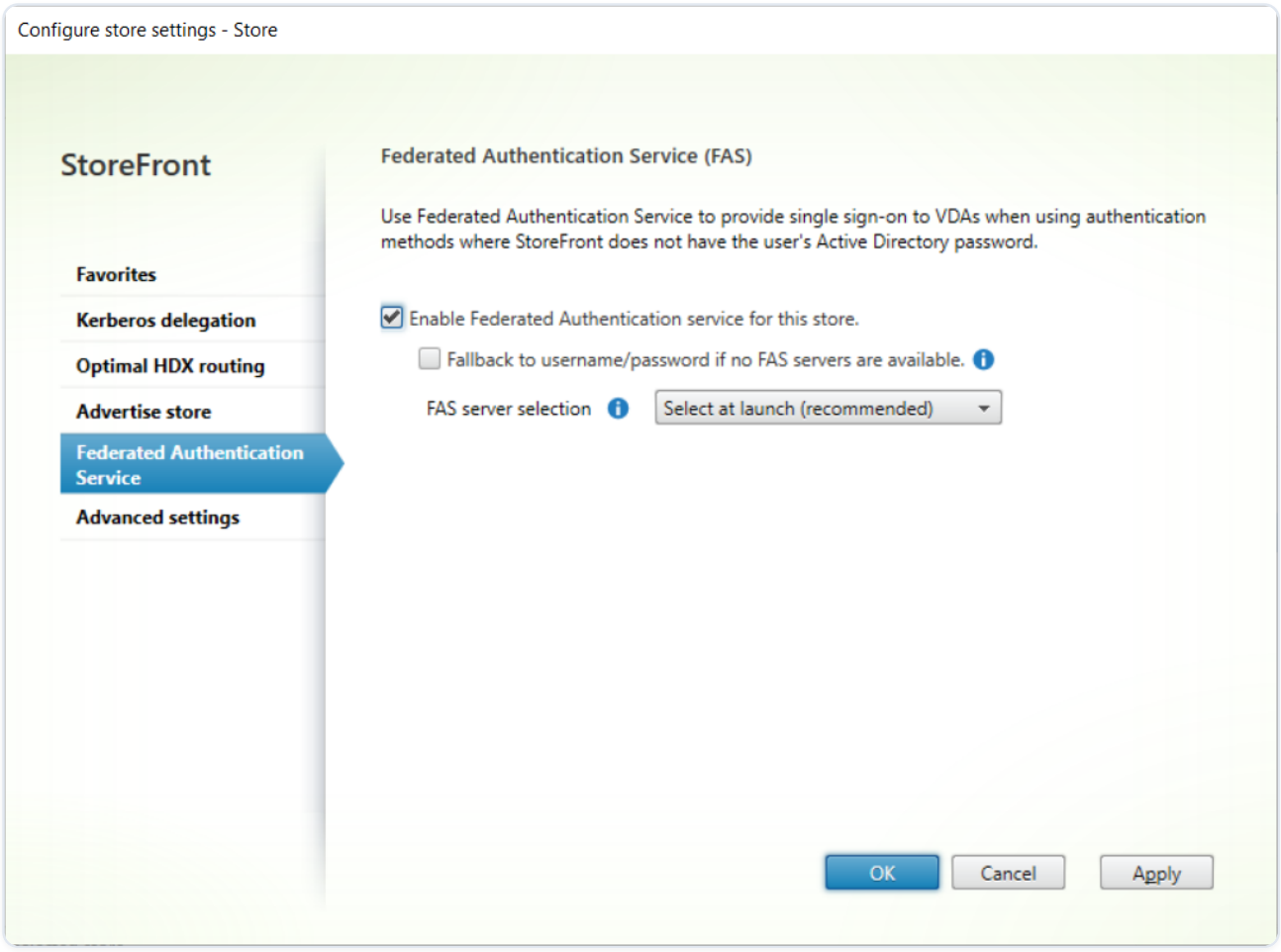
New options in three dots menu

The three-dots menu on tiles for machines with active sessions now provides log off and disconnect options. These options function identically to the corresponding options in Activity Manager.

Configuration FAS in the StoreFront management console

This release enables you to view and modify Federated Authentication Service (FAS) settings for a store directly through the management console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Support for users with Entra ID identities

Previously StoreFront required users to exist in Active Directory. With this release, if users authenticate using OIDC with Microsoft Entra ID at a Citrix Gateway, users with Entra ID can enumerate and launch Citrix DaaS resources that are assigned to their Entra ID identities. For users with hybrid identities, StoreFront also enumerates any resources that are assigned to their Active Directory identity.

- Administrators can configure Entra settings using the StoreFront management console or PowerShell. For more information, see Entra ID using OIDC
- StoreFront supports including Citrix Virtual Apps and Desktops sites for stores using Entra ID authentication via a NetScaler with OIDC. Users with hybrid identities can view resources from both DaaS and Citrix Virtual Apps and Desktops sites. Users with pure Entra ID identities can only view resources from DaaS sites.

It has the following limitations:

- Users must authenticate via a Citrix Gateway rather than directly to StoreFront.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The Citrix Gateway must connect to Entra using OIDC rather than SAML. Users authenticating using SAML continue to be treated as having only Active Directory identities and cannot enumerate resources assigned to Entra ID identities.
- When using multi-site aggregation, it is not possible to map users to sites using their Entra ID identity.

For more information, see Citrix Gateway Entra ID authentication via OIDC.

Entra ID single sign-on to VDAs

If users have authenticated using Entra ID then when they launch a resource hosted on an Entra joined VDA, they can single sign-on to Entra ID joined VDAs.

- Administrators can configure Entra ID single sign-on to VDAs using the StoreFront management console or PowerShell.
- StoreFront supports enabling Entra ID and FAS single sign-on on the same store. Depending on the delivery group's logon type, StoreFront instructs the client to use Entra ID or FAS based SSO.
- StoreFront supports Entra ID single sign-on for resources managed by Citrix DaaS and by Citrix Virtual Apps and Desktops 2603 and above. Citrix Virtual Apps and Desktops VDAs must be hybrid joined.

This is only supported when authenticating via a Citrix Gateway, using a connection to Entra ID via OIDC rather than SAML.

For more information, see Single sign-on to VDAs.

Launch timing telemetry included in ICA file

ICA files now include timestamps of various stages of the launch process to assist with diagnosing launch performance issues. This is included in a section **\[Session Launch Telemetry]**. These timestamps are not included when ICA signing is enabled.

Support for Windows Server Core

You can install StoreFront on Windows Server Core, without the desktop experience. You must install StoreFront using the `-silent` flag. The management console is not available so you must manage StoreFront using PowerShell.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Log improvements

This release improves the information logged in the diagnostics log for many common error conditions.

Command line install location change in behavior

When you initiate a command line install using the `INSTALLDIR` parameter, previously this gave the StoreFront directory, defaulting to `C:\Program Files\Citrix\Receiver StoreFront`. With the new behavior, this gives the location of the Citrix directory, defaulting to `C:\Program Files\Citrix`. StoreFront is now always installed into a sub-directory called `Receiver StoreFront`. This brings StoreFront in line with other Citrix products and resolves an issue where specifying a root directory, for example `D:\`, caused uninstallation to fail.

Citrix Workspace app for HTML5 HDX Client

This release includes Citrix Workspace app for HTML5 HDX client 2603.10

Fixed issues

This release includes the following fixes since StoreFront 2507 LTSR:

- When using Set-STFWebReceiverSiteStyle to set some but not all appearance settings, other appearance settings are reset to their default values.
- SAML authentication may fail due to URL path exceeding 2048 characters.
- Citrix Workspace app downloads get re-enabled when you change launch settings.
- Subscription synchronization could stop after extended uptime.
- After disabling FAS through the management console, if FAS server section was set to **Select at launch**, StoreFront continues to get FAS claims at log ins. This can cause log in failures if FAS is not available.
- In the management console, some controls have the same hotkeys.
- In the management console, some text is cut off when using non-English languages.
- When the user updates any authentication configuration on the store, it resets which authentication methods are enabled on every website to match the store.
- The descriptions for the Citrix StoreFront Telemetry Service and the CitrixStorefrontTelemetryService Users group are not properly localized.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- When performing machine control actions, the client name and address is not passed to the DDC so is missing from the log files.
- Creating an anonymous store using PowerShell might fail with error "Add-STFStoreService : An error occurred creating the Store service Exception of type 'Citrix.DeliveryServices.Framework.Feature.Exceptions.FeatureClassNotFoundException'".
- Users experience intermittent enumeration failures. The event logs shows error "Citrix Store Service. Failed XML health checks".
- StoreFront upgrade fails if a website's custom folder contains a web.config file.
- In the help for PowerShell cmdlet `Add-STFRoamingGateway`, the example for creating a Citrix Gateway service gateway is incorrect.
- The help text for PowerShell commands to set styles is misleading.
- Renaming a site deletes any optimal HDX routing for that site
- If you remove all auth methods apart from SAML, the management console displays a message that the store is inaccessible.
- When attempting to reconnect to a resource using Activity Manager, where the resource is a merge group, reconnection fails.
- The `X-XSS-Protection` header is deprecated and should be removed.
- If StoreFront is onboarded to Citrix Analytics you might find significantly increased CPU usage.
- The descriptions of event logs generated by the Citrix StoreFront Telemetry Service are not localized.
- On the management console appearance tab, the reset to default button does not work.
- StoreFront management console does not display previously uploaded logo.
- Renaming a site does not warn the admin that this will remove all user favorites.
- In the management console some controls have duplicate access key shortcuts.
- In the management console when an admin changes the UI experience then selects **Cancel**, the change is still saved in the console.
- The example returned by get-help for Set-STFWebReceiverService is incorrect
- When NTLM is disabled, favorites are not synchronizing between StoreFront servers.
- After removing a gateway using the PowerShell command Remove-STFRoamingGateway, the removed gateway might still be included in the list of beacons.
- Running a PowerShell that requires elevation displays the misleading error message "The source was not found, but some or all event logs could not be searched."

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Fixes to the modern end user experience:

- If allowRestart flag on the delivery group has been set to `false`, users are able to restart or power off their machine using the tile menu or Activity Manager. With this change, users no longer see options to shut down, force shutdown, and restart option, which prevents users from restarting their machine.
- Some buttons are not reachable using the keyboard.
- The power status is not displayed for resources with App Protection.
- On the store login screen, the buttons and other form elements use the default blue color instead of the administrator configured branding colors.
- When the modern experience loads in a web browser or Citrix Workspace app, the spinner and Citrix logo use an outdated teal color instead of the current blue Citrix branding colors.
- The "Always display navigation tabs" setting is not honored when user has fewer than 20 resources.
- The bottom of the options (3-dot) menu may be hidden by a custom notification at the bottom of the page.
- Improve description of shutdown and force shutdown.
- When the language is Japanese, resource tiles are sorted incorrectly.

Known issues

- When using SAML authentication direct to StoreFront from Citrix Workspace app for iOS or Citrix Workspace app for Android, authentication fails with one of the following errors:
  - "You cannot have the _ri parameter with any of the following: _cx, _id, _cs, _hf, _rt or _ps"
  - "For a browser, you must supply all of the following: _cx, _id, and _cs, _ps and _hf are optional. For a native client _rt must be supplied and _ps is optional"
- When using the Classic UI, downloaded ICA files may not include an .ica extension.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Get started

Prerequisites

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 prerequisites 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

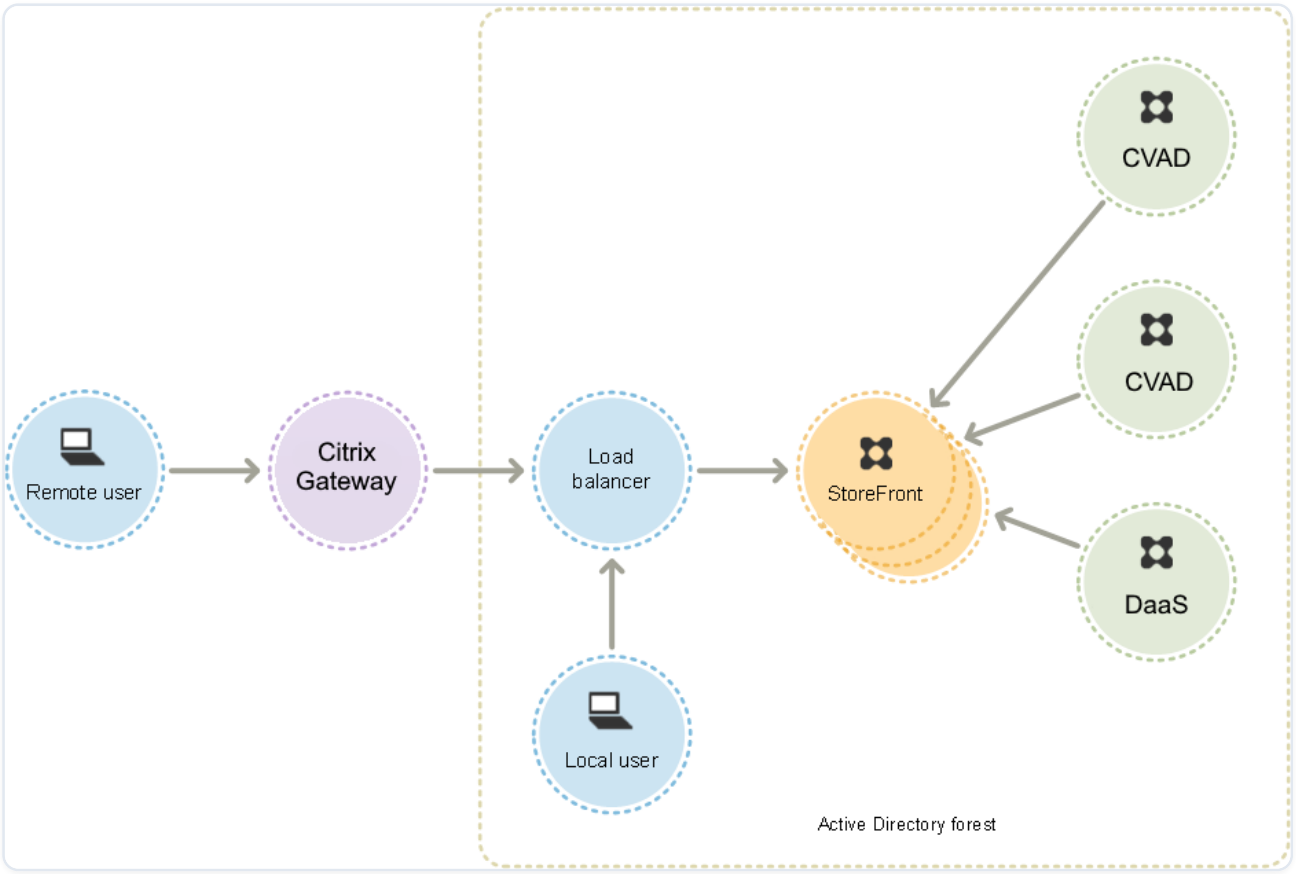
1. For redundancy and scalability, deploy a load balancer and add further servers to the StoreFront server group.
2. Secure your deployment.
3. Optimize the end user experience.
4. Enable remote access using a Citrix Gateway.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Plan your StoreFront deployment

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

For improved capacity and resiliency, you can use multiple StoreFront servers behind a load balancer. This is known as a StoreFront server group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Use a load balancer with built-in monitors and session persistency, such as NetScaler ADC. For more information, see Load balancing with NetScaler® ADC.

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.

Beyond 3 servers in a server group, the performance gains become more limited. 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.

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 oad 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

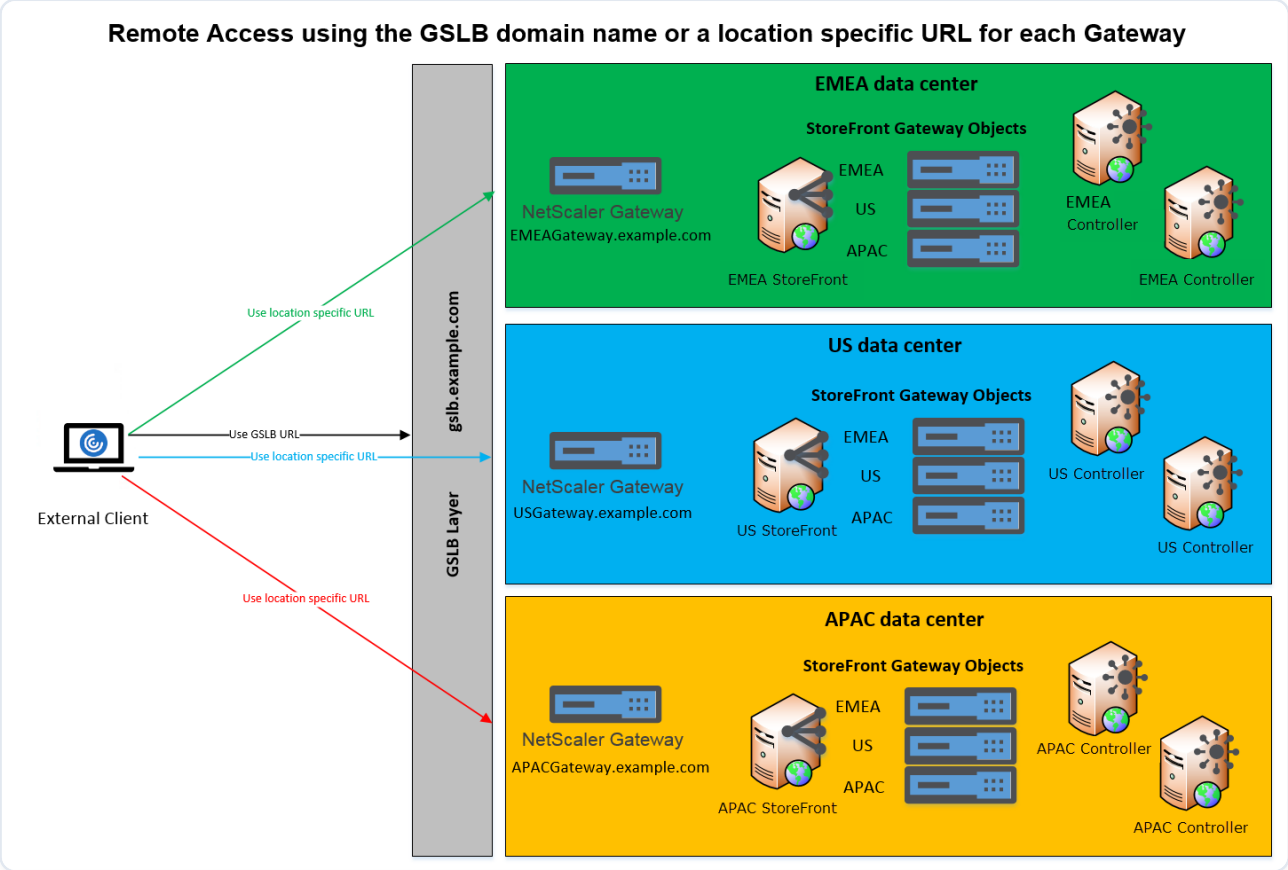
`emeagateway.example.com` - Europe gateway

`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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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 can be installed on Windows Server Core without the desktop experience. You must install StoreFront using the `-silent` flag. The management console is not available so you must manage StoreFront using PowerShell.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 2603 and higher requires .NET 10, and StoreFront 2411 to 2511 requires .NET 8. If it is not already installed then the installer automatically installs .NET.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

        - 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 TCP port 443 or 80 respectively. You can allow clients to connect to StoreFront directly, however commonly clients connect to a load balancer or gateway which forwards traffic to StoreFront. You can modify the ports used in IIS configuration. It is recommended that you use HSTS to force web browsers to use HTTPS.
- TCP port 808 is used for:
  - synchronizing subscriptions within a server group. This only applies if favorites are enabled and you are using the local database, rather than an external SQL server database.
  - Synchronizing subscriptions between server groups. This only applies if you have enabled Synchronizing subscriptions.
- A TCP port randomly selected from all unreserved ports is used for communications between the StoreFront servers in a server group.
- 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.

When you install StoreFront, a Windows Firewall rules are configured enabling access to the StoreFront executables. You must ensure that any firewalls or other devices on your internal network do not block traffic to any of the unassigned TCP ports.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 2607 LTSR
- Citrix Virtual Apps and Desktops 2603
- Citrix Virtual Apps and Desktops 2511
- Citrix Virtual Apps and Desktops 2507 LTSR
- Citrix Virtual Apps and Desktops 2503
- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Gateway 14.1
- Citrix Gateway 13.1

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

User device requirements

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

* 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,

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 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 *application* 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

KEYWORD NAME	DESCRIPTION
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
`Citrix.ClientUserAgent`	The user agent of the client	`Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/51.0.2704.103 Safari/537.36`
`Citrix.StoreFrontStoreUrl`	The URL of the store the user is connected to	`https://storefront.example.com/Citrix/Store`

Install StoreFront

Before installing

Before you install and configure StoreFront, review the System Requirements.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

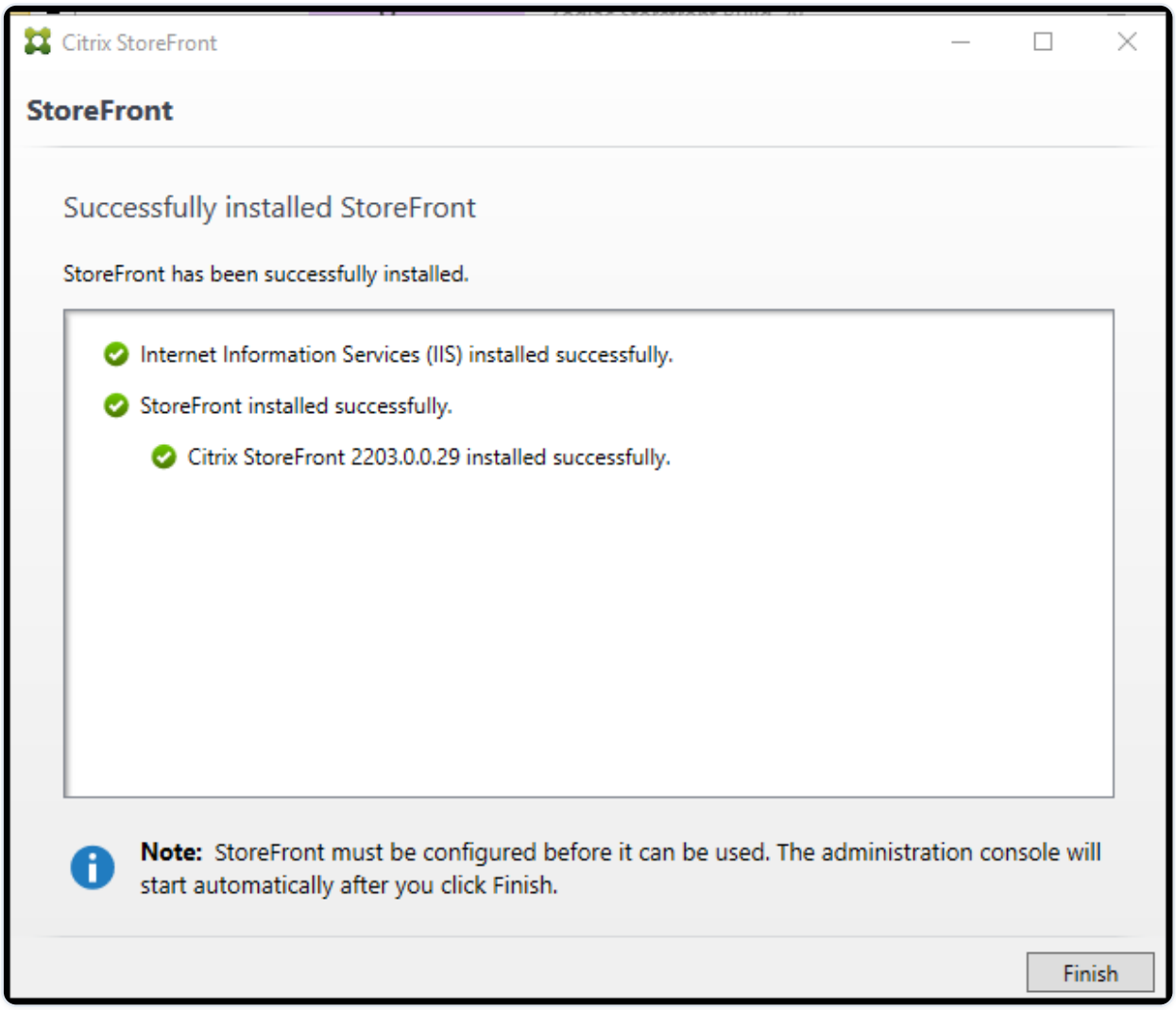
Install StoreFront

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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

```
CitrixStoreFront-x64.exe [-silent] [-INSTALLDIR installationlocation]
[-WINDOWS_CLIENT filelocation\filename.exe] [-MAC_CLIENT
filelocation\filename.dmg]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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™

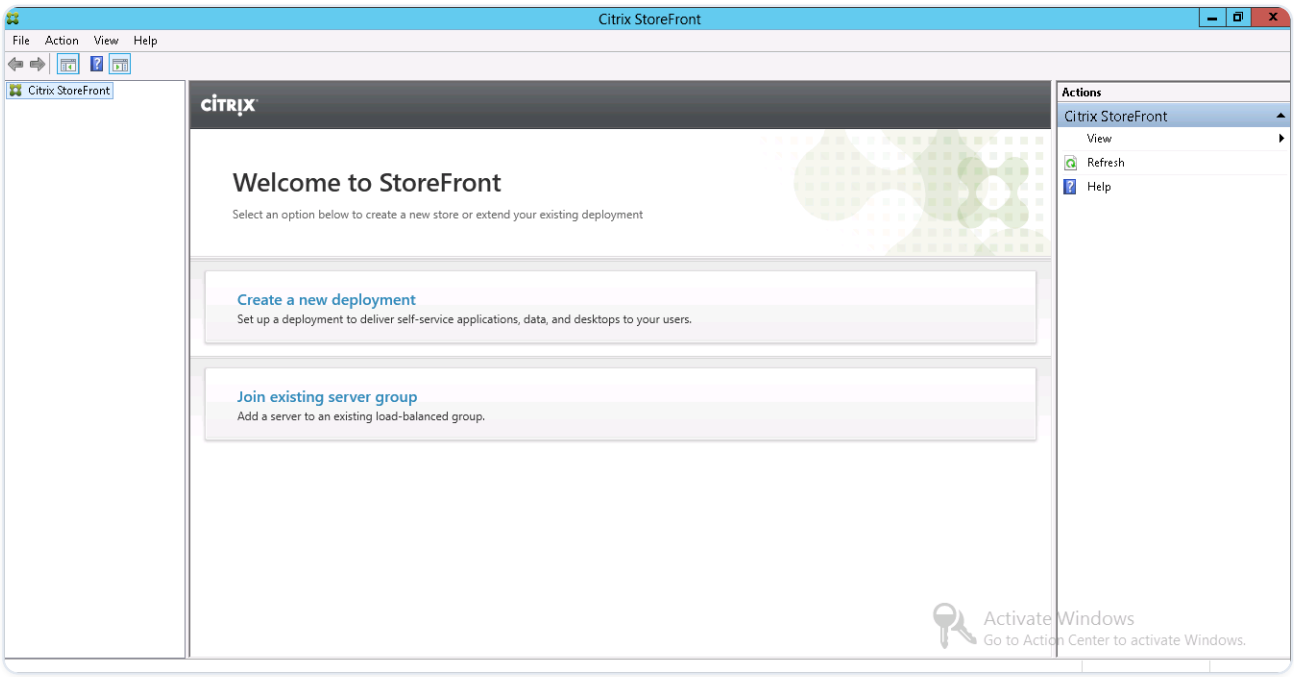
You can install StoreFront on the same server as Citrix Virtual Apps and Desktops. Run the Citrix Virtual Apps and Desktops installer and under **Extend Deployment** choose **Citrix StoreFront**.

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.



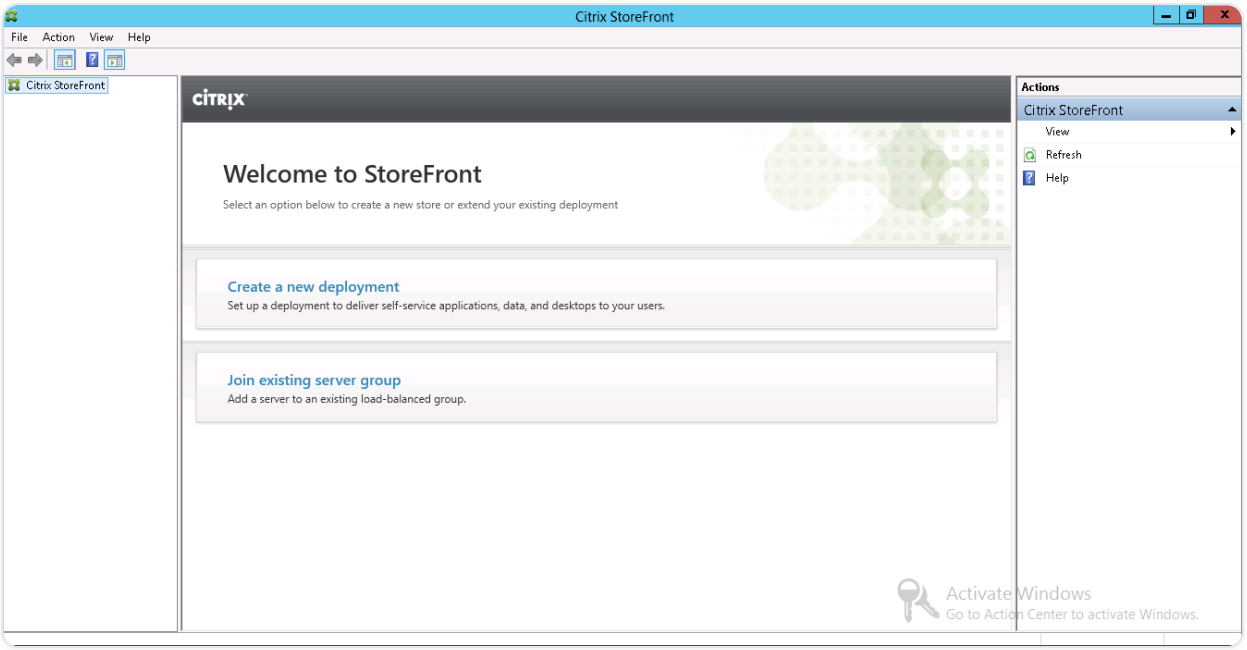
- Create a deployment. Configure the first server in a new StoreFront deployment. Single-server deployments are ideal for evaluating StoreFront or for small production deployments. Once you have configured your first StoreFront server, you can add more servers to the group at any time to increase the 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

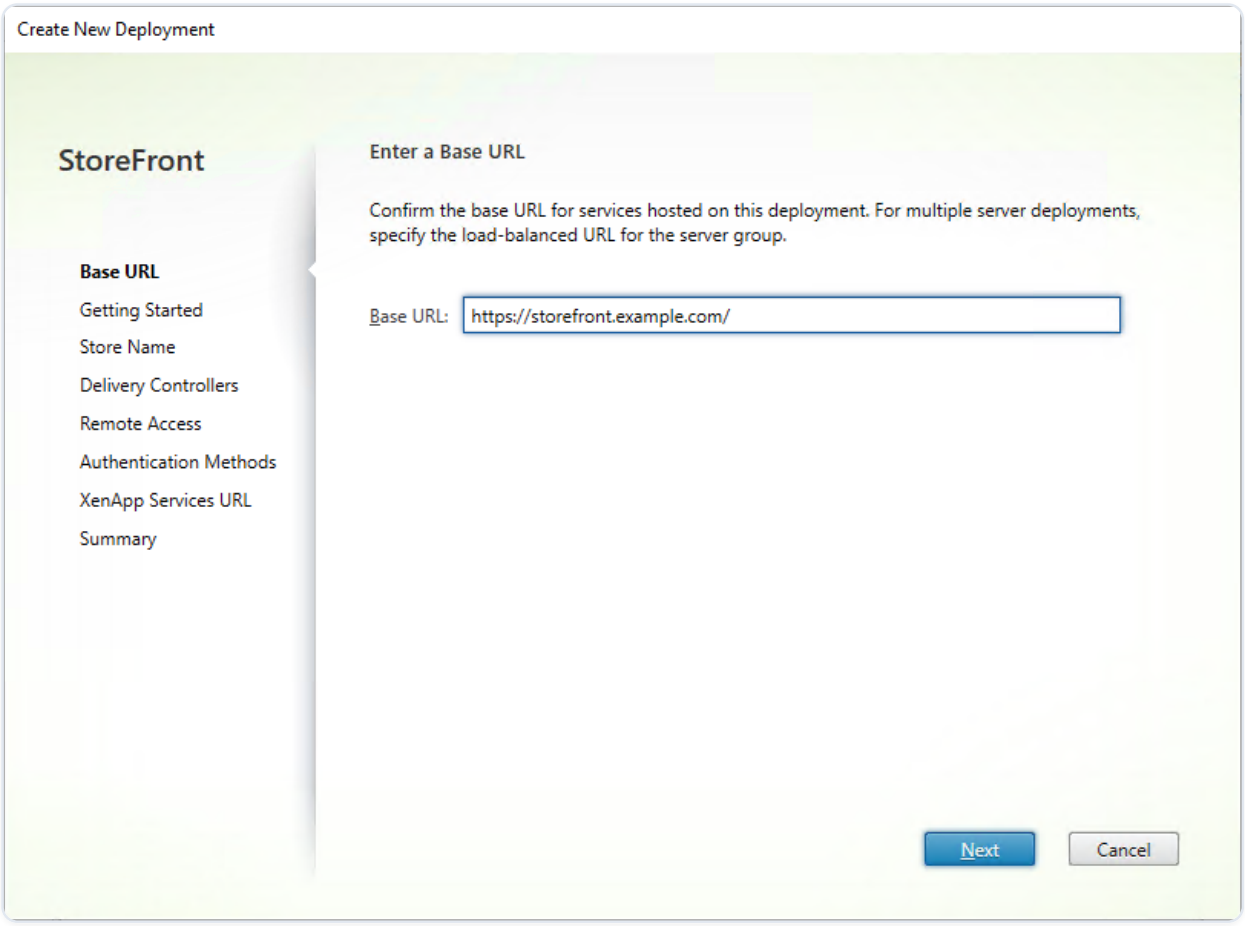
1. If the StoreFront management console is not already open after installation of StoreFront, open it.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Add-STFDeployment -SiteID 1 -HostBaseURL "https://apps.example.com"

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

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 keylogging and screen-capturing malware.
- **Better telemetry** because the native app offers extensive information for monitoring purposes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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.

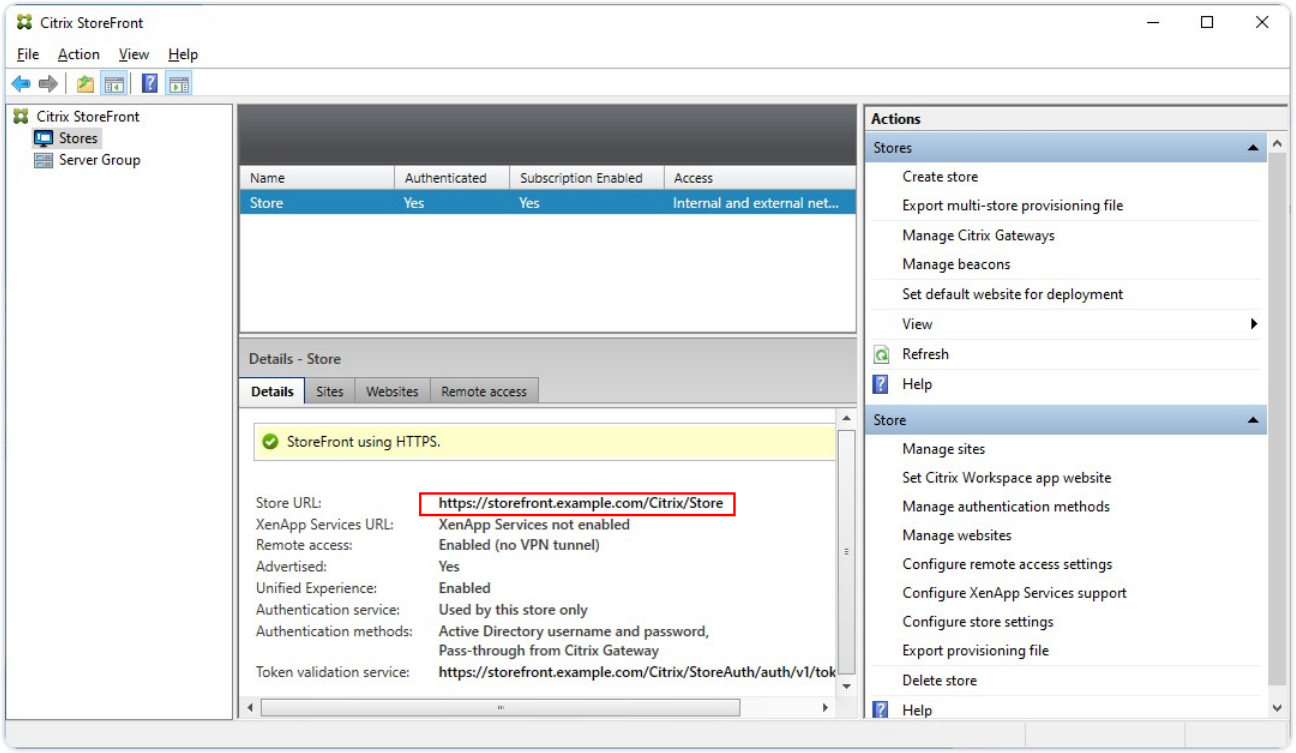
IMPORTANT:

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

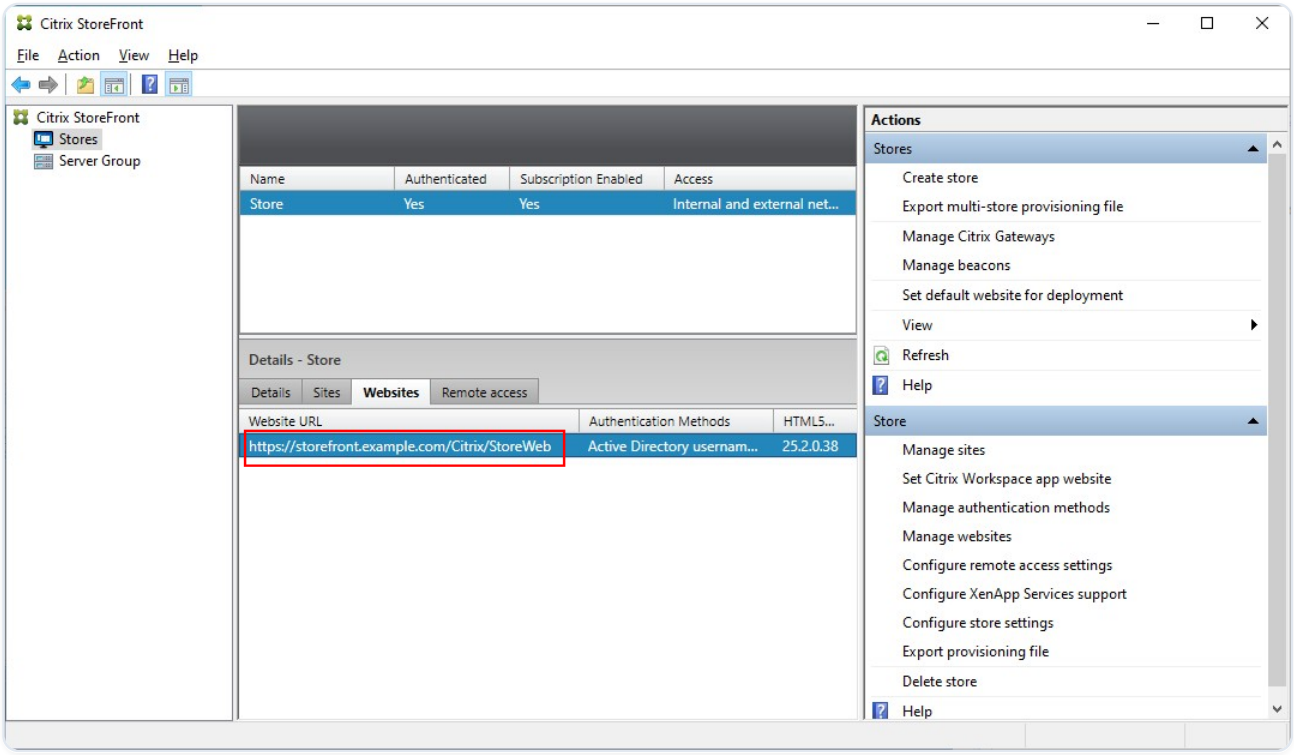
Internal users can navigate directly to the store website URL. Where there are multiple websites in your StoreFront deployment, you can configure one of them as the default URL that users are redirected to when the user navigates to the base URL.

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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

Citrix Workspace launcher is a component of Citrix Workspace app that allows a store website to detect Citrix Workspace app and launch virtual apps and desktops without requiring an `.ICA` file download. It registers the protocol `receiver` and uses this to communicate with Citrix Workspace app.

When the user first goes to a Workspace URL a supported operating system and browser and Citrix Web Extensions is not installed, it attempts to invoke the Citrix Workspace Launcher using a URL starting `receiver://`. For more information on the user experience see Classic experience and Modern experience. To configure Citrix Workspace launcher, see Enable Citrix Workspace Launcher.

If Citrix Workspace launcher detects a supported version of Citrix Workspace app then it 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For managed web browsers, it is recommended that you configure the browser to automatically accept the `receiver` protocol to avoid prompts.

- On Microsoft Edge, you can use the policy AutoLaunchProtocolsComponentEnabled.
- On Chrome enterprise, you can use the policy Auto Launch Protocols From Origins.
- On Firefox, you can use the policy AutoLaunchProtocolsFromOrigins.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix Workspace launcher does not work when using smartcard authentication via a Citrix Gateway.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

checks that website against the list of URLs you entered to ensure that the request originates from a trusted website.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage Deployment

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

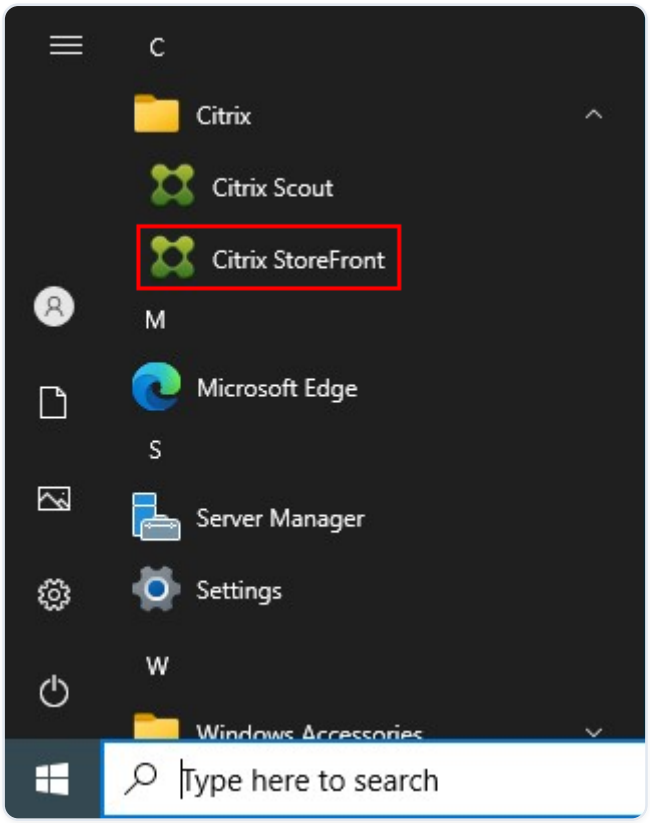
TOPIC	DESCRIPTION
StoreFront Management Console	Open the StoreFront management console GUI to configure StoreFront
StoreFront PowerShell modules	Use the StoreFront PowerShell modules to automate StoreFront configuration
Configure the base URL	Configure the base URL that users enter to connect to the 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StoreFront Management console

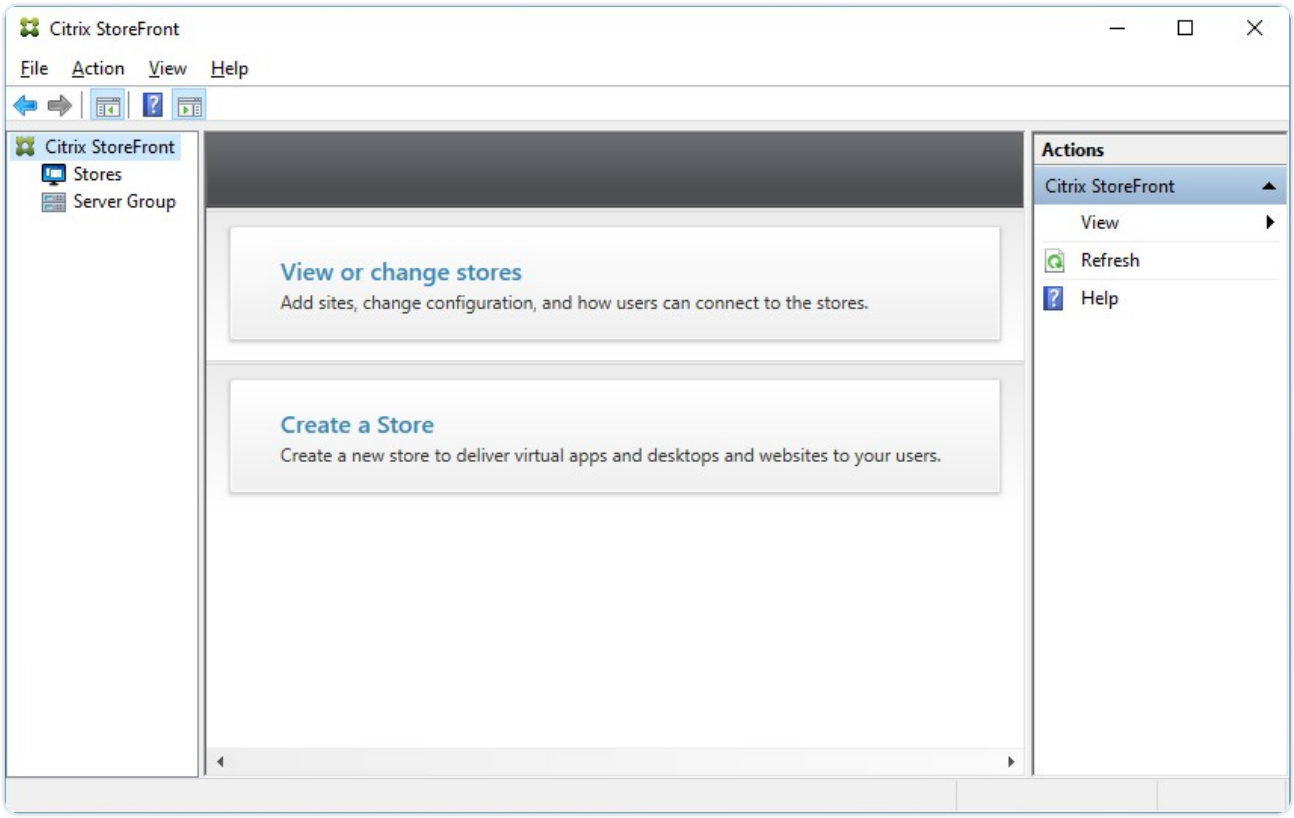
Most of aspects of StoreFront can be configured using the StoreFront management console.

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



This opens the StoreFront management console.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

```
-  Use the PowerShell ISE, Visual Studio Code or a similar tool to edit
the script.

-  Use variables to assign values that are to be reused or modified.

-  Remove any commands that are not required.

-  Note that StoreFront cmdlets can be identified by the prefix STF.
```

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.
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Sets the error handling requirements and imports the required StoreFront modules. Imports are not required in modern versions of PowerShell.

```
Param(

    [Parameter(Mandatory=$true)]

    [Uri]$HostbaseUrl,

    [long]$SiteId = 1,

    [ValidateSet("XenDesktop","XenApp","AppController","VDIinaBox")]

    [string]$Farmtype = "XenDesktop",

    [Parameter(Mandatory=$true)]

    [string[]]$FarmServers,

    [string]$StoreVirtualPath = "/Citrix/Store",

    [bool]$LoadbalanceServers = $false,

    [int]$Port = 80,

    [int]$SSLRelayPort = 443,

    [ValidateSet("HTTP","HTTPS","SSL")]

    [string]$TransportType = "HTTP"

    )

    # Import StoreFront modules. Required for versions of PowerShell
earlier than 3.0 that do not support autoloading

    Import-Module Citrix.StoreFront

    Import-Module Citrix.StoreFront.Stores

    Import-Module Citrix.StoreFront.Authentication
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    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`.

```
# Determine the Authentication and Receiver virtual path to use based
of the Store

$authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"

$receiverVirtualPath = "$($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.

```
# Determine if the deployment already exists

$existingDeployment = Get-STFDeployment

if(-not $existingDeployment)

{

    # Install the required StoreFront components

    Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId
-Confirm:$false

}

elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)

{

    # The deployment exists but it is configured to the desired
hostbase url
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    Write-Output "A deployment has already been created with the
specified hostbase url on this server and will be used."

}

else

{

    Write-Error "A deployment has already been created on this server
with a different host base url."

}
```

- 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.

```
# Determine if the authentication service at the specified virtual path
exists

$authentication = Get-STFAuthenticationService -VirtualPath
$authenticationVirtualPath

if(-not $authentication)

{

    # Add an Authentication service using the IIS path of the Store
appended with Auth

    $authentication = Add-STFAuthenticationService
$authenticationVirtualPath

}

else

{

    Write-Output "An Authentication service already exists at the
specified virtual path and will be used."
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}
```

- 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.

```
# Determine if the store service at the specified virtual path exists

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

if(-not $store)

{

# Add a Store that uses the new Authentication service configured to
publish resources from the supplied servers

$store = Add-STFStoreService -VirtualPath $StoreVirtualPath
-AuthenticationService $authentication -FarmName $Farmtype -FarmType
$Farmtype -Servers $FarmServers -LoadBalance $LoadbalanceServers `

        -Port $Port -SSLRelayPort $SSLRelayPort -TransportType
$TransportType

}

else

{

    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."

    # Get the number of farms configured in the store

    $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.Count

    # Append the farm to the store with a unique name

    Add-STFStoreFarm -StoreService $store -FarmName "Controller$
($farmCount + 1)" -FarmType $Farmtype -Servers $FarmServers
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-LoadBalance $LoadbalanceServers -Port $Port `

        -SSLRelayPort $SSLRelayPort -TransportType $TransportType

}
```

- Adds a website at the specified IIS virtual path to access applications published in the store created above.

```
# Determine if the receiver service at the specified virtual path
exists

$receiver = Get-STFWebReceiverService -VirtualPath $receiverVirtualPath

if(-not $receiver)

{

    # Add a Receiver for Web site so users can access the applications
and desktops in the published in the Store

    $receiver = Add-STFWebReceiverService -VirtualPath
$receiverVirtualPath -StoreService $store

}

else

{

    Write-Output "A Web Receiver service already exists at the
specified virtual path and will be used."

}
```

- Enables XenApp services for the store so older Citrix Receiver or Citrix Workspace app clients can connect to published applications.

```
# Determine if PNA is configured for the Store service

$storePnaSettings = Get-STFStorePna -StoreService $store
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
if(-not $storePnaSettings.PnaEnabled)

{

# Enable XenApp services on the store and make it the default for this
server

Enable-STFStorePna -StoreService $store -AllowUserPasswordChange
-DefaultPnaService

}
```

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.

```
Param(

    [Parameter(Mandatory=$true)]

    [Uri]$HostbaseUrl,

    [Parameter(Mandatory=$true)]

    [long]$SiteId = 1,

    [string]$Farmtype = "XenDesktop",

    [Parameter(Mandatory=$true)]

    [string[]]$FarmServers,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    [string]$StoreVirtualPath = "/Citrix/Store",
    [bool]$LoadbalanceServers = $false,
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP",
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$GatewaySTAUrls,
    [string]$GatewaySubnetIP,
    [Parameter(Mandatory=$true)]
    [string]$GatewayName
)
Set-StrictMode -Version 2.0


# Any failure is a terminating failure.
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
# Import StoreFront modules. Required for versions of PowerShell
earlier than 3.0 that do not support autoloading

Import-Module Citrix.StoreFront

Import-Module Citrix.StoreFront.Stores

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.

```
# Create a simple deployment by invoking the SimpleDeployment example

$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition
-Parent

$scriptPath = Join-Path $scriptDirectory "SimpleDeployment.ps1"

& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers
$FarmServers -StoreVirtualPath $StoreVirtualPath -Farmtype $Farmtype \`

    -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.

```
# Determine the Authentication and Receiver sites based on the Store

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$authentication = Get-STFAuthenticationService -StoreService $store

$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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
# Get the Citrix Receiver for Web CitrixAGBasic and ExplicitForms
authentication method from the supported protocols

# Included for demonstration purposes as the protocol name can be used
directly if known

$receiverMethods = Get-STFWebReceiverAuthenticationMethodsAvailable |
Where-Object { $_ -match "Explicit" -or $_ -match "CitrixAG" }

# Enable CitrixAGBasic in Receiver for Web (required for remote access)

Set-STFWebReceiverService $receiverForWeb -AuthenticationMethods
$receiverMethods
```

- Enables CitrixAGBasic on the authentication service. This is required for remote access.

```
# Get the CitrixAGBasic authentication method from the protocols
installed.

# Included for demonstration purposes as the protocol name can be used
directly if known

$citrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-Object
{ $_ -match "CitrixAGBasic" }

# Enable CitrixAGBasic in the Authentication service (required for
remote access)

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.

```
# Add a new Gateway used to access the new store remotely

Add-STFRoamingGateway -Name "NetScaler10x" -LogonType Domain -Version
Version10_0_69_4 -GatewayUrl $GatewayUrl `

    -CallbackUrl $GatewayCallbackUrl -SecureTicketAuthorityUrls
$GatewaySTAUrls
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
# Get the new Gateway from the configuration (Add-STFRoamingGateway
will return the new Gateway if -PassThru is supplied as a parameter)

$gateway = Get-STFRoamingGateway -Name $GatewayName

# If the gateway subnet was provided then set it on the gateway object

if($GatewaySubnetIP)

{

    Set-STFRoamingGateway -Gateway $gateway -SubnetIPAddress
$GatewaySubnetIP

}

# Register the Gateway with the new Store

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.

```
Param(

    [Parameter(Mandatory=$true)]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    [Uri]$HostbaseUrl,

    [long]$SiteId = 1,

    [string]$Farmtype = "XenDesktop",

    [Parameter(Mandatory=$true)]

    [string[]]$FarmServers,

    [string]$StoreVirtualPath = "/Citrix/Store",

    [bool]$LoadbalanceServers = $false,

    [int]$Port = 80,

    [int]$SSLRelayPort = 443,

    [ValidateSet("HTTP","HTTPS","SSL")]

    [string]$TransportType = "HTTP",

    [Parameter(Mandatory=$true)]

    [Uri]$GatewayUrl,

    [Parameter(Mandatory=$true)]

    [Uri]$GatewayCallbackUrl,

    [Parameter(Mandatory=$true)]

    [string[]]$GatewaySTAUrls,

    [string]$GatewaySubnetIP,

    [Parameter(Mandatory=$true)]

    [string]$GatewayName,

    [Parameter(Mandatory=$true)]

    [Uri]$OptimalGatewayUrl,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    [Parameter(Mandatory=$true)]

    [string[]]$OptimalGatewaySTAUrls,

    [Parameter(Mandatory=$true)]

    [string]$OptimalGatewayName

)

Set-StrictMode -Version 2.0

# Any failure is a terminating failure.

$ErrorActionPreference = 'Stop'

$ReportErrorShowStackTrace = $true

$ReportErrorShowInnerException = $true

# Import StoreFront modules. Required for versions of PowerShell
earlier than 3.0 that do not support autoloading

Import-Module Citrix.StoreFront

Import-Module Citrix.StoreFront.Stores

Import-Module Citrix.StoreFront.Roaming
```

- Calls into the remote access deployment script to configure the basic deployment and add remote access.

```
# Create a remote access deployment

$scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.Definition
-Parent

$scriptPath = Join-Path $scriptDirectory "RemoteAccessDeployment.ps1"

& $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -FarmServers
$FarmServers -StoreVirtualPath $StoreVirtualPath -Farmtype $Farmtype `
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    -LoadbalanceServers $LoadbalanceServers -Port $Port  -SSLRelayPort
$SSLRelayPort -TransportType $TransportType `

    -GatewayUrl $GatewayUrl -GatewayCallbackUrl $GatewayCallbackUrl
-GatewaySTAUrls $GatewaySTAUrls -GatewayName $GatewayName
```

- Adds the preferred optimal launch gateway and get it from the list of configured gateways.

```
# Add a new Gateway used for remote HDX access to desktops and apps

$gateway = Add-STFRoamingGateway -Name $OptimalGatewayName -LogonType
UsedForHDXOnly -GatewayUrl $OptimalGatewayUrl
-SecureTicketAuthorityUrls $OptimalGatewaySTAUrls -PassThru
```

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

```
# Get the Store configured by SimpleDeployment.ps1

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

# Register the Gateway with the new Store for launch against all of the
farms (currently just one)

$farmNames = @($store.FarmsConfiguration.Farms | foreach
{ $_.FarmName })

Register-STFStoreOptimalLaunchGateway -Gateway $gateway -StoreService
$store -FarmName $farmNames
```

Configure the base URL

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 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`.

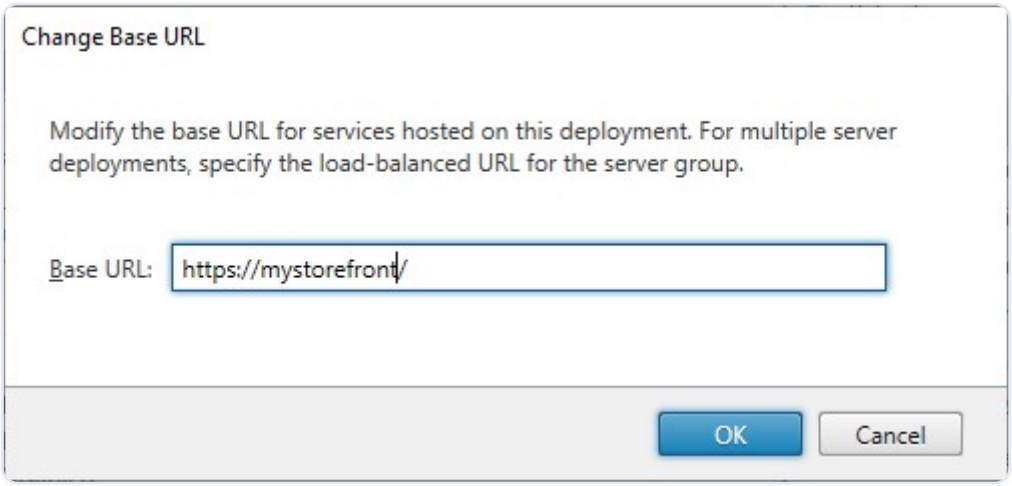
- For a single server deployment without a load balancer, enter the URL of the server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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**.



Configure server groups

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

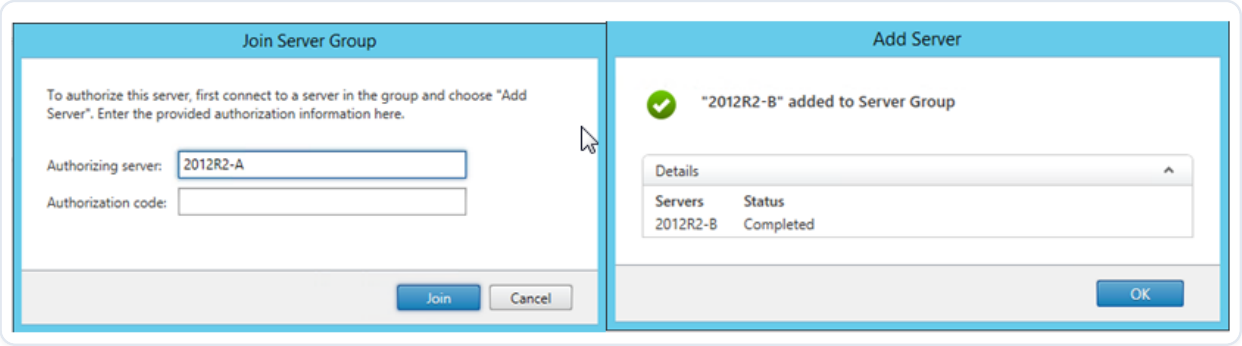
When you add a new server to a server group, StoreFront service accounts are added as members of the local administrators group on the new server. These services require local administrator permissions to join and synchronize with the server group. If you use Group Policy to prevent addition of new members 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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 use 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 initiate the Propagate Changes task.

Manage the subscriptions database

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
$store=Get-STFStoreService -VirtualPath '/Citrix/Store'

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

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__Cit`
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

```
function Remove-SubscriptionData

{

    [CmdletBinding()]



    [Parameter(Mandatory=$False)][String]$Store = "Store"



    $SubsService = "Citrix Subscriptions Store"



    # Path to Subscription Data in StoreFront version 2.6 or later



    $SubsPath = "C:
\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\Subscriptio
nsStore\1__Citrix_$Store\*"



    Stop-Service -displayname $SubsService



    Remove-Item $SubsPath -Force -Verbose



    Start-Service -displayname $SubsService
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    Get-Service -displayname $SubsService

}


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:

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/
<yourstore>"

Export-STFStoreSubscriptions -StoreService $StoreObject -FilePath
"$env:USERPROFILE\Desktop\Subscriptions.txt"
```

If you are managing a multiple-server deployment, you can run this PowerShell cmdlet on any server within the StoreFront server group. Each server in the server group maintains an identical synced copy of the subscription data from its peers. If you believe you are experiencing issues with subscription synchronization between the Storefront servers, then export the data from all servers in the group and compare them to see differences.

Restore subscription data

Use Restore-STFStoreSubscriptions to overwrite your existing subscription data. You can restore a Store's subscription data using the tab separated .txt file backup you created earlier using Export-STFStoreSubscriptions.

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/
<yourstore>"

Restore-STFStoreSubscriptions -StoreService $StoreObject -FilePath
"$env:USERPROFILE\Desktop\Subscriptions.txt"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For more information on Restore-STFStoreSubscriptions, see `<https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/2607/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 restored 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/
<yourstore>"

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/2607/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).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

NO OF RECORDS	SIZE MB
500,000	64.10
800,000	102.00
1,000,000	128.00
1,300,000	166.00
1,500,000	192.00
1,700,000	218.00
2,000,000	256.00

Store Subscription Counters

You can use Microsoft Windows Performance monitor counters (**Start > Run > perfmon**) to show, for example, the total numbers of subscription records on the server or number of records synchronized between StoreFront server groups.

View the Subscription Counters using PowerShell

```
Get-Counter -Counter "\Citrix Subscription Store(1__citrix_store)
\Subscription Entries Count (including unpurged deleted records)"



Get-Counter -Counter "\Citrix Subscription Store
Synchronization\Subscriptions Store Synchronizing"



Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number
Subscriptions Synchronized"



Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number
Subscriptions Transferred"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Store subscription data using Microsoft SQL Server

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 Configure subscription synchronization	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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ESENT	SQL
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.	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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

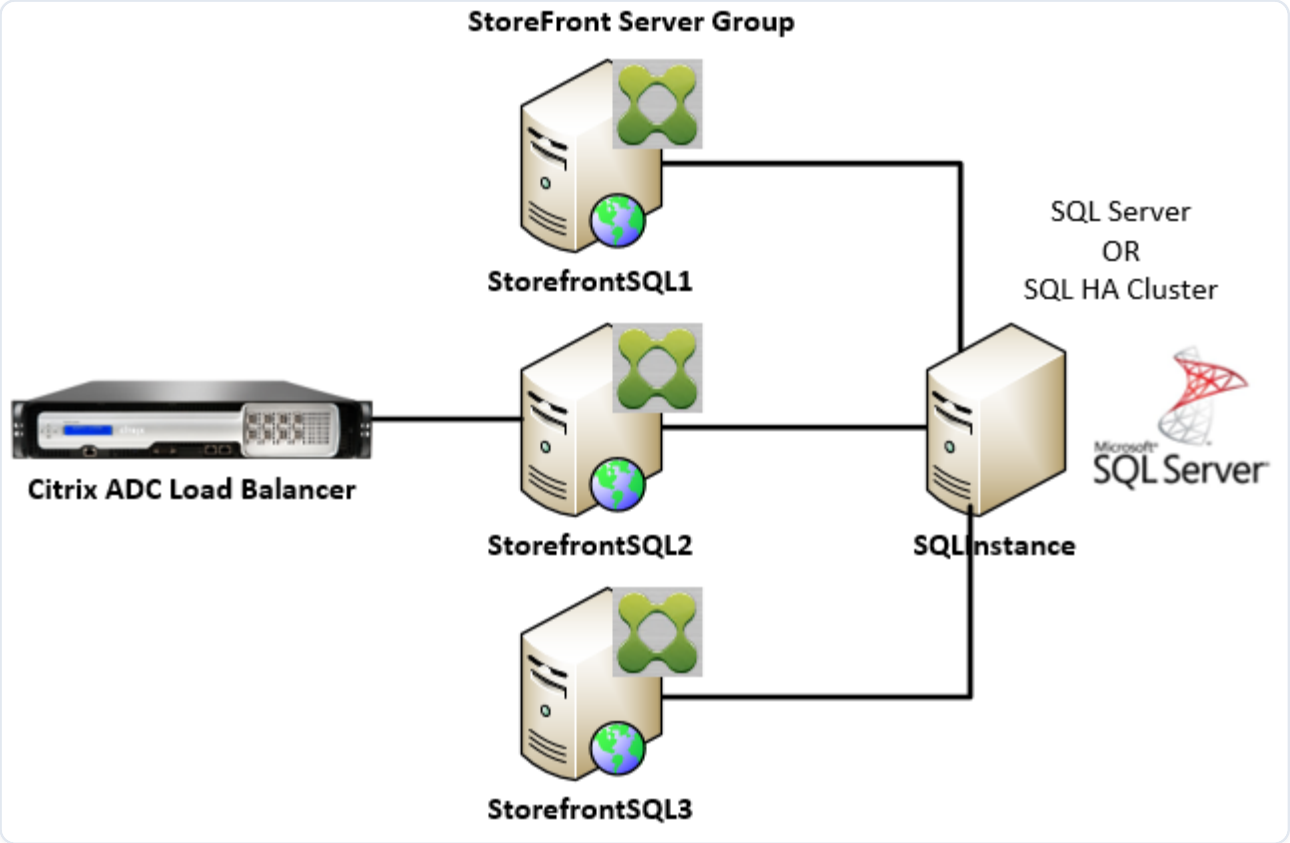
SCENARIO 2: SINGLE STOREFRONT SERVER AND A LOCAL MICROSOFT SQL SERVER INSTANCE INSTALLED

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



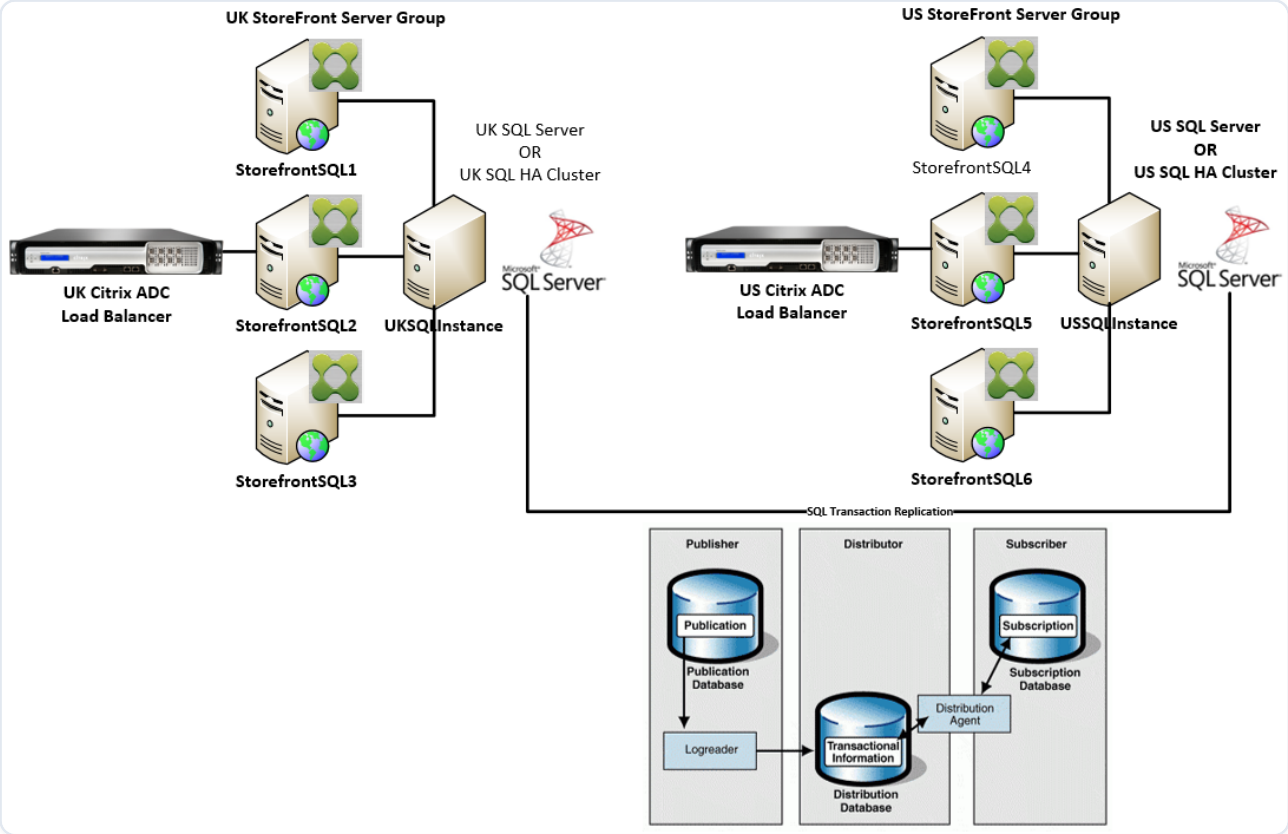
SCENARIO 4: MULTIPLE STOREFRONT SERVER GROUPS AND A DEDICATED MICROSOFT SQL SERVER INSTANCE IN EACH DATA CENTER PER SERVER GROUP

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

```
# Create Local Group for StoreFront servers on DB Server

$LocalGroupName = "StoreFrontServers"

$Description = "Contains StoreFront Server Machine Accounts or StoreFront
AppPool Virtual Accounts"



# Check whether the Local Group Exists

if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))

{

    Write-Host "$LocalGroupName already exists!" -ForegroundColor "Yellow"

}

else

{
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Write-Host "Creating $LocalGroupName local security group"
-ForegroundColor "Yellow"



# Create Local User Group

$Computer = [ADSI]"WinNT://$env:ComputerName,Computer"

$LocalGroup = $Computer.Create("group",$LocalGroupName)

$LocalGroup.setinfo()

$LocalGroup.description = $Description

$Localgroup.SetInfo()

Write-Host "$LocalGroupName local security group created" -ForegroundColor
"Green"

}

$Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"



# Add IIS APPPOOL\DefaultAppPool

$objAccount = New-Object System.Security.Principal.NTAccount("IIS
APPPOOL\DefaultAppPool")

$StrSID =
$objAccount.Translate([System.Security.Principal.SecurityIdentifier])

$DefaultSID = $StrSID.Value



$Account = [ADSI]"WinNT://$DefaultSID"

$Group.Add($Account.Path)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
# Add IIS APPPOOL\Citrix Receiver for Web

$objAccount = New-Object System.Security.Principal.NTAccount("IIS
APPPOOL\Citrix Receiver for Web")

$StrSID =
$objAccount.Translate([System.Security.Principal.SecurityIdentifier])

$WebRSID = $StrSID.Value



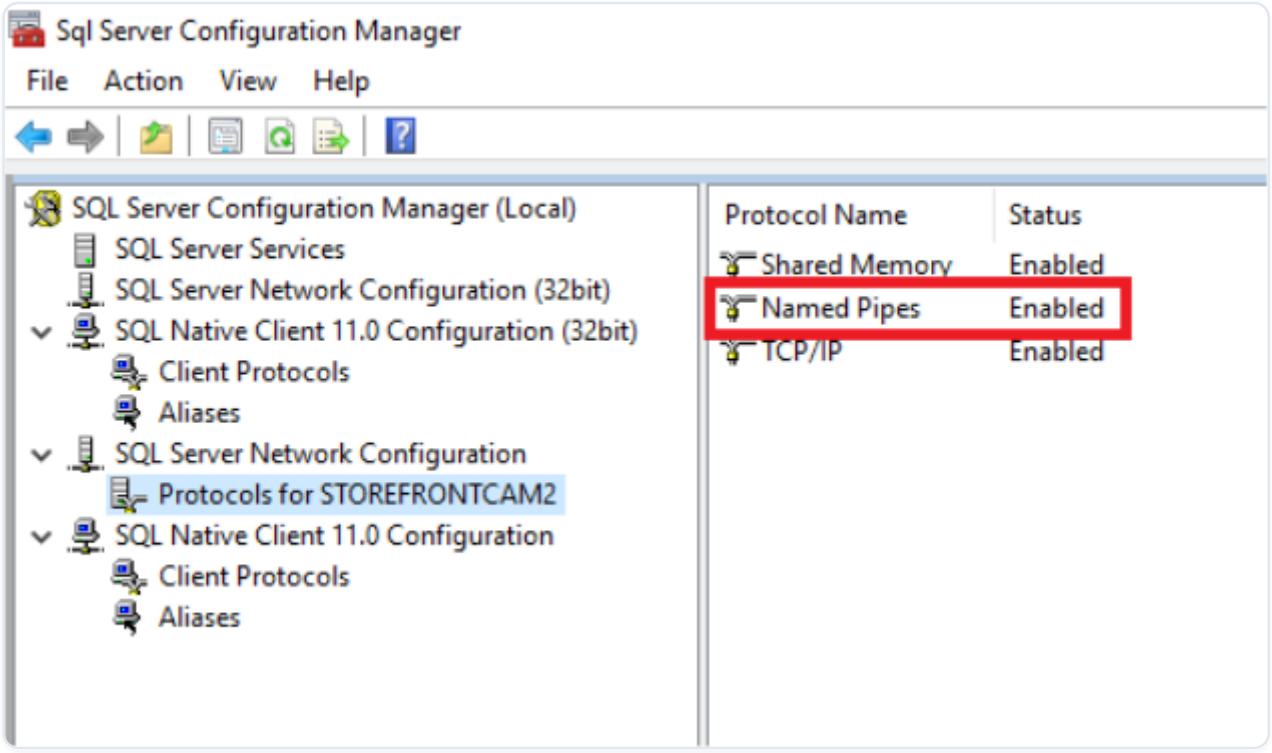
$Account = [ADSI]"WinNT://$WebRSID"

$Group.Add($Account.Path)



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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

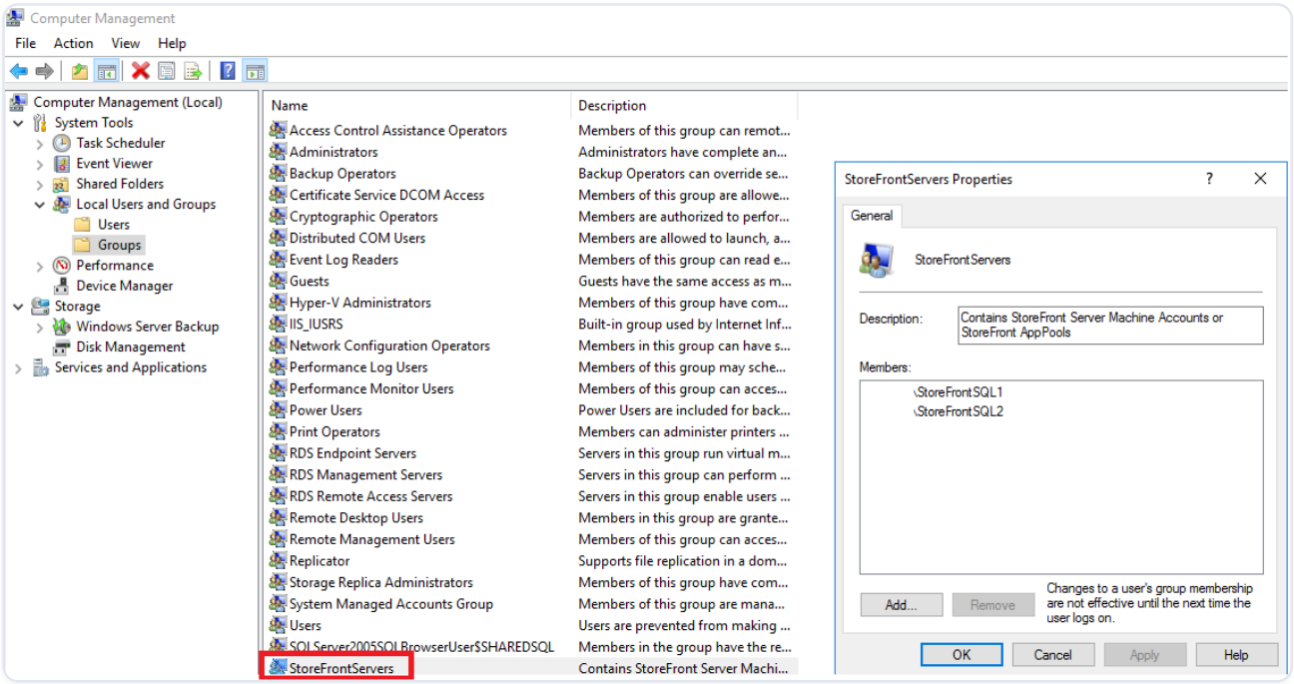
Ensure the Windows firewall rules are correctly configured to allow SQL server connections using either a specific port or dynamic ports. Refer to Microsoft documentation for how to do this in your environment.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
function Add-RemoteSTFMachineAccounts

{

[CmdletBinding()]

param([Parameter(Mandatory=$True)][string]$Domain,

[Parameter(Mandatory=$True)][array]$StoreFrontServers)



# Create Local Group for StoreFront servers on DB Server

$LocalGroupName = "StoreFrontServers"

$Description = "Contains StoreFront Server Machine Accounts or StoreFront
AppPool virtual accounts"



# Check whether the Local Security Group already exists

if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))

{

    Write-Host "$LocalGroupName already exists!" -ForegroundColor "Yellow"

}

else

{

    Write-Host "Creating $LocalGroupName local group" -ForegroundColor
"Yellow"



    # Create Local Security Group

    $Computer = [ADSI]"WinNT://$env:ComputerName,Computer"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    $LocalGroup = $Computer.Create("group",$LocalGroupName)

    $LocalGroup.setinfo()

    $LocalGroup.description = $Description

    $Localgroup.SetInfo()

Write-Host "$LocalGroupName local group created" -ForegroundColor "Green"

}

Write-Host "Adding $StoreFrontServers to $LocalGroupName local group"
-ForegroundColor "Yellow"



foreach ($StoreFrontServer in $StoreFrontServers)

{

    $Group = [ADSI]"WinNT://$env:ComputerName/$LocalGroupName,group"

    $Computer = [ADSI]"WinNT://$Domain/$StoreFrontServer$"

    $Group.Add($Computer.Path)

}

Write-Host "$StoreFrontServers added to $LocalGroupName" -ForegroundColor
"Green"

}

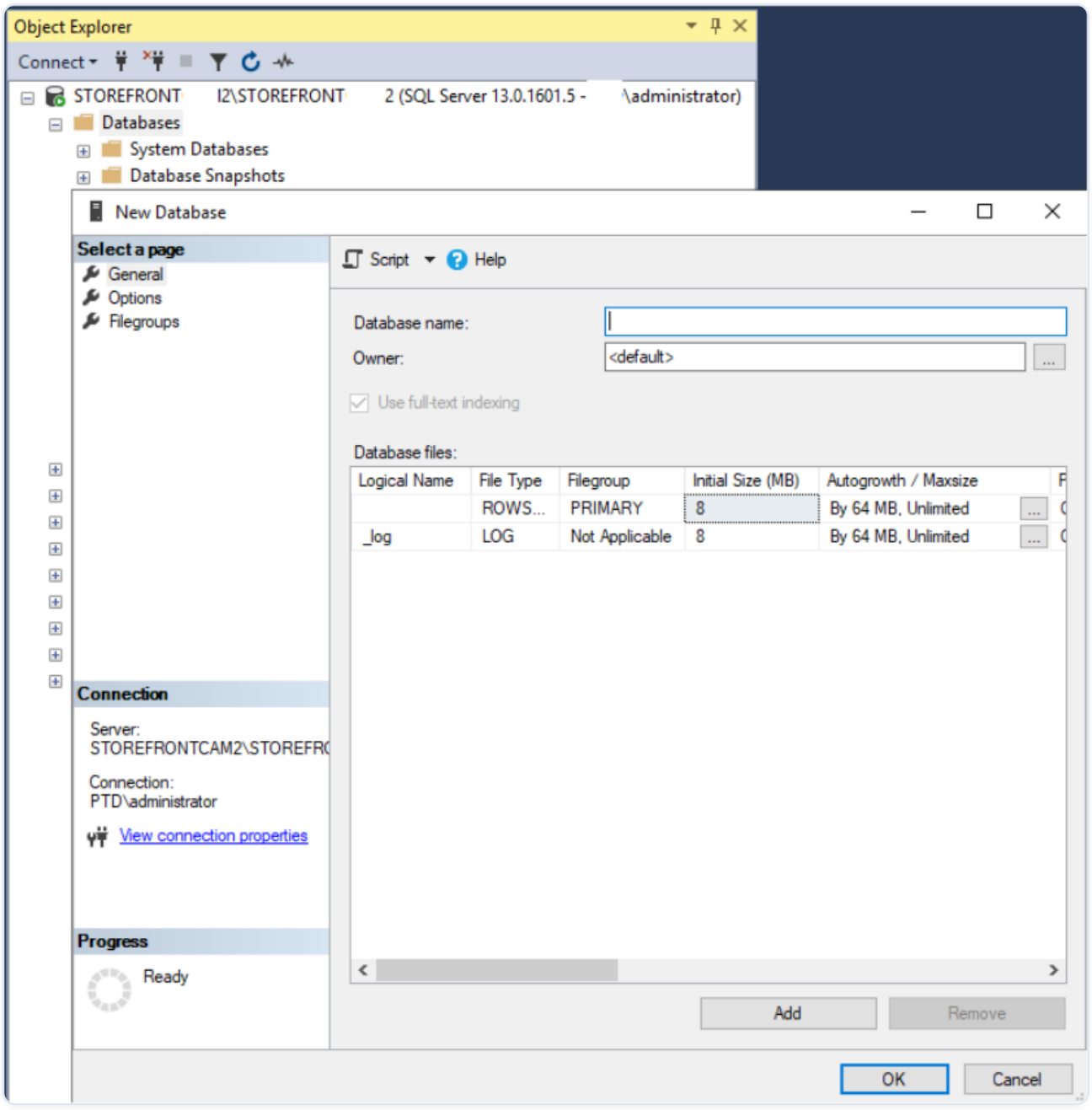
Add-RemoteSTFMachineAccounts -Domain "example" -StoreFrontServers
@("StoreFrontSQL1","StoreFrontSQL2")
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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*.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
  ```

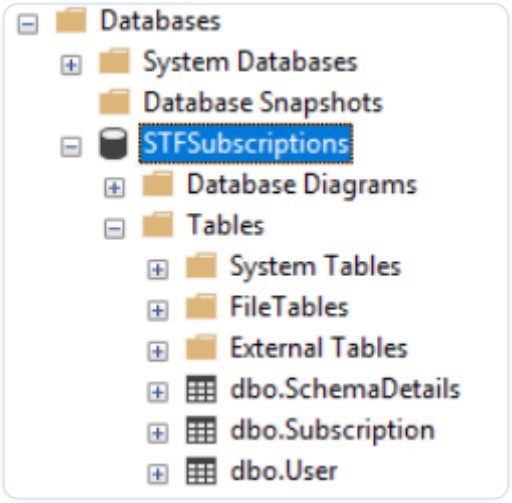
  ```
  C:\Program Files\Microsoft SQL Server\MSSQL13.SQL2016\MSSQL\DATA\STFSubscriptions.ldf
  ```

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

  ```
  CREATE LOGIN [SQL2016\StoreFrontServers] FROM WINDOWS;
  ```

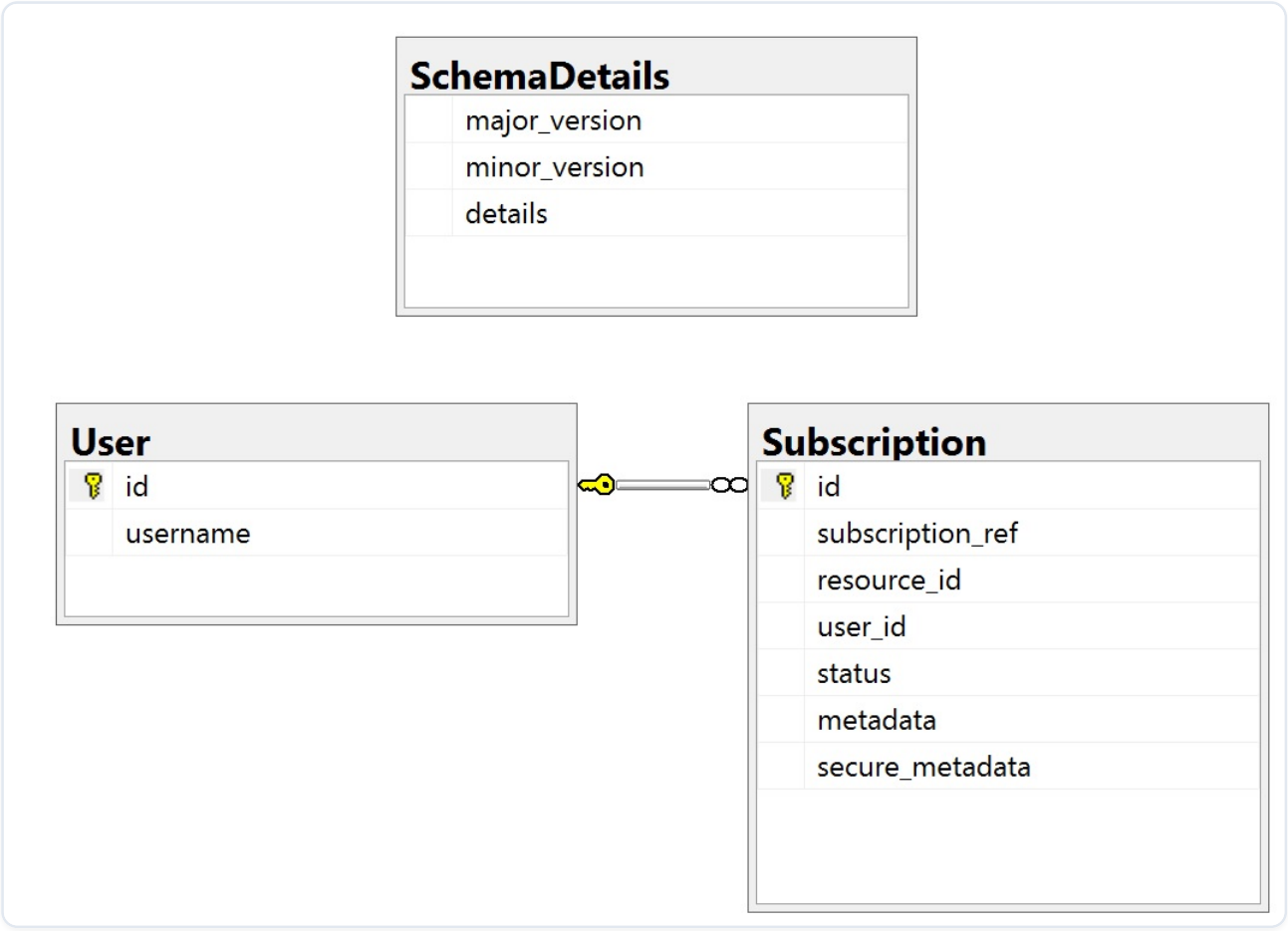
  ```
  ALTER LOGIN [SQL2016\StoreFrontServers]
  ```

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$SiteID = 1

$StoreVirtualPath = "/Citrix/Store1"



# Sets SQL DB Connection String

$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath
$StoreVirtualPath



# Removes the SQL DB Connection string and reverts back to using ESENT

Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject
-UseLocalStorage

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**

```
$SiteID = 1

$VirtualPath= "/Citrix/Store1"

$DBName = "Store1"

$DBServer = "SQL2016Ent"

$DBLocalServer = "localhost"

$SQLInstance = "StoreFrontInstance"



# For a remote database instance
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$ConnectionString = "Server=$DBServer\
$SQLInstance;Database=$DBName;Trusted_Connection=True;"
```

OR

```
# For a locally installed database instance

$ConnectionString = "$DBLocalServer\
$SQLInstance;Database=$DBName;Trusted_Connection=True;"



# Sets SQL DB Connection String

$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath "/Citrix/
Store"

Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject
-ConnectionString $ConnectionString

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



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

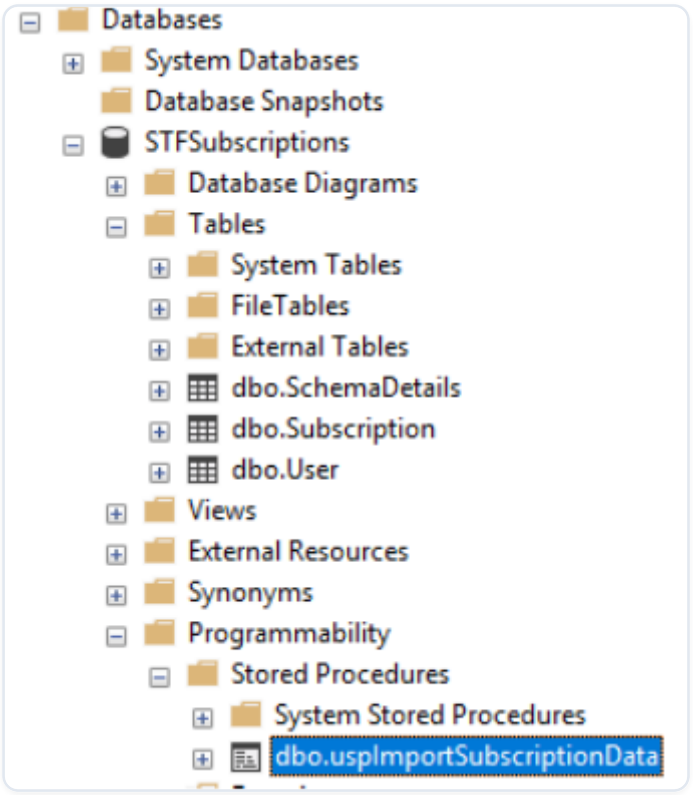
Before executing *Create-ImportSubscriptionDataSP.sql*, change `USE [STFSubscriptions]` to match the database under which you want to create the Stored Procedure.

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.

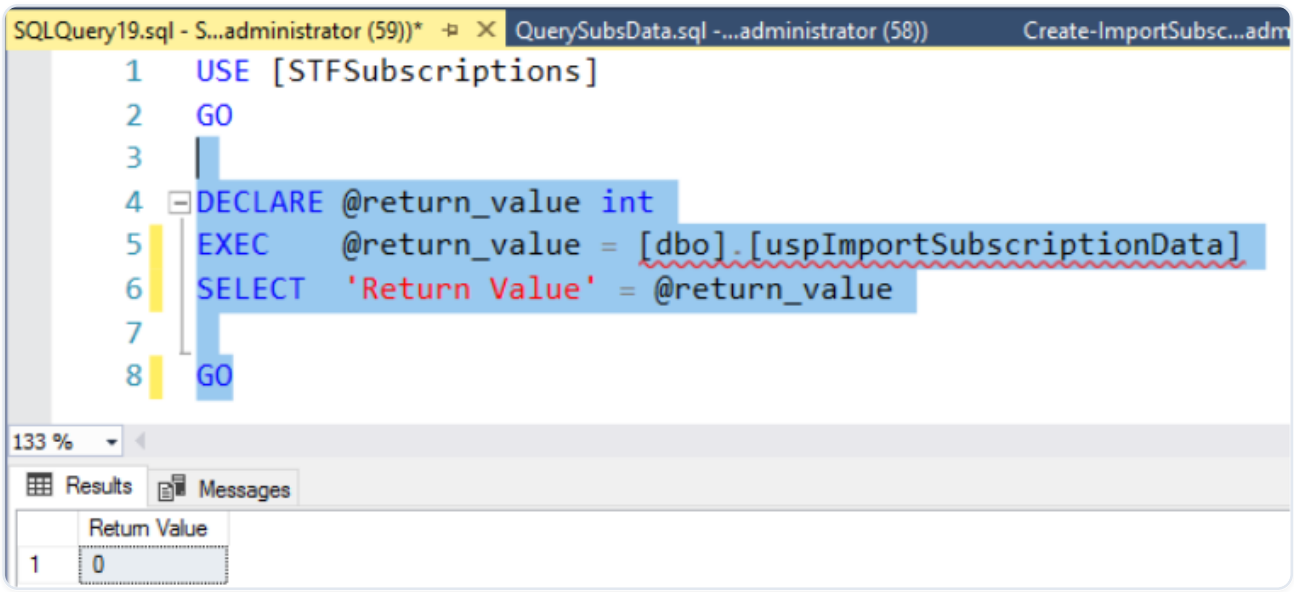
After successful creation of the Stored Procedure the following message is shown in the SQL console, and the ImportSubscriptionDataSP Stored Procedure is added to the database:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
SELECT COUNT(*) AS TotalSubscriptions

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

```
SELECT COUNT(*) AS TotalUsers

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.

```
-- Get all SQL subscription records

Use [STFSubscriptions]

SELECT * FROM [Subscription]

SELECT * FROM [User]
```

```
-- Get all subscription records for a particular user SID

Use [STFSubscriptions]

SELECT * FROM [Subscription]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
INNER JOIN [User]

ON [Subscription].[user_id] = [User].[id]

WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-xxxx'



-- Get total number of Subscription records for a particular user SID

Use [STFSubscriptions]

SELECT COUNT(Subscription.id)

FROM [Subscription]

INNER JOIN [User]

ON [Subscription].[user_id] = [User].[id]

WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-xxxx'
```

```
-- Get all subscription records for a particular delivery controller

Use [STFSubscriptions]

SELECT * FROM [Subscription]

WHERE [resource_id] LIKE 'DeliveryController.%'



-- OR for aggregated resources use the name of the aggregation group

Use [STFSubscriptions]

SELECT * FROM [Subscription]

WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-- Get all subscription records for a particular application

Use [STFSubscriptions]

SELECT * FROM [Subscription]

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 redundant 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.

```
-- Update the site name used in all subscriptions.

Use [STFSubscriptions]

UPDATE [Subscription]

SET [resource_id] = REPLACE(resource_id,'OldSiteName.','NewSiteName.')

WHERE [resource_id] LIKE 'OldDeliveryController.%'
```

```
-- After enabling multi-site aggregation, update the resource_id

Use [STFSubscriptions]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
UPDATE [Subscription]

SET [resource_id] =
REPLACE(resource_id,'OldDeliveryController.','DefaultAggregationGroup.')

WHERE [resource_id] LIKE 'OldDeliveryController.%'
```

```
-- Delete all subscription records for a particular site

Use [STFSubscriptions]

DELETE FROM [Subscription]

WHERE [resource_id] LIKE 'site.%'
```

```
-- OR for aggregated resources use the name of the aggregation group

Use [STFSubscriptions]

DELETE FROM [Subscription]

FROM [Subscription]

WHERE [resource_id] LIKE 'DefaultAggregationGroup.%'
```

```
-- Delete all subscription records for a particular application

Use [STFSubscriptions]

DELETE FROM [Subscription]

FROM [Subscription]

WHERE [resource_id] LIKE '%.Application'
```

```
-- Delete all subscription records for an application published via a
specific site

Use [STFSubscriptions]
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
DELETE FROM [Subscription]

FROM [Subscription]

WHERE [resource_id] = 'Site.Application'
```

```
-- Delete all subscription records for a particular user SID

-- relies on cascade to delete records from [Subscription]

Use [STFSubscriptions]

DELETE FROM [User]

WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-xxxx'
```

```
-- Delete ALL subscription data from a particular database and reset the
primary key clustered index to start numbering from 0.

-- USE WITH EXTREME CARE AND NOT ON LIVE PRODUCTION DATABASES.

-- Can be useful whilst debugging data import issues to start with a clean
database.



Use [STFSubscriptions]

DELETE FROM [Subscription]

DBCC CHECKIDENT ([Subscription], RESEED, 0)

DELETE FROM [User]

DBCC CHECKIDENT ([User], RESEED, 0)
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Subscriptions synchronization

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:

   ```
   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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/Citrix/
Store"

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:

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/Citrix/
Store"

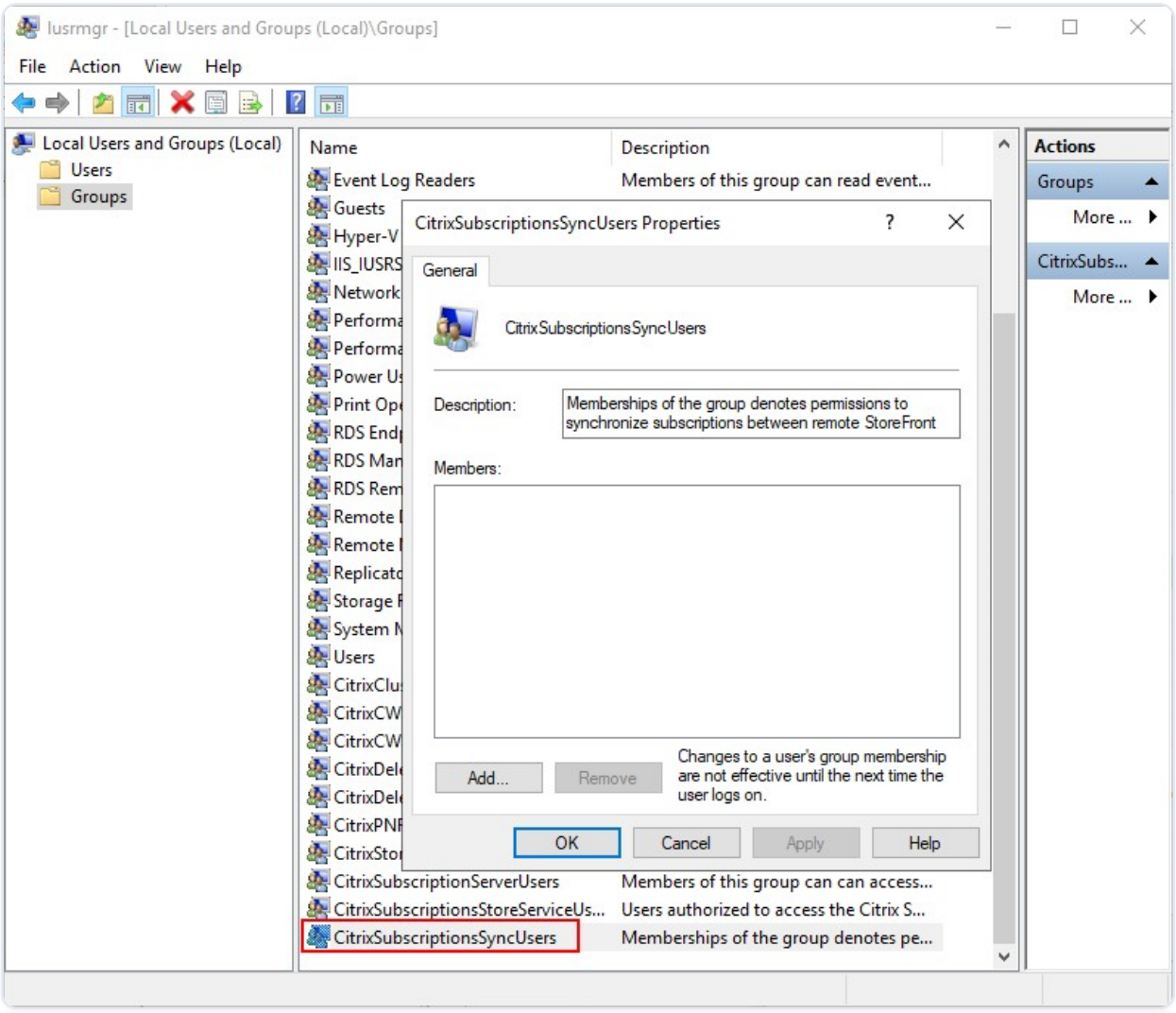
Add-STFSubscriptionSynchronizationSource -FriendlyName
"SyncFromUSStore" -StoreService $StoreObject
-RemoteStoreFrontAddress "USloadbalancedStoreFront.example.com"
```

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 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)>`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



5. When you have configured the schedule as you intend, use the Citrix StoreFront management console, or the PowerShell below, to propagate the subscription synchronization schedules and sources to the all other servers in the group.

```
Publish-STFServerGroupConfiguration
```

   For more information about propagating changes in a multiple server StoreFront deployment, see Configure server groups.

6. To remove an existing subscription synchronization schedule, run the following command, then propagate the configuration change to the other StoreFront servers in the deployment.

```
Clear-STFSubscriptionSynchronizationSchedule

Publish-STFServerGroupConfiguration
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. To remove a specific subscription synchronization source, run the following command, then propagate the configuration change to the other StoreFront servers in the deployment.

```
Remove-STFSubscriptionSynchronizationSource -FriendlyName
"SyncFromUKStore"

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.

```
Clear-STFSubscriptionSynchronizationSource

Publish-STFServerGroupConfiguration
```

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

```
Get-STFSubscriptionSynchronizationSchedule
```

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

```
Get-STFSubscriptionSynchronizationSource
```

Upgrade StoreFront

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 2607 from:

- StoreFront 2603
- StoreFront 2511
- StoreFront 2507 LTSR (any CU)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- StoreFront 2503.1
- StoreFront 2503
- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

Upgrade a StoreFront server group during scheduled maintenance downtime

To upgrade a StoreFront server group of multiple servers, during scheduled downtime, complete the following steps:

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

4. Enable user access to the upgraded server group by enabling the load balancing URL.

Upgrade a StoreFront server group without scheduled downtime

Simultaneously upgrading the servers in a live StoreFront server group is not supported. However you can achieve a live upgrade by creating a new sever group with identical configuration, upgrading it then migrating user connections to the new server group. Users need to re-authenticate to StoreFront when they are transferred between server groups.

For example to upgrade a StoreFront server group of three servers A, B, and C:

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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, favorites can be lost (step 9). This can cause the new server group to have a slightly outdated copy of the subscriptions database after upgrade, and any new favorites to be lost.

This has no functional impact because favorites data is not essential for users to be able to log on and launch resources. Users would, however, need to favorite 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 favorite 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Things to consider when exporting and importing a StoreFront configuration

- Do you currently use any Citrix® published authentication SDK examples, such as Magic Word authentication or third party authentication customizations? If so, you must install these packages on ALL importing servers BEFORE importing a configuration containing extra authentication methods. The configuration import fails if required authentication SDK packages are not installed on any of the importing servers. If importing a configuration into a server group, install the authentication packages on all members of the group.
- You can encrypt or decrypt your configuration backups. The exporting and importing PowerShell cmdlets support both use cases.
- You can decrypt encrypted backups (.ctxzip) later, but StoreFront cannot re-encrypt unencrypted backup files (.zip). If an encrypted backup is required, perform the export again using a PowerShell credential object containing a password of your choice.
- The SiteID of the website in IIS where StoreFront is currently installed (exporting server) must match the SiteID of the target website in IIS (importing server) where you want to restore the backed up StoreFront configuration.

PowerShell cmdlets

Export-STFConfiguration

PARAMETER	DESCRIPTION
-TargetFolder (String)	The export path to the backup archive. Example: "\$env:userprofile\desktop\"
-Credential (PSCredential Object)	Specify a credential object to create an encrypted .ctxzip backup archive during export. The PowerShell credential object should contain the password to use for encryption and decryption. Do not use **-Credential** at the same time as the **-NoEncryption** parameter. Example: \$CredObject
-NoEncryption (Switch)	Specify that the backup archive should be an unencrypted .zip. Do not use **-NoEncryption** at the same time as the **-Credential** parameter.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

PARAMETER	DESCRIPTION
-ZipFileName (String)	The name for the StoreFront configuration backup archive. Do not add a file extension, such as .zip or .ctxzip. The file extension is added automatically depending on whether the **-Credential** or **-NoEncryption** parameter is specified during export. Example: "backup"
-Force (Boolean)	This parameter automatically overwrites backup archives with the same file name as existing backup files already present in the specified export location.

IMPORTANT:

The **SiteID** parameter found in StoreFront 3.5 was deprecated in version 3.6. It is no longer necessary to specify the **SiteID** when performing an import, as the SiteID contained within the backup archive is always be used. Ensure the SiteID matches the existing StoreFront website already configured within IIS on the importing server. **SiteID 1** to **SiteID 2** configuration imports are NOT supported.

Import-STFConfiguration

PARAMETER	DESCRIPTION
-ConfigurationZip (String)	The full path to the backup archive you want to import. This should also include the file extension. Use .zip for unencrypted and .ctxzip for encrypted backup archives. Example: `$env:userprofile\desktop\backup.ctxzip`
-Credential (PSCredential Object)	Specify a credential object to decrypt an encrypted backup during import. Example: `$CredObject`
-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: `https://<importingserver>.example.com`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Unprotect-STFConfigurationBackup

PARAMETER	DESCRIPTION
-TargetFolder (String)	The export path to the backup archive. Example: `$env:userprofile\desktop`
-Credential (PSCredential Object)	Use this parameter to create an unencrypted copy of the encrypted backup archive. Specify the PowerShell credential object containing the password to use for decryption. Example: `$CredObject`
-EncryptedConfigurationZip (String)	The full path of the encrypted backup archive you want to decrypt. You must specify the file extension .ctxzip. Example: `$env:userprofile\\desktop\ \backup.ctxzip`
-OutputFolder (String)	The path to create an unencrypted copy (.zip) of the encrypted (.ctxzip) backup archive. The original encrypted copy of the backup is retained so it can be reused. Do not specify a file name and file extension for the unencrypted copy. Example: `$env:userprofile\desktop`
-Force (Boolean)	This parameter automatically overwrites backup archives with the same file name as existing backup files already present in the specified export location.

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:

```
$env:PSModulePath =
[Environment]::GetEnvironmentVariable('PSModulePath','Machine')

$SDKModules = 'C:\Program Files\Citrix\Receiver
StoreFront\PowerShellSDK\Modules\Citrix.StoreFront'
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Import-Module "$SDKModules\Citrix.StoreFront.psd1" -verbose

Import-Module
"$SDKModules.Authentication\Citrix.StoreFront.Authentication.psd1"
-verbose

Import-Module "$SDKModules.Roaming\Citrix.StoreFront.Roaming.psd1"
-verbose

Import-Module "$SDKModules.Stores\Citrix.StoreFront.Stores.psd1" -verbose

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.

```
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.

```
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.

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

Copy the backup.zip file to the desktop of server B.

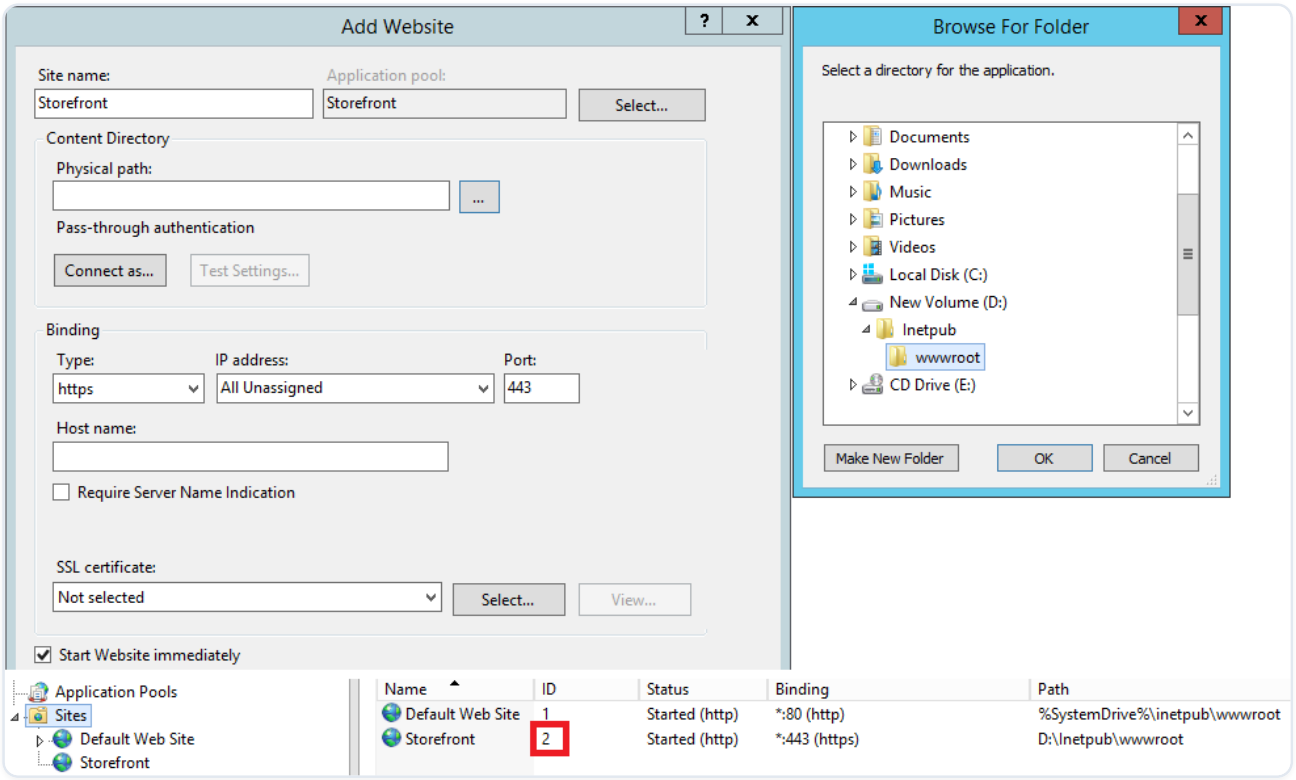
© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

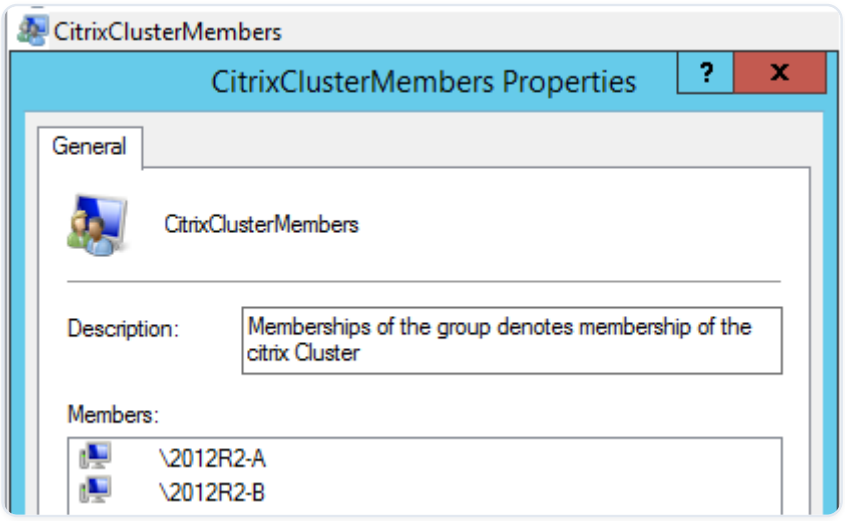
```
Import-STFConfiguration -configurationZip
"$env:userprofile\desktop\backup.ctxzip" -HostBaseURL "https://
serverB.example.com"
```

Server group scenarios

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

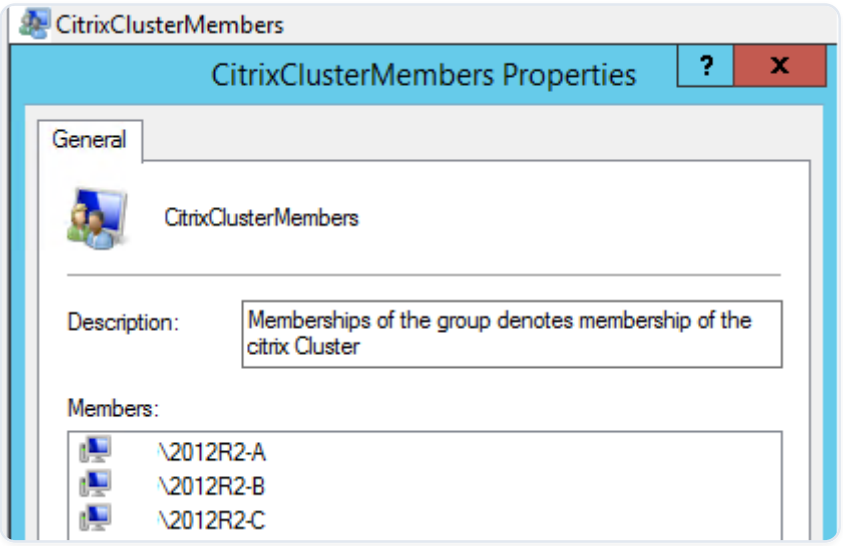
A previous configuration backup was taken while only two StoreFront servers, 2012R2-A and 2012R2-B, were members of the server group. Within the backup archive is a record of the **CitrixClusterMembership** at the time the backup was taken containing only the two original servers 2012R2-A and 2012R2-B. 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

```
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

```
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.

```
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name

$Password = Read-Host -Prompt "Enter password" -AsSecureString

$CredObject = New-Object System.Management.Automation.PSCredential($User,
$Password)
```

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

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

Create an identical PowerShell Credential Object within your PowerShell session on the importing server.

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

Unprotect an existing encrypted backup archive

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name

$Password = Read-Host -Prompt "Enter password" -AsSecureString

$CredObject = New-Object System.Management.Automation.PSCredential($User,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$Password)

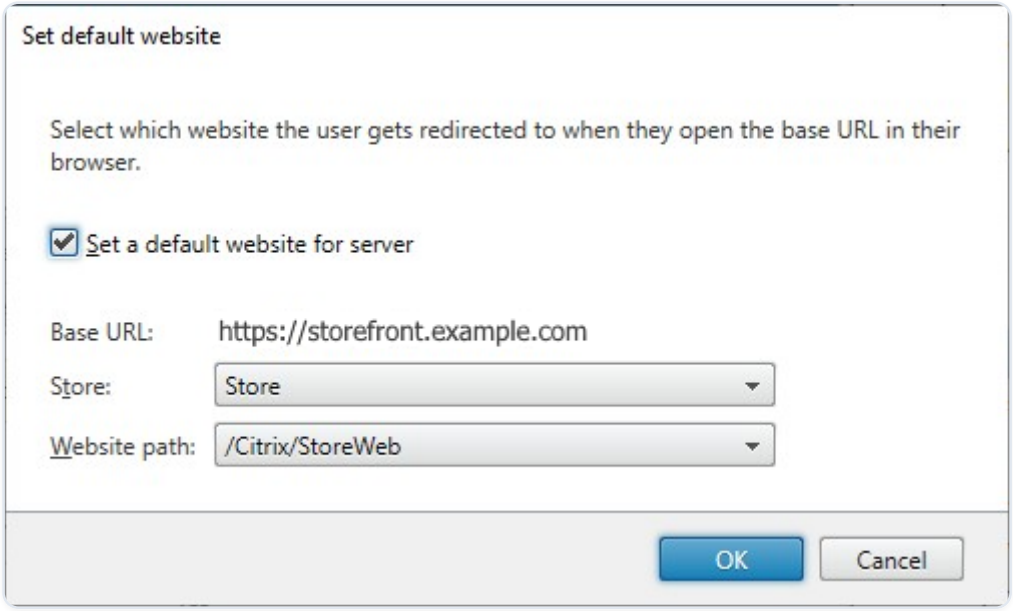


Unprotect-STFConfigurationExport -encryptedConfigurationZip
"$env:userprofile\desktop\backup.ctxzip" -credential $CredObject
-outputFolder "c:\StoreFrontBackups" -Force
```

Default website for deployment

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
    a. Select **Set a default website for server**
    b. Select a **Store**
    c. Select a **Website path**.
4. Select **OK** to save the changes.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

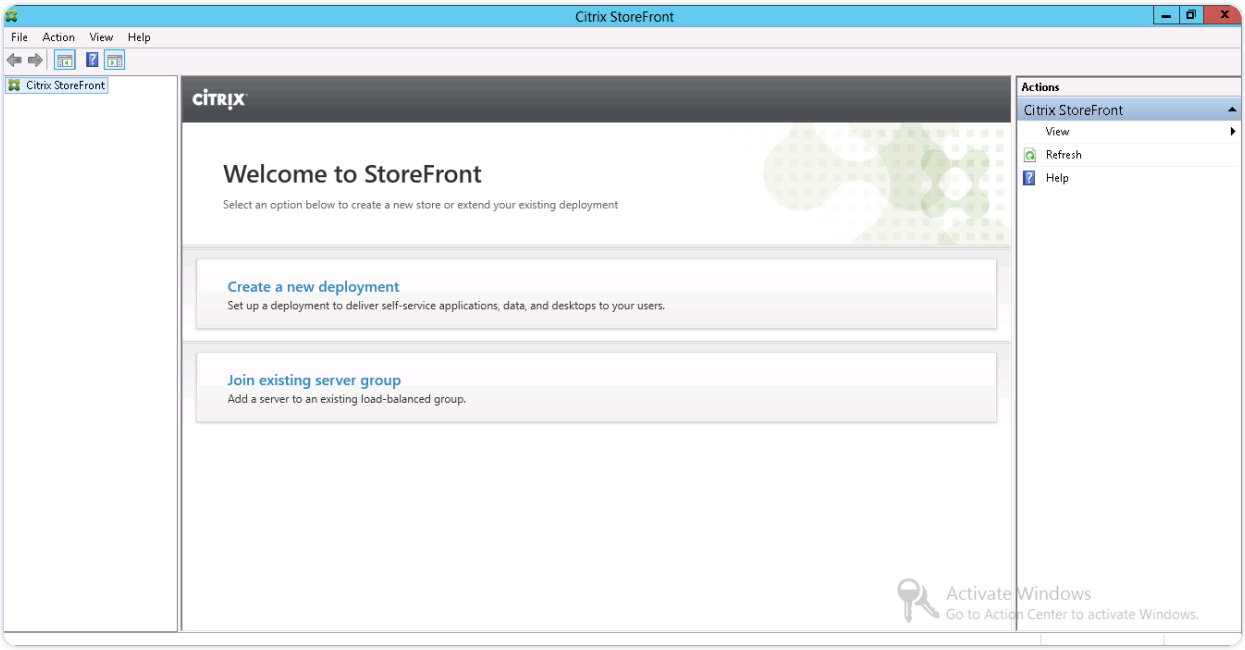
Reset a server to factory defaults

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.

```
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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

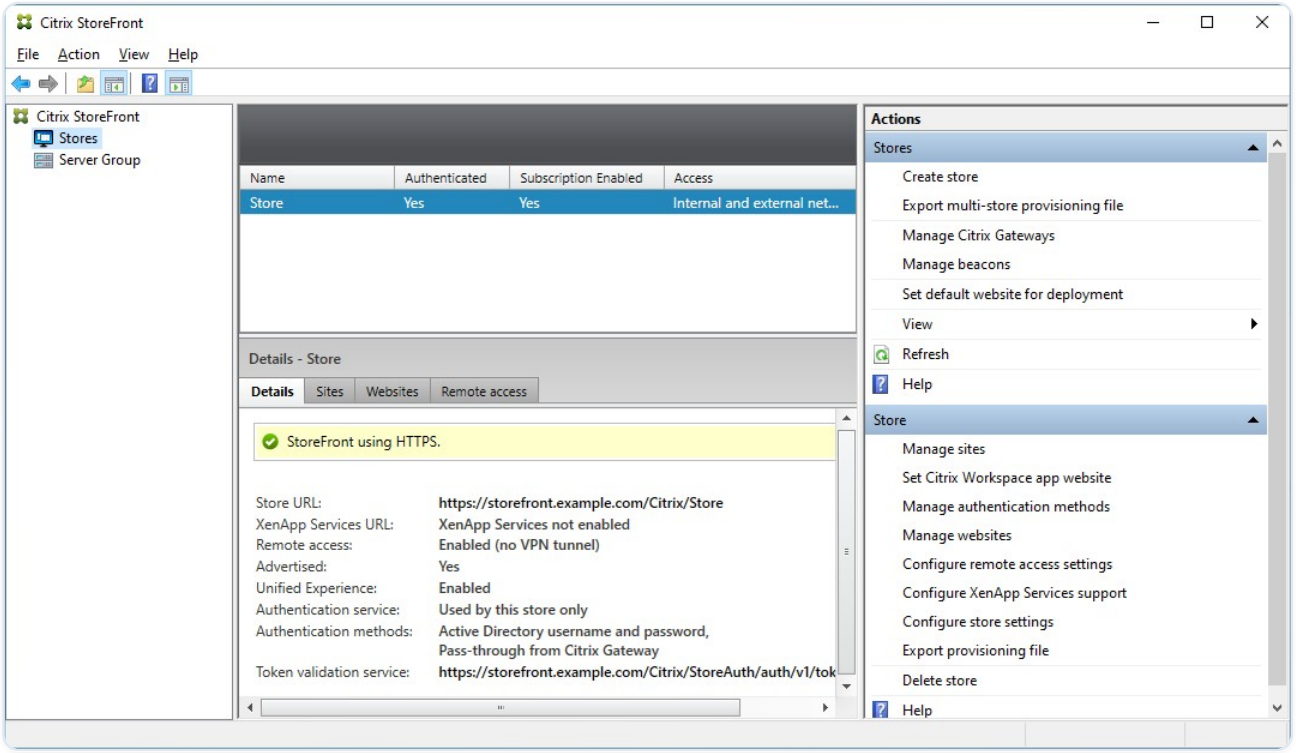
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage stores

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TAB	DETAIL
Sites	Lists all sites that have been configured for the store
Websites	Lists all websites 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
Manage sites	Add and remove sites.
Set Citrix Workspace app website	Configure which website is used when accessing the store using Citrix Workspace app
Manage authentication methods	Choose which methods users can use to authenticate to the store
Manage websites	Manage the website used to access the store
Configure remote access settings	Configure access to stores through Citrix Gateway for users connecting from public networks.
Configure XenApp® services support	Enable or disable the XenApp services URL
Configure store settings	Opens the Configure store settings windows where you can configure Favorites, Kerberos Delegation, Optimal HDX routing, Advertise Store and Advanced Settings

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

TASK	DETAIL
Default ica settings	Configure HDX settings by adding them to default.ica
Citrix Workspace app Configuration	Use StoreFront to configure Citrix Workspace app
Configure Federated authentication service	Configure Federated authentication service (FAS) for single sign-on to VDAs

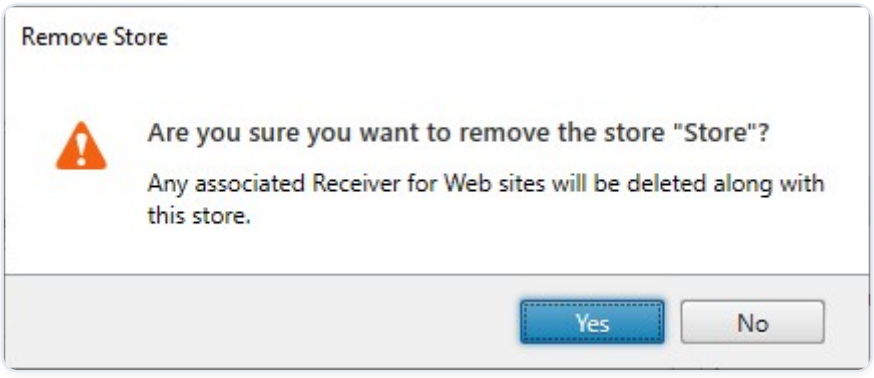
Export provisioning files

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Create store

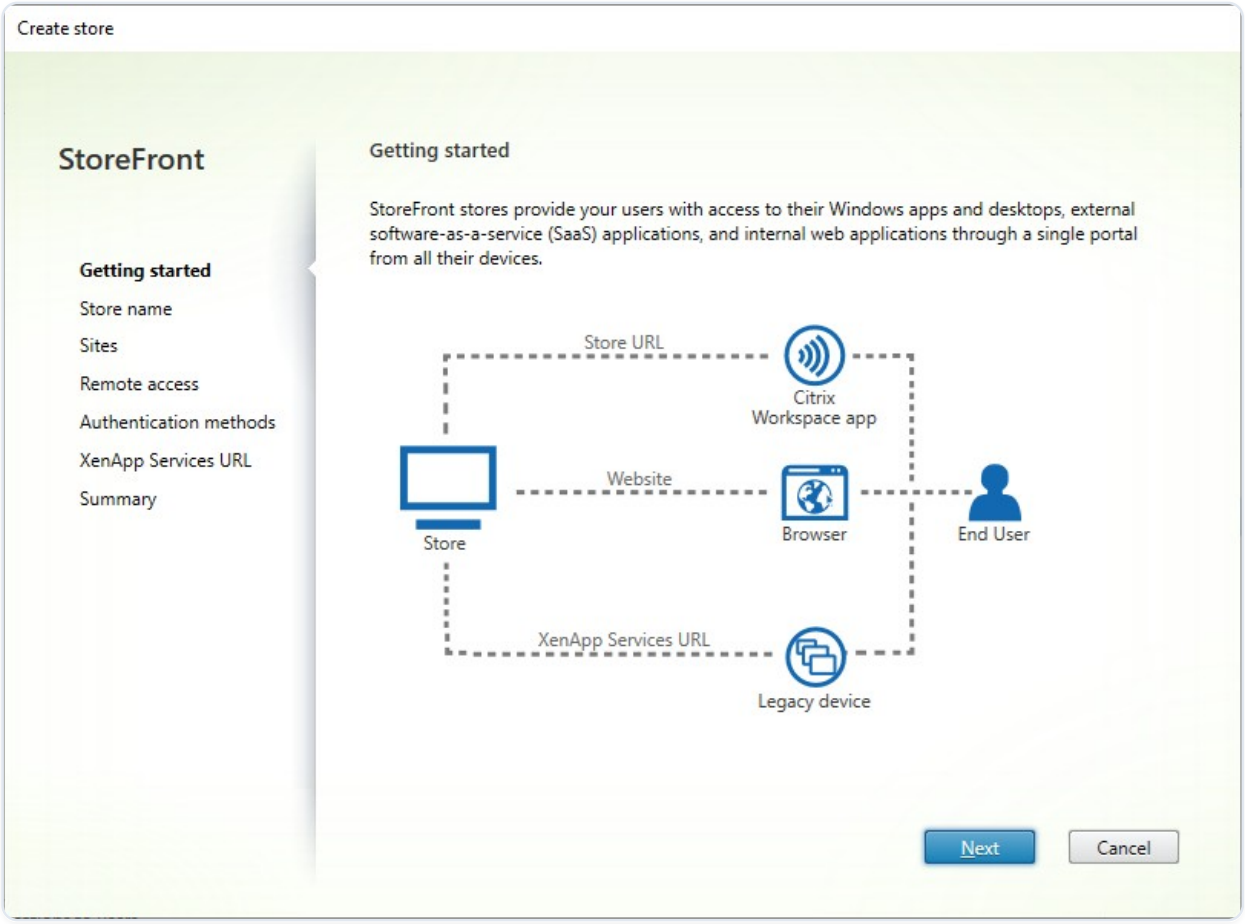
You can create as many stores as you need; for example, you can create a store for a particular group of users or to group together a specific set of resources.

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**.

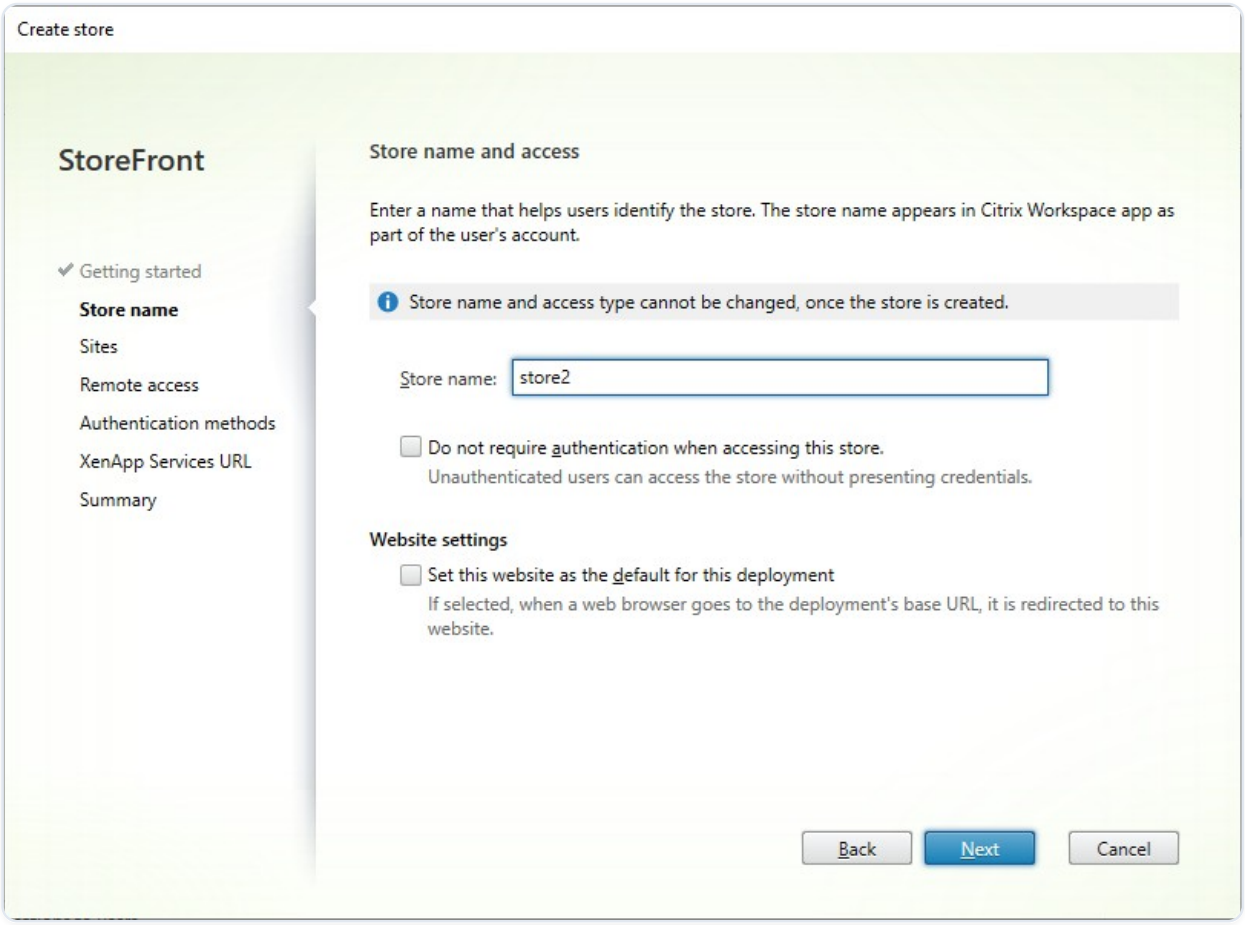


Click **Next**

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

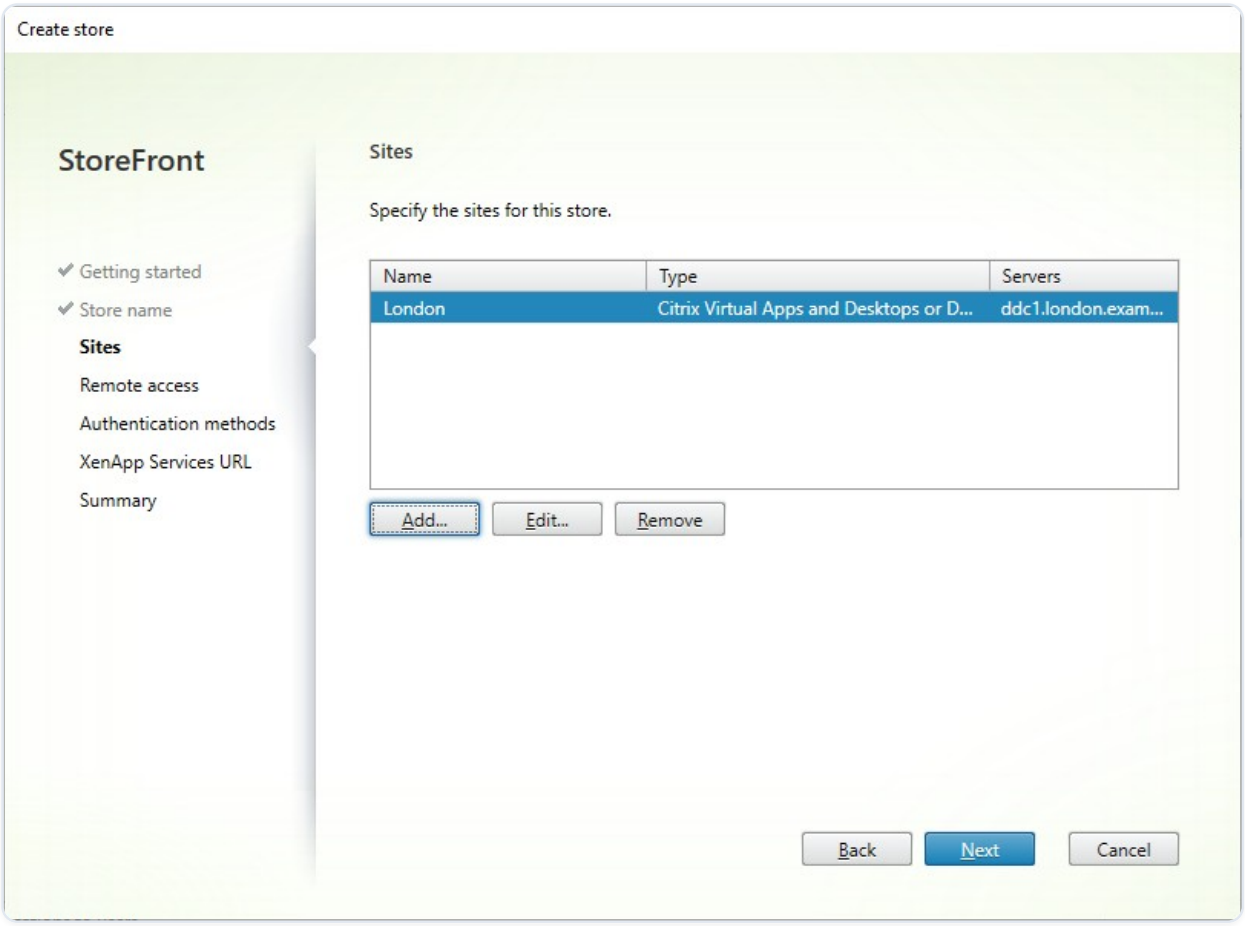
- Enter a store name
- If you wish to allow users to access the store anonymously, or unauthenticated, tick **Allow only unauthenticated users to access this store**. When you create an unauthenticated store, **Authentication Methods** and **Remote Access** pages are not available, and **Server Group 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.)



Click **Next**

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

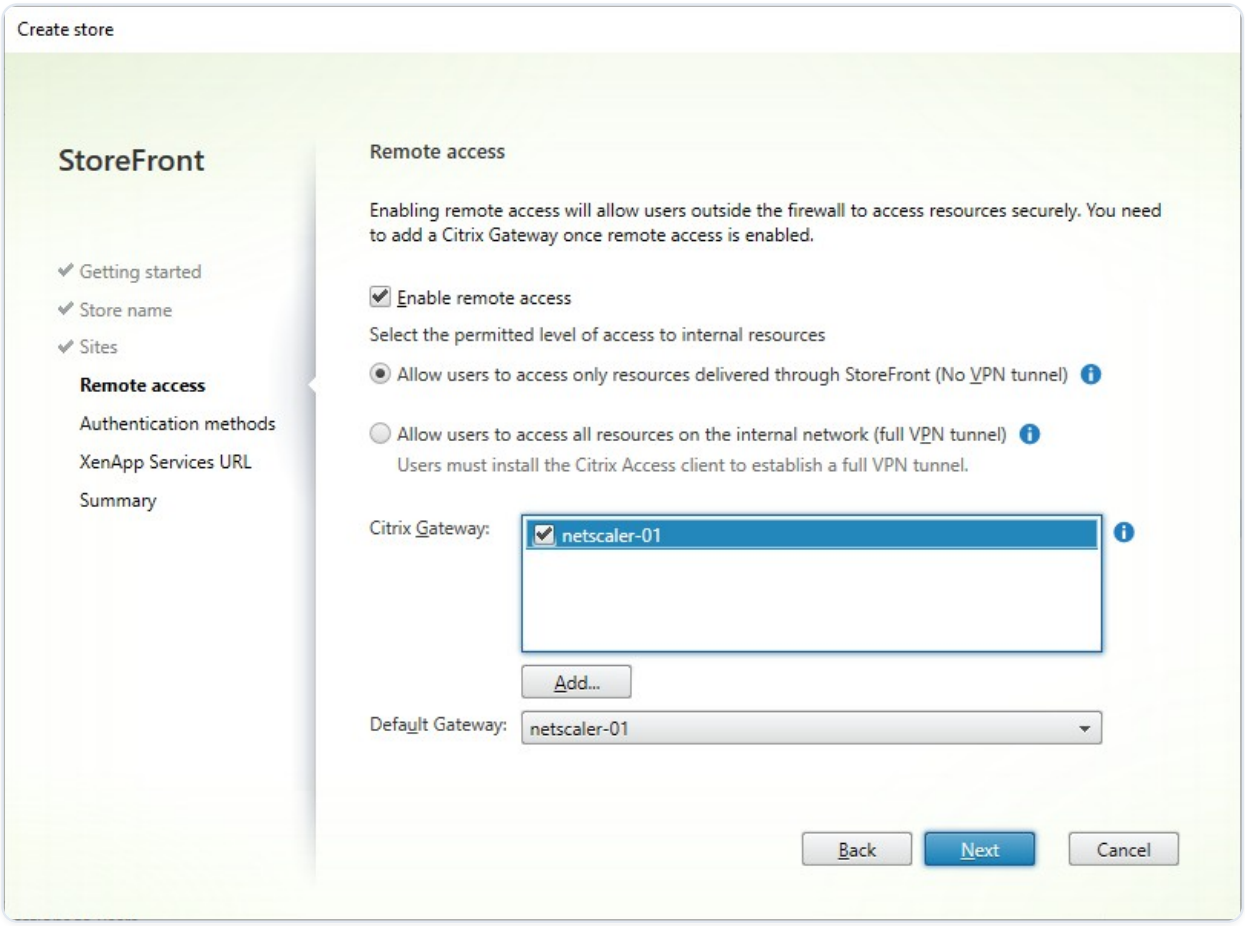
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

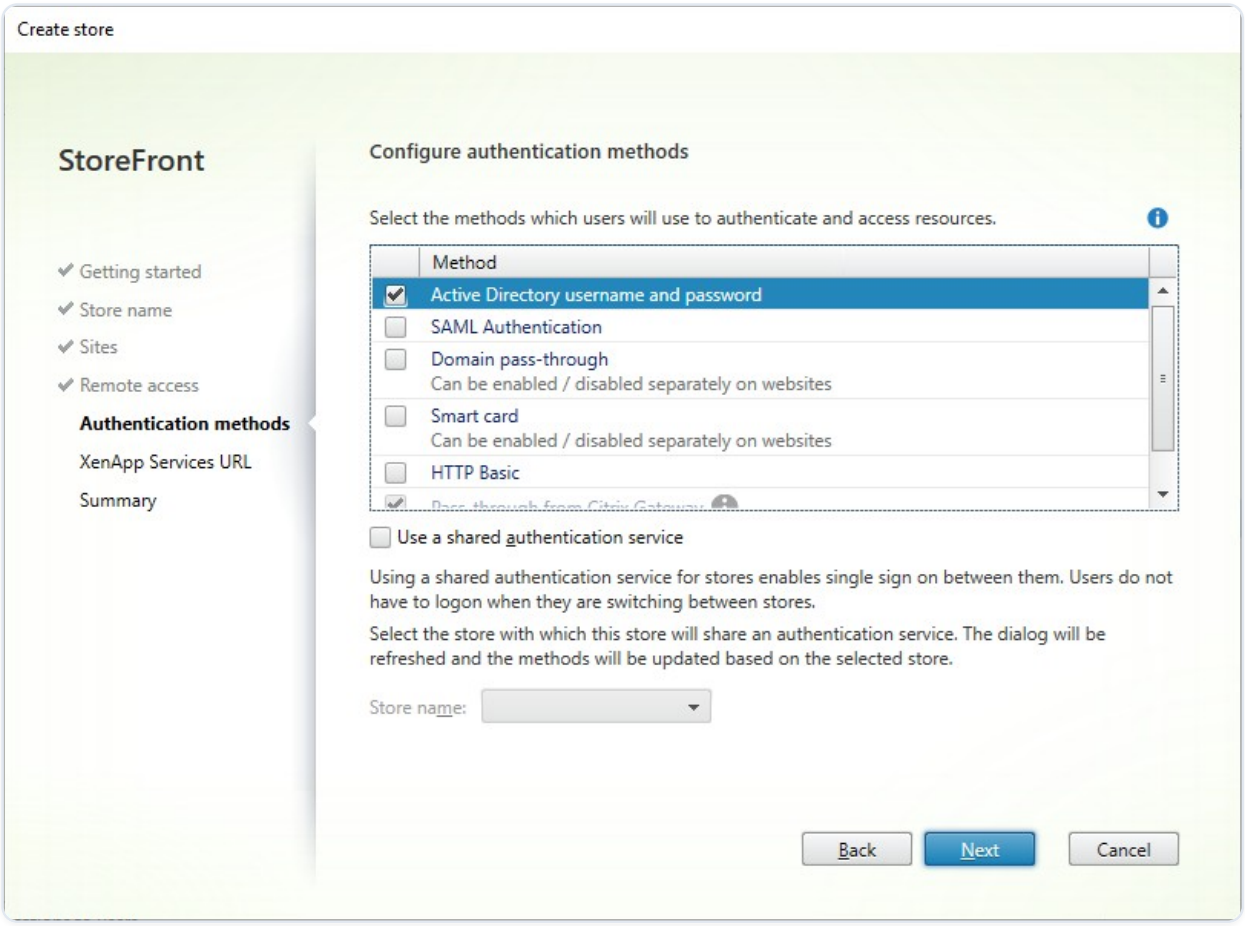


5. On the **Authentication Methods** tab, select the methods your users will use to authenticate to the store and click **Next**.

   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.

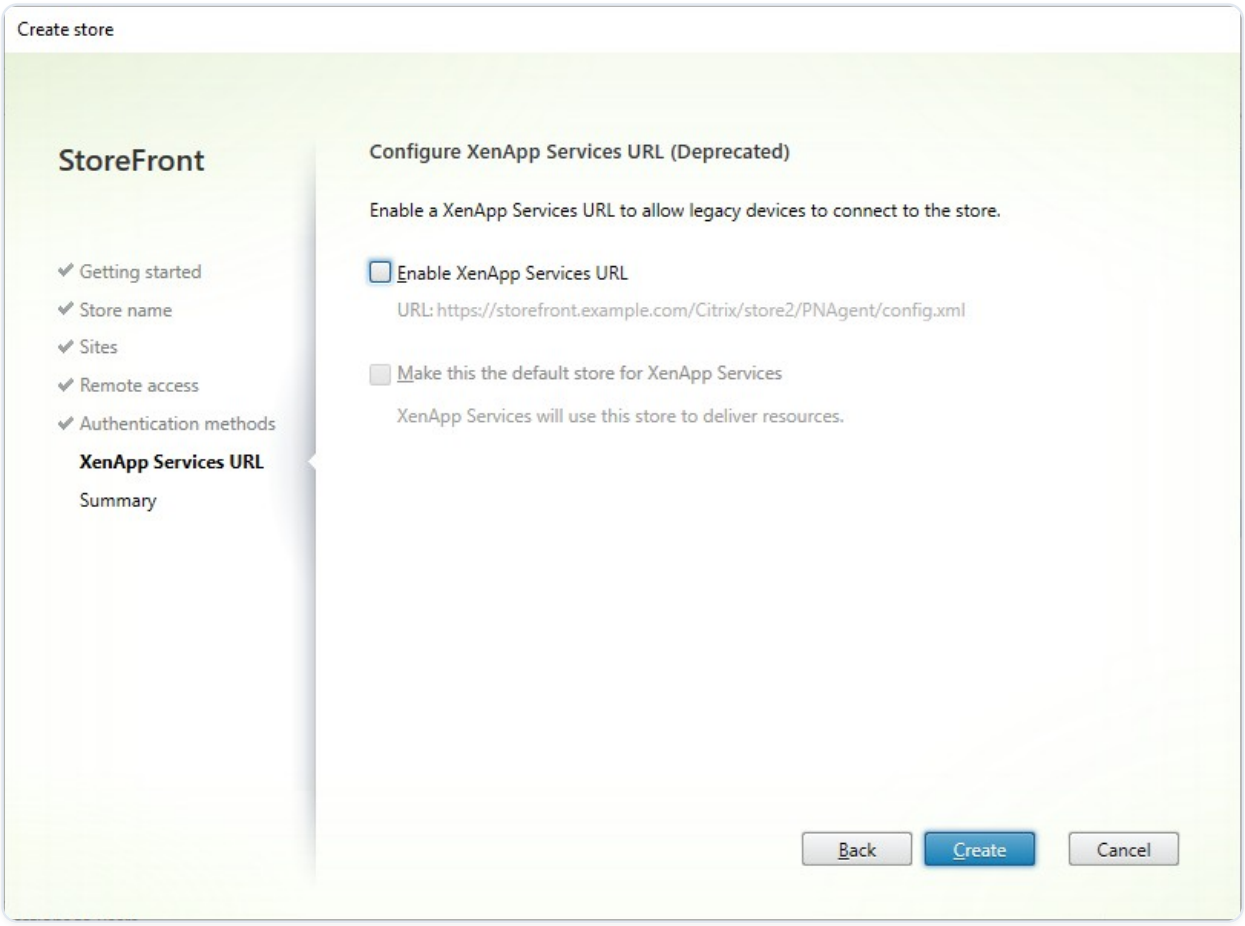
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click **Next**

6. On the **XenApp® Services URL** tab, if you have legacy devices requiring PNAgent select **Enable XenApp Services URL**, otherwise clear it.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Choose a virtual path for the store and set this as the `-VirtualPath` parameter. Typically this is /Citrix/.
- 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

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 differnet 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:

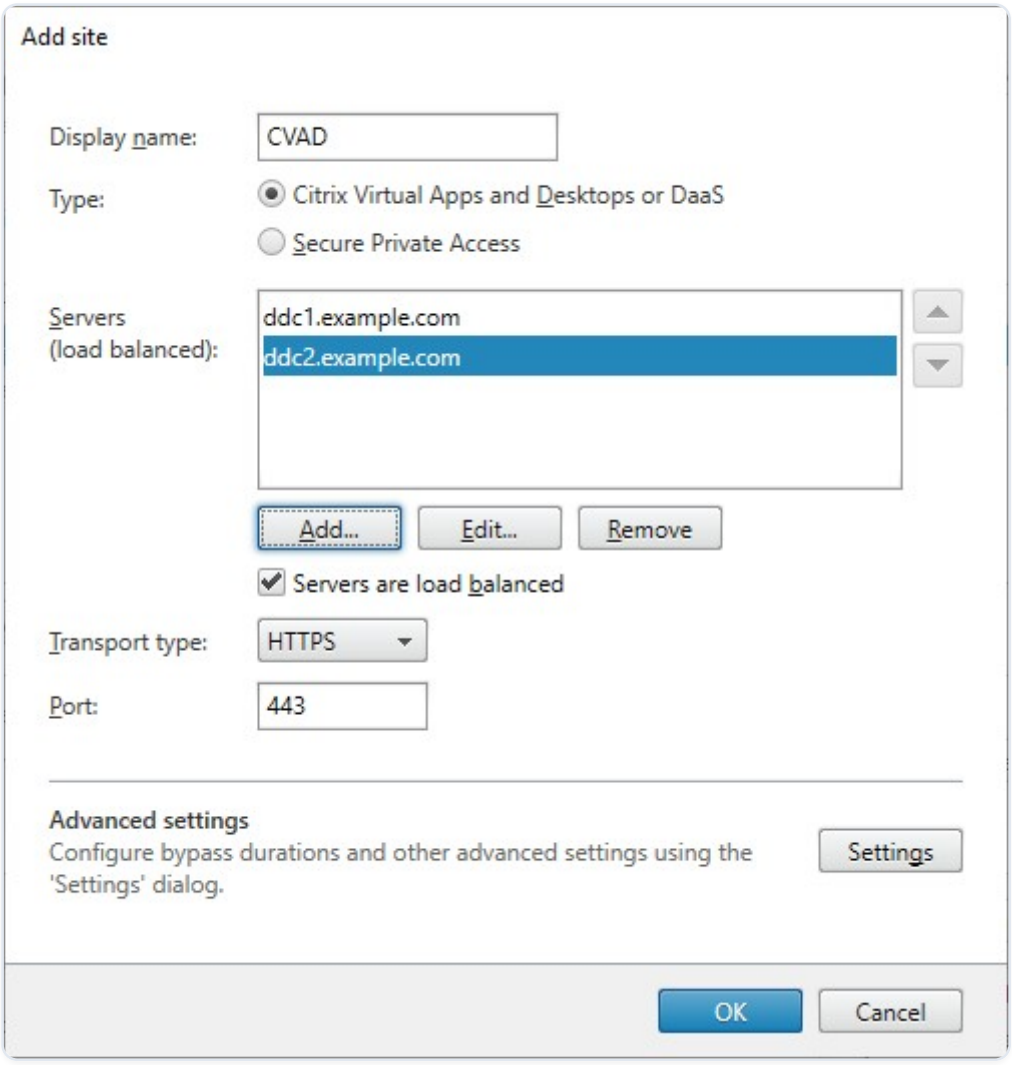
        - TLS_AES_256_GCM_SHA384
        - TLS_AES_128_GCM_SHA256

      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**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

```
$store = Get-STFStoreService -VirtualPath [path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [site name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [Security key]
```

Add Citrix Virtual Apps and Desktops™ site using PowerShell

To add a site, also known as a farm, run cmdlet Add-STFStoreFarm with `FarmType` `XenDesktop`

For example to add a site called "CVAD" with a security key:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$store = Get-STFStoreService -VirtualPath [path to store]

Add-STFStoreFarm -StoreService $store -FarmName "CVAD" -FarmType
XenDesktop -Port 443 -TransportType HTTPS -Servers
@("ddc1.example.com","ddc2.example.com") -XMLValidationEnabled $true
-XMLValidationSecret "MySecret"
```

Add Citrix Desktops as a Service site

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 Clond 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 severs 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- If you have a multi-zone geographically diverse deployment where DDCs have differnet 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:

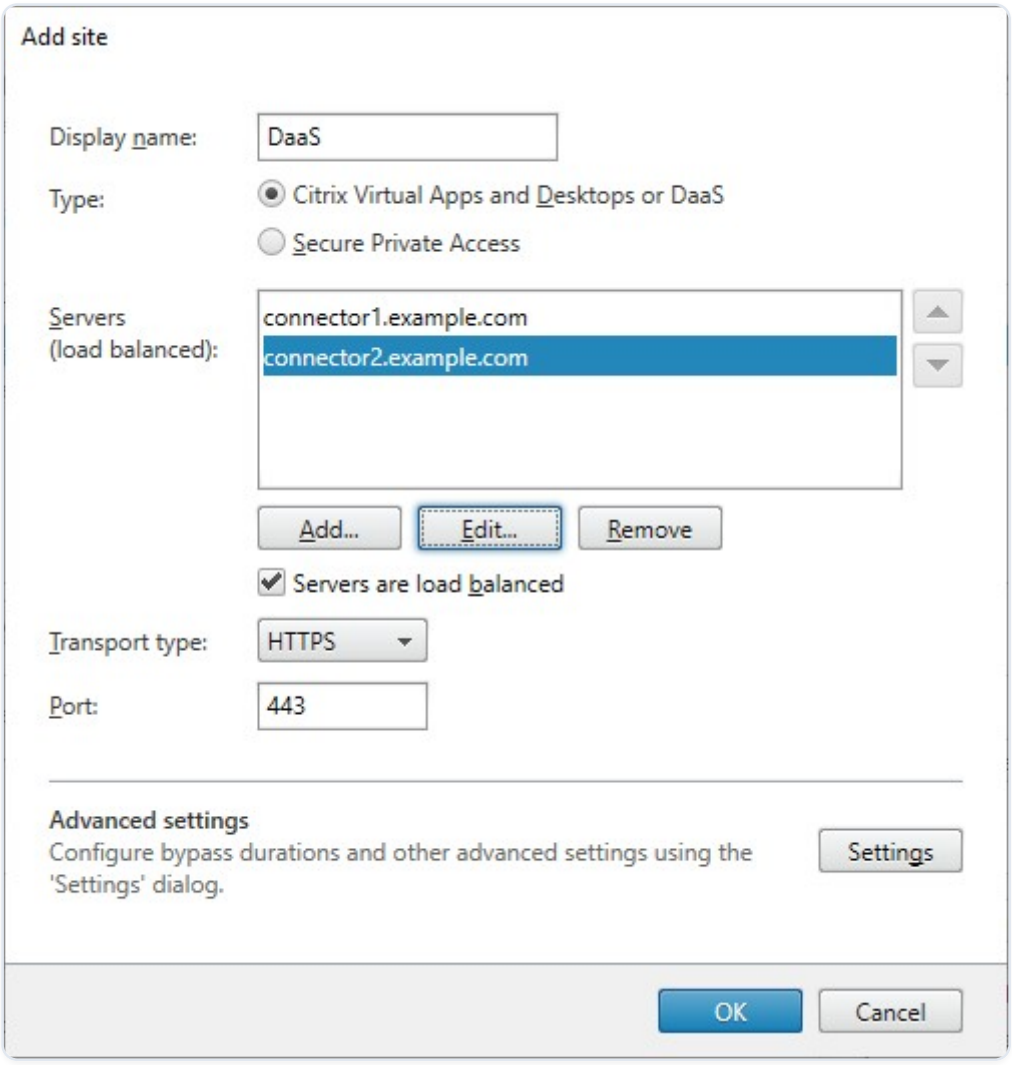
     - TLS_AES_256_GCM_SHA384
     - TLS_AES_128_GCM_SHA256

     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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

```
$store = Get-STFStoreService -VirtualPath [Path to store]

$farm = Get-STFStoreFarm -StoreService $store -FarmName [Site name]

Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
-XMLValidationSecret [Security key]
```

Add Citrix Desktops as a Service site using PowerShell

To add a site, also known as a farm, run cmdlet Add-STFStoreFarm with `FarmType` `XenDesktop`.

For example to add a site called "DaaS" with a security key:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$store = Get-STFStoreService -VirtualPath [path to store]

Add-STFStoreFarm -StoreService $store -FarmName "DaaS" -FarmType
XenDesktop -Port 443 -TransportType HTTPS -Servers
@("connector1.example.com","connector2.example.com") -XMLValidationEnabled
$true -XMLValidationSecret "MySecret"
```

Add Citrix Secure Private Access site

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**.
9. If you have configured a security key (recommended), then you must add the key using PowerShell. For example:

   ```
   $store = Get-STFStoreService -VirtualPath [Path to store]

   $farm = Get-STFStoreFarm -StoreService $store -FarmName [Site name]

   Set-STFStoreFarm -Farm $farm -XMLValidationEnabled $true
   -XMLValidationSecret [Security key]
   ```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Add Citrix Secure Private Access site using PowerShell

To add a site, also known as a farm, run cmdlet Add-STFStoreFarm with `FarmType` `SPA`

For example to add a site called "SPA Apps" with a security key:

```
$store = Get-STFStoreService -VirtualPath [path to store]

$farm = Add-STFStoreFarm -StoreService $store -FarmName "SPA Apps"
-FarmType SPA -Port 443 -TransportType HTTPS -ServiceUrls https://spa-
service.example.com -XMLValidationEnabled $true -XMLValidationSecret
"MySecret"
```

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

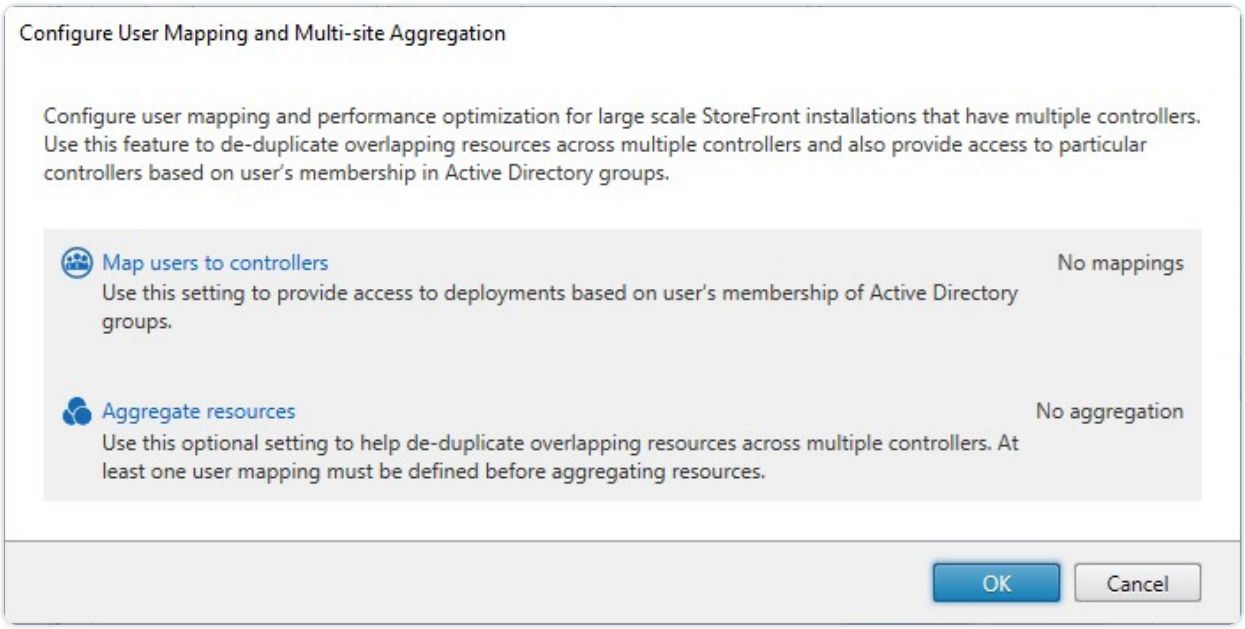
> This filters entire sites. In addition, within a site, applications may be filtered by user group within Citrix Virtual Apps and Desktops Studio configuration.

To configure specific sites for particular user groups:

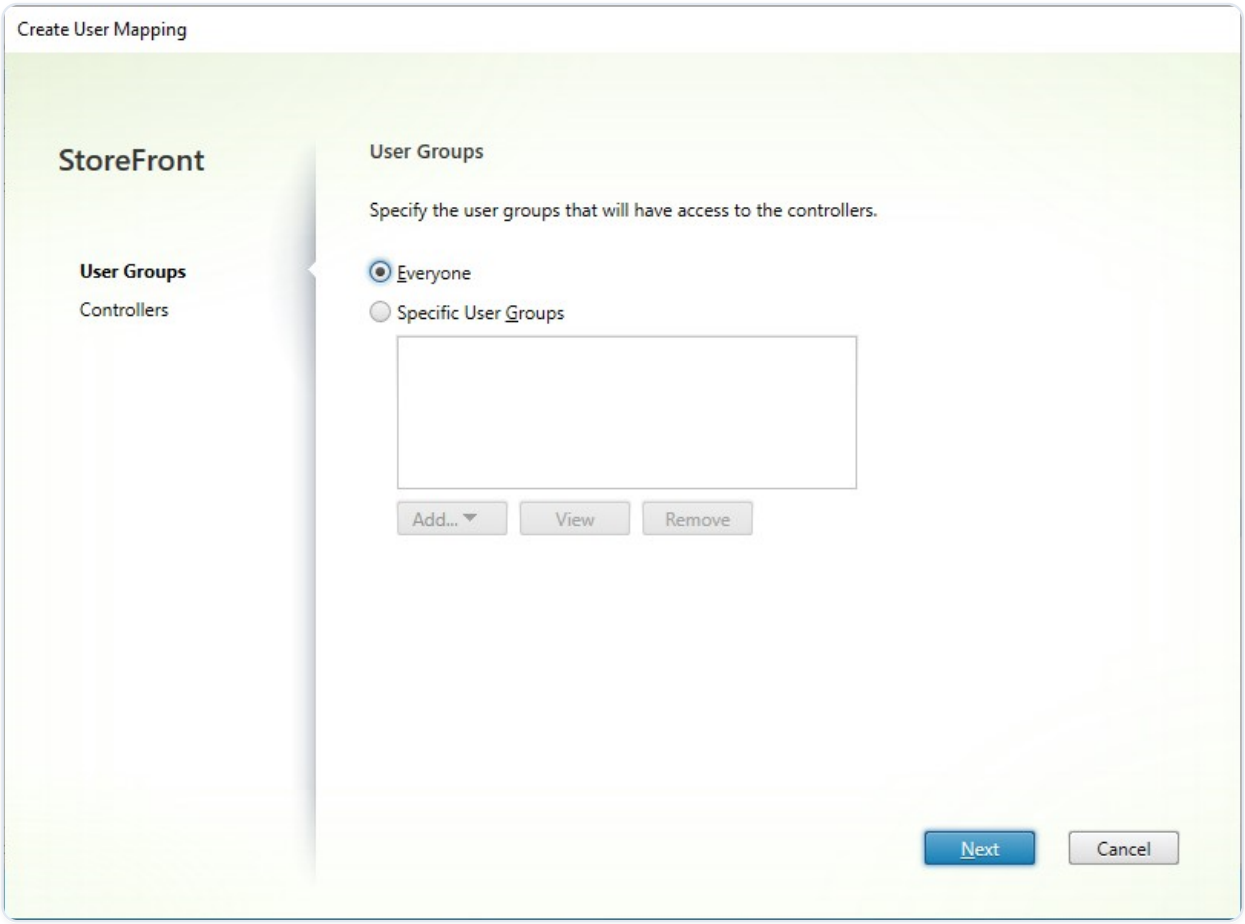
1. From the **Manage sites** screen, under **User mapping and multi-site aggregation configuration**, click **Configure**. This option is only available if two or more sites are configured.

   This opens the **Configure user mapping and multi-site** Aggregation screen.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

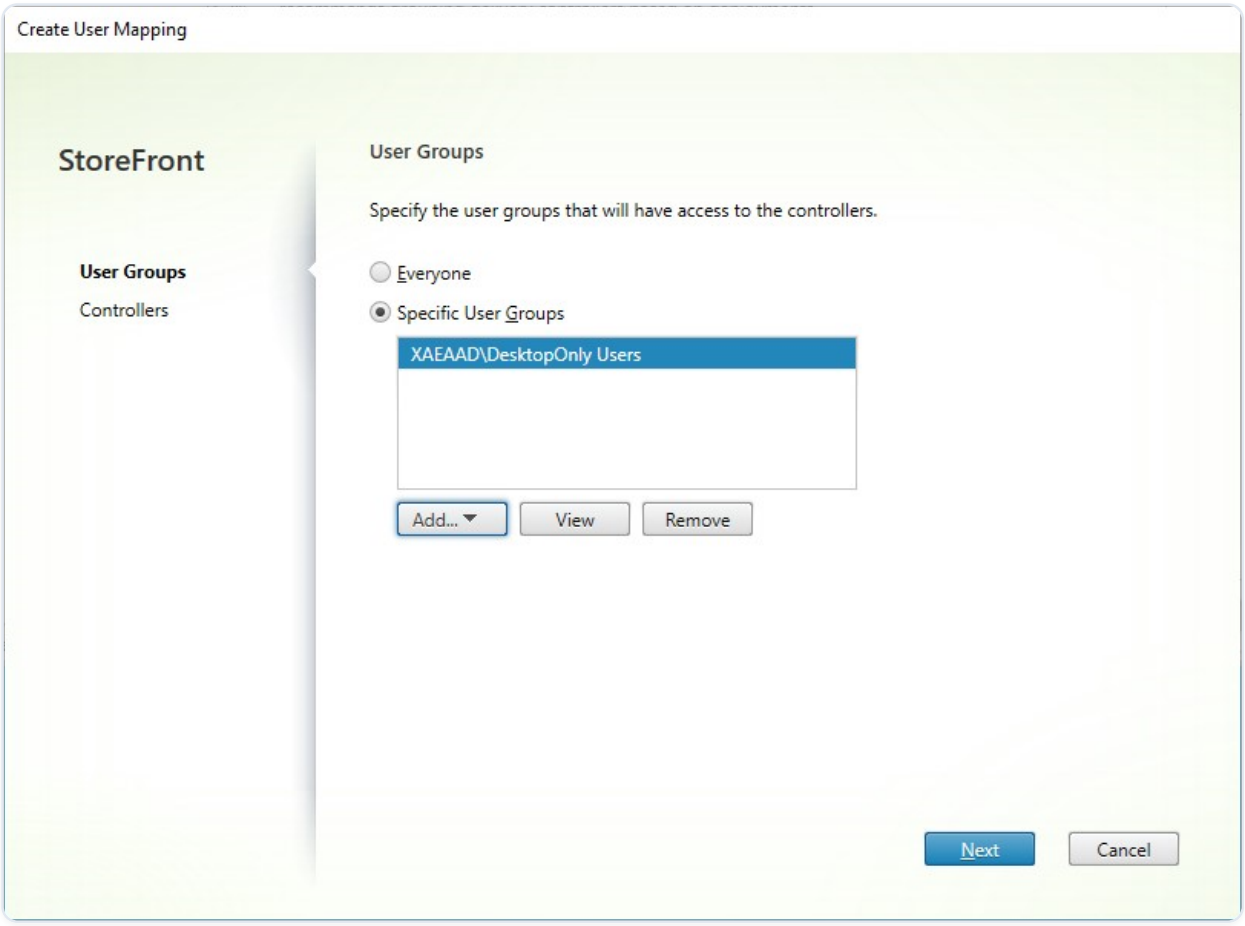


2. Click **Map users to sites**. This opens the **Create user mapping** screen to create your first mapping. You will be able to create further mappings later.

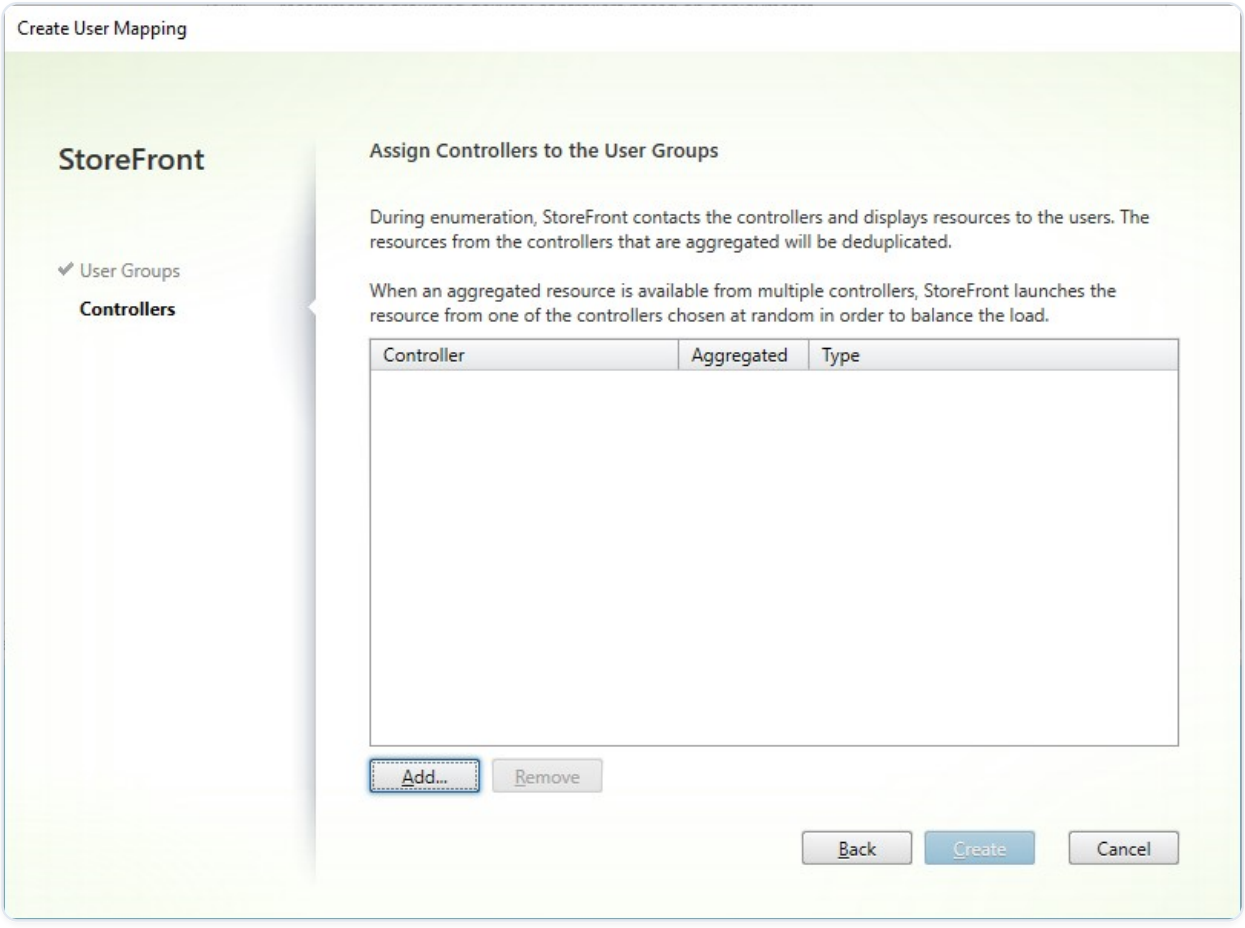


3. Either choose **Everyone** or choose **Specific user groups** and add one or more group.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

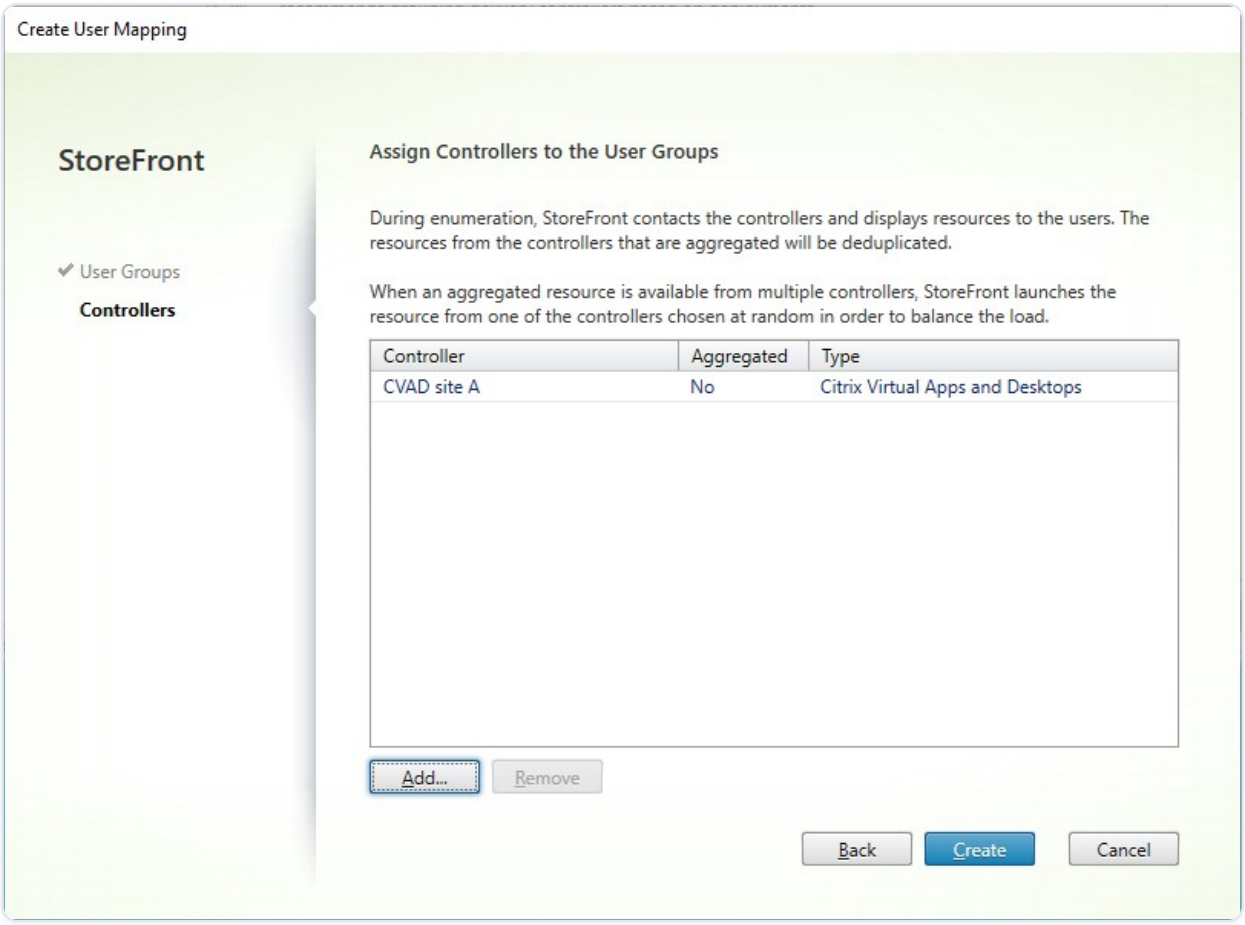


4. Click **Next**. This takes you to the **Sites** tab.



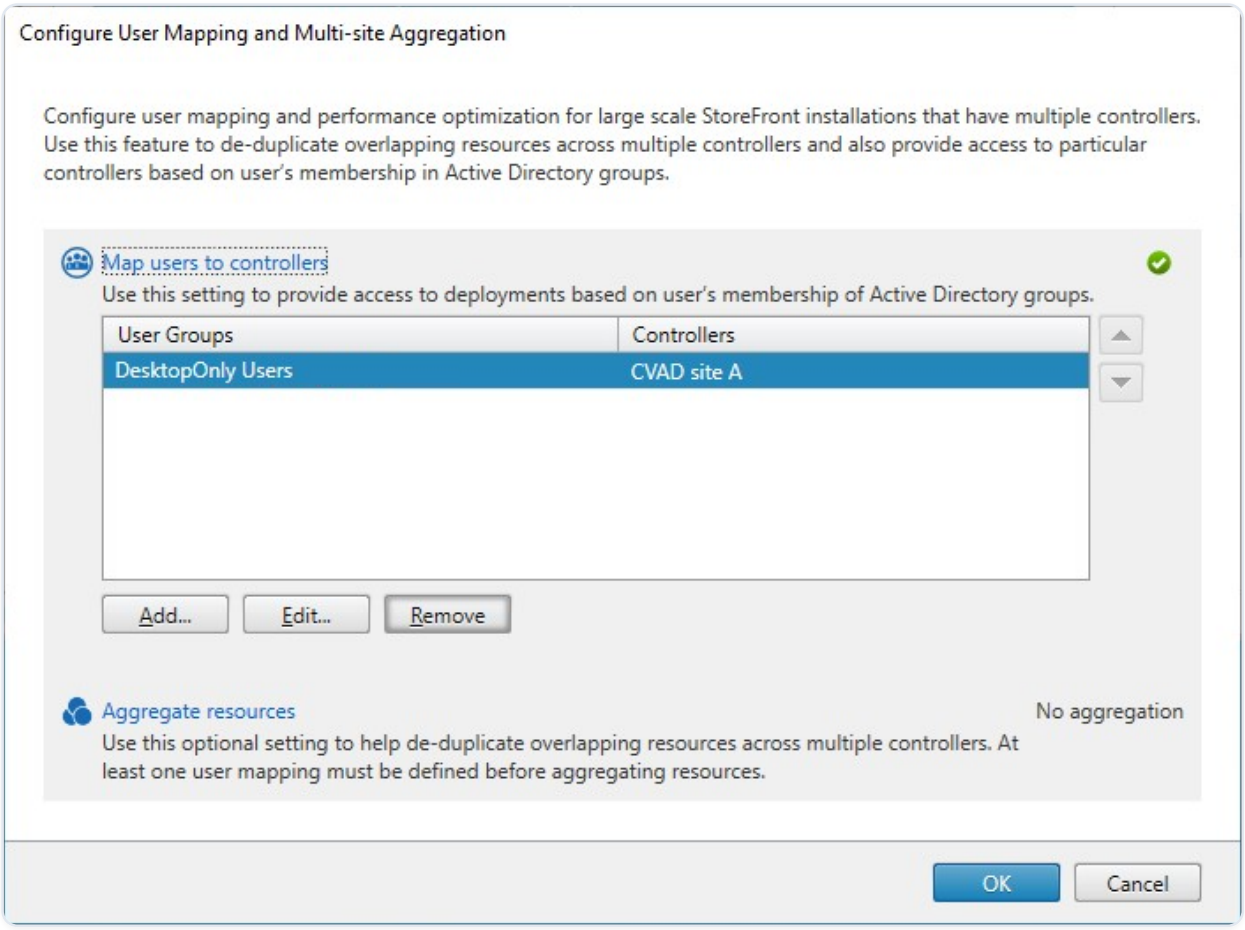
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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



6. Click **Create**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

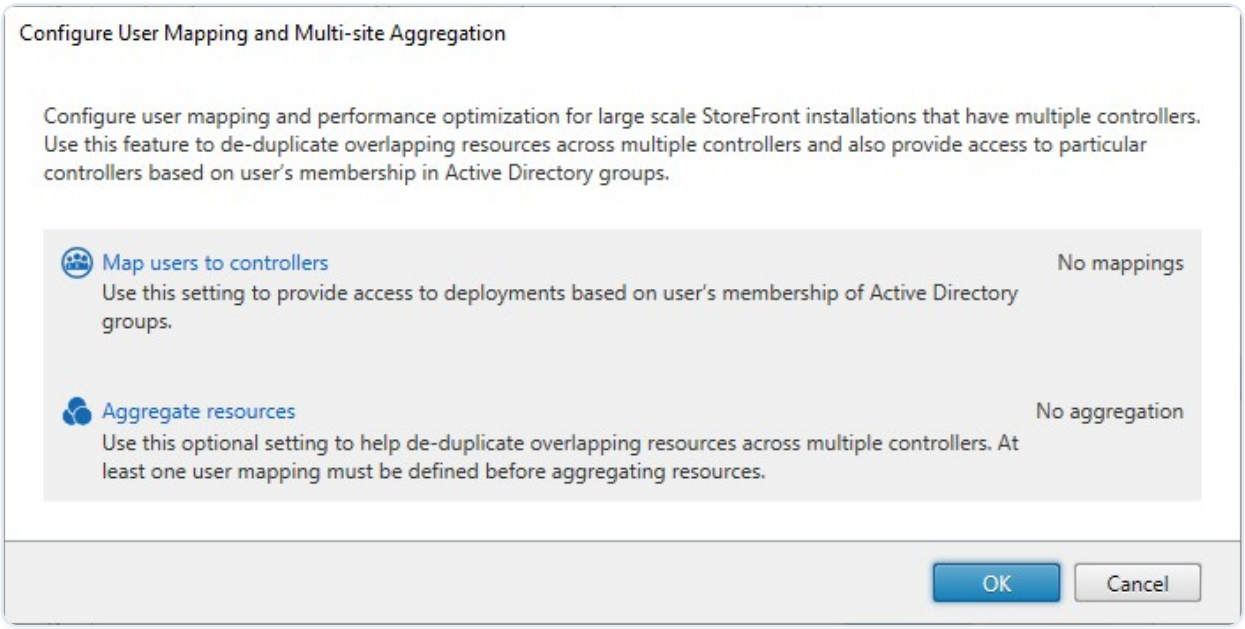
If a launch fails from one site then StoreFront tries other suitable sites, unless:

- 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.

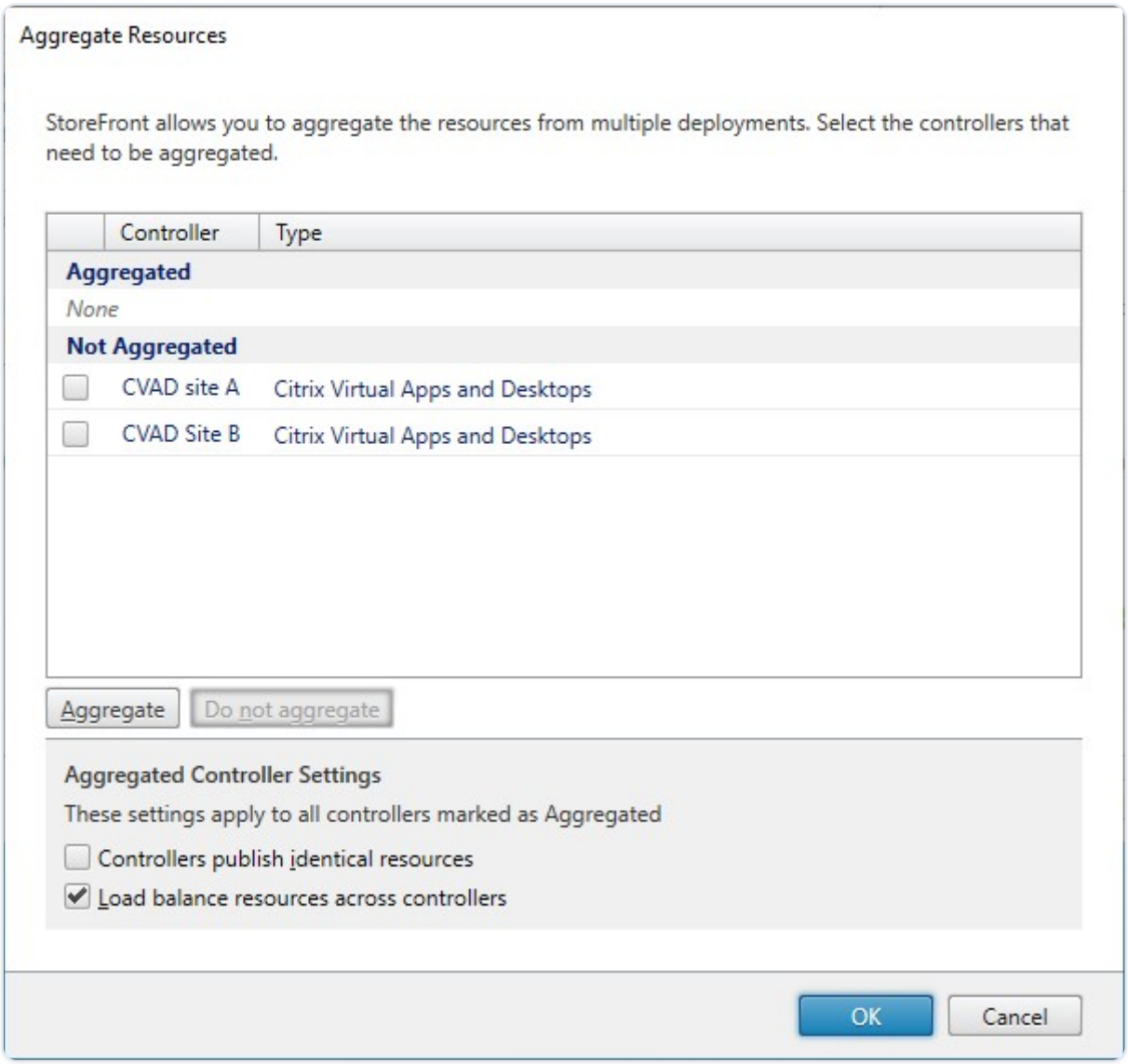
To configure multi-site aggregation:

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

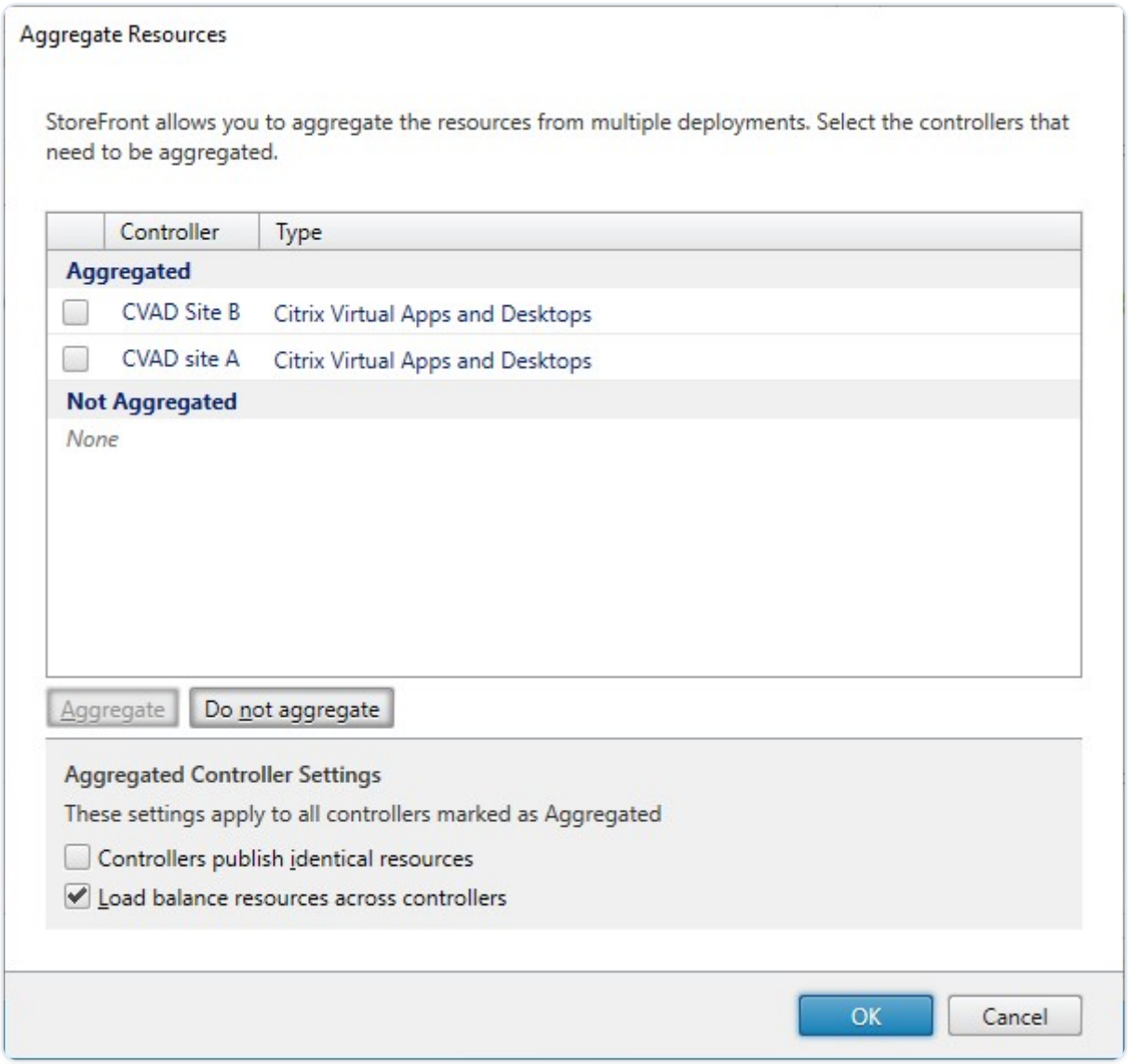


2. Click **Aggregate resources**. This shows the **Aggregate Resources** screen.



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

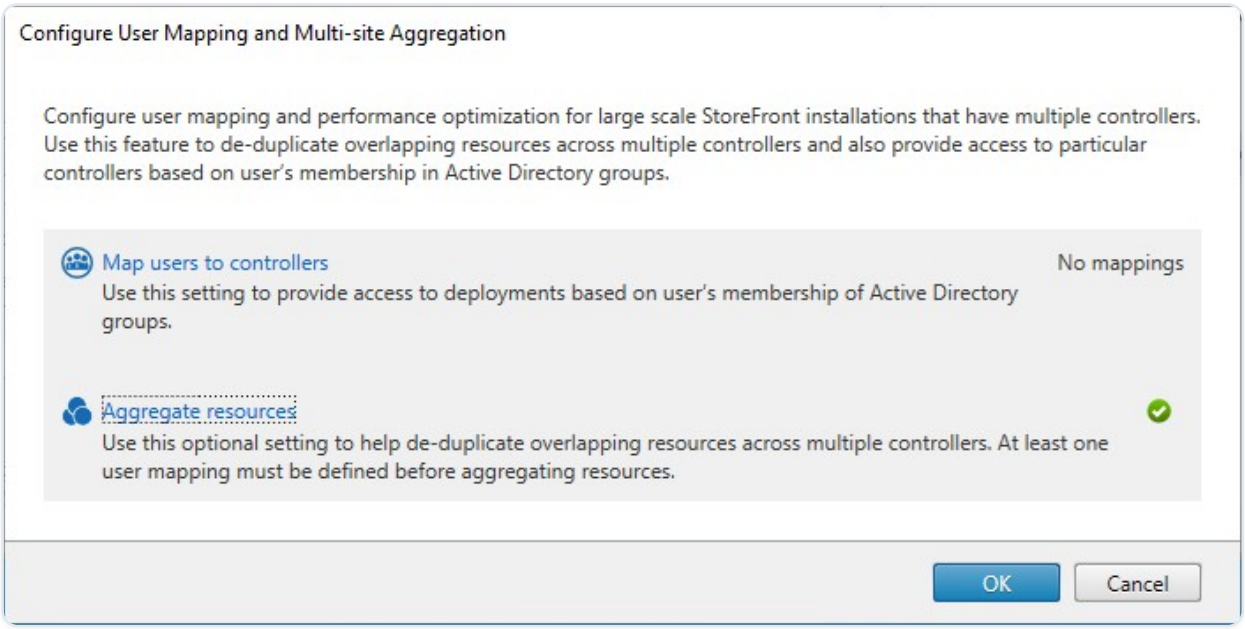


4. Select **Aggregated Controller Settings** options as required:

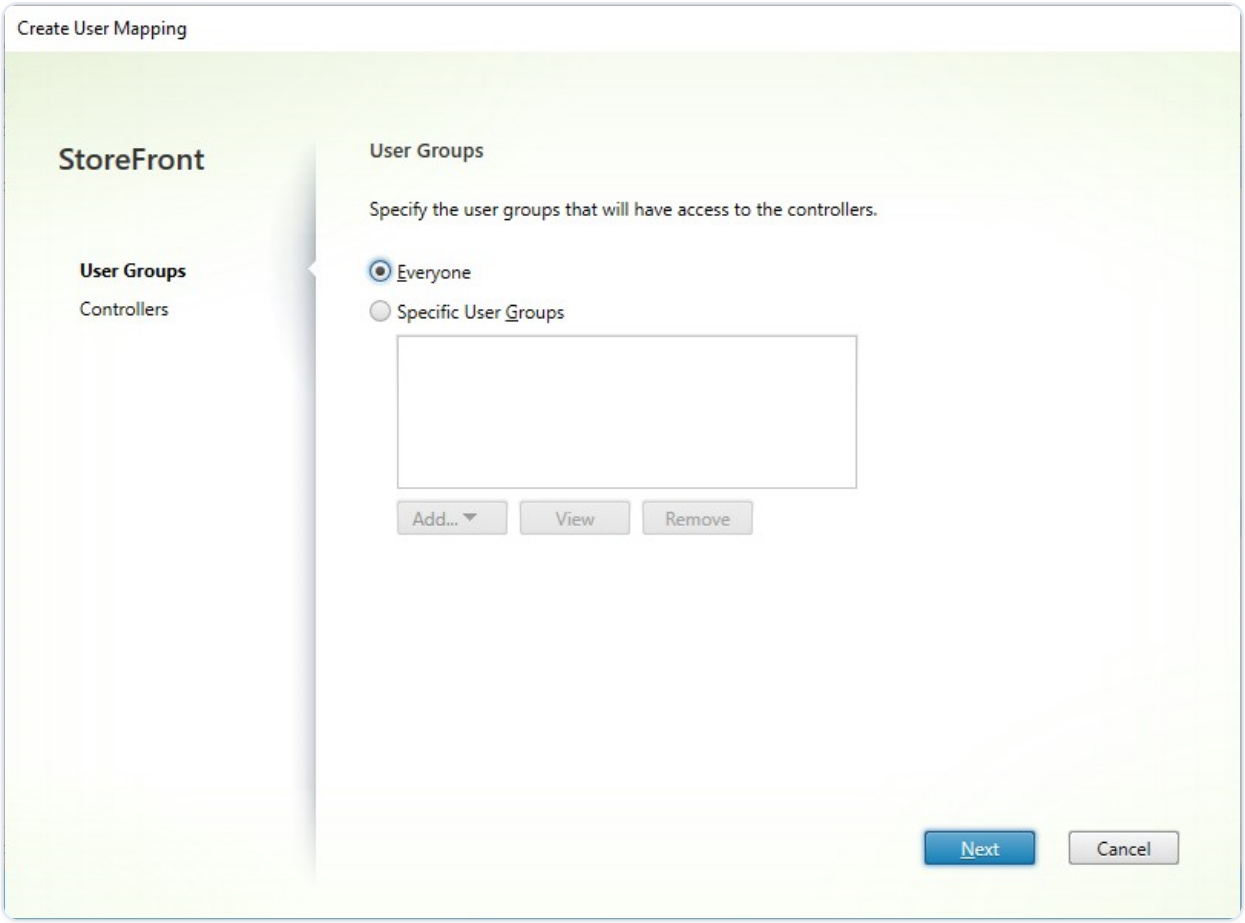
    - **Sites publish identical resources** - When selected, StoreFront enumerates resources from only one of the controllers in the aggregated set. When not selected, StoreFront enumerates resources from all controllers in the aggregated set (to accumulate the user's entire set of available resources). 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

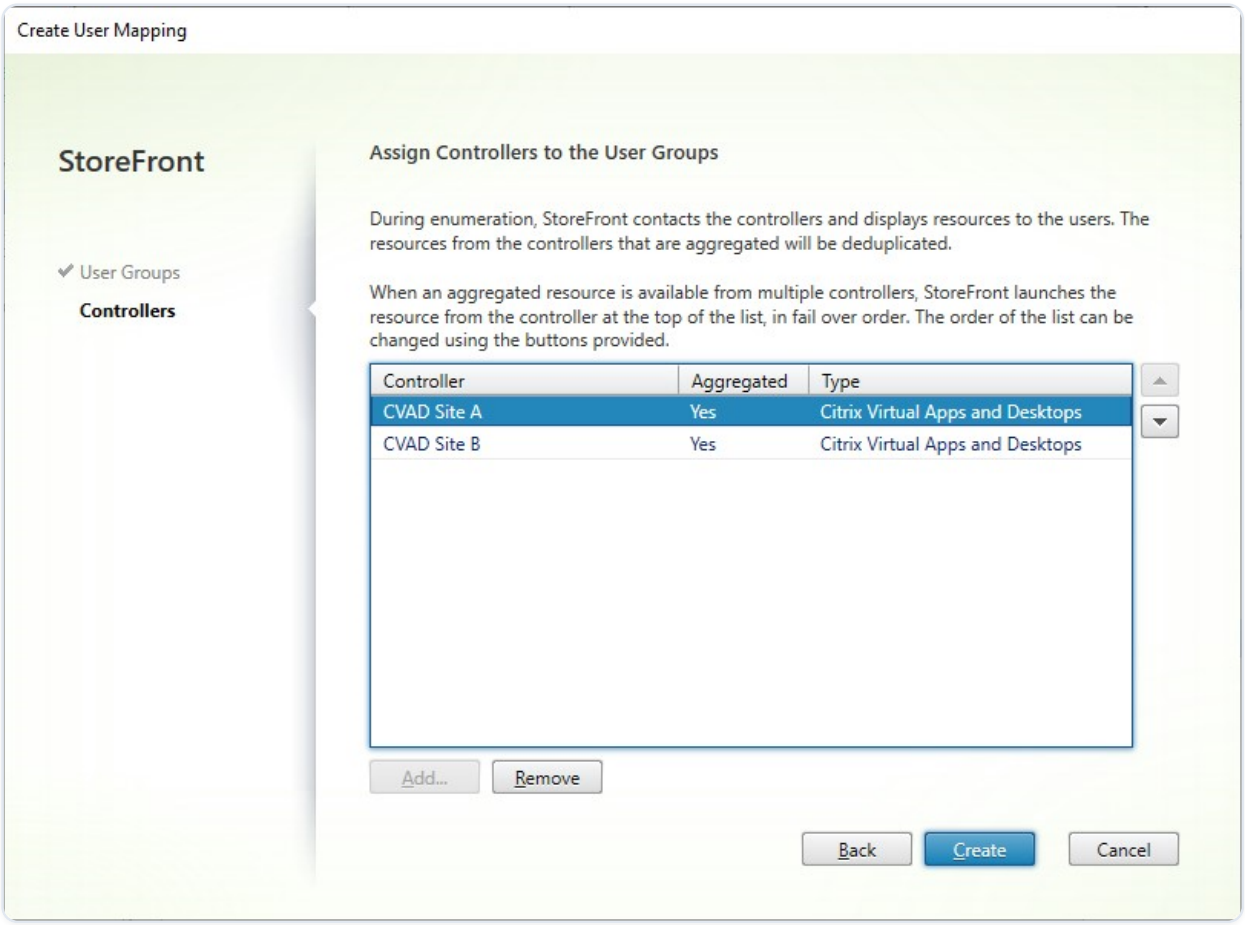


7. Either choose **Everyone** or choose **Specific User Groups** and add one or more group. For instance you may wish to choose a group representing users in a particular location. You can

© 1997–2026 Citrix Systems, Inc. All rights reserved.

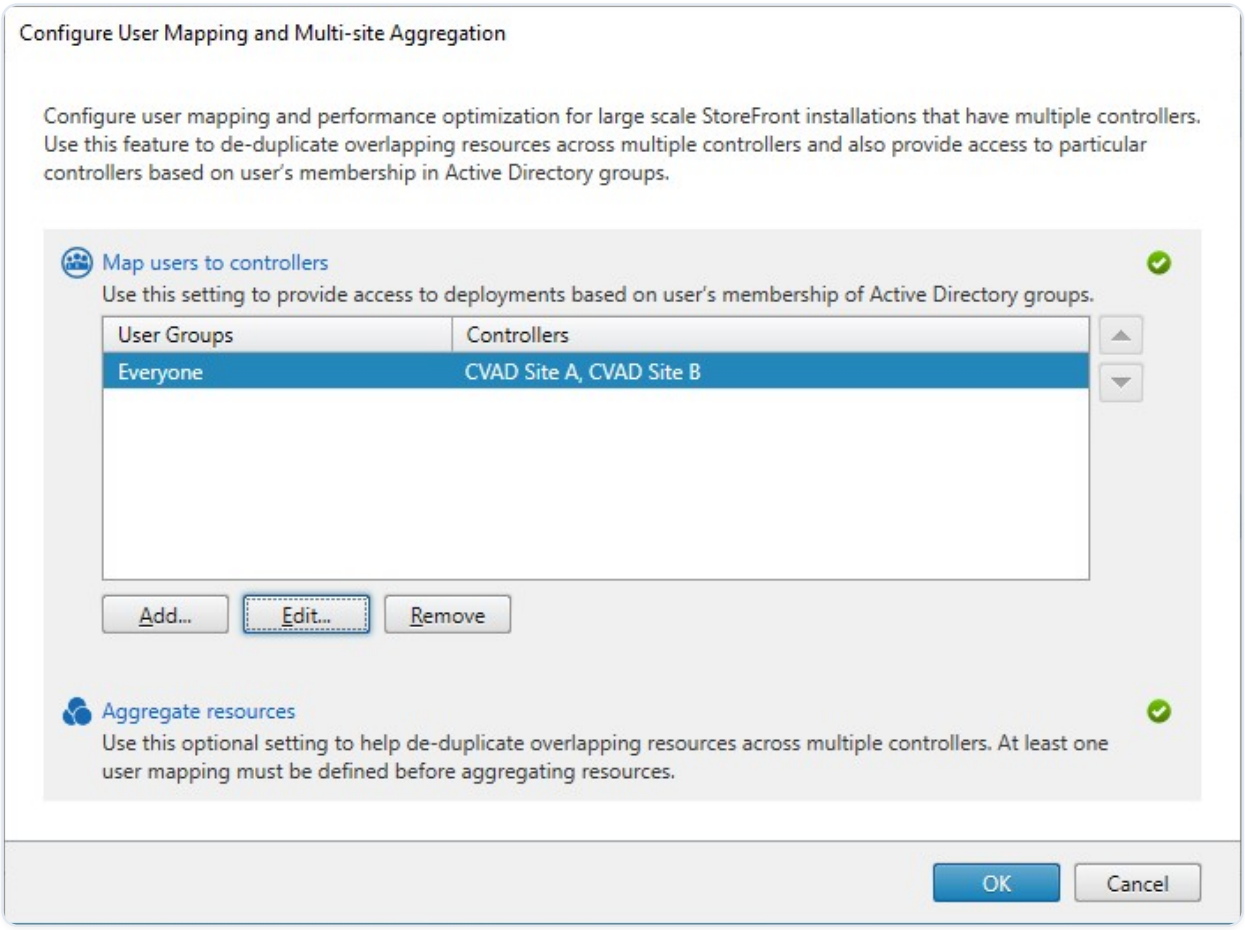
use Active Directory Groups in domains trusted by the StoreFront server. It is not possible to use Entra ID groups.

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.



10. Press **Create** to return to **Configure user mapping and multi-site aggregation**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- `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.

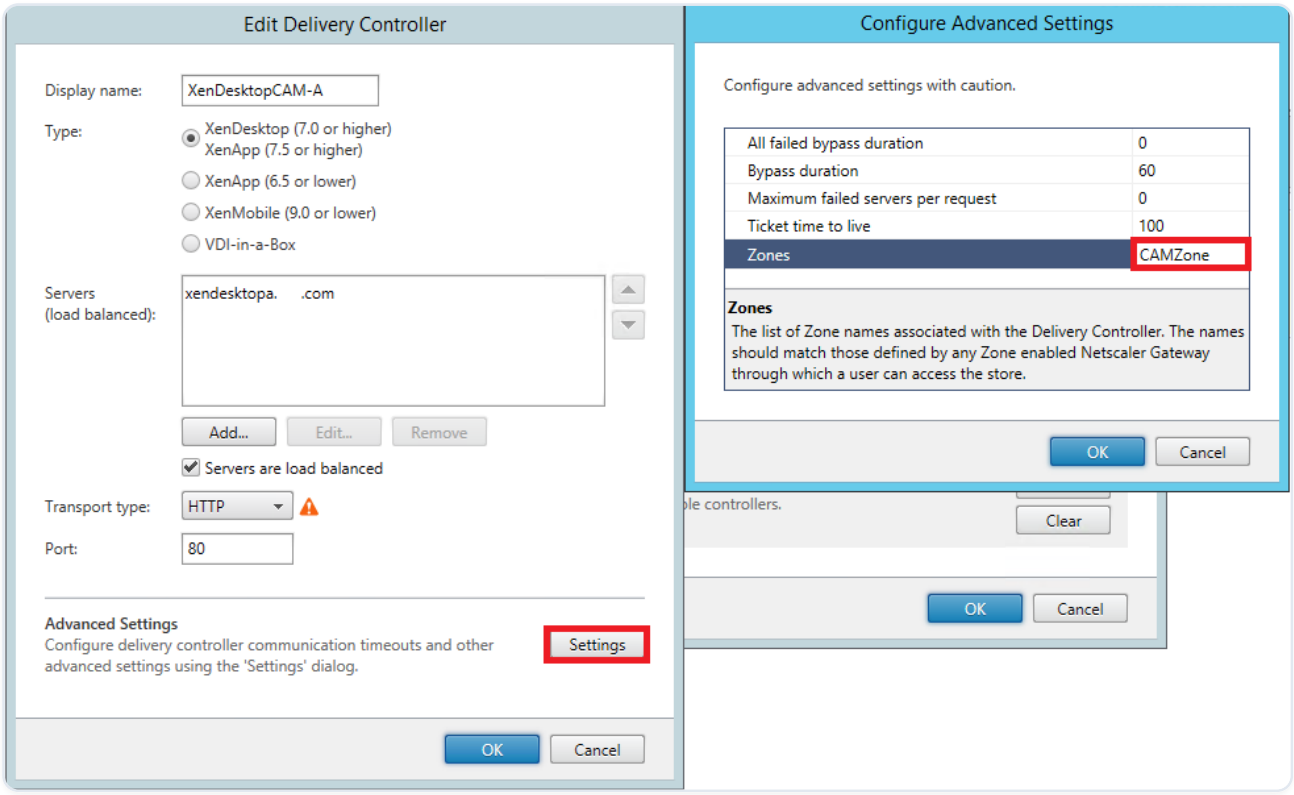
Zone preference

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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 Citrix Workspace™ app website

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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Authentication

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
Active Directory username and password	Users enter their Active Directory username and password.
Domain pass-through	Windows devices single sign-on using the account they used to log in to Windows.
Smart card	Users swipe a smart card and enter a PIN. This uses the certificate stored on the smart card to authenticate the user.
SAML	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 Web API developer documentation. HTTP Basic does not provide a user interface for users to authenticate.
Pass-through from Citrix Gateway	Allow users to authenticate at a Citrix Gateway.

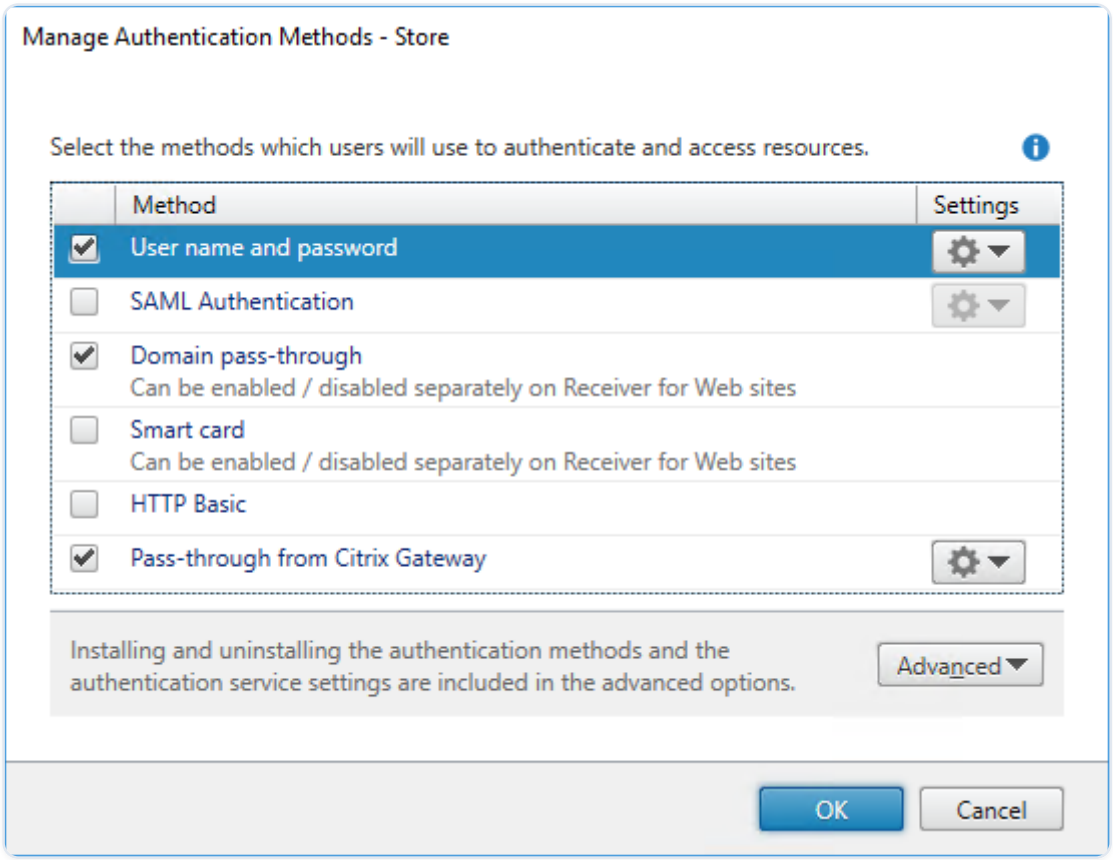
Alternatively, when creating a new store, you can disable authentication and instead allow anonymous access to the stores. See Create store.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**.

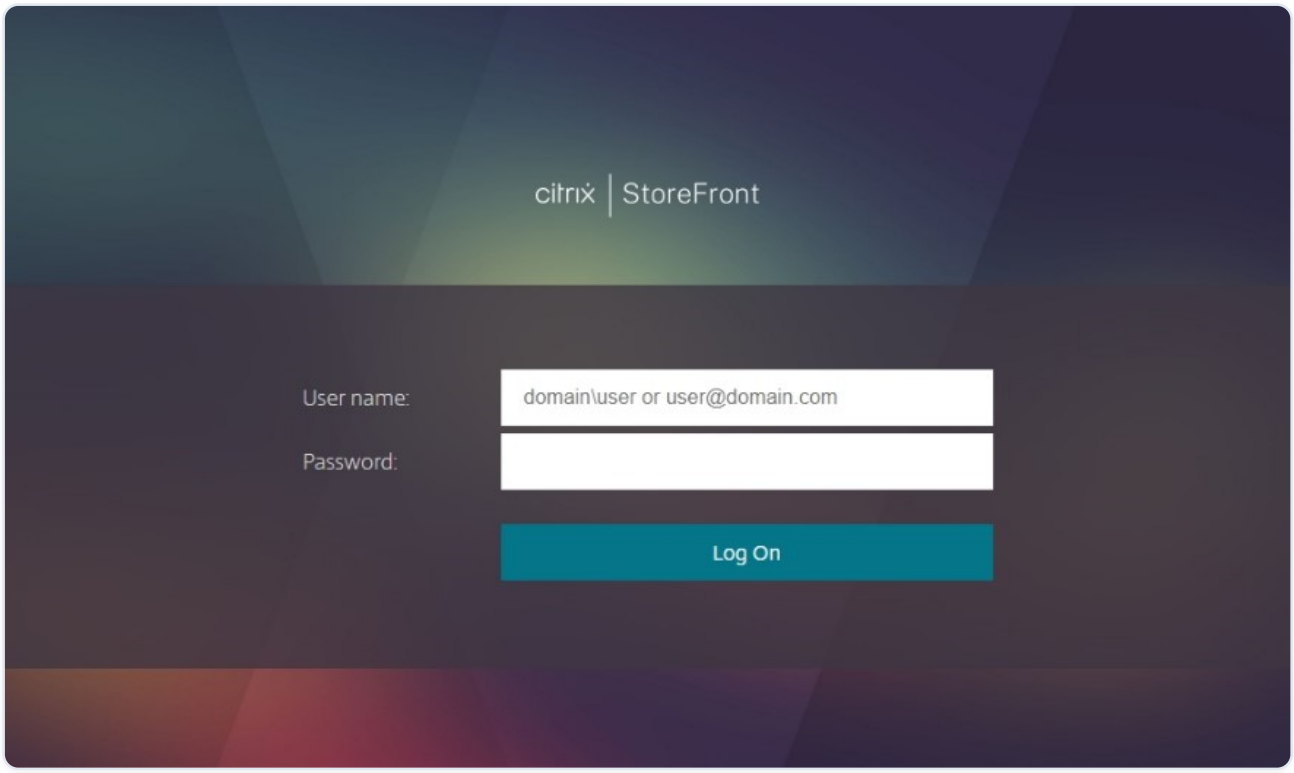
Single sign-on to VDAs

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



.

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.

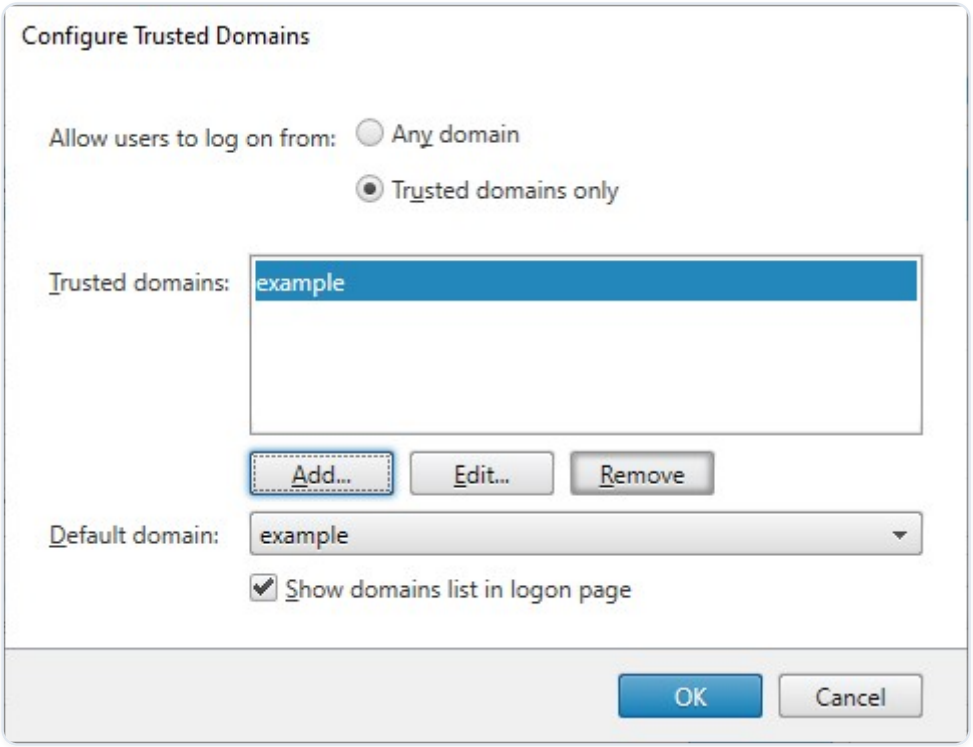
1. Select the Stores node in the left pane of the Citrix StoreFront management console and, in the results pane, select the appropriate authentication method. In the Actions pane, click **Manage Authentication Methods**.
2. From the **username and password > Settings** list, select **Configure Trusted 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

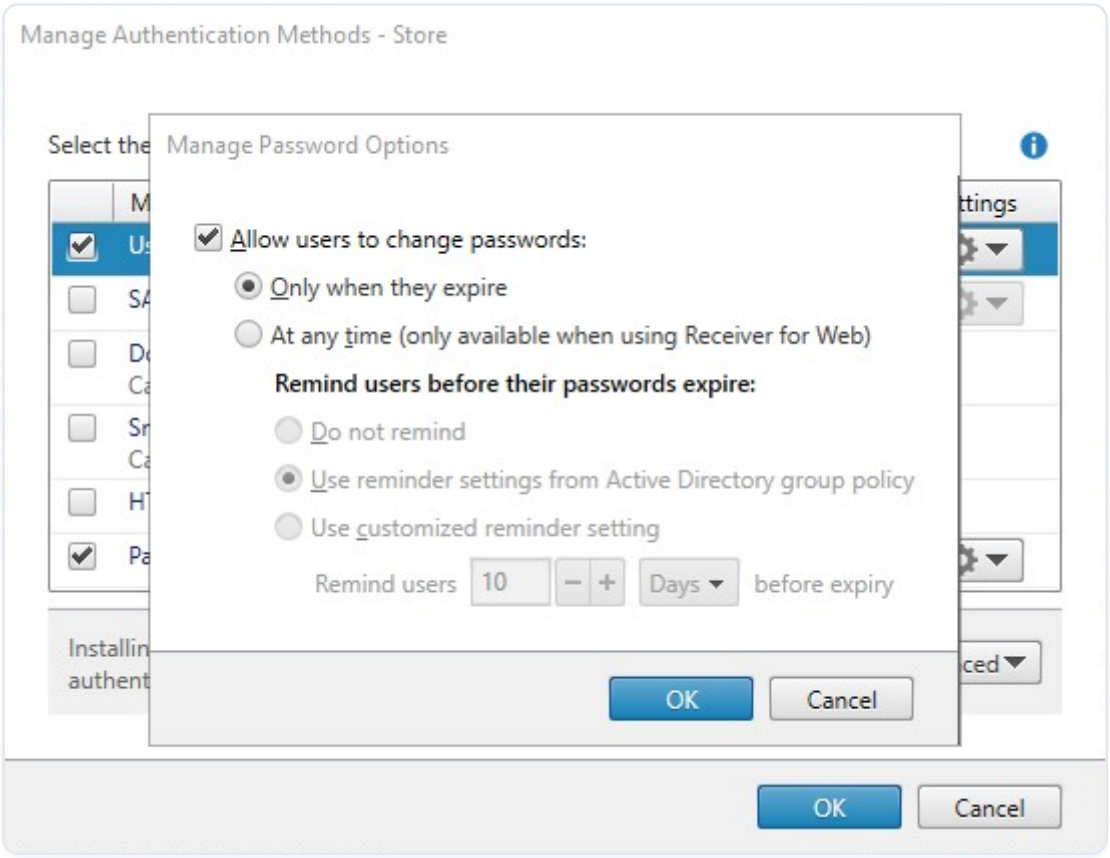
   - **Do not remind** - The UI does not display password expiry reminders. It only notifies users as the point the password has expired.
   - **Use reminder settings from Active Directory group policy** - After logging in, the user interface notifies if their password is going to expire in the number days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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 security policy **Network access: Restrict clients allowed to make remote calls to SAM** then you must include any users who need to change their passwords.

Note 3:

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

PowerShell

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

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

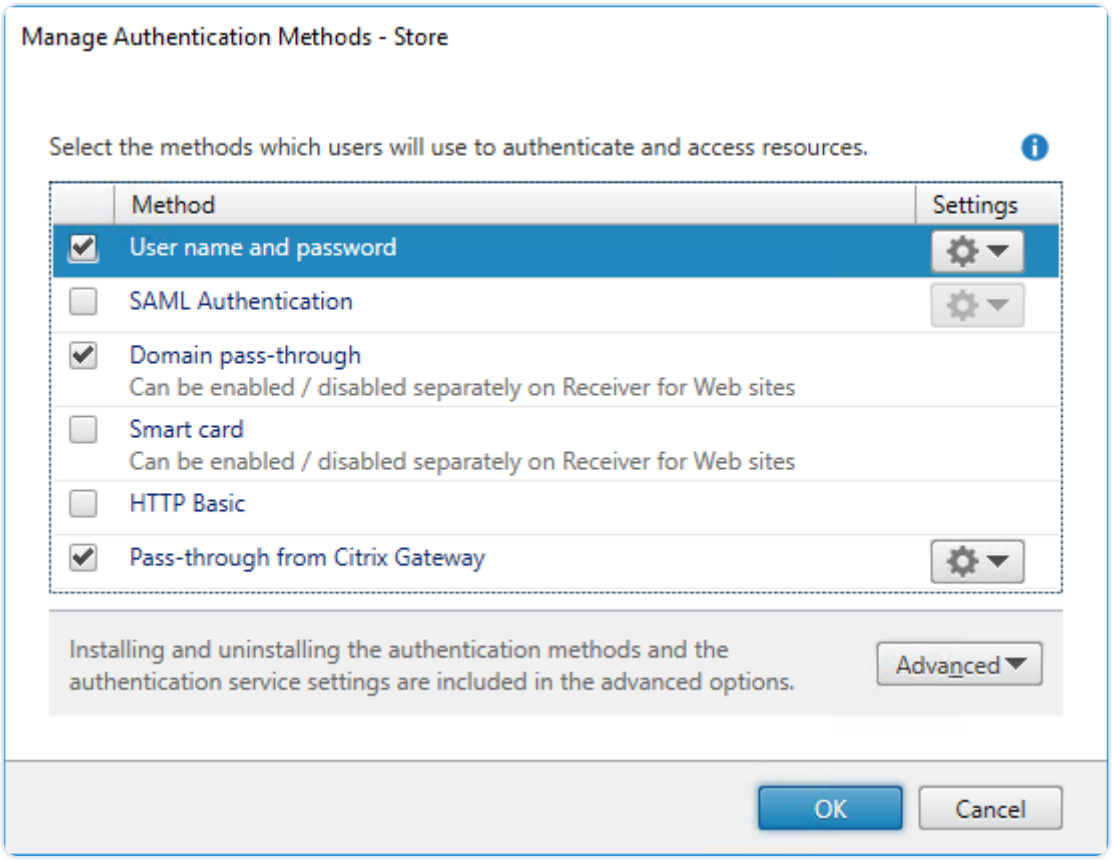
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

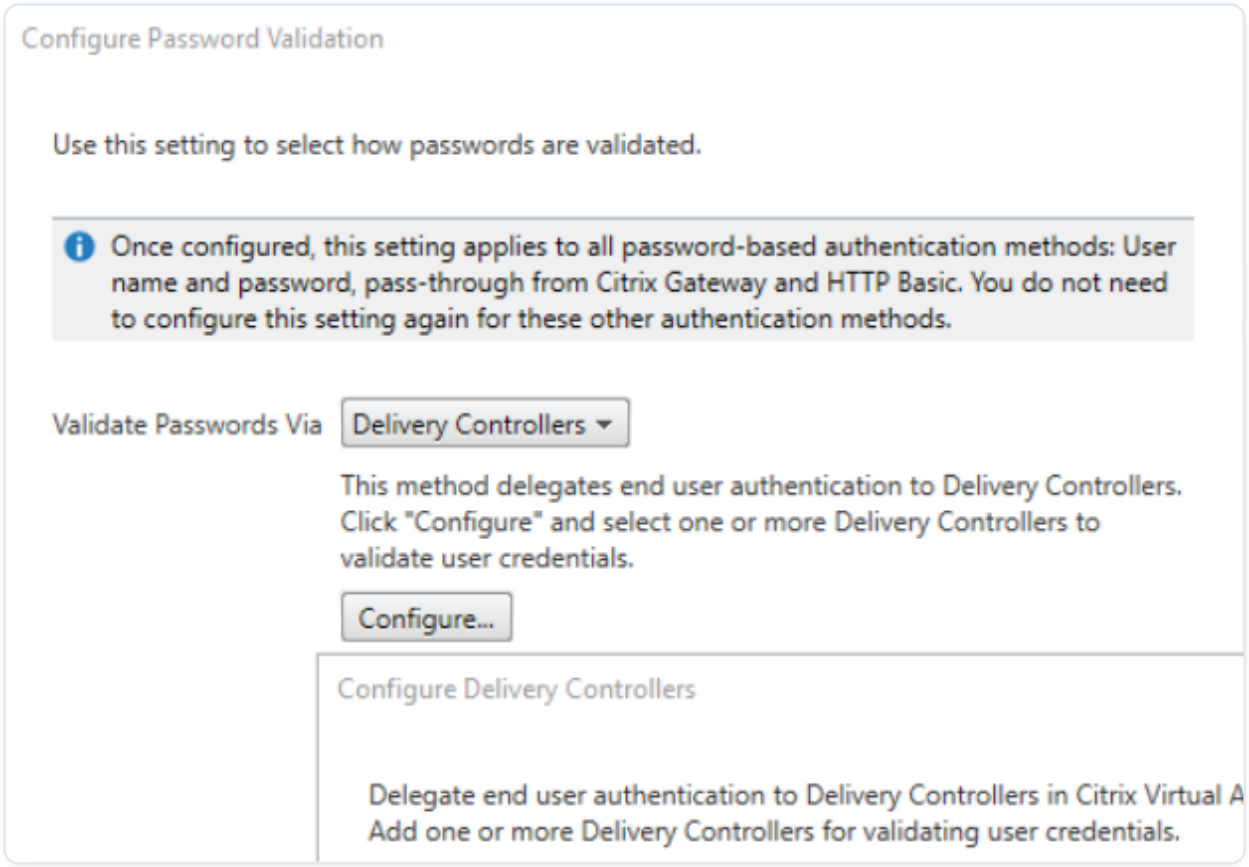
1. In the **Manage Authentication Methods** window, from the **username and password > Settings** drop-down menu, select **Configure Password Validation**.



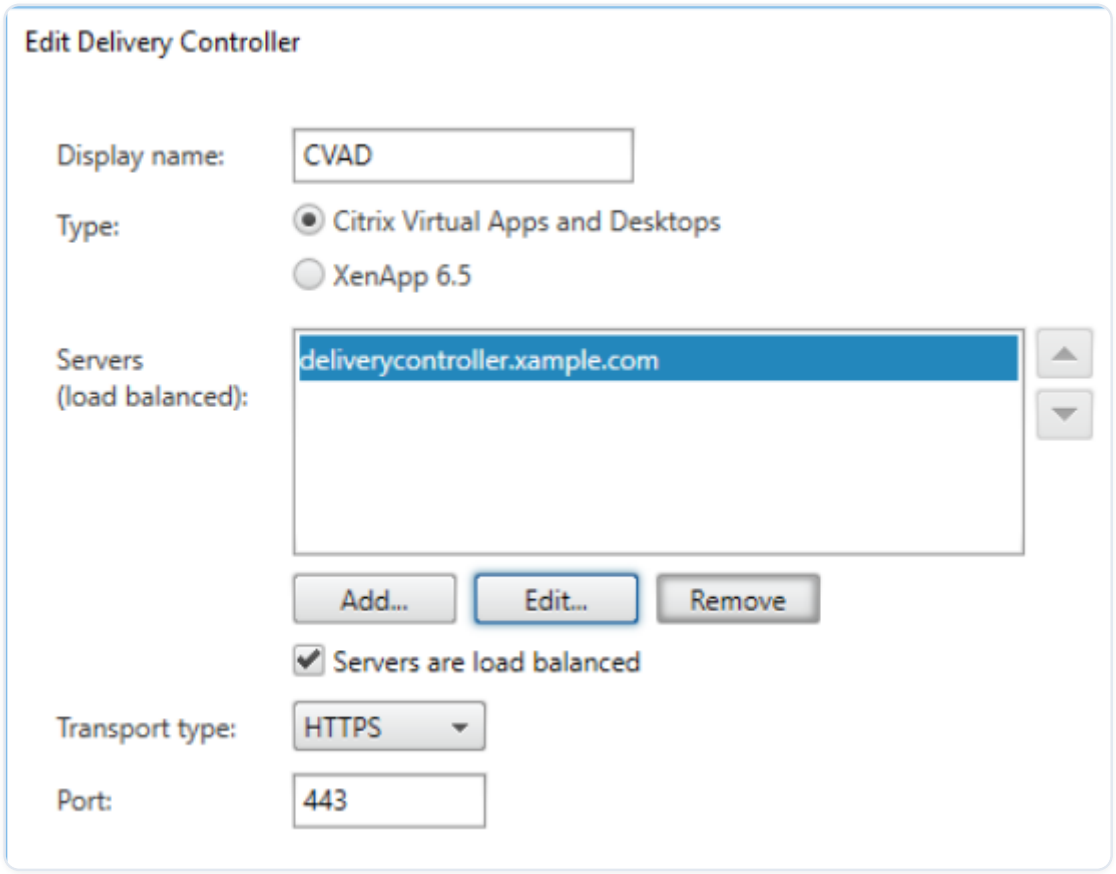
2. From the **Validate Password Via** drop down, choose:

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
@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.

```
<data name="AuthenticateHeadingText" xml:space="preserve">

    <value>My Company Name</value>

</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\\Auth\App_Data\Templates\UsernamePassword.tfrm.
2. Locate the following line in the file.

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

3. Comment the statement as shown below.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<!-- @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

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 Configure Microsoft Entra ID for SAML authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

The SAML assertion must include a `<saml:NameID>` element populated with the user's User Principal Name (UPN). StoreFront looks up this UPN in Active Directory. StoreFront does not support users in other directories. When using Entra ID, the user must have a hybrid identity.

To enable or disable SAML authentication for a store, 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 disable or enable SAML authentication for each 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/SamlForms/AssertionConsumerService`
- The Metadata service, normally `https://[storefront host]/Citrix/[StoreName]Auth/SamlForms/ServiceProvider/Metadata`

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.

```
# Change this value for your Store

$storeVirtualPath = "/Citrix/Store"



$auth = Get-STFAuthenticationService -Store (Get-STFStoreService
-VirtualPath $storeVirtualPath)

$spId =
$auth.AuthenticationSettings["samlForms"].SamlSettings.ServiceProvider.Uri
.AbsoluteUri

$acs = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.VirtualPath
+ "/SamlForms/AssertionConsumerService")

$md = New-Object System.Uri $auth.Routing.HostbaseUrl, ($auth.VirtualPath
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
+ "/SamlForms/ServiceProvider/Metadata")

$samlTest = New-Object System.Uri $auth.Routing.HostbaseUrl,
($auth.VirtualPath + "/SamlTest")

Write-Host "SAML Service Provider information:

Entity ID: $spId

Assertion Consumer Service: $acs

Metadata: $md

Test Page: $samlTest"
```

Example of the output:

```
SAML Service Provider information:

Entity ID: https://storefront.example.com/Citrix/StoreAuth

Assertion Consumer Service: https://storefront.example.com/Citrix/
StoreAuth/SamlForms/AssertionConsumerService

Metadata: https://storefront.example.com/Citrix/StoreAuth/SamlForms/
ServiceProvider/Metadata

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-Module "Citrix.StoreFront*" -ListAvailable | Import-Module



# Remember to change this with the virtual path of your Store.

$StoreVirtualPath = "/Citrix/Store"



$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store



# To read the metadata directly from the Identity Provider, use the
following:

# Note again this is only allowed for https endpoints

Update-STFSamlIdPFromMetadata -AuthenticationService $auth -Url https://
example.com/FederationMetadata/2007-06/FederationMetadata.xml



# If the metadata has already been download, use the following:

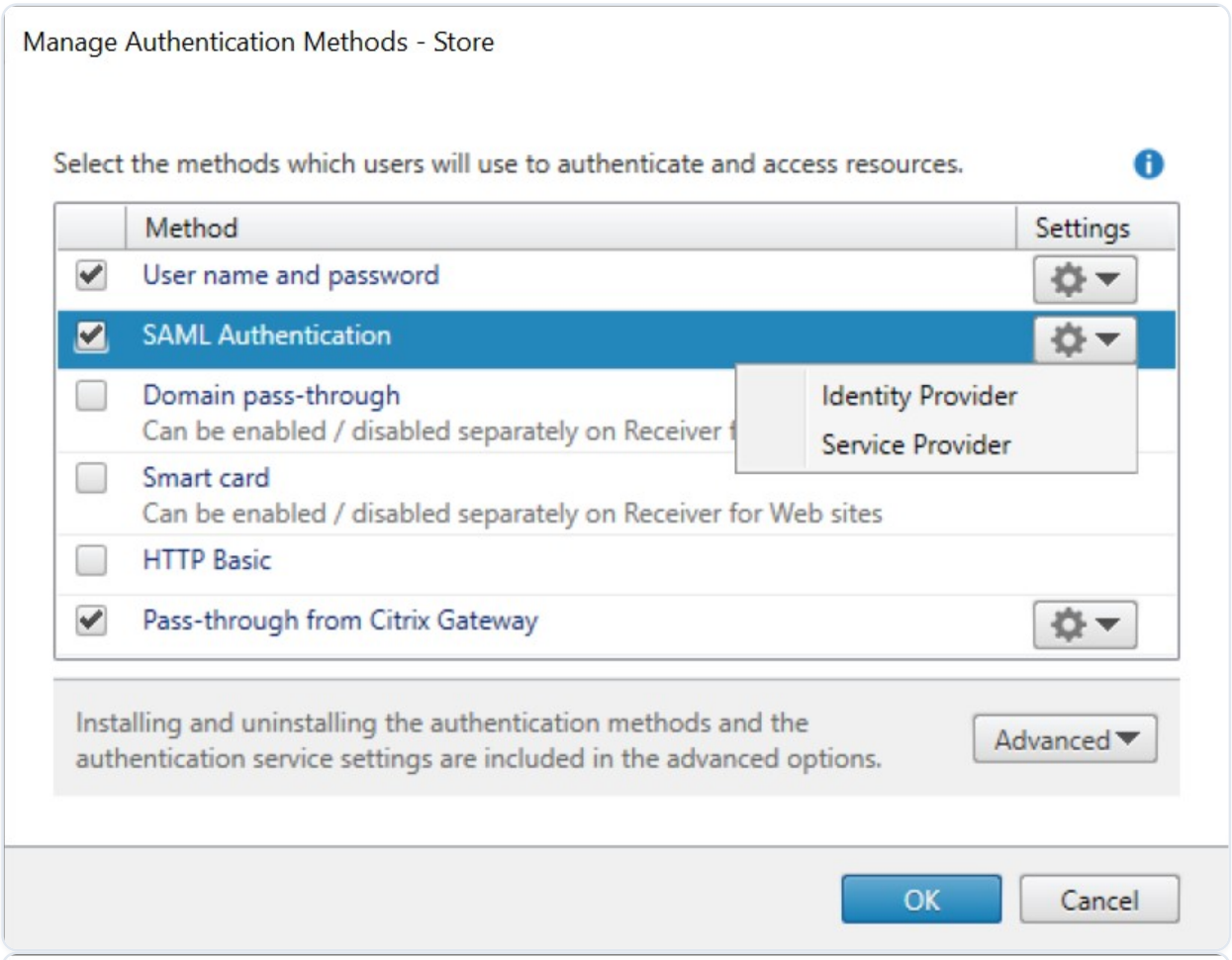
# Note: Ensure that the file is encoded as UTF-8

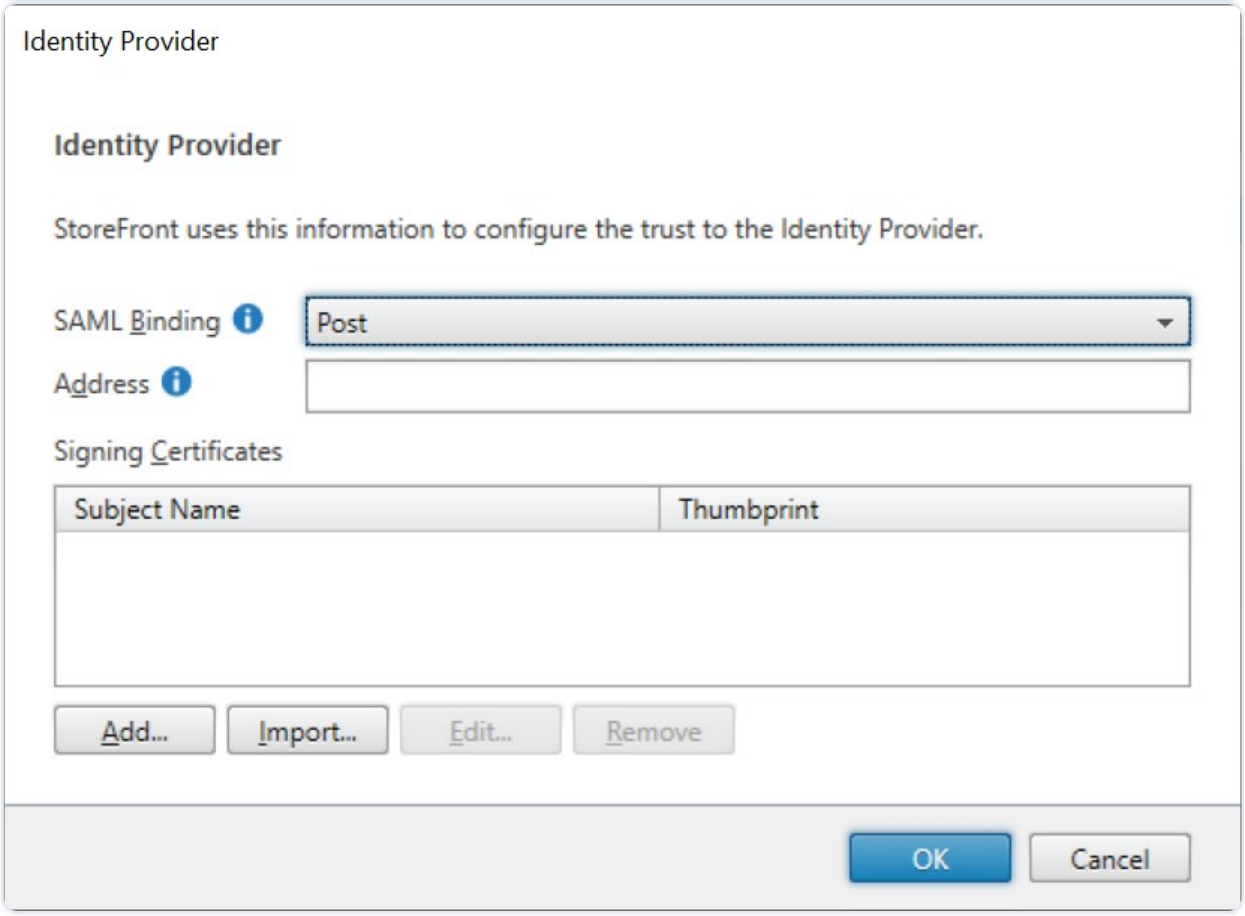
Update-STFSamlIdPFromMetadata -AuthenticationService $auth -FilePath "C:
\Users\exampleusername\Downloads\FederationMetadata.xml"
```

Configure Identity Provider

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.





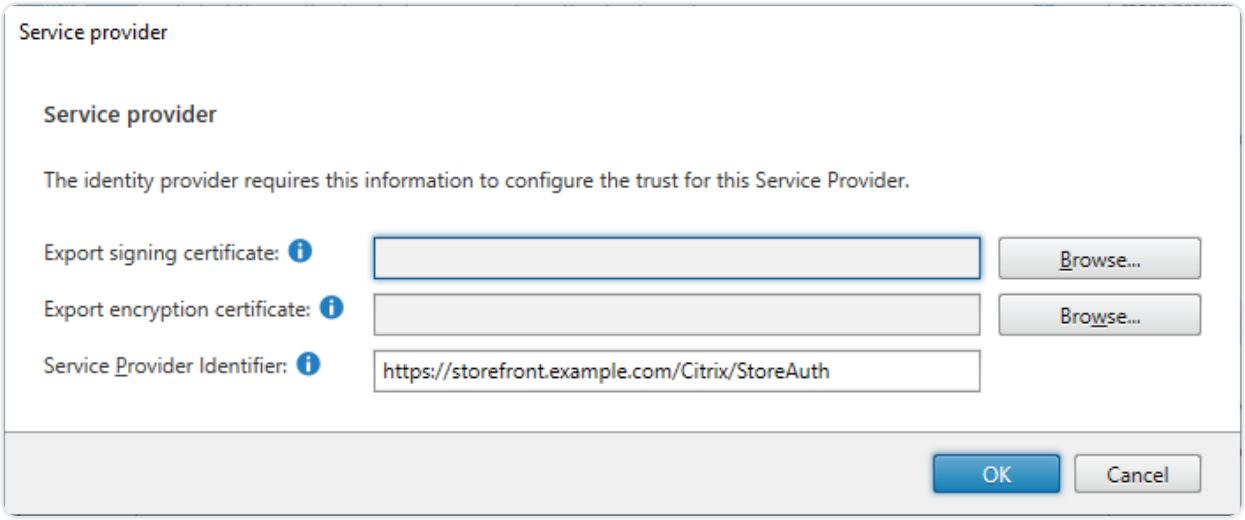
2. Choose **SAML Binding** of **Post** or **Redirect**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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. For Active Directory joined resources, use Federated Authentication Service to provide single sign-on.

Known issues

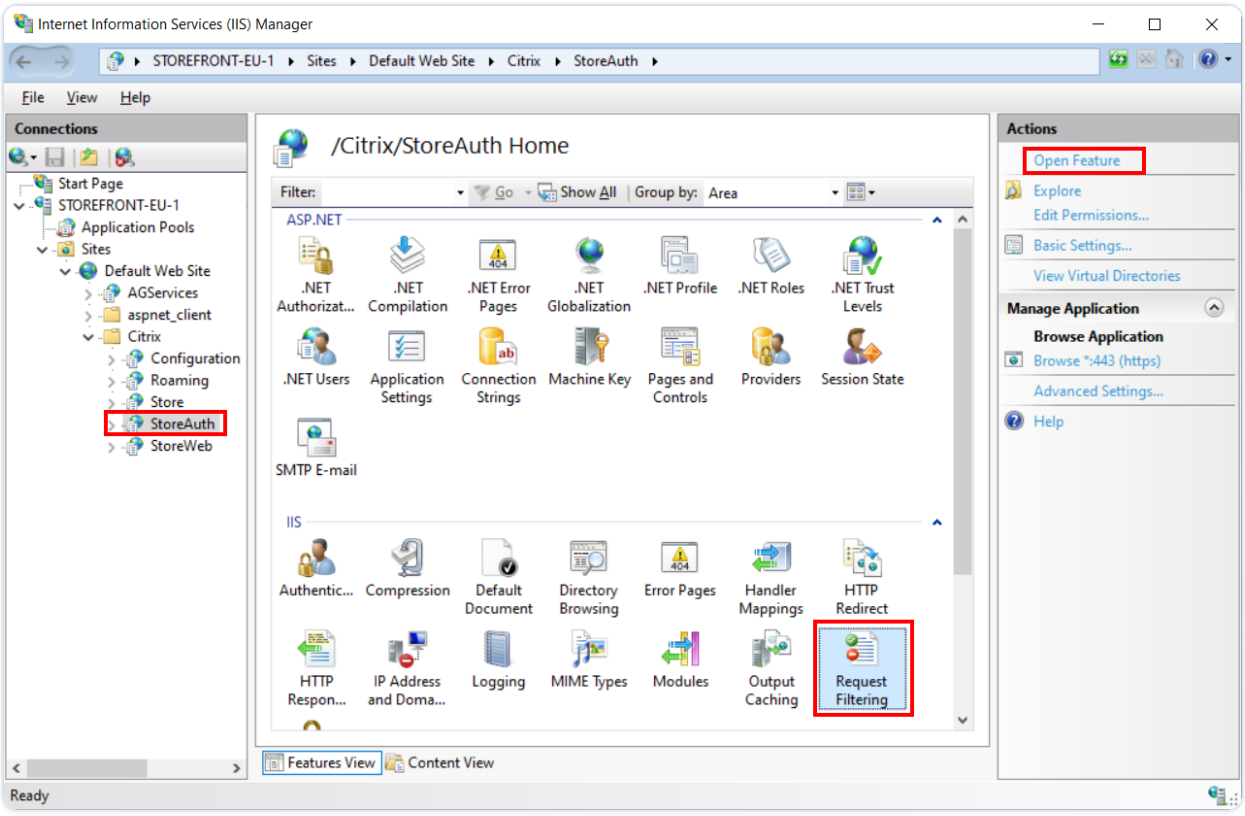
With StoreFront 2607, when using SAML authentication direct to StoreFront from {Citrix Workspace app for iOS or Citrix Workspace app for Android, authentication may fail.

- {Citrix Workspace app for iOS displays error "You cannot have the _ri parameter with any of the following: _cx, _id, _cs, _hf, _rt or _ps"
- Citrix Workspace app for Android displays error "For a browser, you must supply all of the following: _cx, _id, and _cs, _ps and _hf are optional. For a native client _rt must be supplied and _ps is optional".

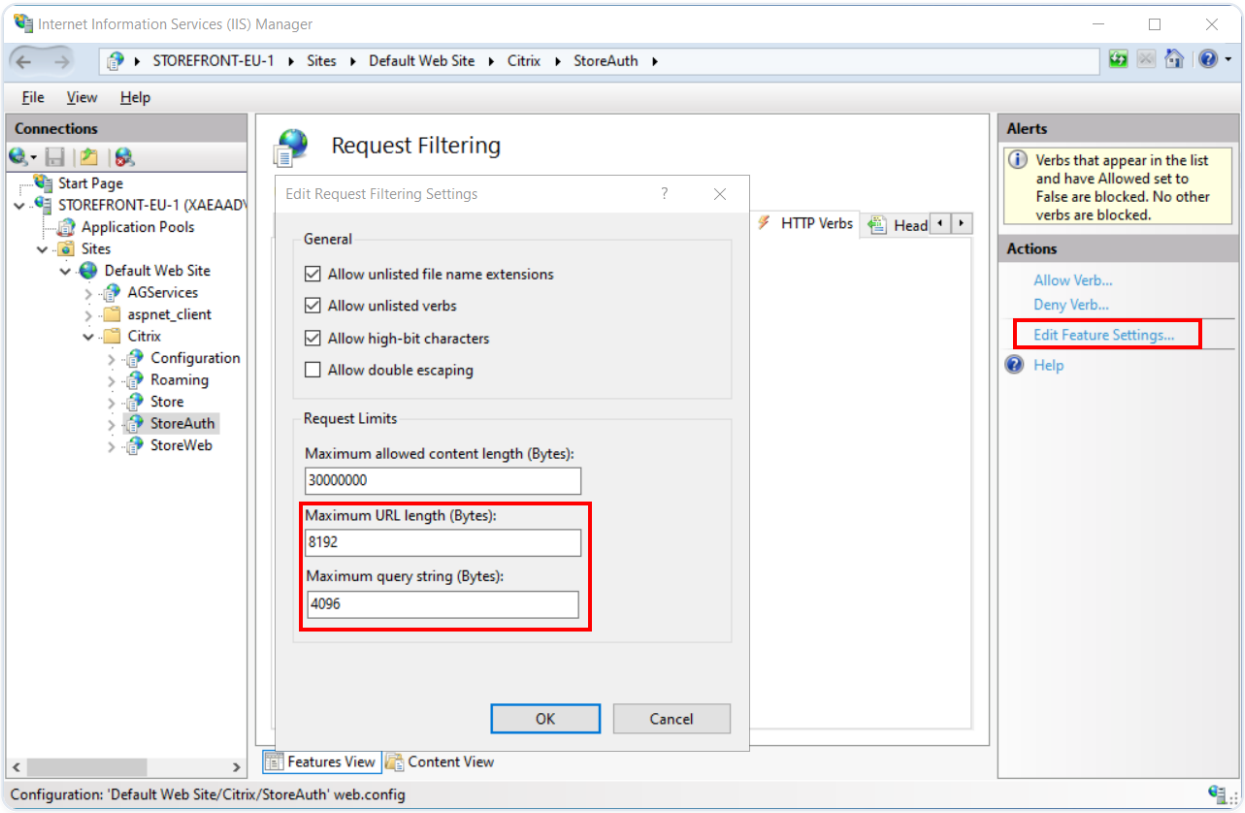
When using StoreFront prior to 2607, authentication may fail with HTTP Error 404.15 - Not Found. This occurs when the query string is too long and is blocked by IIS request filtering. By default IIS sets a query string limit of 2048 and a total URL length of 4096. To work around this, increase the maximum URL and query string lengths.

1. Open Internet Information Services (IIS) Manager.
2. In the **Connections** pane, expand the server select the authentication virtual directory.
3. From the main pane, open **Request Filtering**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



4. In the **Actions** pane, click **Edit Feature Settings...**
5. Increase the **Maximum URL length (Bytes)** and **Maximum query string (Bytes)**.



6. Select **OK** to save your changes.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Microsoft Entra ID SAML authentication

This article describes how to configure Microsoft Entra ID as a SAML identity provider for StoreFront.

For general SAML configuration information, see SAML authentication.

Prerequisites

- Users must have a hybrid identity. The on-premises Active Directory UPN must be synchronized to Entra ID (either to the Entra ID UPN or the on-premises UPN attribute).
- StoreFront must be accessible via HTTPS with a valid certificate.
- You must have administrator access to your Entra ID tenant.

Create an enterprise application

1. Sign in to the Microsoft Entra admin center.
2. Navigate to **Identity** > **Applications** > **Enterprise applications**.
3. Click **New application**.
4. Click **Create your own application**.
5. Enter a name such as **Citrix StoreFront**.
6. Select **Integrate any other application you don't find in the gallery (Non-gallery)**.
7. Click **Create**.

Configure enterprise application for SAML authentication

1. In the enterprise application you created, navigate to **Manage** > **Single sign-on**.
2. Select **SAML** as the single sign-on method.
3. In the **Basic SAML Configuration** section, click **Edit**.
4. Configure the following values:

   - **Identifier (Entity ID)**: `https://[storefront-host]/Citrix/[StoreName]Auth`
   - **Reply URL (Assertion Consumer Service URL)**: `https://[storefront-host]/Citrix/[StoreName]Auth/SamlForms/AssertionConsumerService`

   Replace `[storefront-host]` with your StoreFront server's fully qualified domain name and `[StoreName]` with your store name (for example, `Store`).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

TIP

To find the exact URLs for your store, see StoreFront SAML Endpoints.

5. Click **Save**.

Configure attributes and claims

StoreFront requires the user's Active Directory UPN in the SAML **Name ID** claim to look up the user.

1. In the **Attributes & Claims** section, click **Edit**.
2. Click on the **Unique User Identifier (Name ID)** claim.
3. If the Active Directory UPN is the same as the Entra ID UPN then confirm that the **Source attribute** is set to `user.userprincipalname`. If the Active Directory UPN is different to the Entra ID UPN then change the **Source attribute** to `user.onpremisesuserprincipalname`
4. Click **Save**.

IMPORTANT

The UPN sent in the Name ID claim must match the user's UPN in Active Directory. StoreFront looks up this UPN in Active Directory to authenticate the user.

Assign users

1. Navigate to **Manage** > **Users and groups**.
2. Click **Add user/group**.
3. Select the users or groups that need access to StoreFront.
4. Click **Assign**.

Configure StoreFront

You can configure StoreFront to use Entra ID as the identity provider using metadata exchange or manual configuration.

OPTION 1: METADATA EXCHANGE (RECOMMENDED)

1. In the Entra ID enterprise application, navigate to **Manage** > **Single sign-on**.
2. In the **SAML Certificates** section, copy the **App Federation Metadata Url**.
3. On the StoreFront server, open PowerShell as administrator and run:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-Module "Citrix.StoreFront*" -ListAvailable | Import-Module



$StoreVirtualPath = "/Citrix/Store"

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath

$auth = Get-STFAuthenticationService -StoreService $store



Update-STFSamlIdPFromMetadata -AuthenticationService $auth -Url
"https://login.microsoftonline.com/[tenant-id]/federationmetadata/
2007-06/federationmetadata.xml"
```

Replace `[tenant-id]` with your Entra ID tenant ID or use the App Federation Metadata Url you copied.

OPTION 2: MANUAL CONFIGURATION

1. In the Entra ID enterprise application, navigate to **Manage** > **Single sign-on**.
2. Note the **Login URL** from the **Set up** section.
3. Download the **Certificate (Base64)** from the **SAML Certificates** section.
4. On the StoreFront server, import the certificate and configure the identity provider. See Configure Identity Provider.

Test the configuration

1. Navigate to `https://[storefront-host]/Citrix/[StoreName]Auth/SamlTest`
2. You are redirected to the Entra ID sign-in page. Sign in with a user account that:
   - Is assigned to the enterprise application
   - Has a hybrid identity with a UPN synchronized from Active Directory
3. After successful authentication, you are redirected back to the test page showing the identity claims.
4. Verify that the **NameID** claim contains the user's Active Directory UPN.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Troubleshooting

AUTHENTICATION FAILS WITH "USER NOT FOUND"

This error occurs when StoreFront cannot find the user in Active Directory. Verify that:

- The user has a hybrid identity with their UPN synchronized from Active Directory to Entra ID.
- The **Name ID** claim is configured correctly:
  - If on-premises UPN matches Entra ID UPN: Name ID should use `user.userprincipalname`
  - If on-premises UPN differs from Entra ID UPN: Name ID should use `user.onpremisesuserprincipalname`
- The StoreFront server can communicate with the domain controllers.

REDIRECTION LOOP

If users experience a redirection loop between StoreFront and Entra ID:

- Verify that the **Reply URL** in Entra ID matches the Assertion Consumer Service URL exactly.
- Check for conflicting authentication methods enabled on the store.
- Review IIS logs on the StoreFront server for error details.

CERTIFICATE ERRORS

If you see certificate validation errors:

- Verify that the signing certificate from Entra ID is correctly imported into StoreFront.
- Check that the certificate has not expired.
- Ensure the certificate is trusted by the StoreFront server.

Domain pass-through authentication

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

StoreFront Configuration

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

To use domain pass-through with a web browser, the website must successfully detect Citrix Workspace app using either Citrix Web Extension or Citrix Workspace Launcher. You might need to update users' web browser configuration to allow domain pass-through authentication.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. To enable pass-through of smart card credentials for users who access stores without Citrix Gateway, add the following setting in the 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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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

When using a Citrix Gateway for remote access to a store, typically it is configured so that users must first authenticate at the gateway. To avoid StoreFront needing to re-authenticate the user, you can enable **Pass-through from Citrix Gateway** authentication. This has three variations:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- The gateway passes the Active Directory username and password to StoreFront, StoreFront uses them to authenticate the user.
- The gateway passes the Active Directory username but no password to StoreFront. StoreFront is configured to trust the gateway and does not authenticate the user.
- The gateway passes an Entra ID access token to StoreFront. StoreFront is configure to trust the gateway and does not authenticate the user. StoreFront looks up user information using the Microsoft Graph API.

The **Pass-through from Citrix Gateway** authentication method is automatically enabled when you first configure remote access to a store. For more information about configuring StoreFront for access via a Citrix Gateway, see Configure a Citrix Gateway.

Supported Citrix Gateway authentication methods

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

- **Domain** Users log in using their Active Directory username and password.
- **RSA** Users log in using passcodes that are derived from tokencodes generated by security tokens combined, sometimes, with personal identification numbers. If you enable pass-through authentication by security token only, ensure that the resources you make available do not require extra or alternative forms of authentication, such as users' Microsoft Active Directory domain credentials.
- **Smart card** Users log in using a smart card linked to their Active Directory account.
- **RSA + Domain** Users log in using both their domain credentials and security token passcodes.
- **SAML** Users are redirected to a third party IdP to log in via SAML. The SAML assertion must include the UPN of the user's Active Directory account. For more information, see NetScaler as a SAML SP.
    - To configure SAML with Entra ID, see Configure Microsoft Entra ID as SAML IdP and NetScaler as SAML SP. The user must have a hybrid identity. StoreFront does not support pure Entra ID identities when using SAML.
- **OIDC with Entra ID** Users are redirected to Microsoft Entra ID for authentication. The user can either be pure Entra ID or have a hybrid identity. For more information, see Entra ID authentication using OIDC.

To achieve pass-through, in the session profile you must select **Single Sign-on to Web Application**. If you have disabled this setting, or are not using the gateway for authentication, then

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pass-through from Citrix Gateway authentication is not used and you must configure one of the other StoreFront authentication methods.

Double source authentication

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>`.

Multi domain authentication

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.

Enable Gateway pass-through

To enable gateway pass-through authentication for a store when connecting through Citrix Workspace app, in the Authentication Methods window select **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 Edit website | Authentication methods tab.

Configure trusted user domains

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

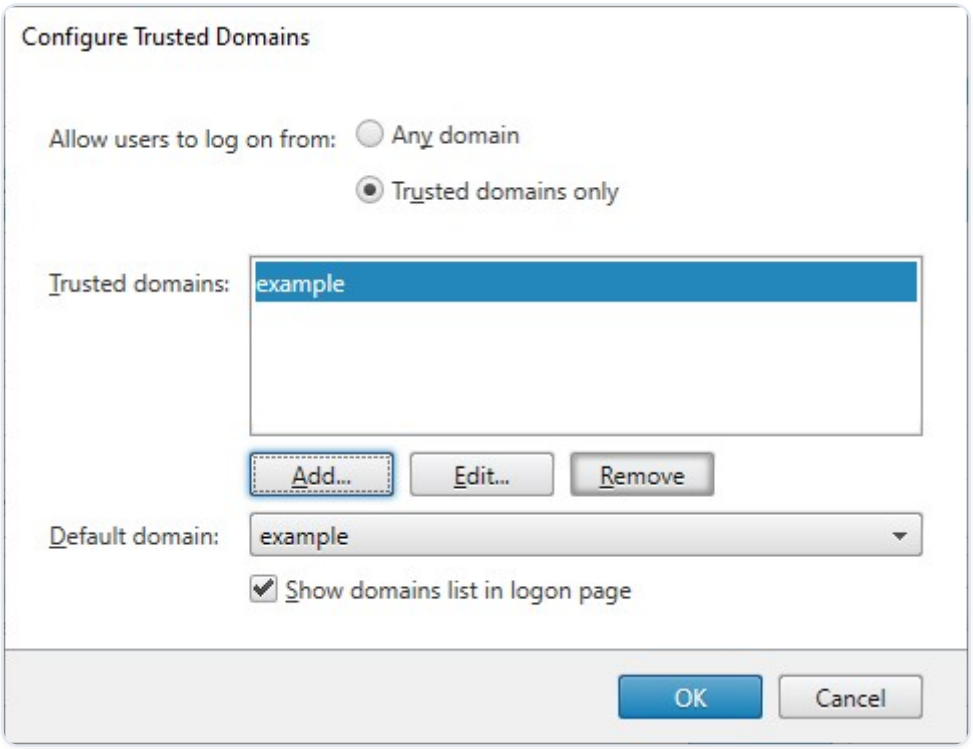
1. In the "Manage Authentication methods" window, from the **Pass-through from Citrix Gateway** > **Settings** drop-down menu, select **Configure Trusted Domains**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



Delegated authentication

By default StoreFront requires the Citrix Gateway to pass through a username and password which StoreFront validates against Active Directory. 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

you enter a callback URL when configuring the gateway so StoreFront can verify the request came from the Citrix Gateway, see Manage Citrix Gateways.

To configure this from the management console, in the **Manage Authentication Methods** window, from the **Pass-through from Citrix Gateway** > **Settings** drop-down menu, select **Configure Delegated Authentication**.

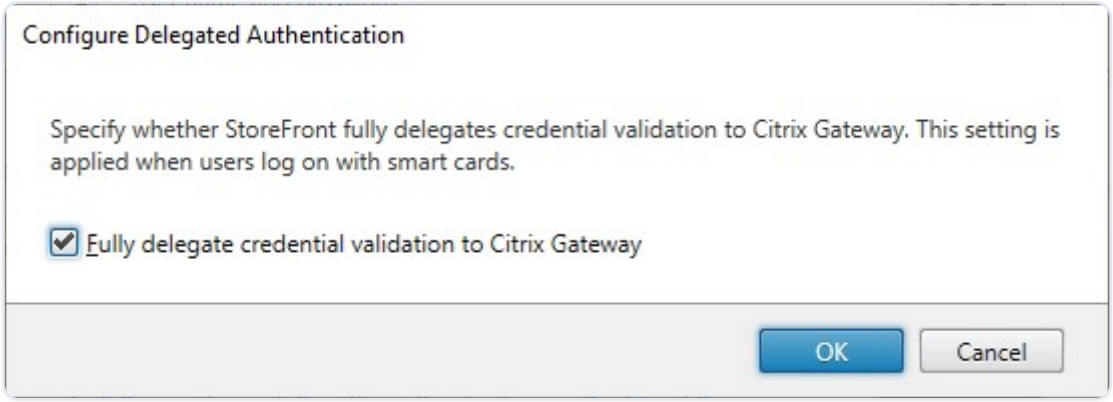
To configure this using PowerShell, run cmdlet Set-STFCitrixAGBasicOptions with parameter `CredentialValidationMode`.

There are three possible options but only two are selectable from the management console.

CREDENTIAL VALIDATION MODE	MANAGEMENT CONSOLE	DESCRIPTION
`Password`	Clear **Fully delegate credential validation to Citrix Gateway**.	StoreFront expects to receive a password from the Citrix Gateway and validates it with Active Directory.
`Kerberos`	Cannot be configured using management console. If configured using PowerShell, displays as **Fully delegate credential validation to Citrix Gateway** selected.	StoreFront ignores any password it receives from the Citrix Gateway. If the gateway is configured with a callback URL then StoreFront validates that the request came from the expected server. It is strongly recommended you configure a callback. In future versions of StoreFront, authentication may fail if a callback is not configured.
`Auto`	Select **Fully delegate credential validation to Citrix Gateway**.	If the request contains a password then StoreFront validates the password with Active Directory. If the request does not contain a password and the gateway is configured with a callback URL then StoreFront validates that the request

© 1997–2026 Citrix Systems, Inc. All rights reserved.

CREDENTIAL VALIDATION MODE	MANAGEMENT CONSOLE	DESCRIPTION
		came from the expected server. Otherwise authentication fails.



.

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 the Citrix Gateway 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**.

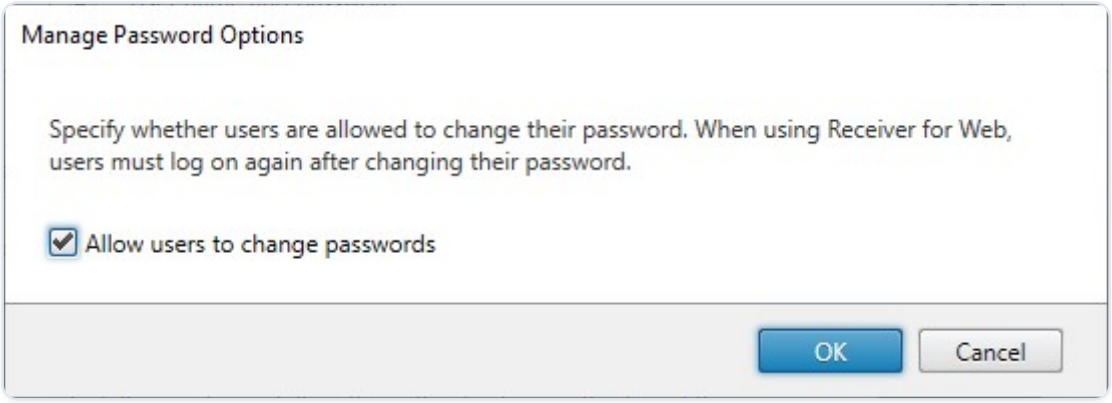
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



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

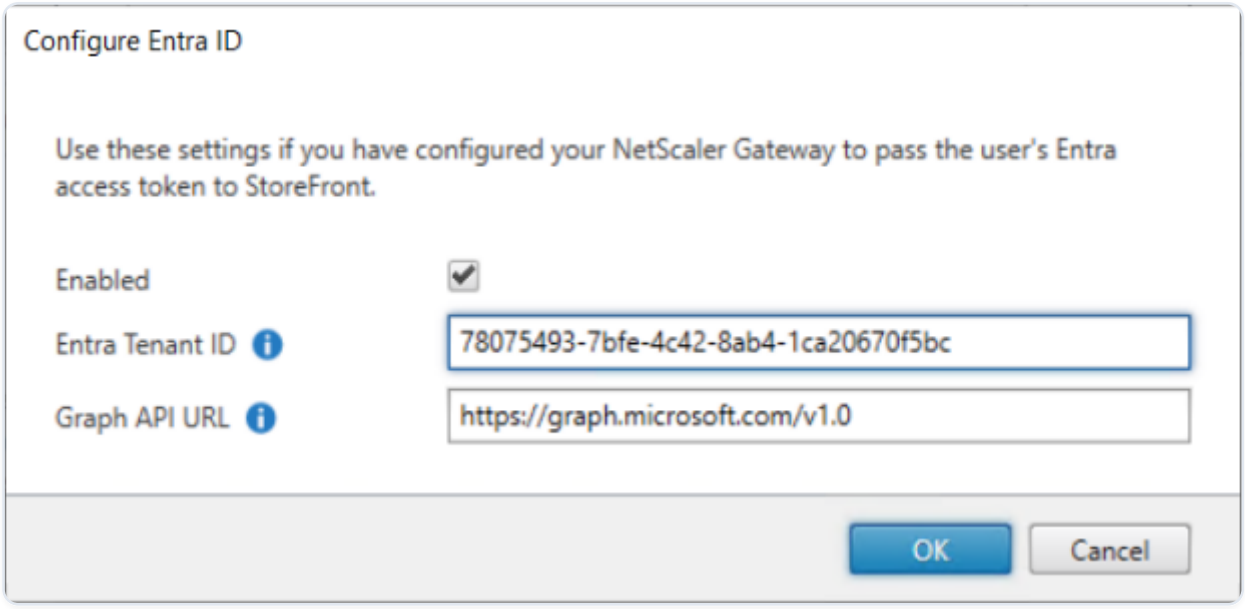
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

Entra ID using OIDC

If you have configured the gateway for Entra ID authentication using OIDC, you must configure StoreFront to read the access token provided by the NetScaler gateway and look up the user information in the Microsoft Graph API.

1. In the **Manage Authentication Methods** window, from the **Pass-through from Citrix Gateway** > **Settings** drop-down menu, select **Manage Password Options**
2. Select **Enabled**.
3. Enter the **Entra Tenant ID**.
4. Optionally enter the **Graph API URL**. If not specified, it uses `https://graph.microsoft.com/v1.0`.



PowerShell

Run the following PowerShell, replacing the Tenant ID with the ID from your Entra ID tenant and `/Citrix/EntraStore` with the store path.

```
$store = Get-STFStoreService /Citrix/EntraStore

$authenticationService = Get-STFAuthenticationService -Store $store
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Set-STFEntraIdSettings -AuthenticationService $authenticationService
-TenantId "<Your tenant id>" -Enabled $true
```

Single sign-on to VDAs

Using Active Directory credentials

When a user authenticates at the gateway using LDAP authentication, the gateway passes the credentials through to StoreFront for authentication to VDA, providing single sign-on. This requires no additional configuration.

Using Federated Authentication Service

When a user authenticates at the gateway using 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 configure Federated Authentication Service to provide single sign-on.

Using Entra ID

If you have configured the Citrix Gateway to use OIDC Entra ID authentication, you can enable Entra ID single sign-on. This feature requires StoreFront 2603 or higher. For more information, see Entra ID single sign-on to VDAs (preview).

Manage websites

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:

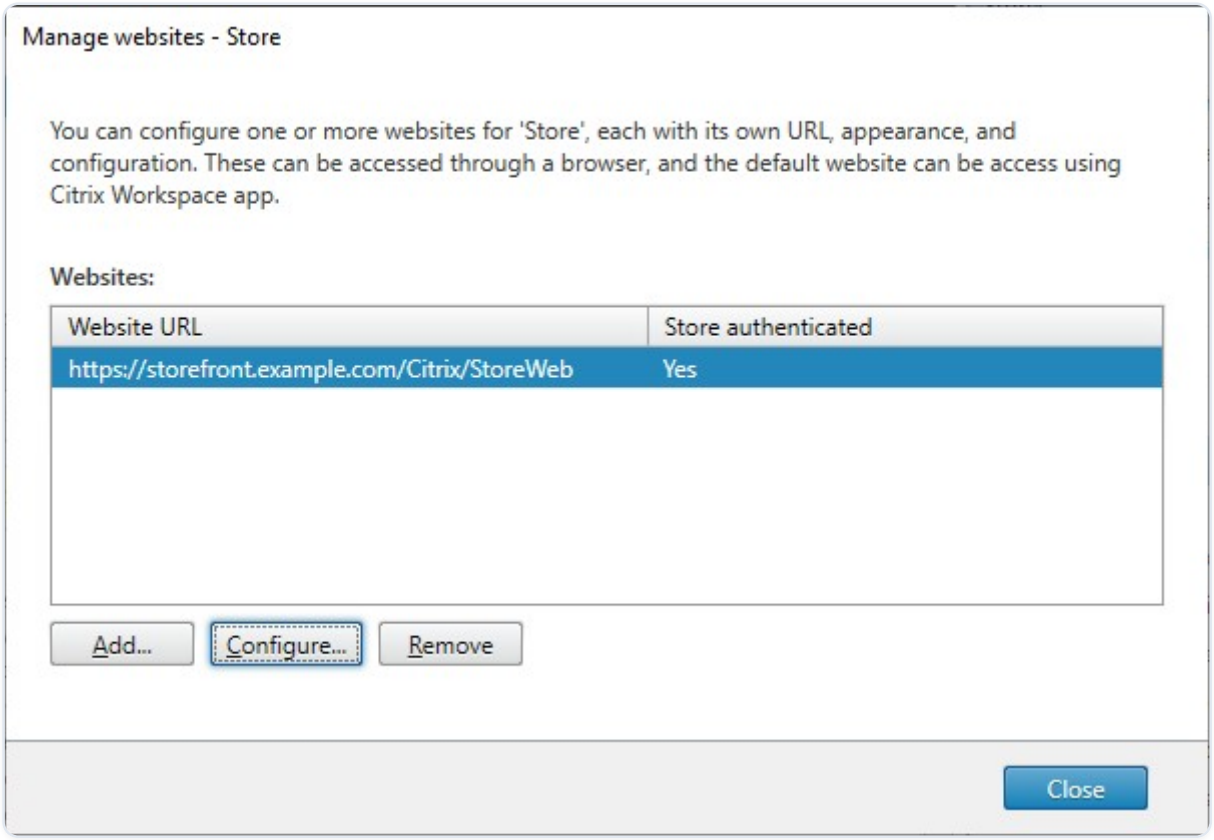
> In multiple server deployments, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once complete, propagate your configuration changes to the server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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**.



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

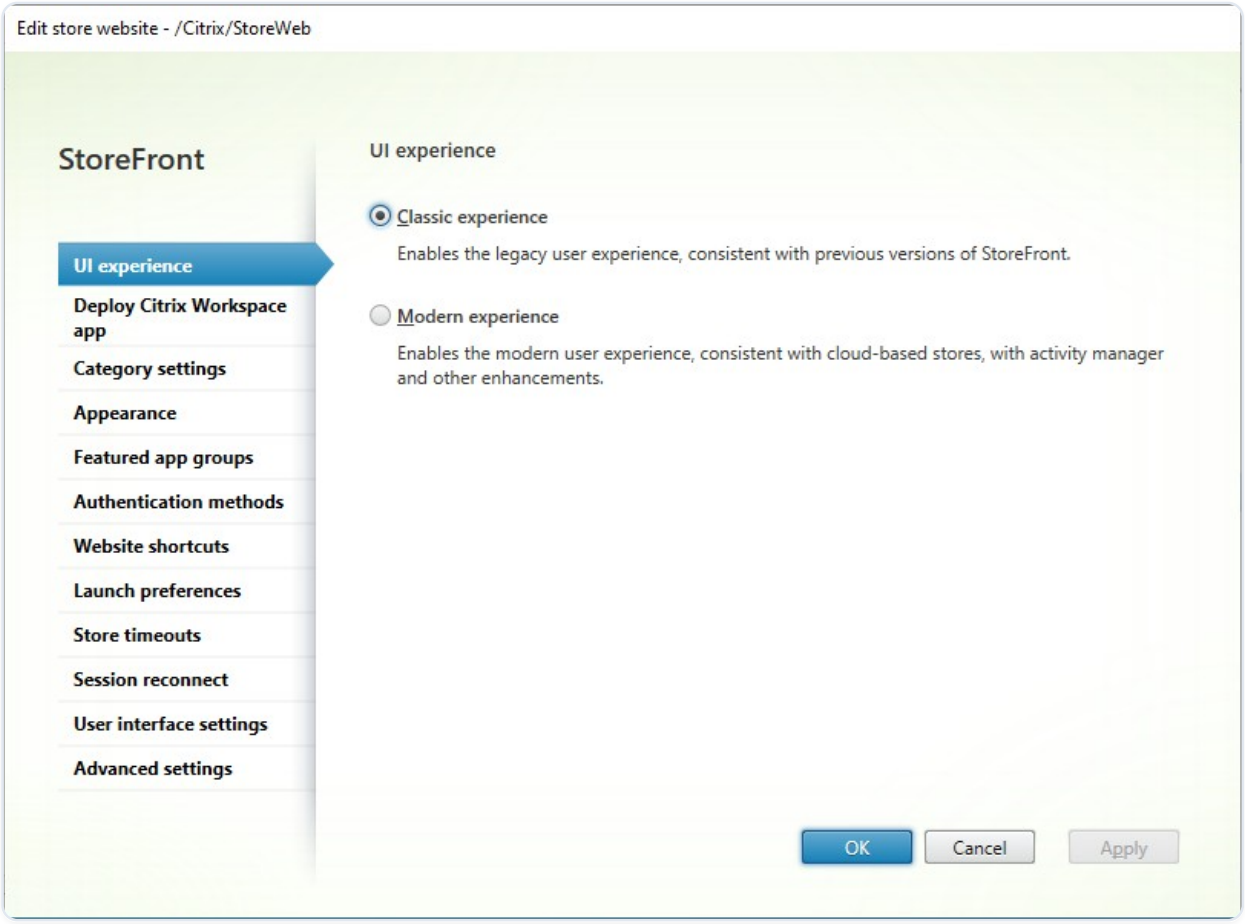
To get a list of websites, use cmdlet Get-STFWebReceiverService.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

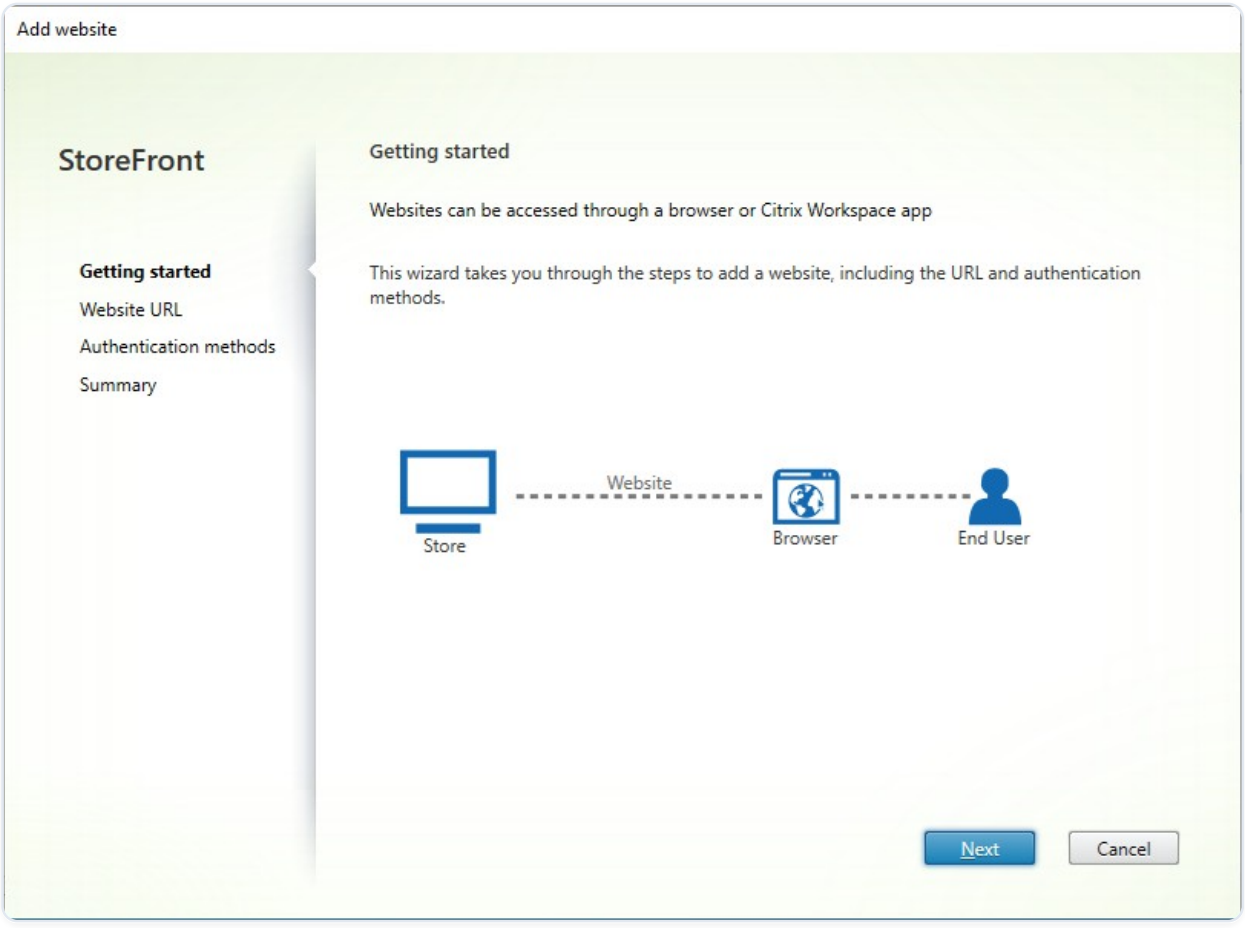
- Pinned links
- Custom announcements
- Dialog after log in
- Advanced Settings

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.

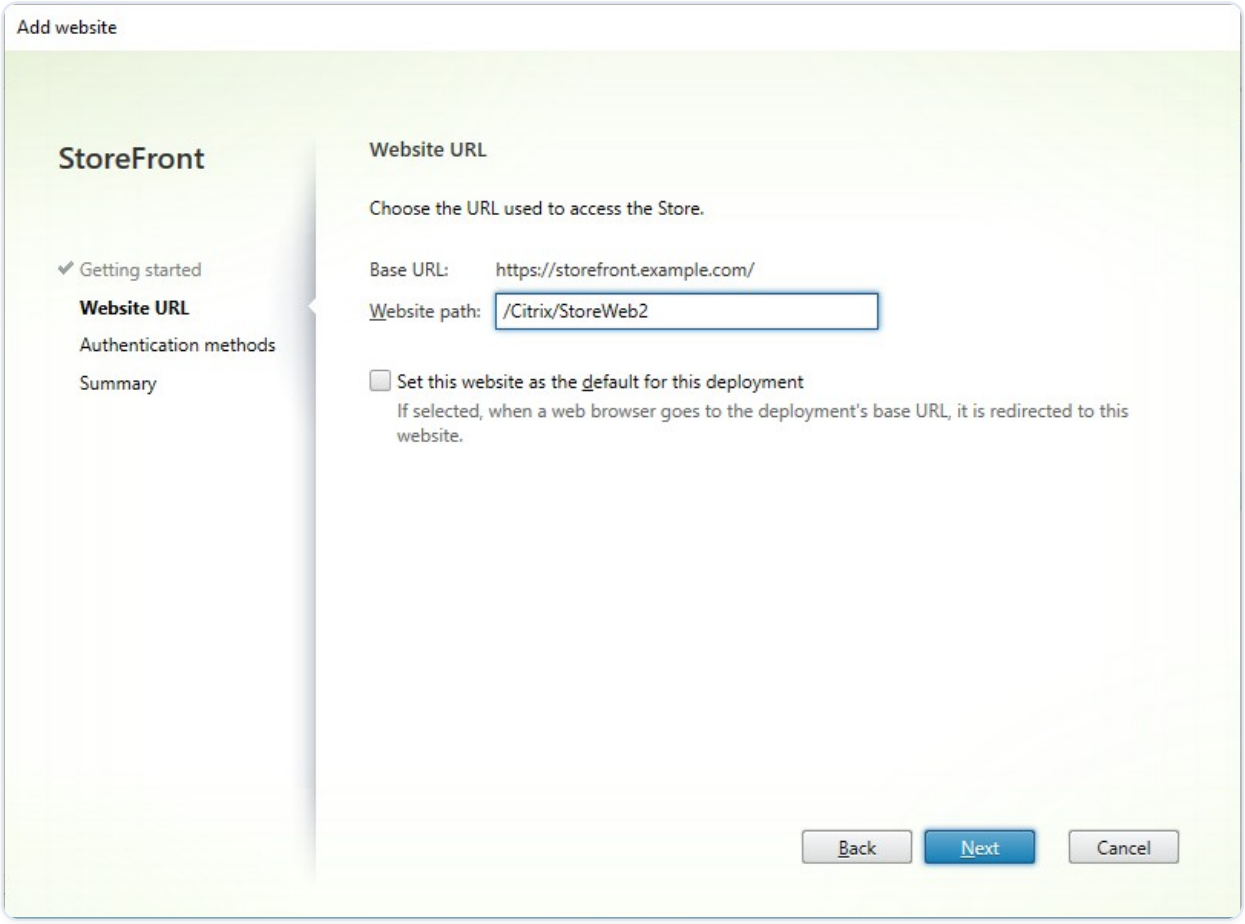
1. Select **Add...**.



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

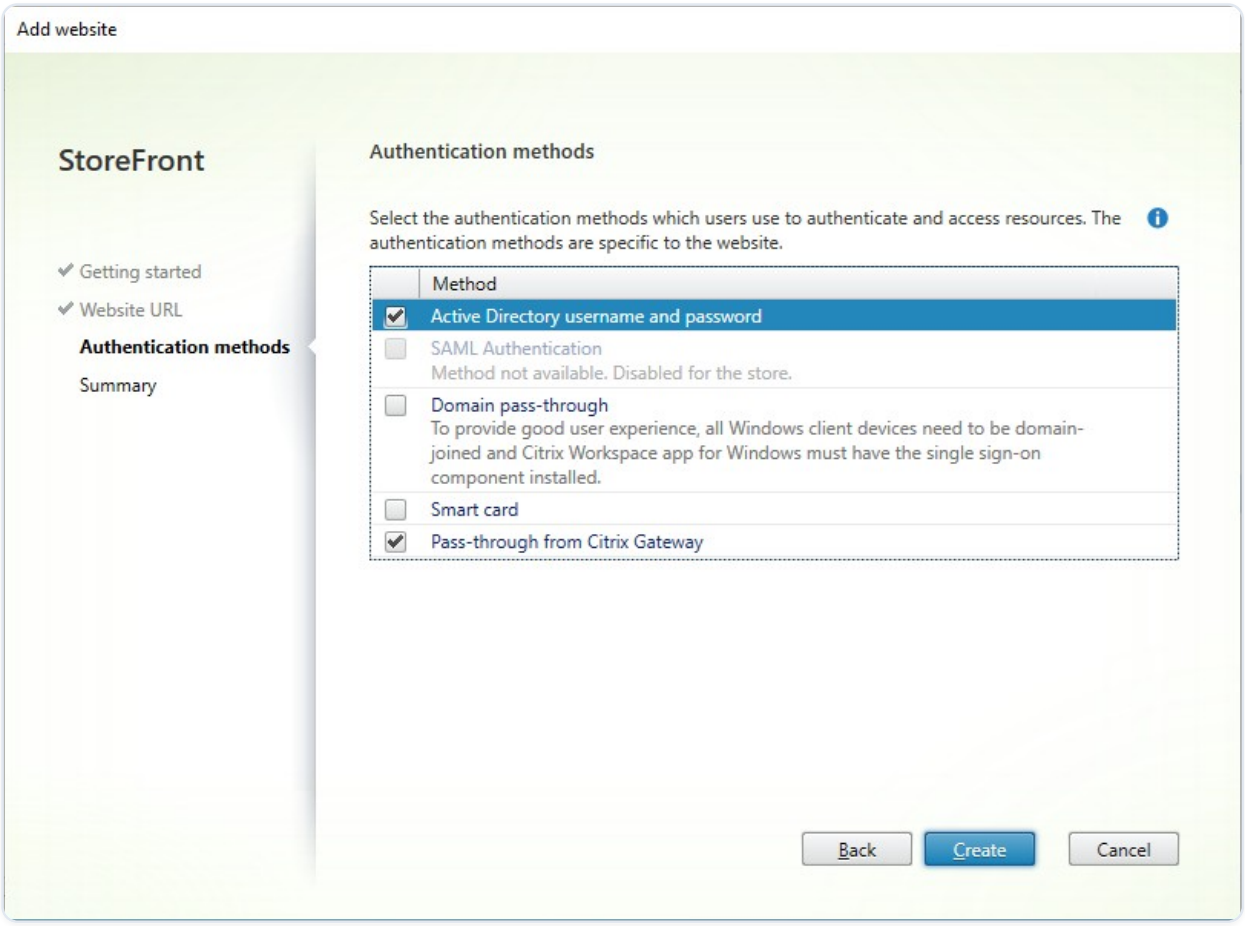
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**.



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

PowerShell

To create a website using PowerShell, run cmdlet `Add-STFWebReceiverService`.

Remove a website

1. Select the **Store** node in the left pane of the Citrix StoreFront management console, select the store for which you want to create the Citrix Receiver for Web site, and click **Manage websites** in the **Actions** pane.
2. Select a site and click **Remove**. When you remove a site, users can no longer use that webpage to access the store.

PowerShell

To remove a website using PowerShell, run cmdlet `Remove-STFWebReceiverService`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

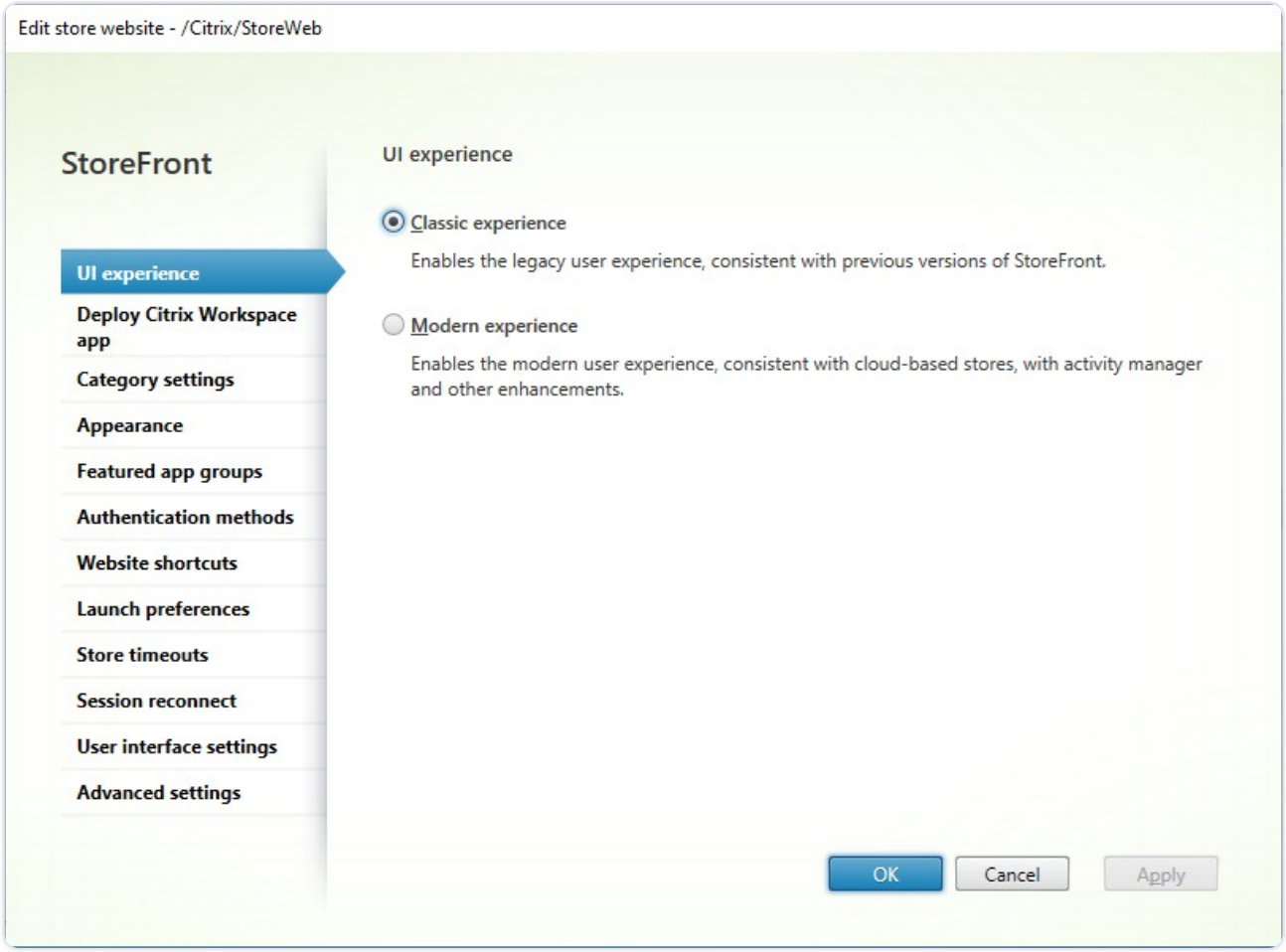
UI Experience

IMPORTANT:

From StoreFront 2311 to 2407, the modern experience is available as a tech preview and should not be used in production. From StoreFront 2411 it is generally available.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

For example:

```
(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:

```
$rfw=Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

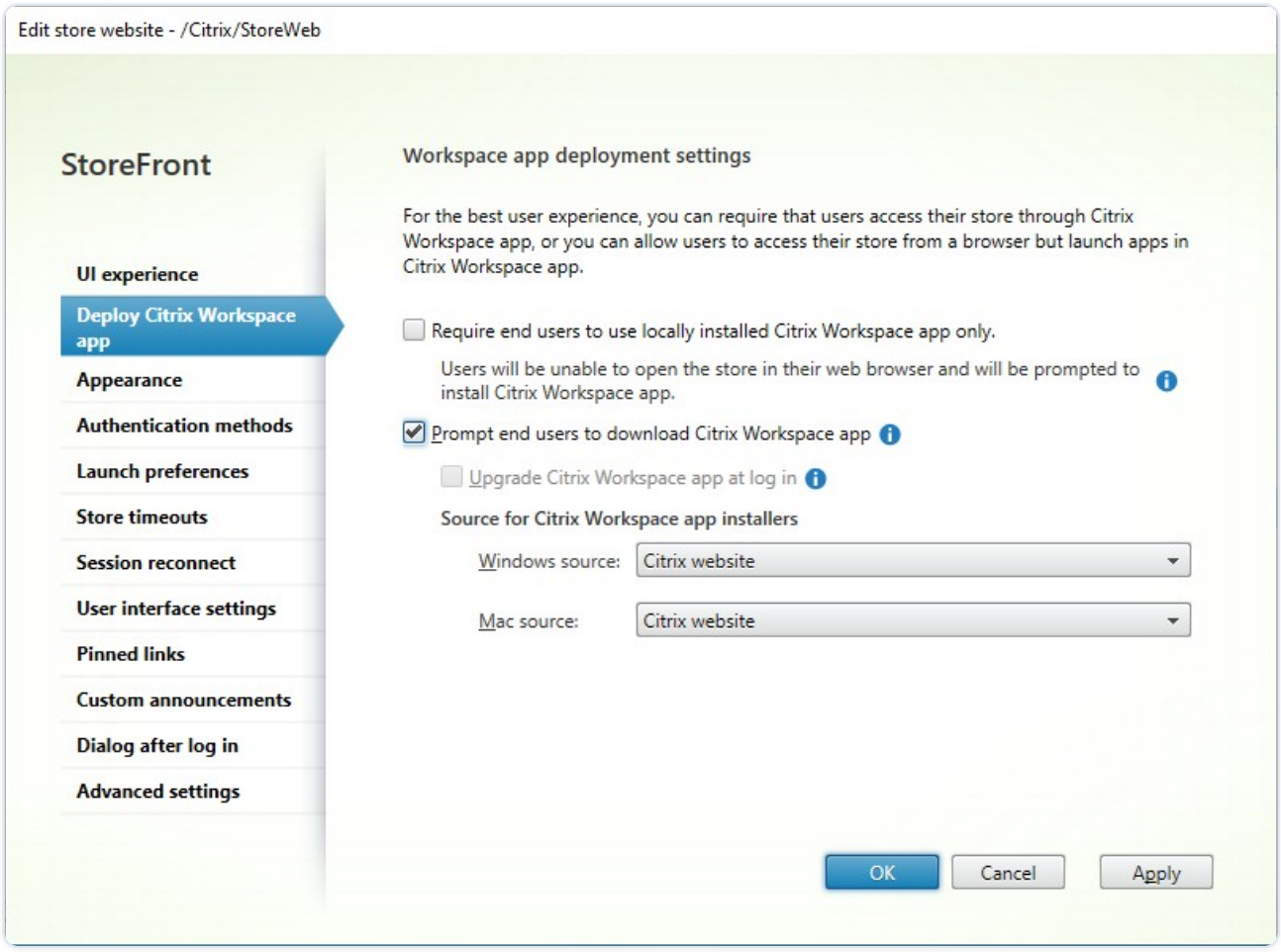
Set-STFWebReceiverService -WebReceiverService $rfw -WebUIExperience
Workspace
```

Citrix Workspace app deployment

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

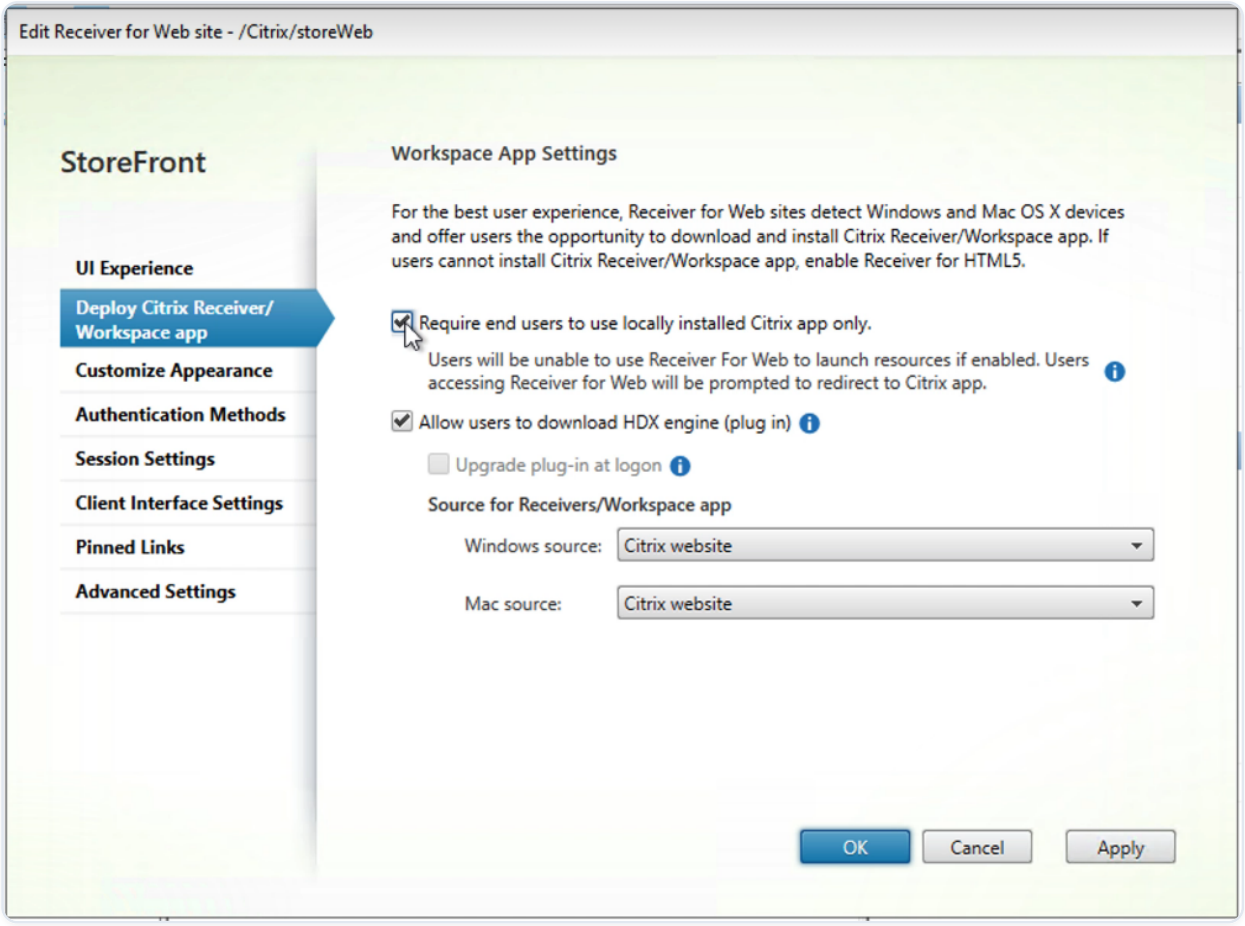
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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 2411 and later:

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

- The minimum required version of StoreFront is 2411.
- Uses 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Run the PowerShell command Set-STFWebReceiverUserInterface

```
$receiver = Get-STFWebReceiverService

Set-STFWebReceiverUserInterface -WebReceiverService $receiver
-ProgressiveWebAppEnabled $true
```

User experience

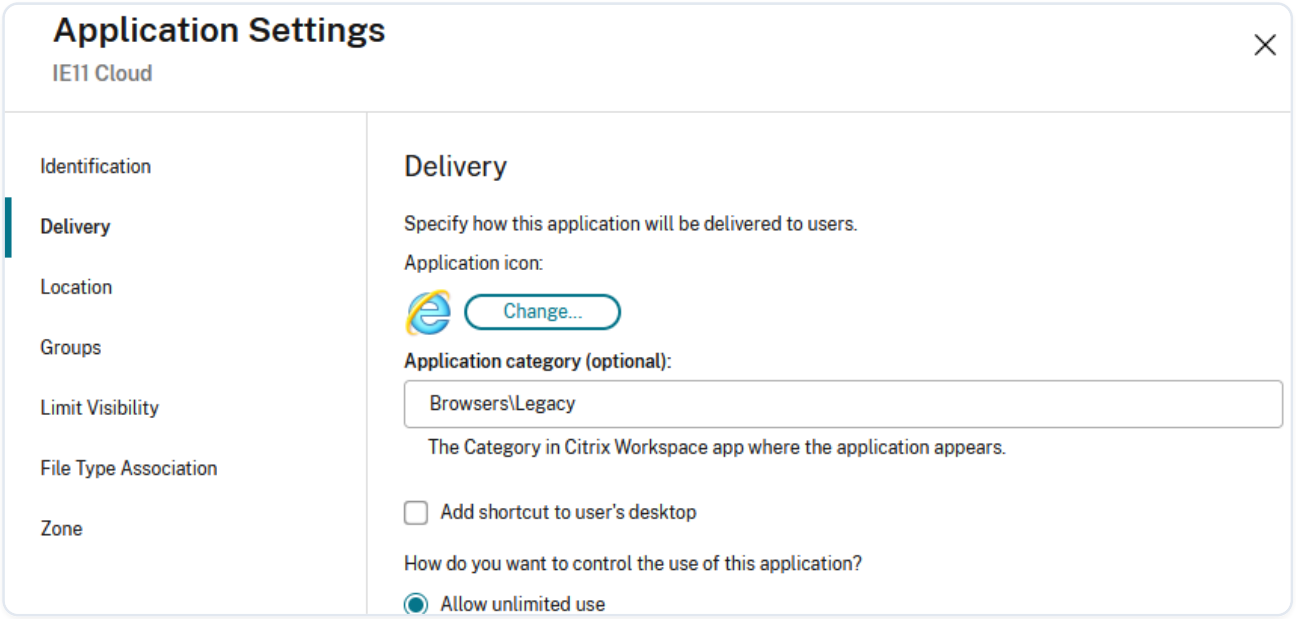
For more information on how users can install the app, see Installing as a progressive web app (preview).

Category Settings

NOTE:

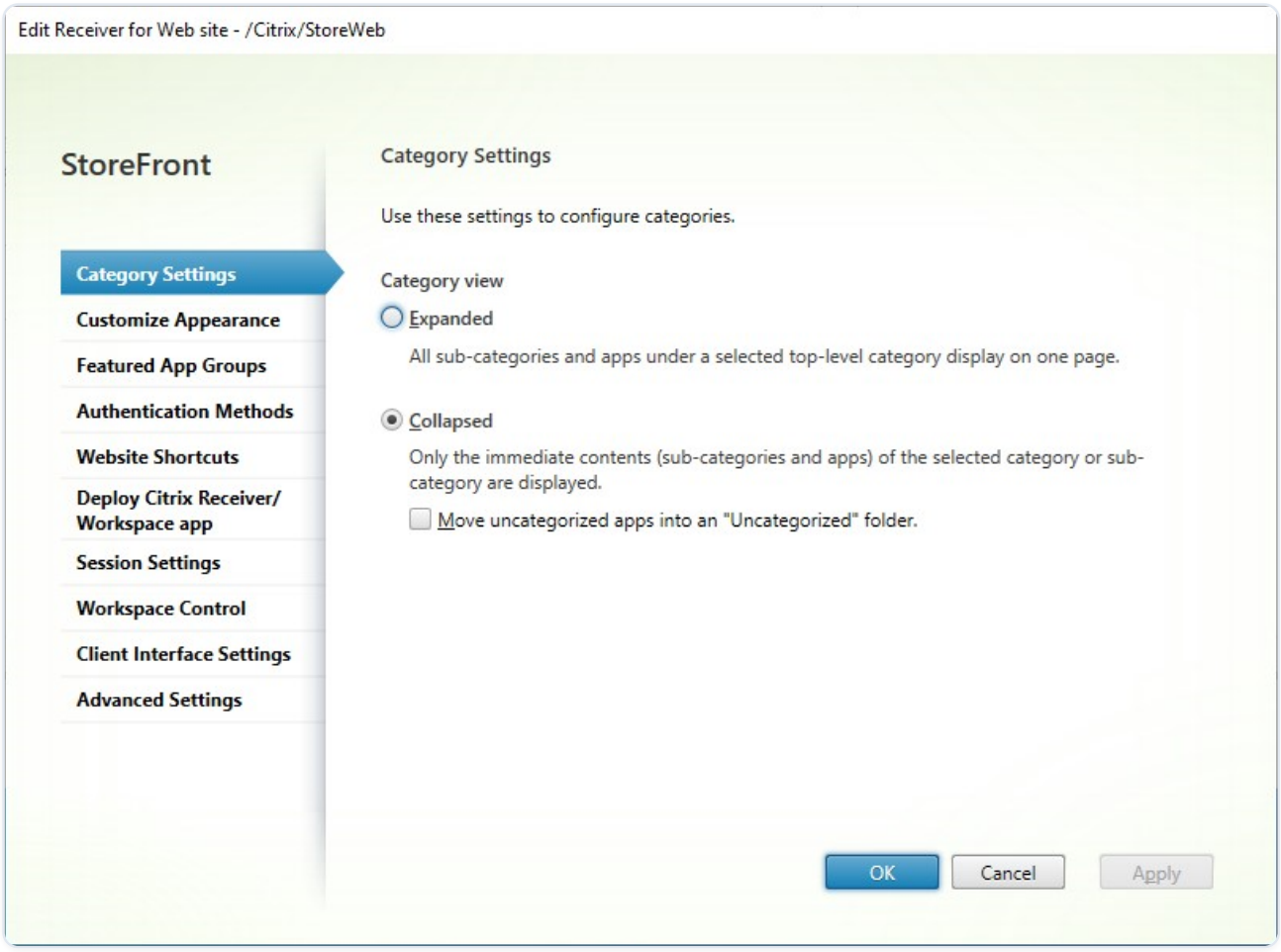
This functionality is only available using the classic experience.

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.



To modify category settings, go to Edit store website and select the **Category Settings** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

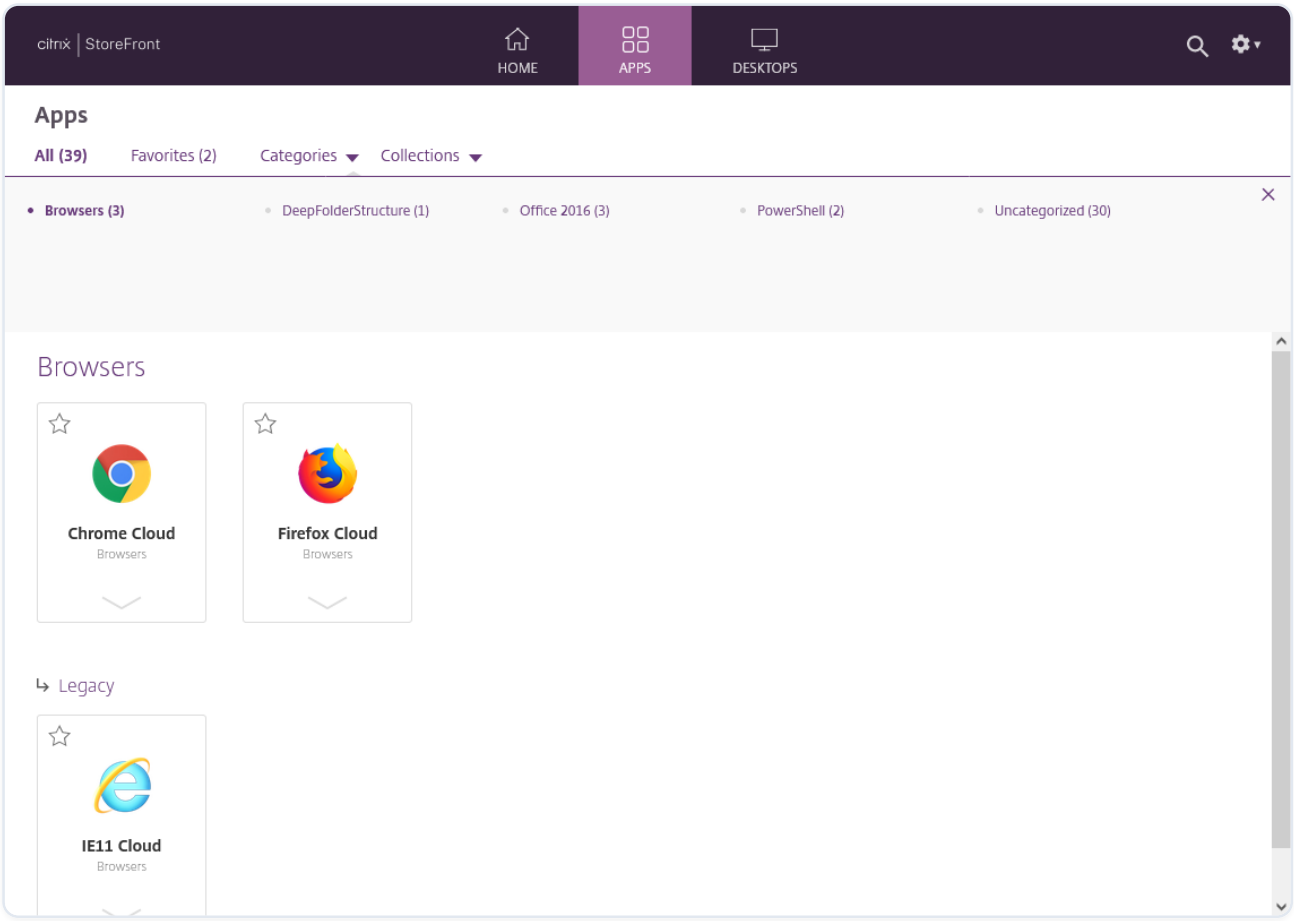


Category view

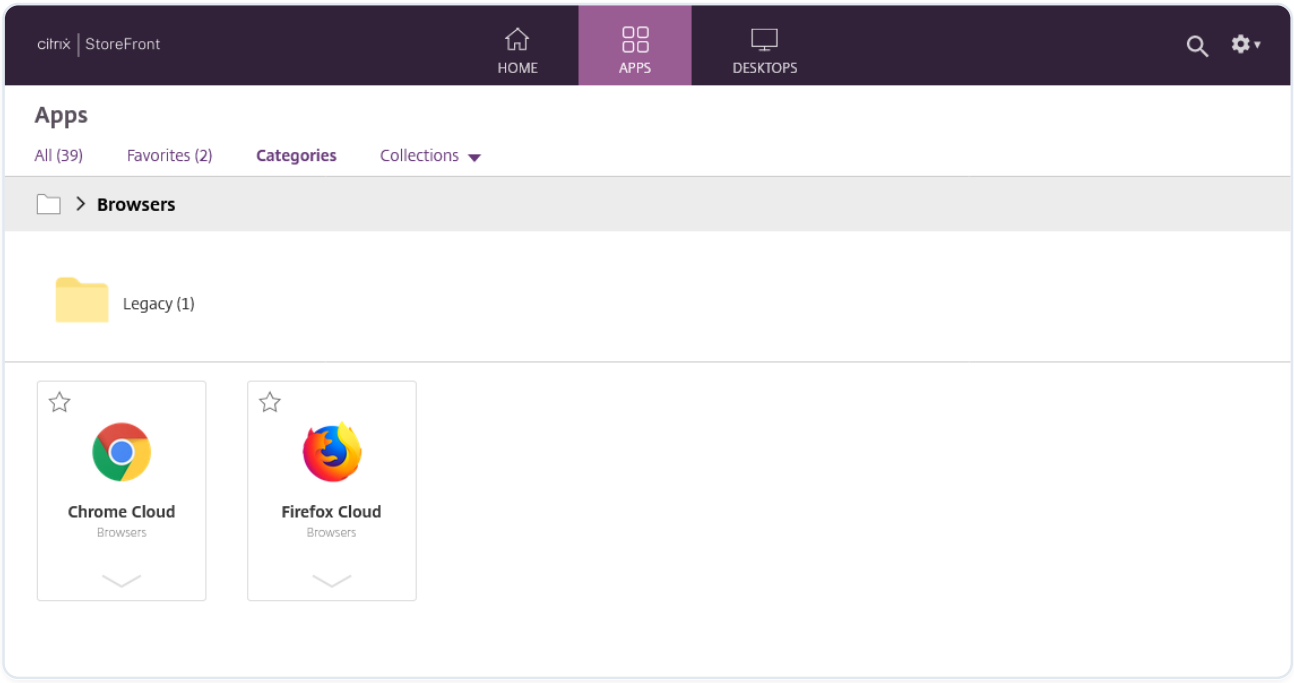
In the expanded view, StoreFront displays a list of top level categories. When the user clicks a top level category, StoreFront displays all apps in all subcategories on one page.

For example, if you have a category Browser with subcategory Legacy then it shows all browsers including those under legacy on one page:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



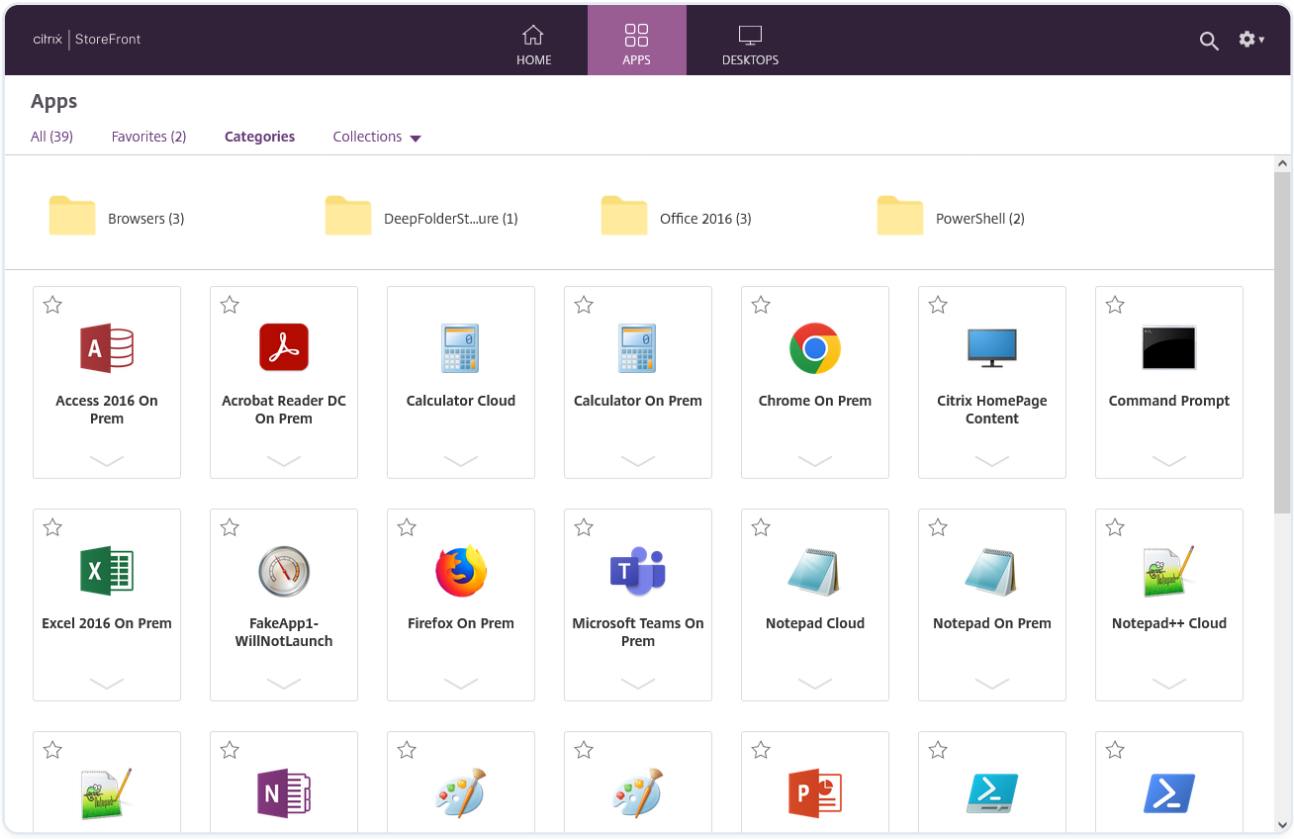
In the collapsed view, StoreFront initially displays a list of top level categories, and optionally all uncategorized apps. When the user clicks a category, StoreFront displays only the immediate contents (subcategories and apps) of the selected category. The user can click each subcategory to expand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



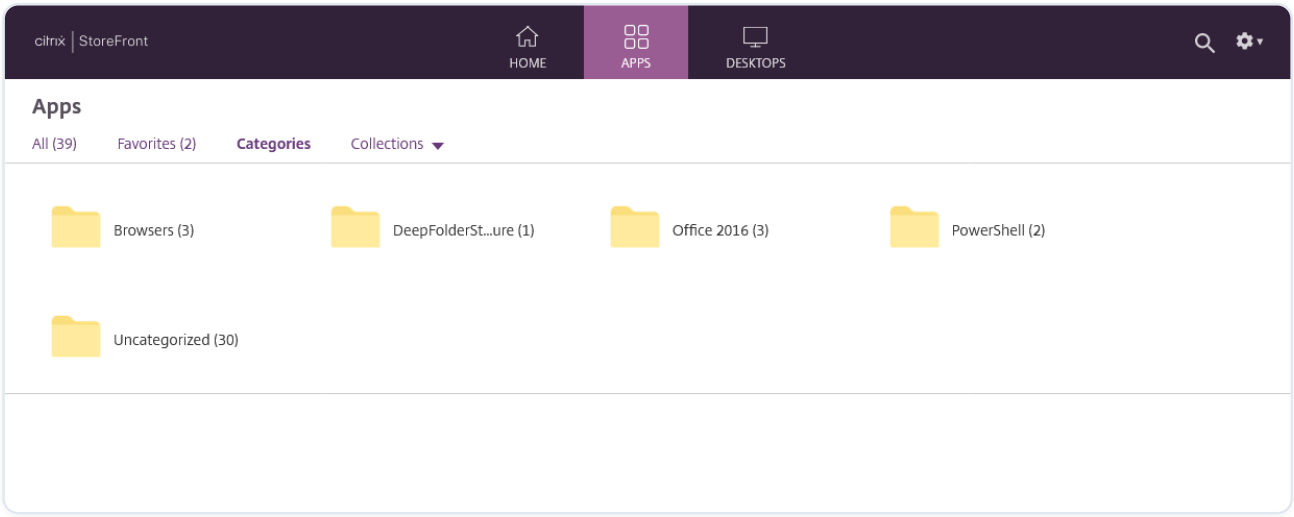
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

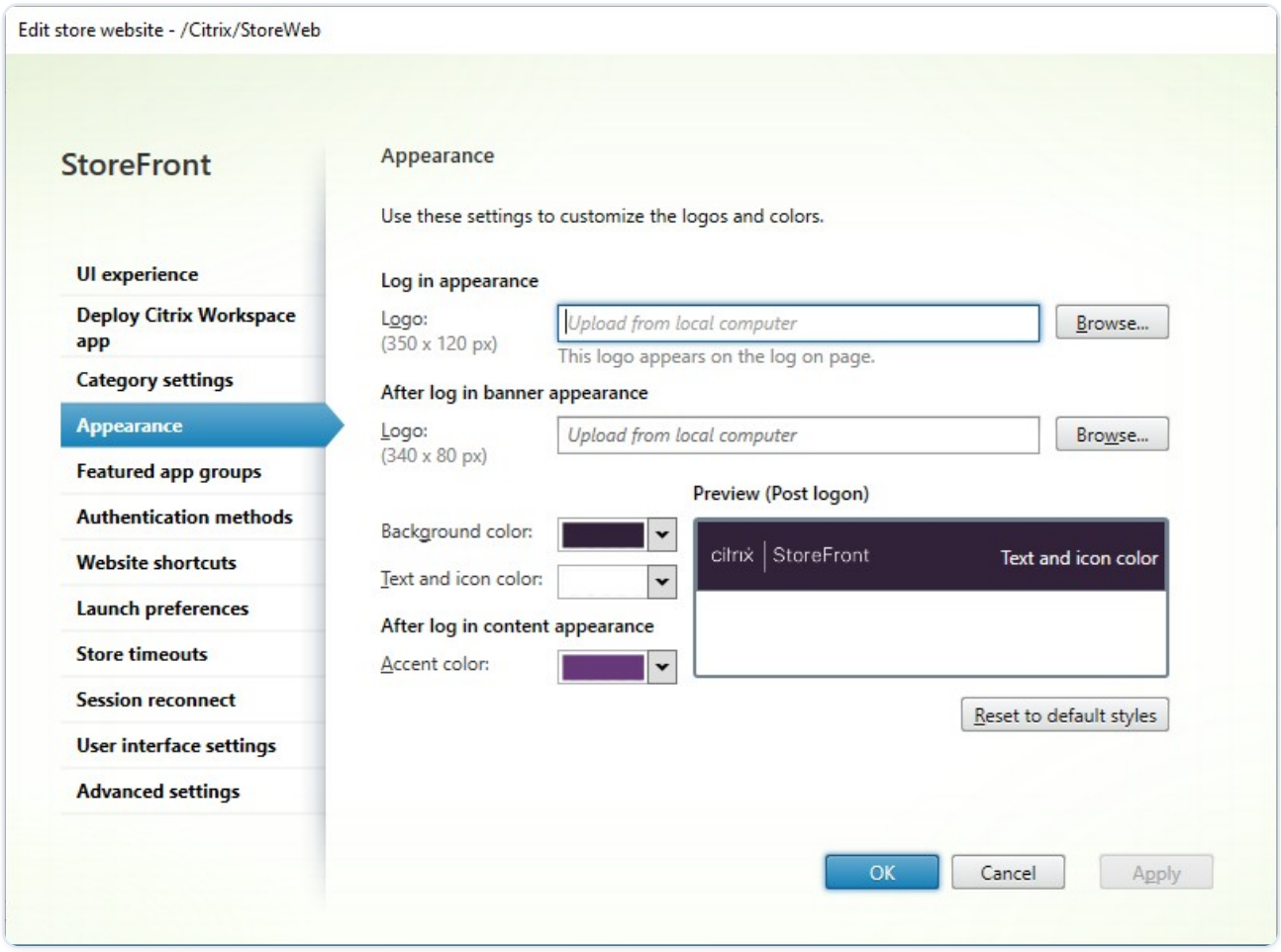
You can modify the logo and colors used within your store website.

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, .gif 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, .gif 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Featured app groups

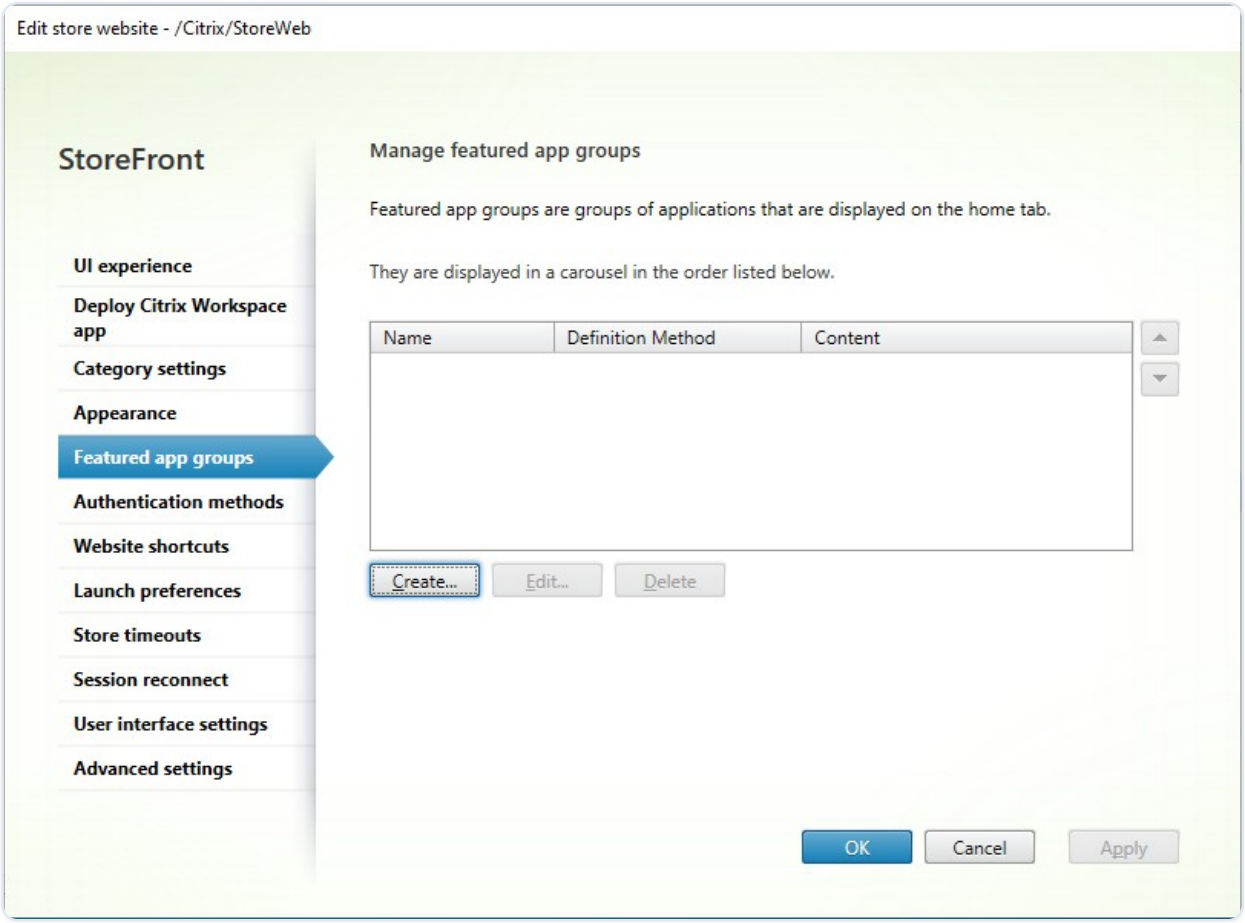
NOTE:

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.

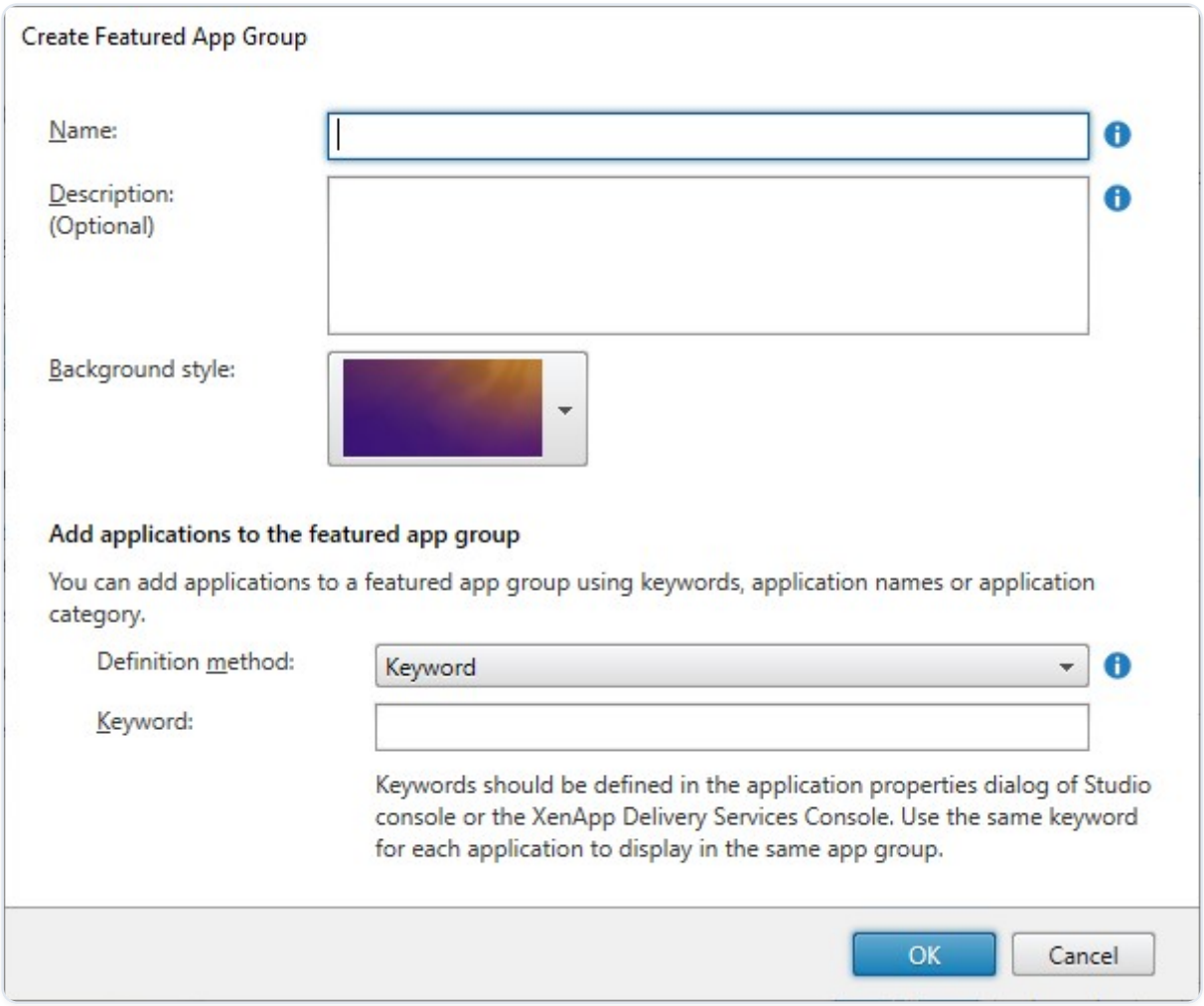


2. Click **Create** to define a new featured app group.
3. Specify a featured app group name, description (optional), background, and the method by which you define the featured app groups. You can choose keywords, application names, or application category.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

OPTION	DESCRIPTION
Keywords	Matches apps based on the keyword, defined Studio by including keywords in the app's description, for example "Use to send and receive emails KEYWORDS:collaboration"
Application category	Matches apps in a specific application category entered in Studio.
Application names	Use the application name to define the featured app group. All applications names matching the name included here in the Create a Featured App Group dialog screen are included in the featured app group. StoreFront does not support wildcards in application names. The match is not case sensitive, but it does match whole words. For example, if you type Excel, StoreFront matches a published app named Microsoft Excel 2013 but typing `Exc` does not match anything.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



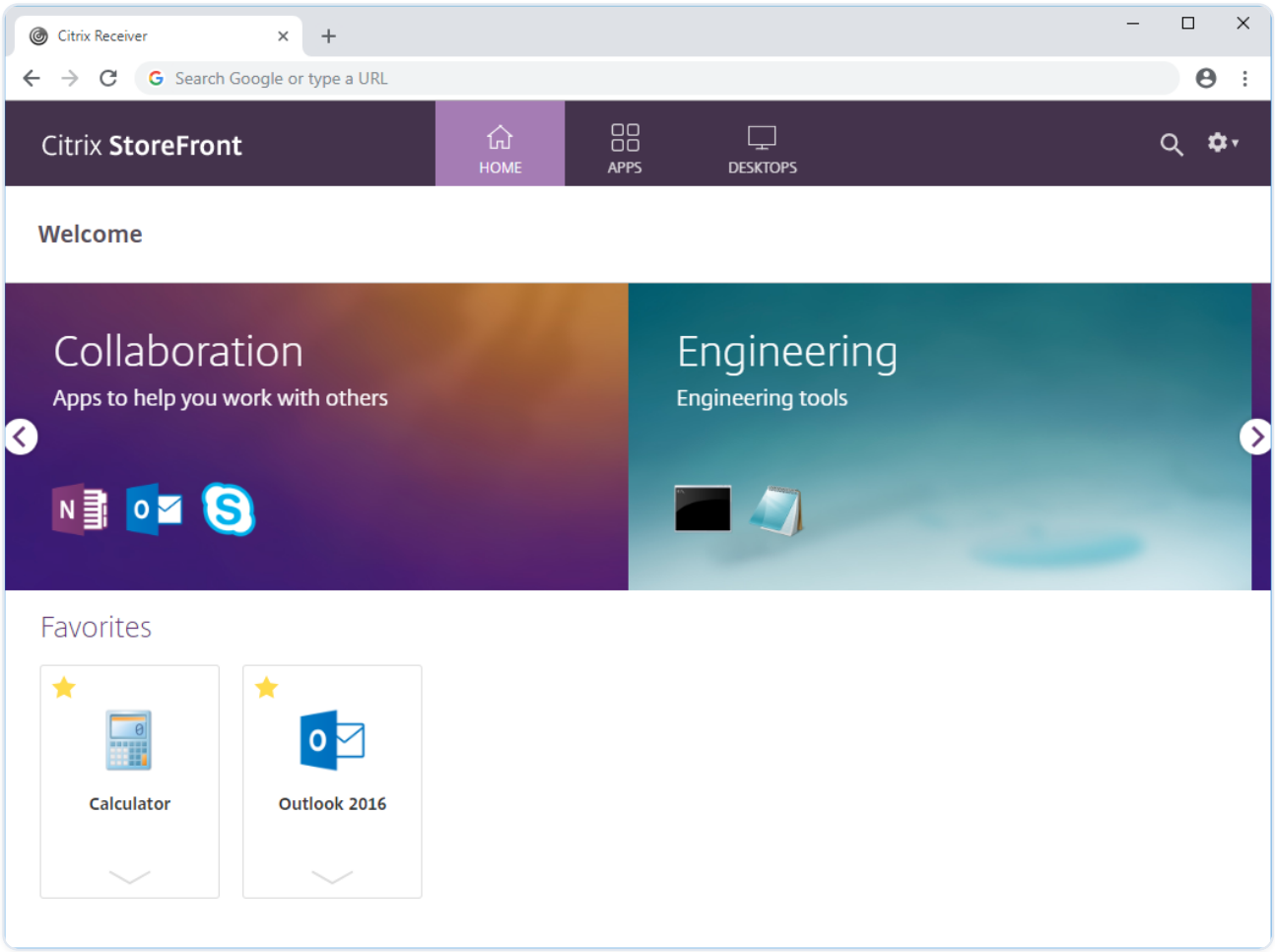
4. Click **OK**

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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...**

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

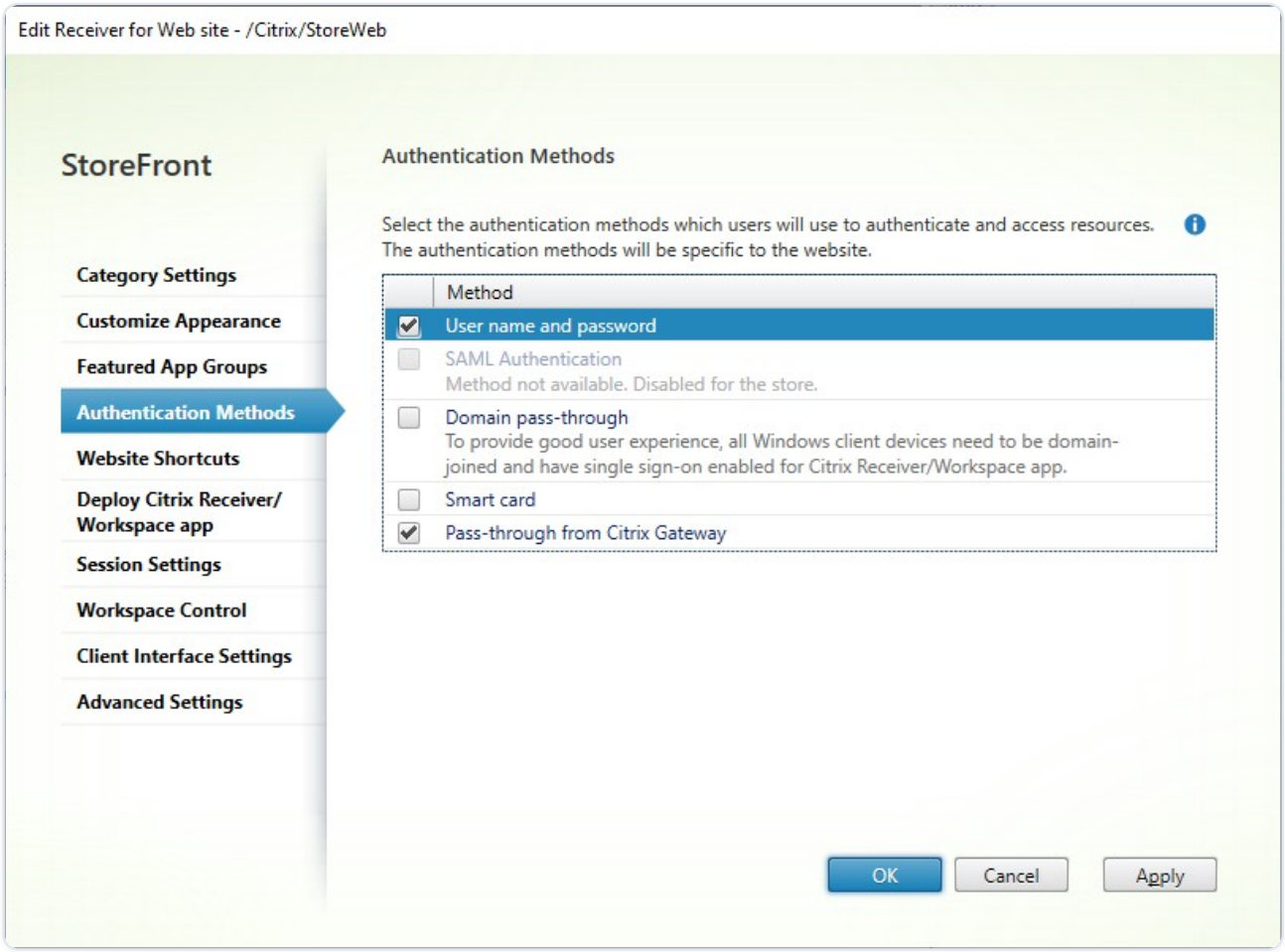
Authentication methods

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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Website shortcuts

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.

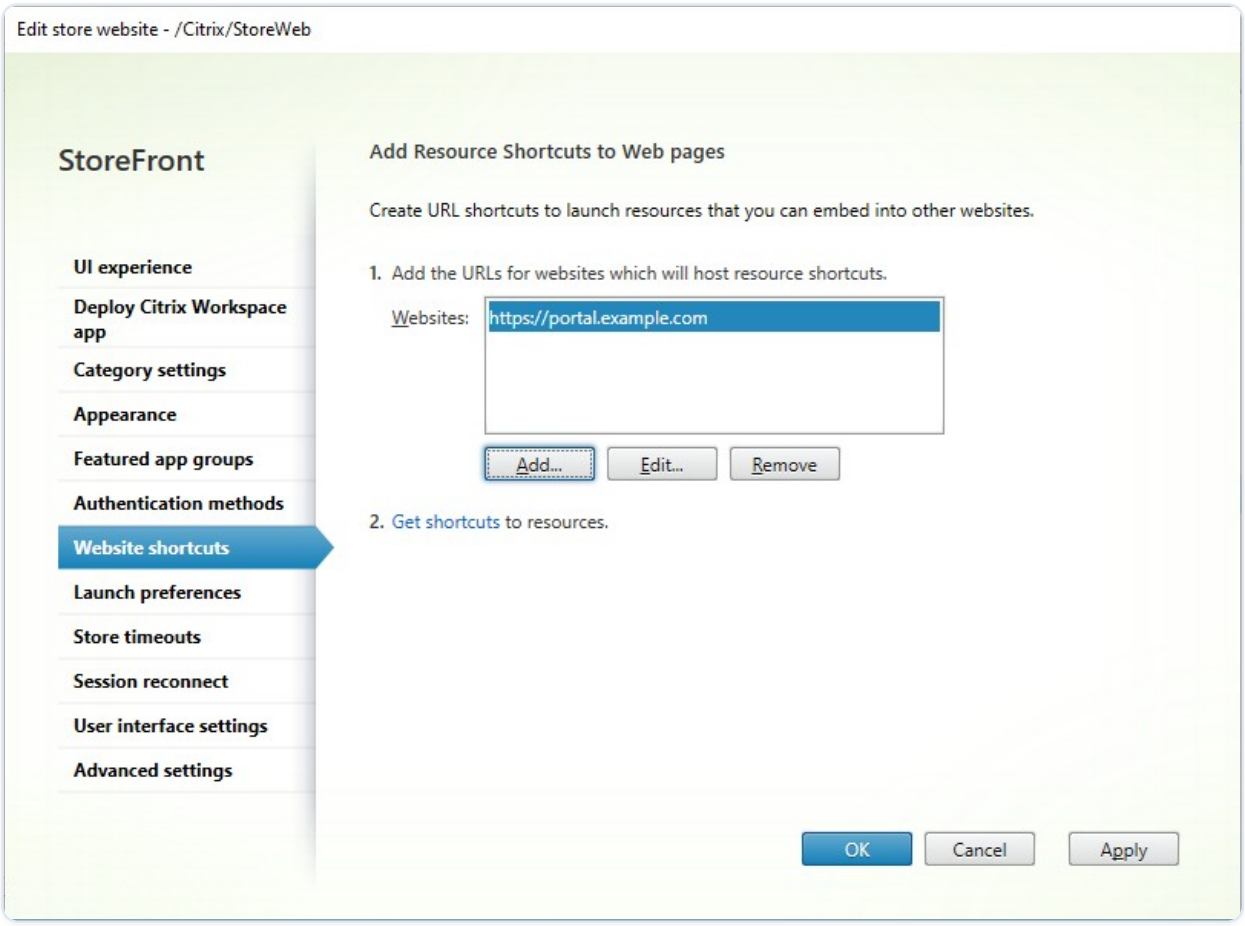
By default, StoreFront warns users if they attempt to launch resource shortcuts from untrusted websites, but users can still choose to launch the resource. To stop these warnings from appearing, on Advanced settings, clear prompt for untrusted shortcuts.

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

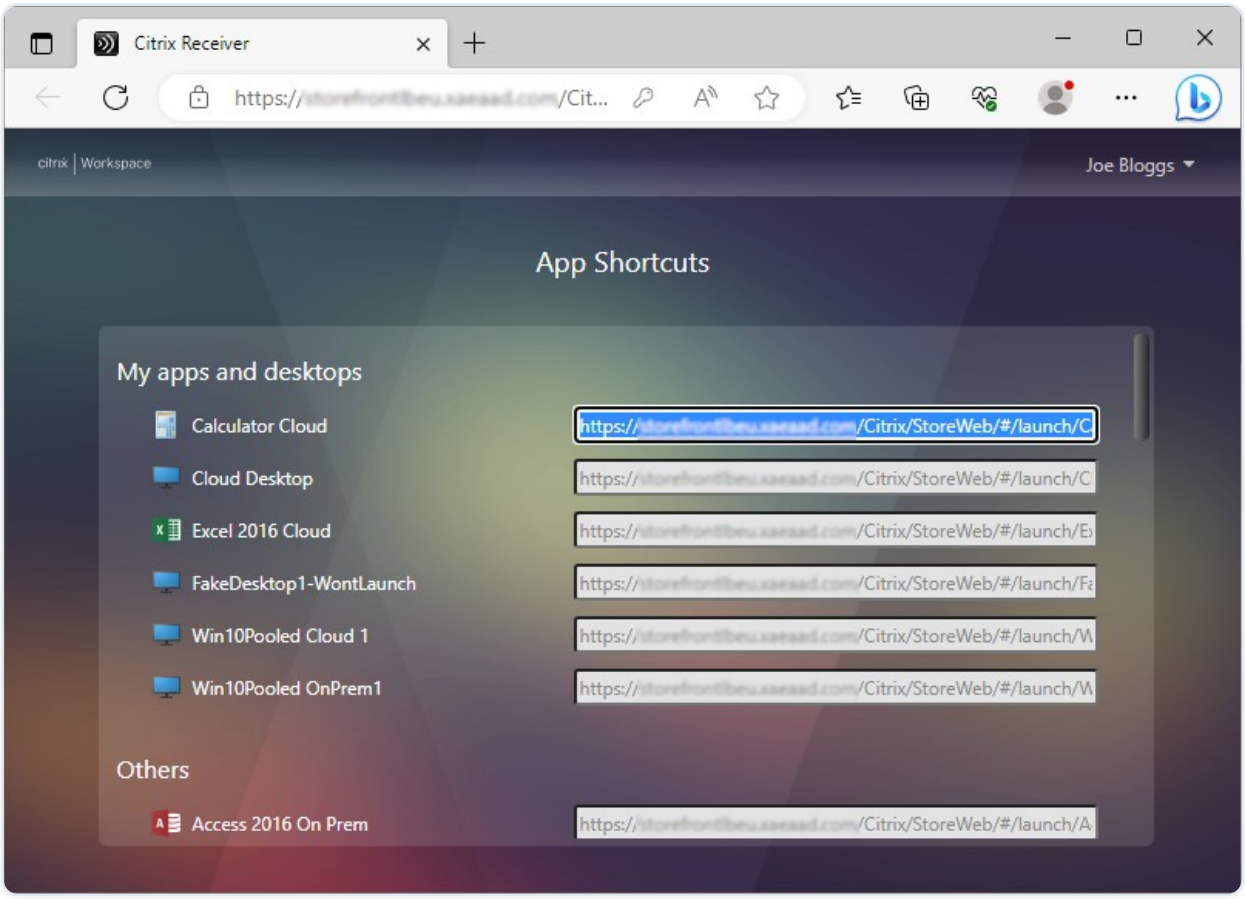
1. On the Edit store website screen, select the **Website Shortcuts** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



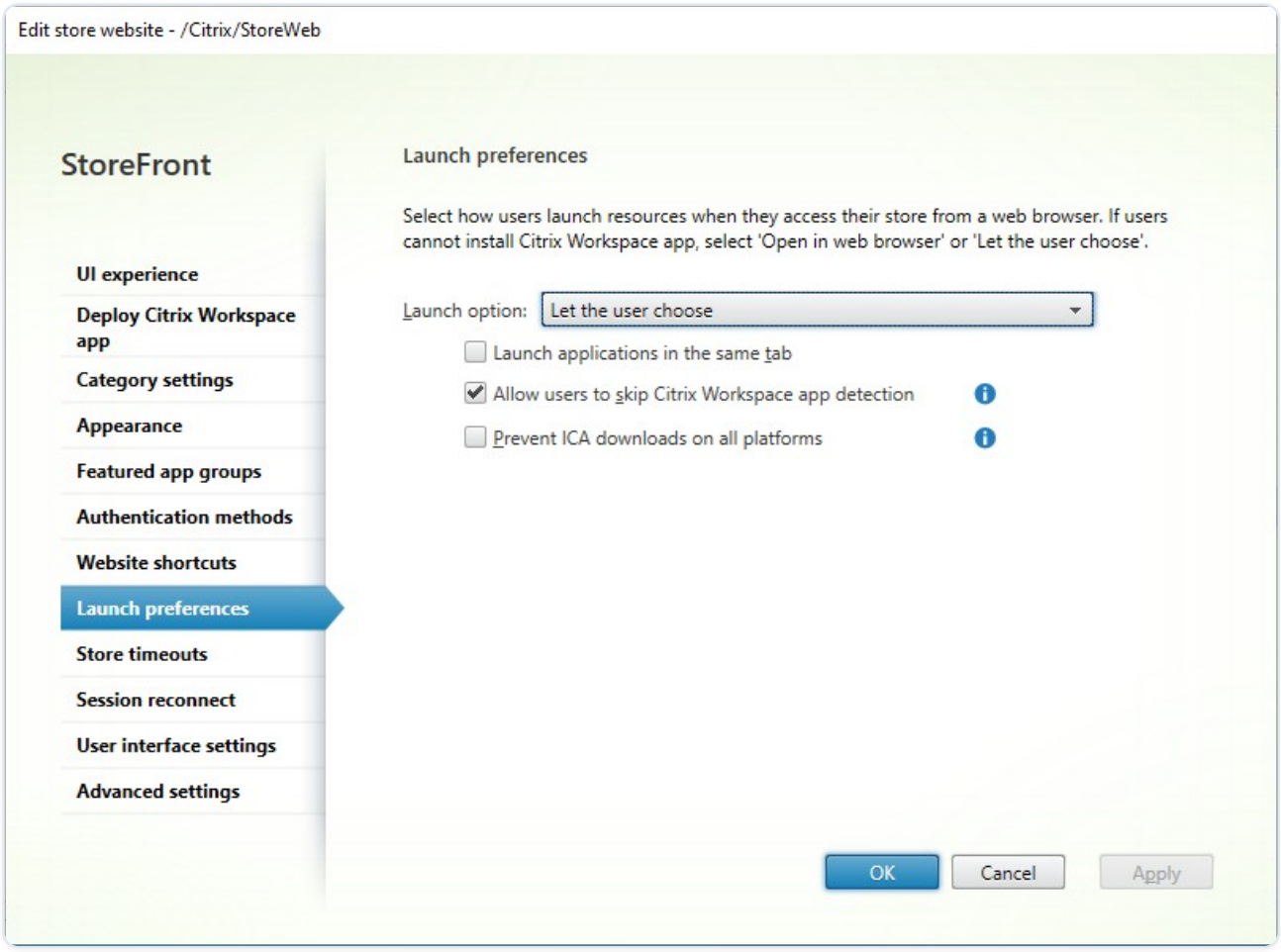
Add trusted websites using PowerShell

To add trusted URLs using PowerShell, run cmdlet Set-STFWebReceiverApplicationShortcuts.

Launch Preferences

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**.

On the modern experience, this setting is not available and resources always open in a new 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 experiences a 6s delay. This does not

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
$receiver = Get-STFWebReceiverService "/Citrix/StoreWeb"

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:

```
$receiver = Get-STFWebReceiverService "/Citrix/StoreWeb"

Set-STFWebReceiverPluginAssistant -WebReceiverService $receiver
-BrowserExtensionEnabled $False
```

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

```
$receiver = Get-STFWebReceiverService "/Citrix/StoreWeb"

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

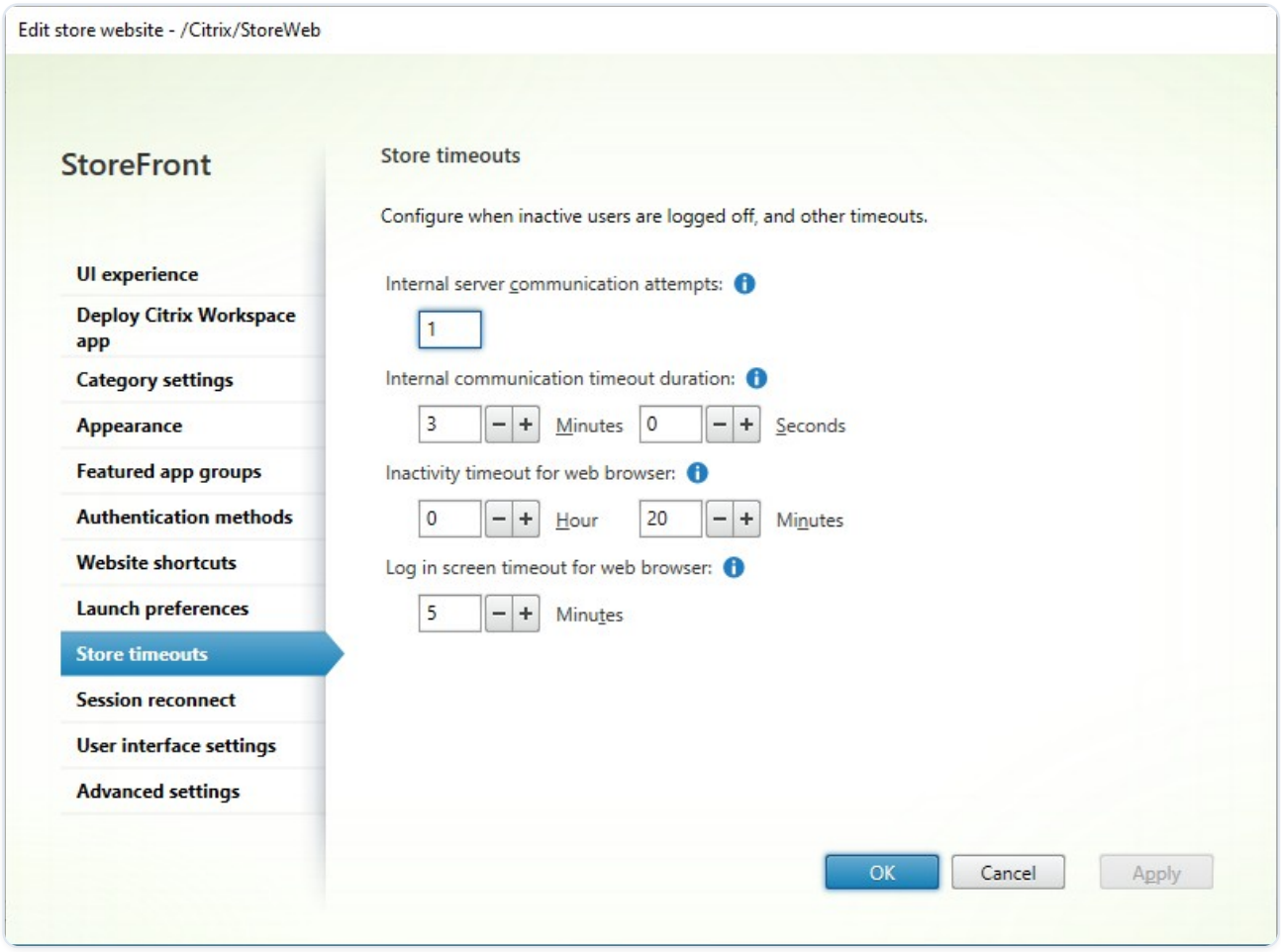
To configure these settings using PowerShell, run cmdlet Set-STFWebReceiverPluginAssistant.

To configure Prevent ICA Downloads, run cmdlet Set-STFWebReceiverUserInterface with parameter `PreventIcaDownloads`.

Store timeouts

To modify store timeouts, go to the Edit store website screen, select the **Store timeouts** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
$rfw = Get-STFWebReceiverService '/Citrix/StoreWeb'

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 displayed in the management console.

To view the current value use Get-STFWebReceiverAuthenticationMethods and check the `TokenLifeTime` property. For example:

```
$rfweb=Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

$rfauth = Get-STFWebReceiverAuthenticationMethods -WebReceiverService
$rfweb

$rfauth.TokenLifeTime.ToString()
```

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$rfweb=Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

$rfauth = Get-STFWebReceiverAuthenticationMethods -WebReceiverService
$rfweb

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
$store = Get-STFStoreService -VirtualPath "[store path]"

$auth = Get-STFAuthenticationService -StoreService $store

$relyingParty = $auth.ProducerService.RelyingParties | Where-Object
{ $_.Id -eq $auth.ProducerService.Id }

$relyingParty.MaxLifetime.ToString()
```

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

To configure the maximum token lifetime run the following PowerShell:

```
$store = Get-STFStoreService -VirtualPath "[store path]"

$auth = Get-STFAuthenticationService -StoreService $store

$relyingParty = $auth.ProducerService.RelyingParties | Where-Object
{ $_.Id -eq $auth.ProducerService.Id }

$relyingParty.MaxLifetime = "[max lifetime]"

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`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Session reconnect

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

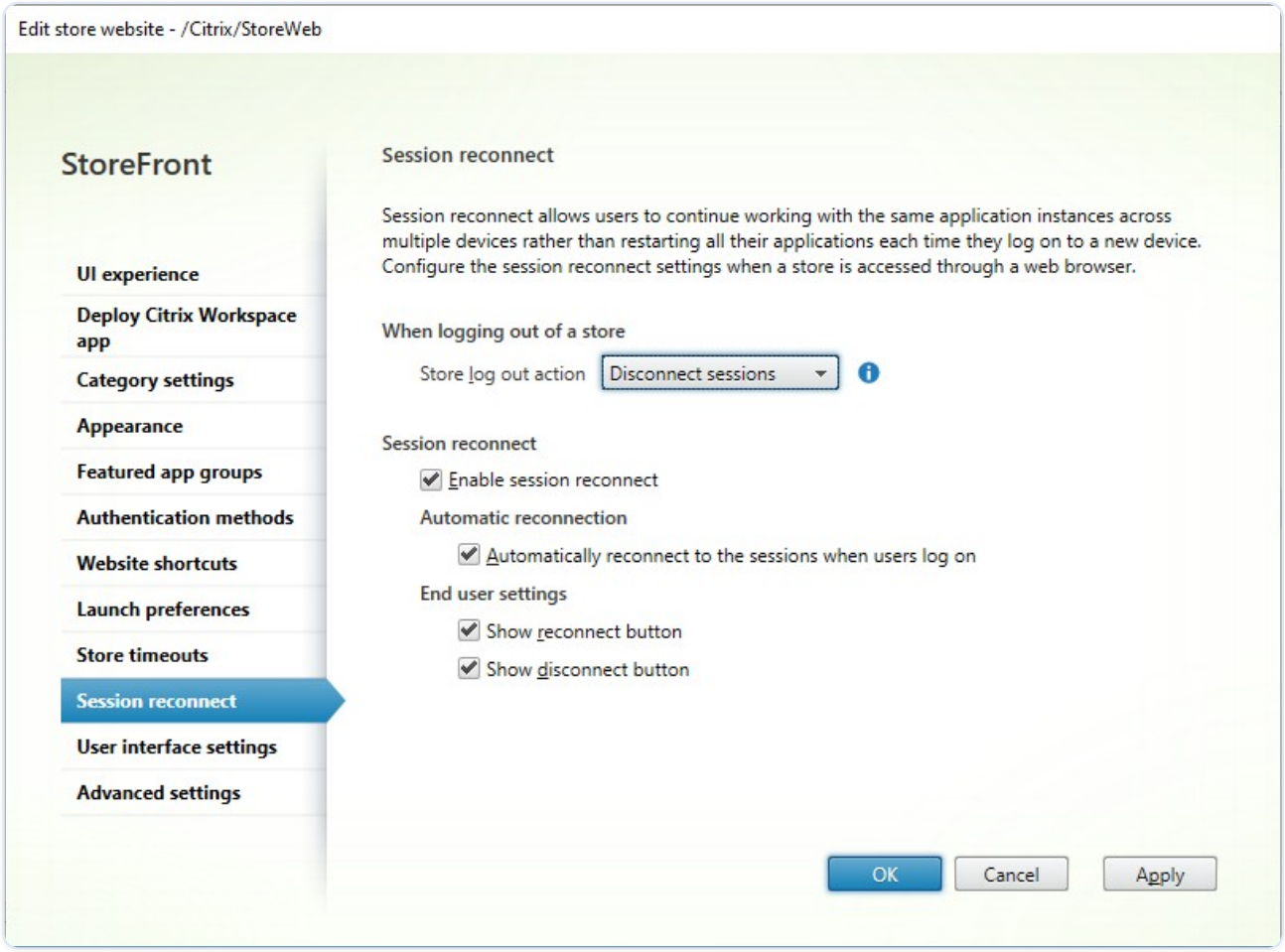
The session reconnect settings within StoreFront management console only apply when accessing the store through a web browser. This is subject to the following requirements and restrictions:

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Session reconnect is not available when resources open within the same browser tab. To configure this, see Citrix Workspace app deployment.

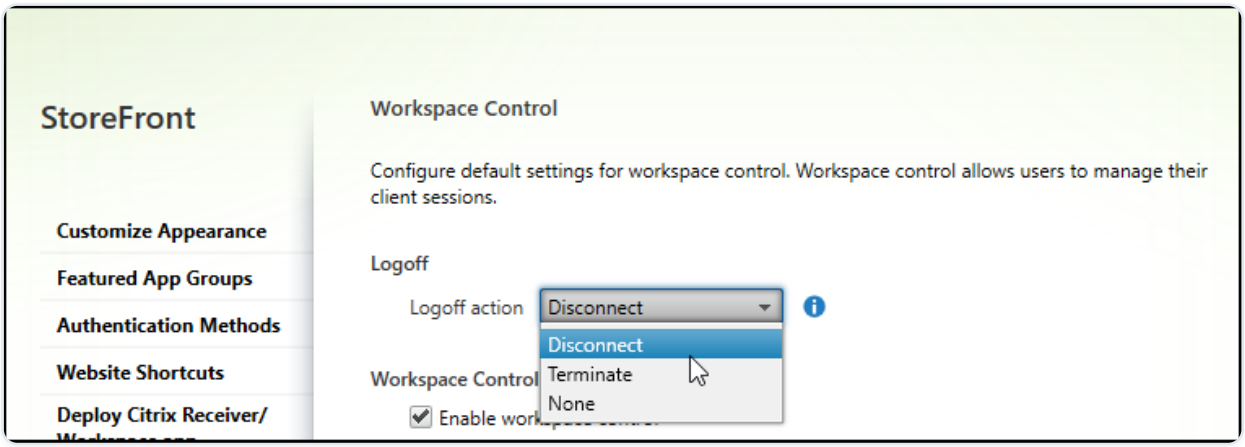
To modify session reconnect settings when a store is accessed through a web browser, select **Session reconnect** on the Edit store website screen.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



- **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.

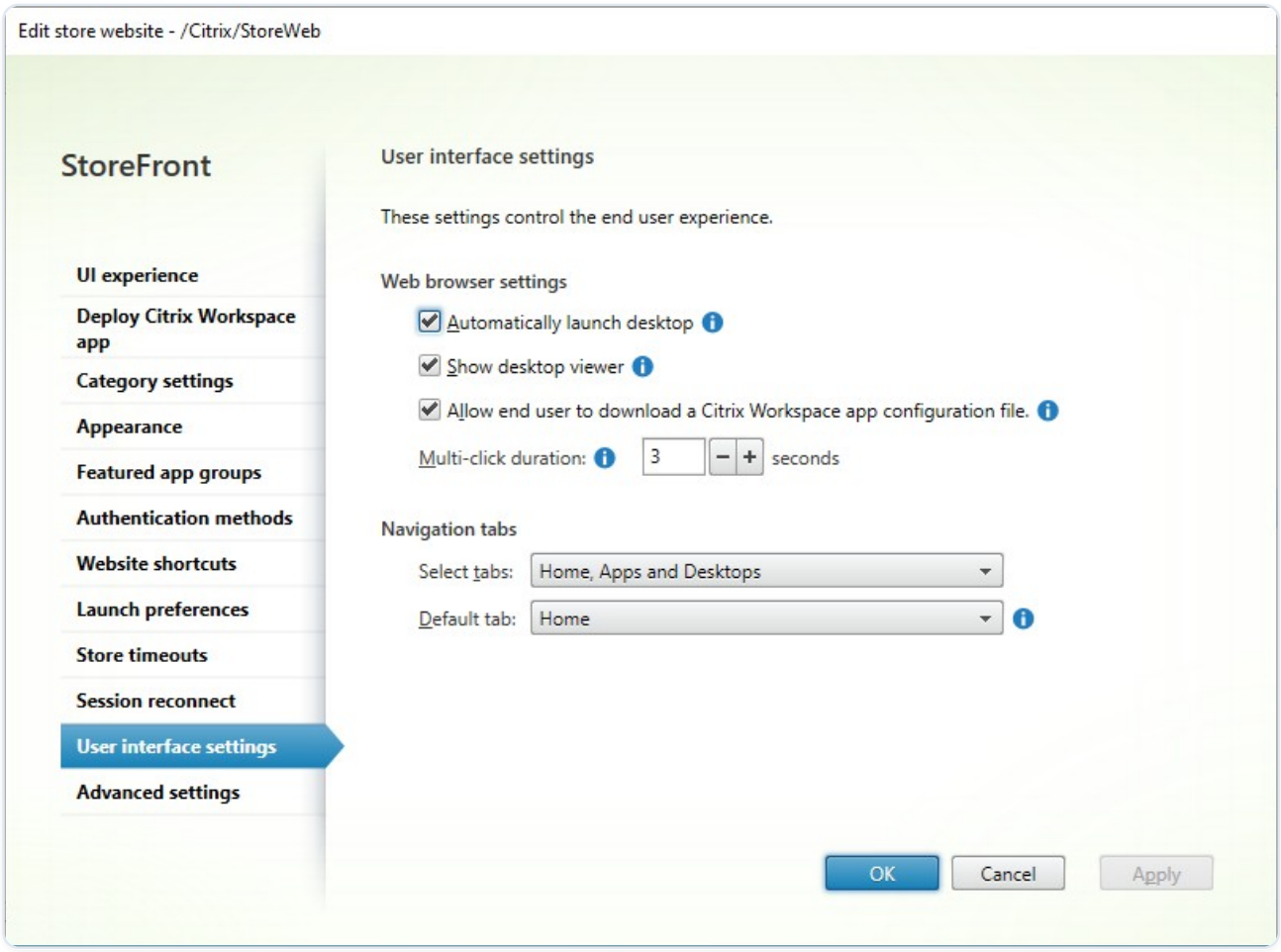
© 1997–2026 Citrix Systems, Inc. All rights reserved.

User interface settings

To modify user interface settings, open the Edit store website screen and the **User interface settings** tab.

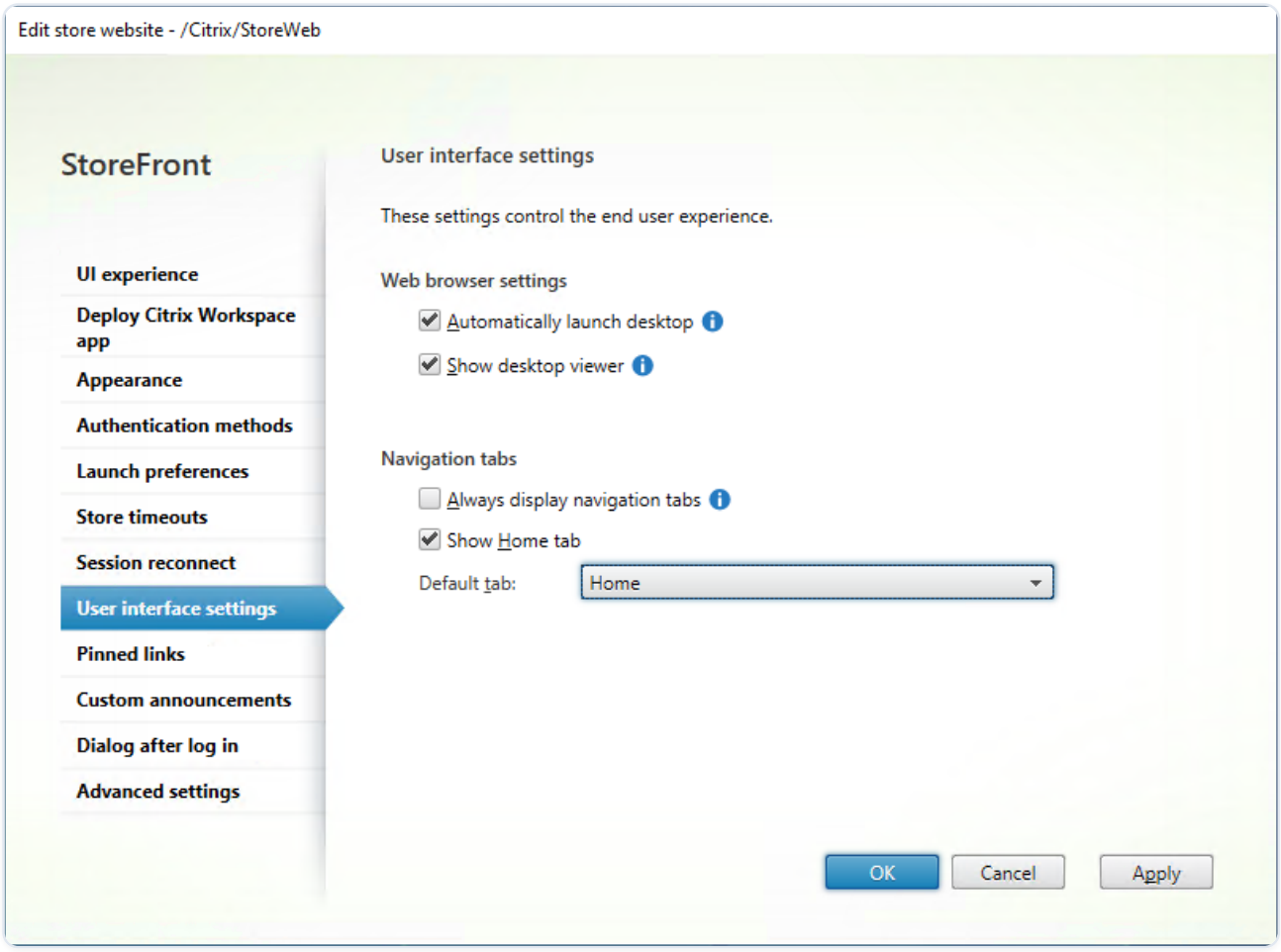
The settings available depend on which UI experience is selected.

For the classic experience:



For the modern experience:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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`.

Detailed Desktop tile

Enable **Show detailed desktop tile** to display larger desktop tiles with additional information. For more information, see Modern experience.

Display Personalize your home screen for first time users

When using the modern experience, the first time a user without any favorites logs in, it displays the **Personalize your home screen** window. To manage this window you must use PowerShell.

To get the current value, call Get-STFWebReceiverUserInterface. For example:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$website = Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

$websiteUI = Get-STFWebReceiverUserInterface -WebReceiverService $website

"Show personalization screen: $($websiteUI.ShowFirstTimeUse)"
```

To disable or enable the window, call Set-STFWebReceiverUserInterface with parameter `ShowFirstTimeUse`. For example:

```
$website = Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

Set-STFWebReceiverUserInterface -WebReceiverService $website
-ShowFirstTimeUse $false
```

Show Activity manager

The modern experience includes Activity manager to allow users to manage their sessions. Activity manager is enabled by default. To manage this setting you must use PowerShell. To get the current value, call Get-STFWebReceiverUserInterface. For example:

```
$website = Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

$websiteUI = Get-STFWebReceiverUserInterface -WebReceiverService $website

"Show Activity manager: $($websiteUI.ShowActivityManager)"
```

To disable or enable Activity manager, call Set-STFWebReceiverUserInterface with parameter `ShowActivityManager`. For example:

```
$website = Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

Set-STFWebReceiverUserInterface -WebReceiverService $website
-ShowActivityManager $false
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Pinned links

NOTE:

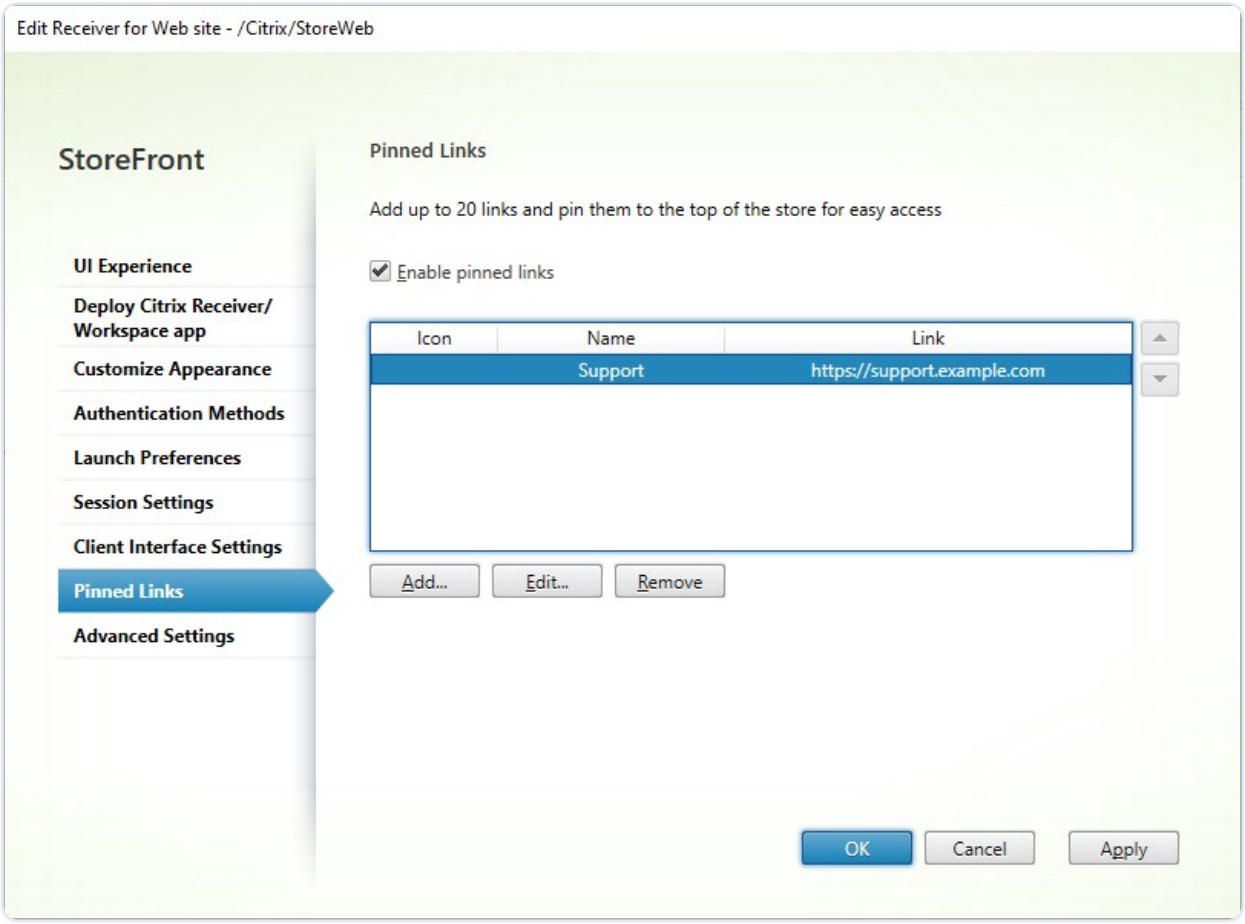
This functionality is available only using the modern experience.

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

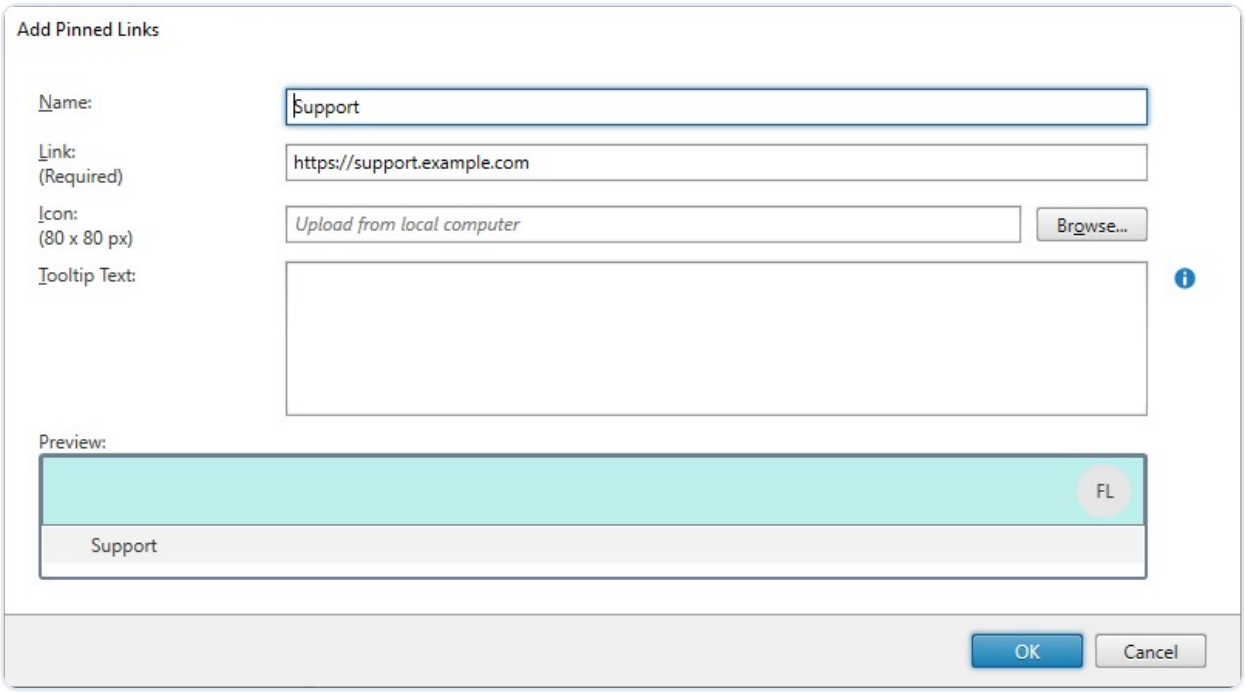
To add a pinned link:

1. Go to Edit store website and select the **Pinned Links** tab.



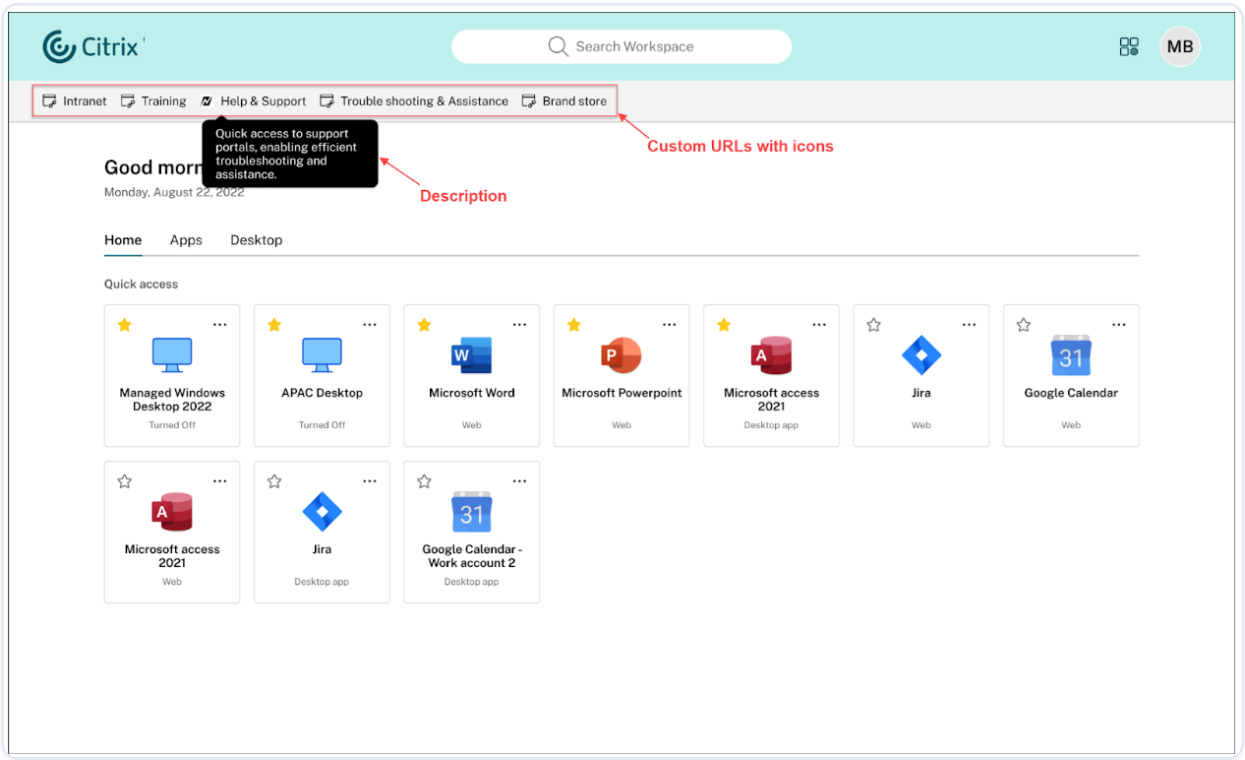
2. Click **Add**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

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

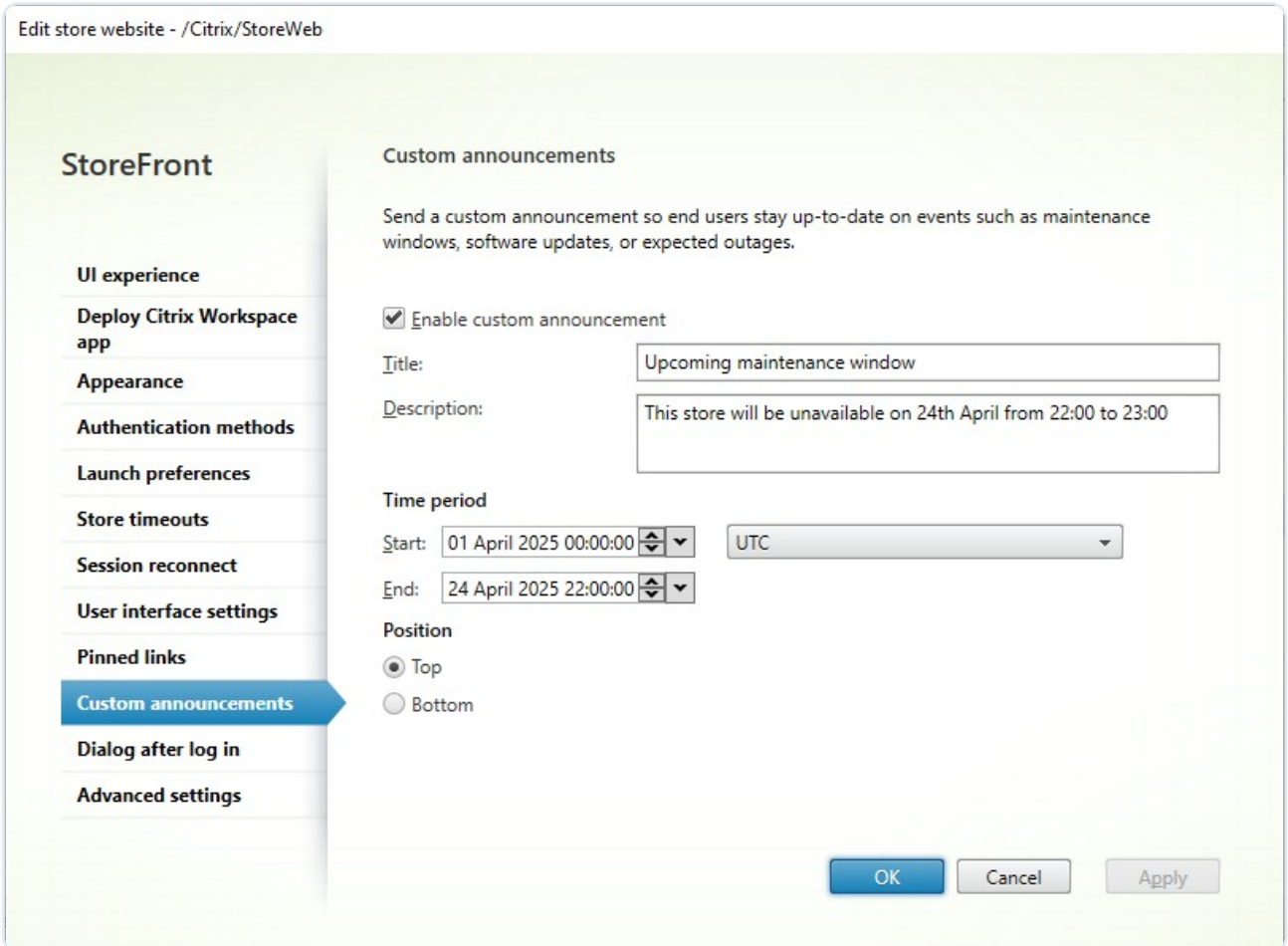
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

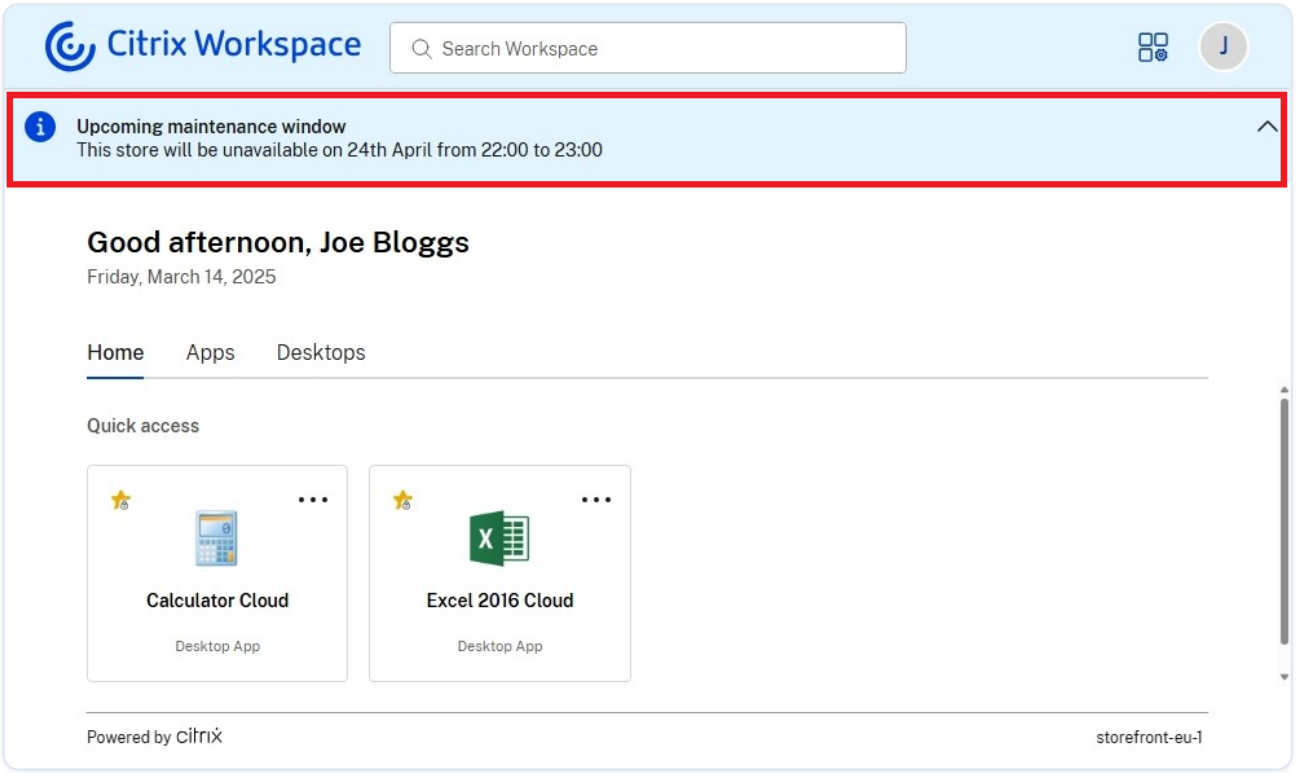
To set or modify a the custom announcement:

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.



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Dialog after login

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.

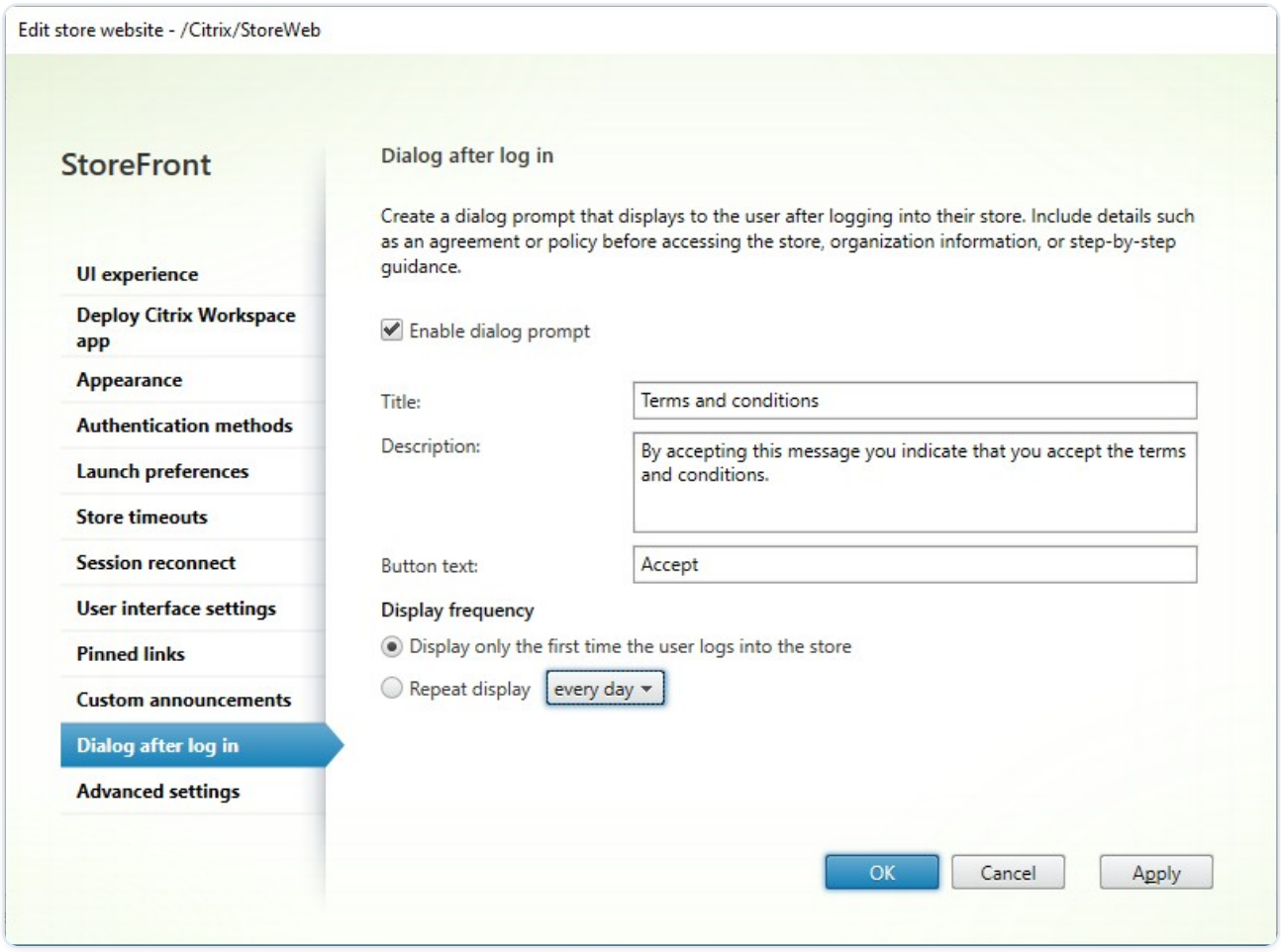
NOTE:

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



For more information on the end user experience, see Modern Experience.

App Protection

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 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:

```
$receiver = Get-STFWebReceiverService -VirtualPath "[virtual path]"

Set-STFWebReceiverAppProtection -WebReceiverService $receiver -Enabled
On
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

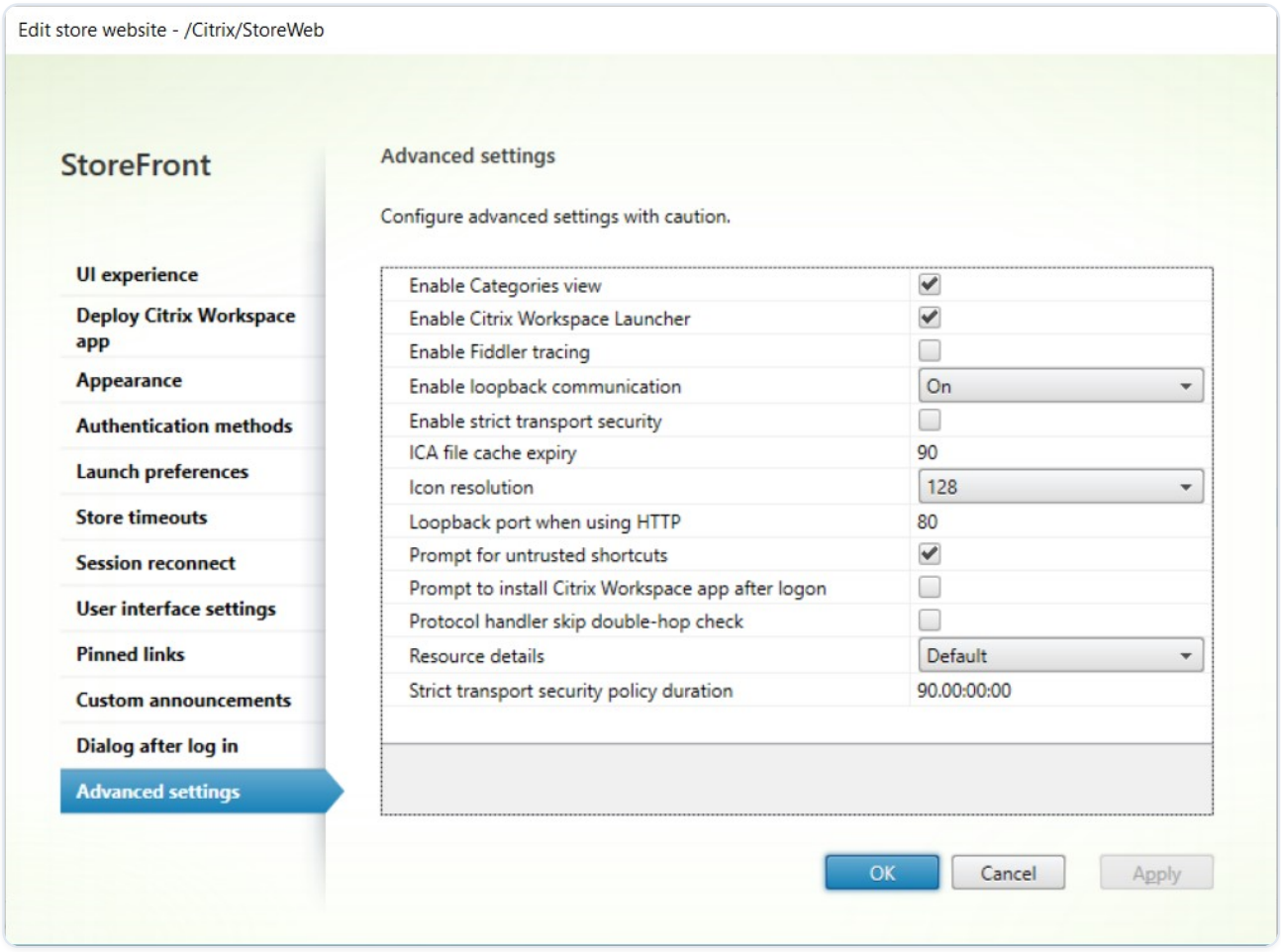
```
$receiver = Get-STFWebReceiverService -VirtualPath "/Citrix/StoreWeb"

Get-STFWebReceiverAppProtection -WebReceiverService $receiver
```

Advanced settings

To modify advanced settings for a website, open the Edit store website screen and select the **Advanced settings** tab.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 the 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 the display of categories, see Category settings.

To modify this setting using PowerShell, run cmdlet `Set-STFWebReceiverUserInterface` with parameters `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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

VALUE	DESCRIPTION
On	The StoreFront web proxy communicates with the store service using the loopback address, ensuring that communication remains on the StoreFront server.
Off	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.
On using HTTP	As **On** but changes the protocol from HTTP to HTTPS. Select this option when using a load balancer that terminates HTTPS, connecting to StoreFront over HTTP. To change the port, see Loopback port when using HTTP

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

When Citrix Workspace Launcher is disabled and the Launch option is set to **Let the user choose**, the store website does not prompt first-time users to choose a launch method. When using the modern experience, the launch method defaults to downloading an ICA file, but users can change this from the settings screen. When using the classic experience, resources launch in a web browser.

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

Disabling this option can result in users downloading ICA files, which is not recommended.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By default, the website uses Citrix Workspace Launcher to detect Citrix Workspace app and launch resources on all supported browsers and operating systems. You can also configure on which browser user agents the website uses Citrix Workspace launcher. To do this, run cmdlet `Set-STFWebReceiverPluginAssistant` with parameter `-ProtocolHandlerPlatforms`. The value is a JavaScript regular expression that the website runs against the web browser's user agent.

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.

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`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

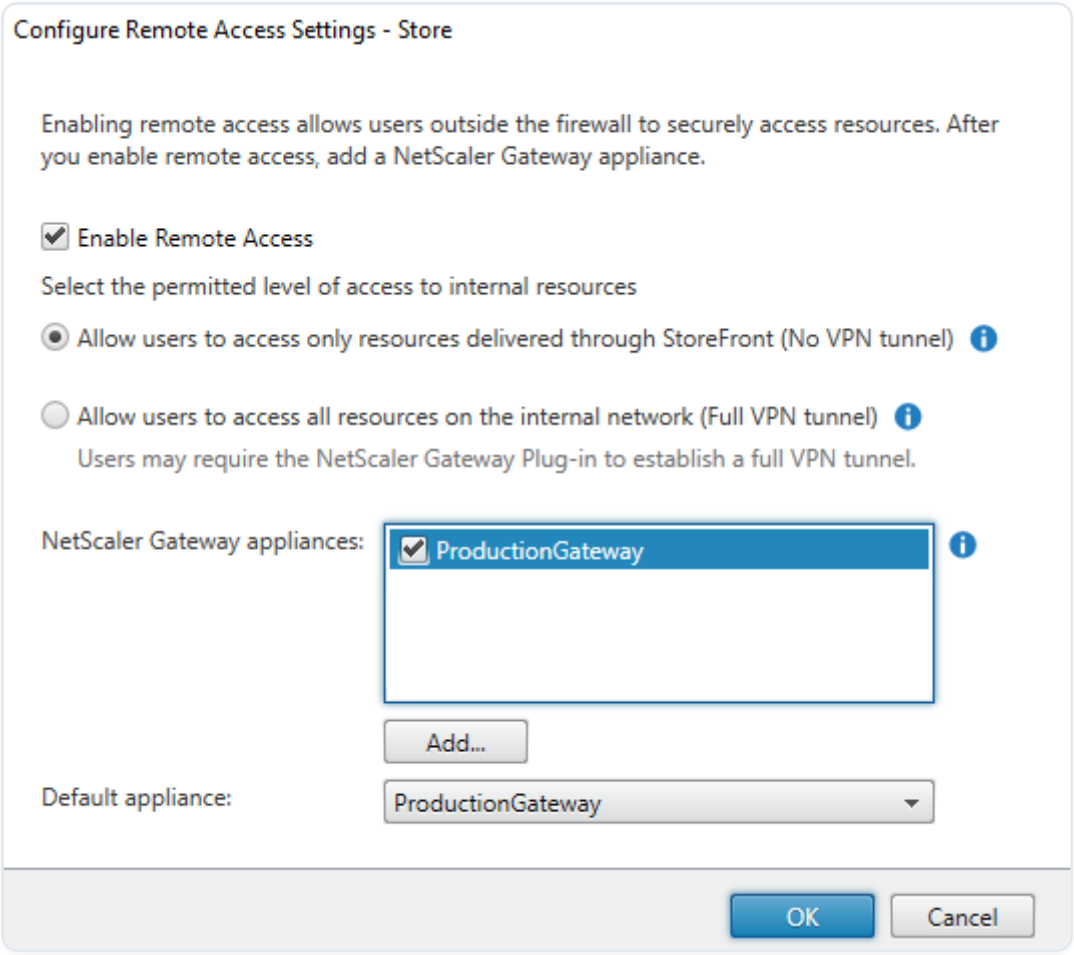
You can configure access to stores through Citrix Gateway for users connecting from public networks. Remote access through a Citrix Gateway cannot be applied to unauthenticated stores.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**.



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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

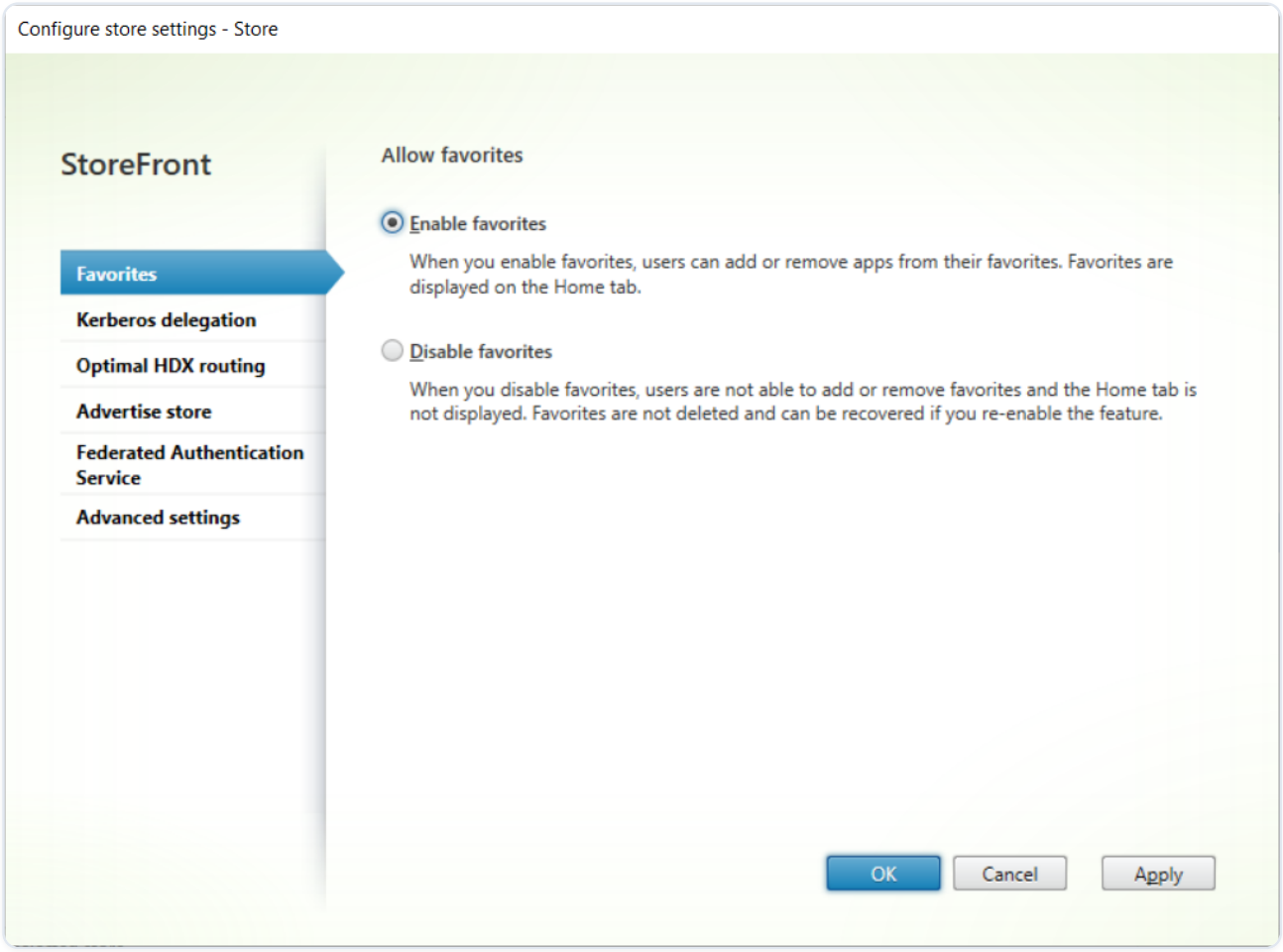
Configure a Store

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
6. Go to the Entra ID SSO tab to configure whether to SSO to Entra joined Windows VDAs.



Favorites

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

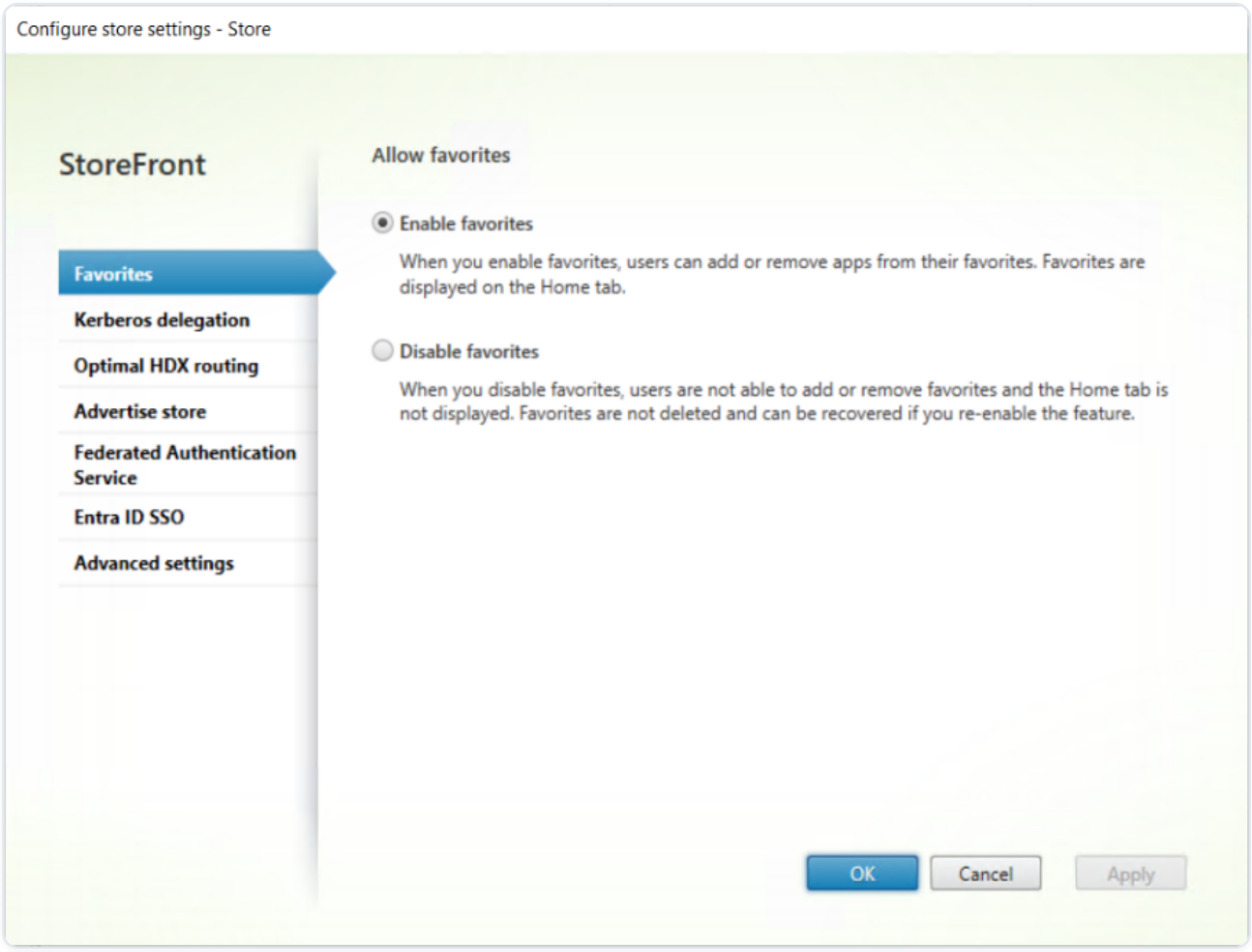
Use the Favorites to do select one of the following options:

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/
<yourstore>"

Set-STFStoreService -StoreService $StoreObject -LockedDown $True -Confirm:
$False
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
$store = Get-STFStoreService -VirtualPath [store path]

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

```
$internalStore=Get-STFStoreService -VirtualPath '/Citrix/Internal'

$internalUri =
$internalStore.SubscriptionStoreClient.ClientEndpoint.Uri.ToString()



$externalStore=Get-STFStoreService -VirtualPath '/Citrix/External'

$externalStore.SubscriptionStoreClient.ClientEndpoint.Uri = $internalUri

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:

```
$store=Get-STFStoreService -VirtualPath '/Citrix/External'

$store.SubscriptionStoreClient.ClientEndpoint.Uri.ToString()
```

Kerberos delegation

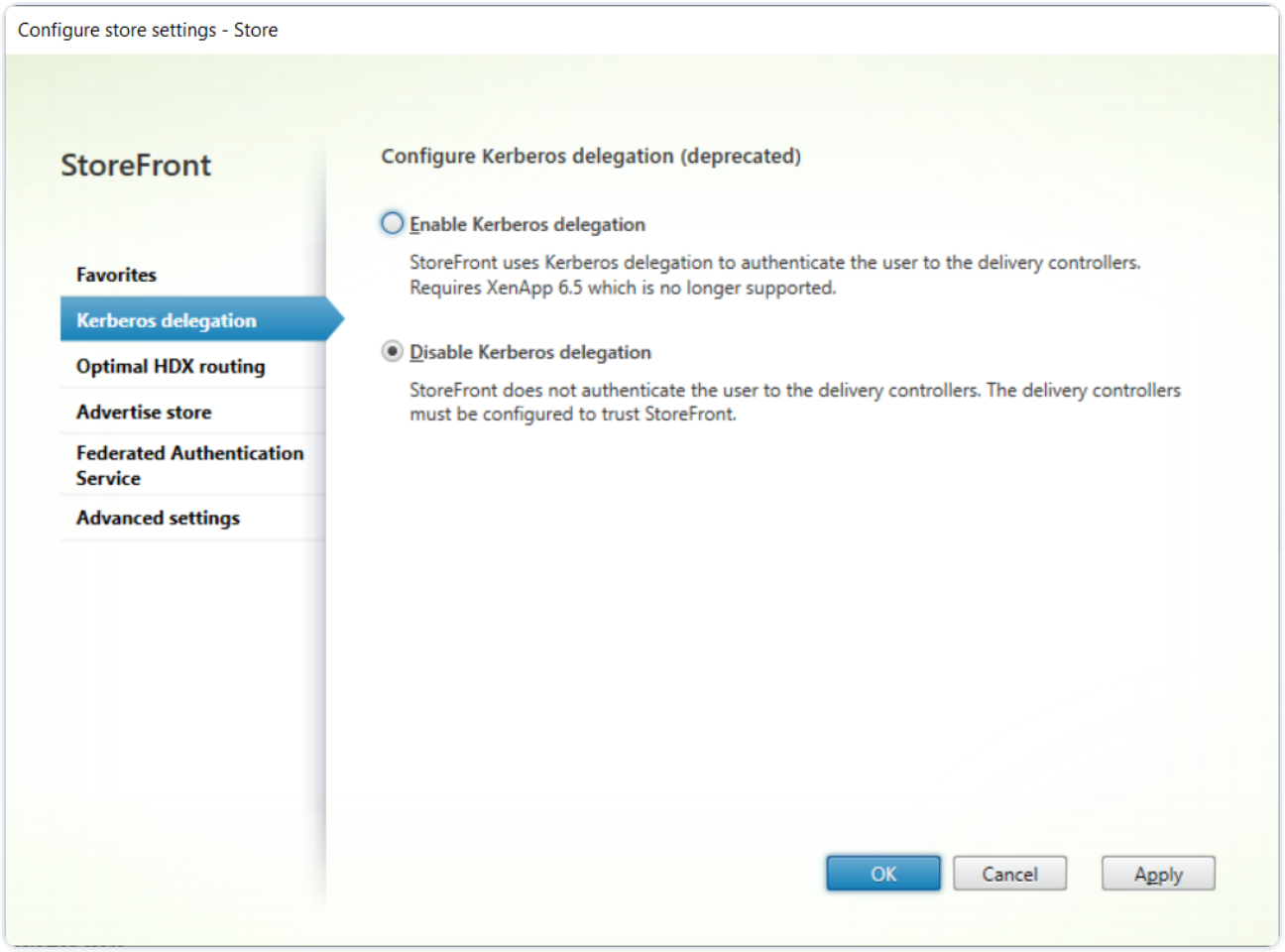
NOTE:

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure optimal HDX™ routing for a store

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

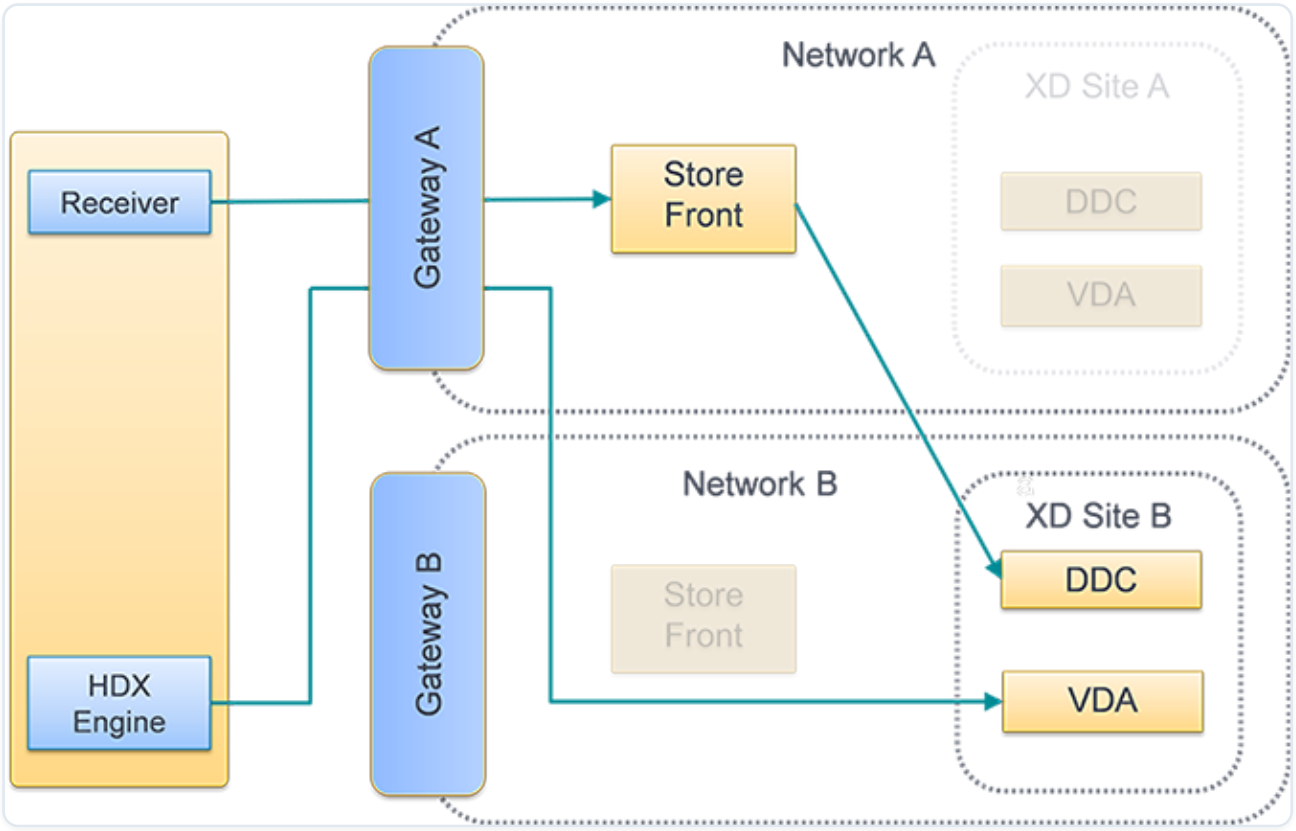
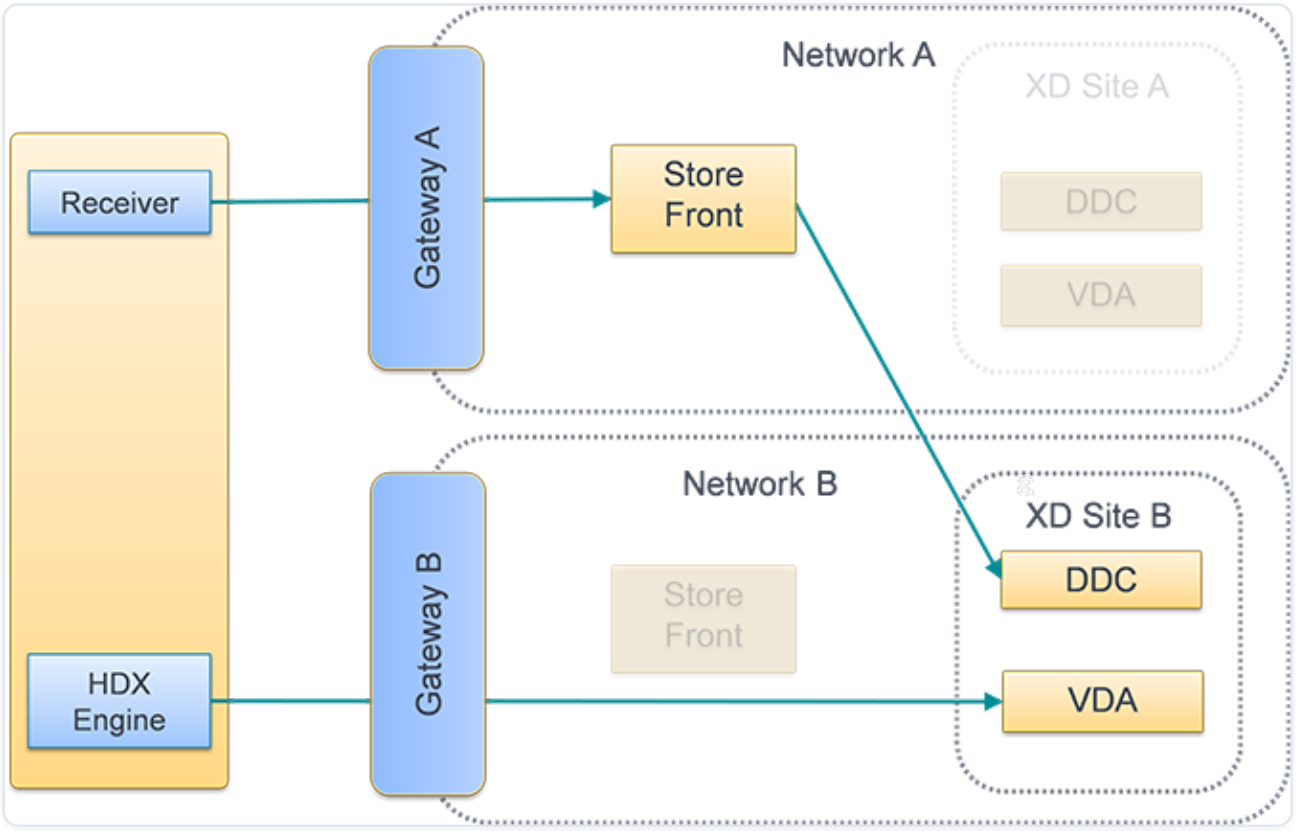


Figure 2. Optimal gateway routing

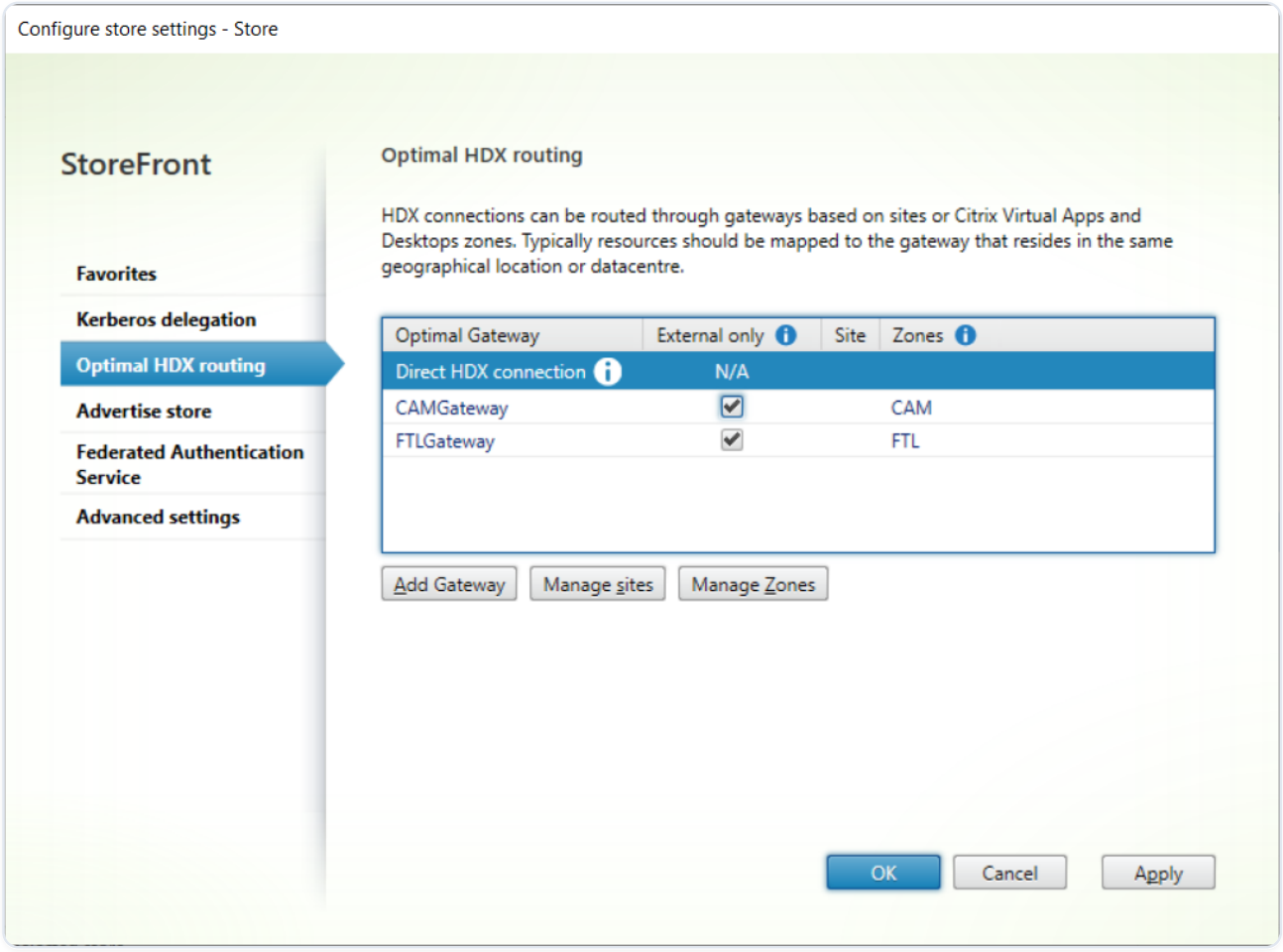


Configure Optimal HDX routing

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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

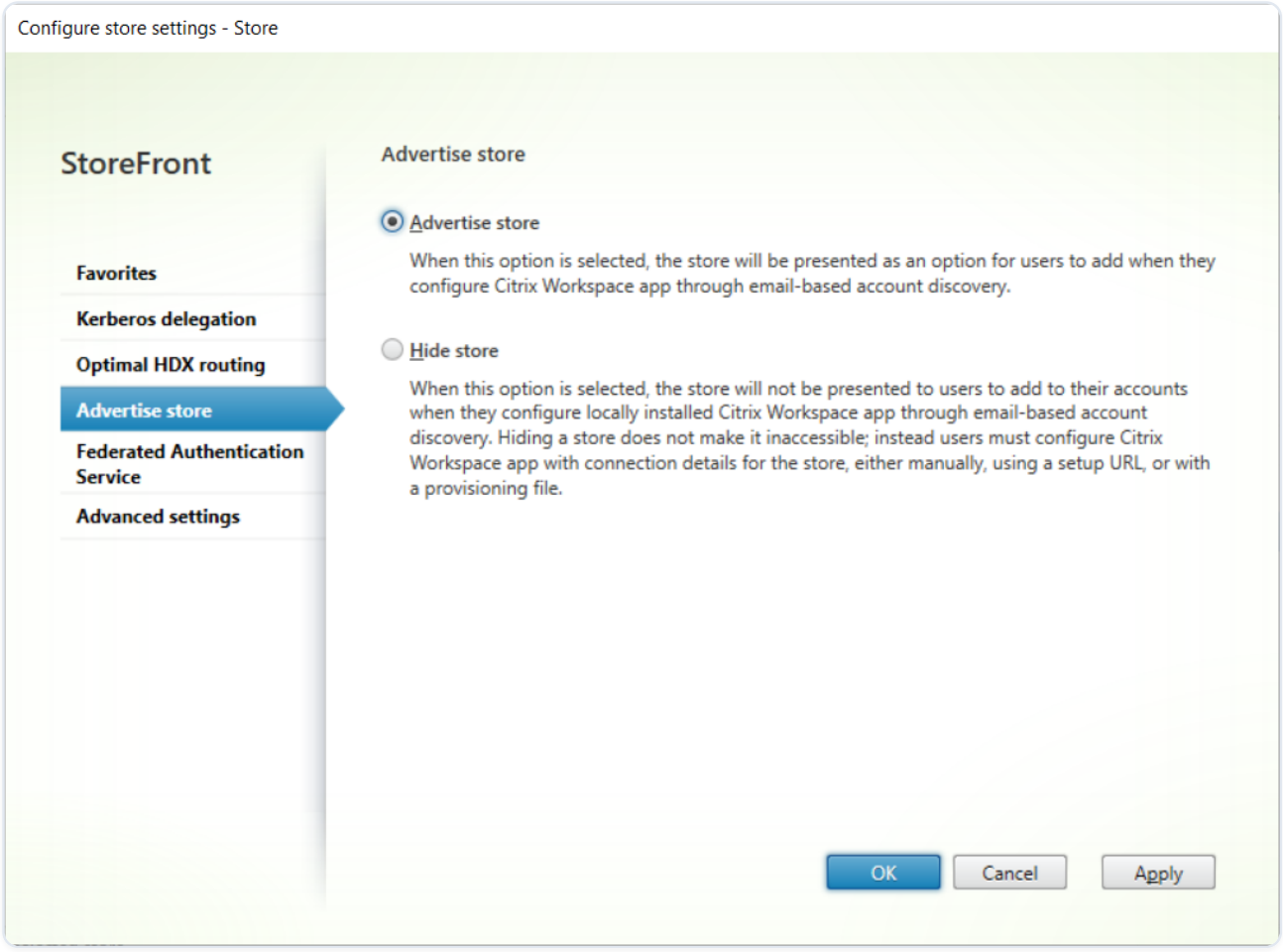
You can choose whether stores are presented to users to add to their accounts when they configure Citrix Workspace app through email-based account discovery or FQDN. By default, when you create a store it is presented as an option for users to add in Citrix Receiver when they discover the StoreFront 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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Advanced store settings

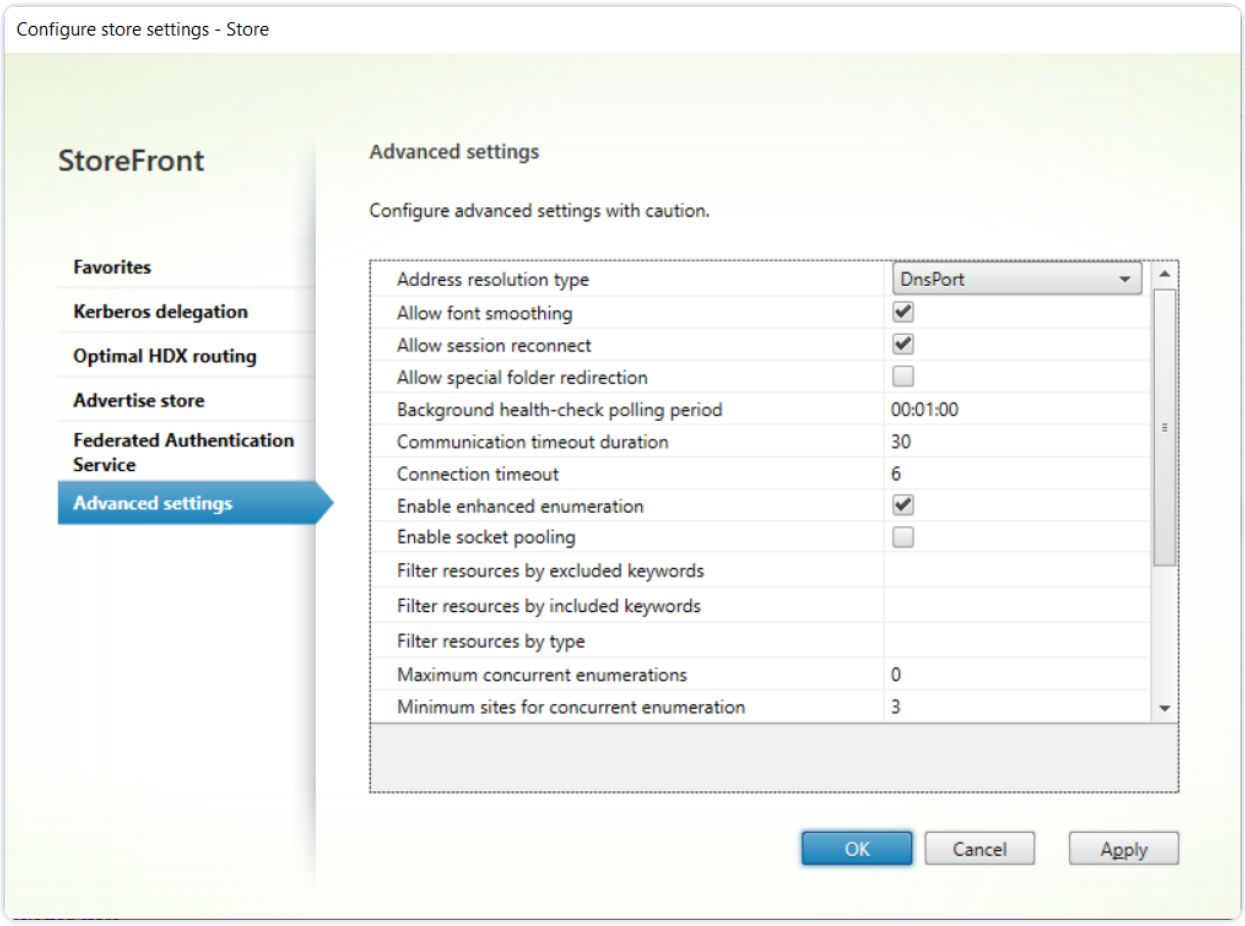
You can configure most advanced store properties by using the Advanced Settings tab in Configure store settings. Some settings can only be modified using PowerShell.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 heath 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 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.

From StoreFront 2308, Advanced health check is enabled by default for new stores. Advanced health check is enabled for existing stores when upgrading from versions earlier than 2402 to 2402 or higher. To enable or disable advanced health check, use the PowerShell cmdlet Set-

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
$storeService = Get-STFStoreService –VirtualPath '/Citrix/Store'

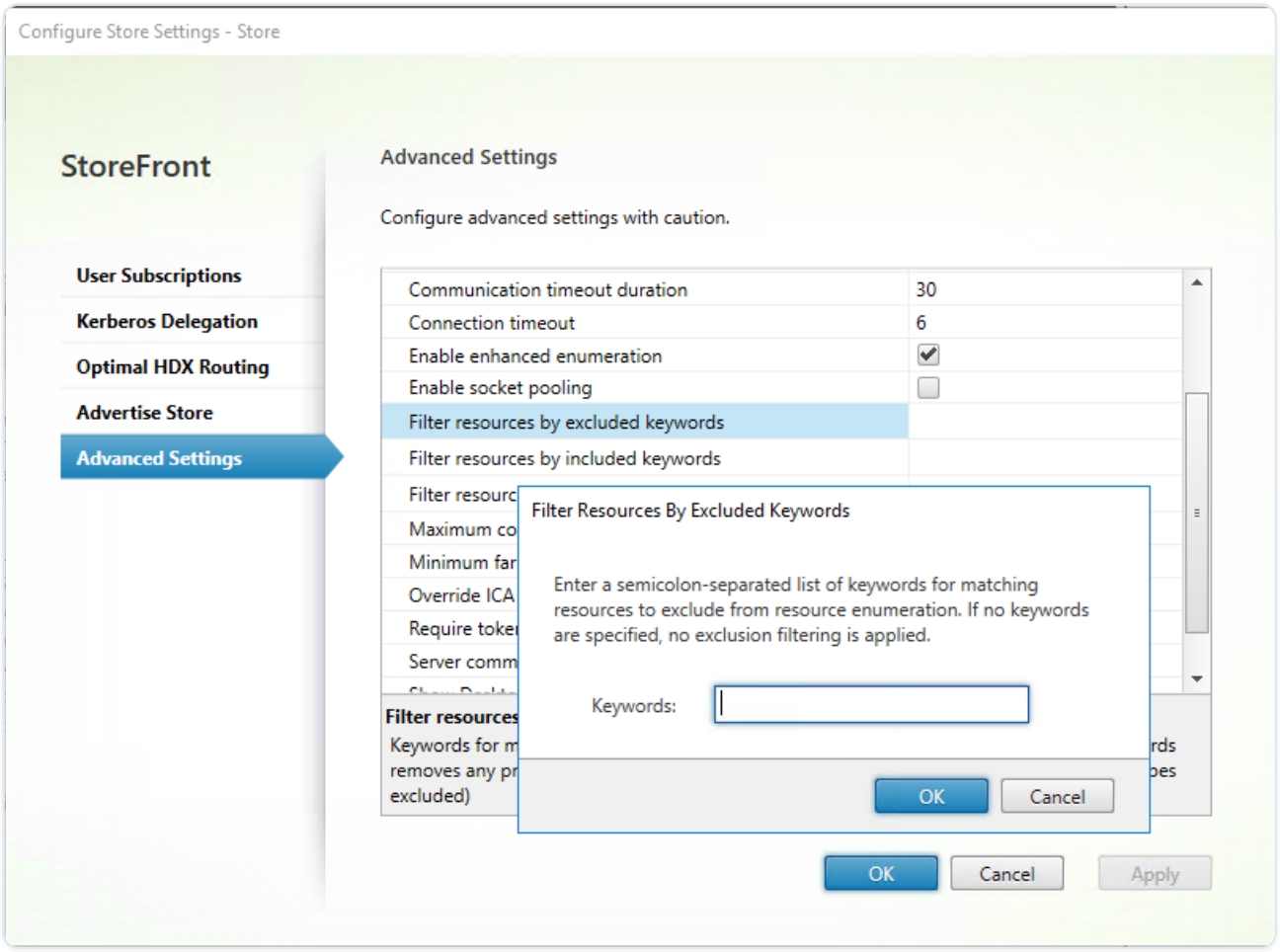
Set-STFStoreFarmConfiguration $storeService -EnableFileTypeAssociation
$false
```

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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Federated Authentication Service (FAS) provides single sign-on to VDAs using certificate authentication. This approach is useful when you have enabled authentication methods such as SAML, where StoreFront does not have the user's Active Directory credentials. Once you enable FAS, it always handles single sign-on, even when using authentication methods where StoreFront has the Active Directory username password.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure FAS using management console

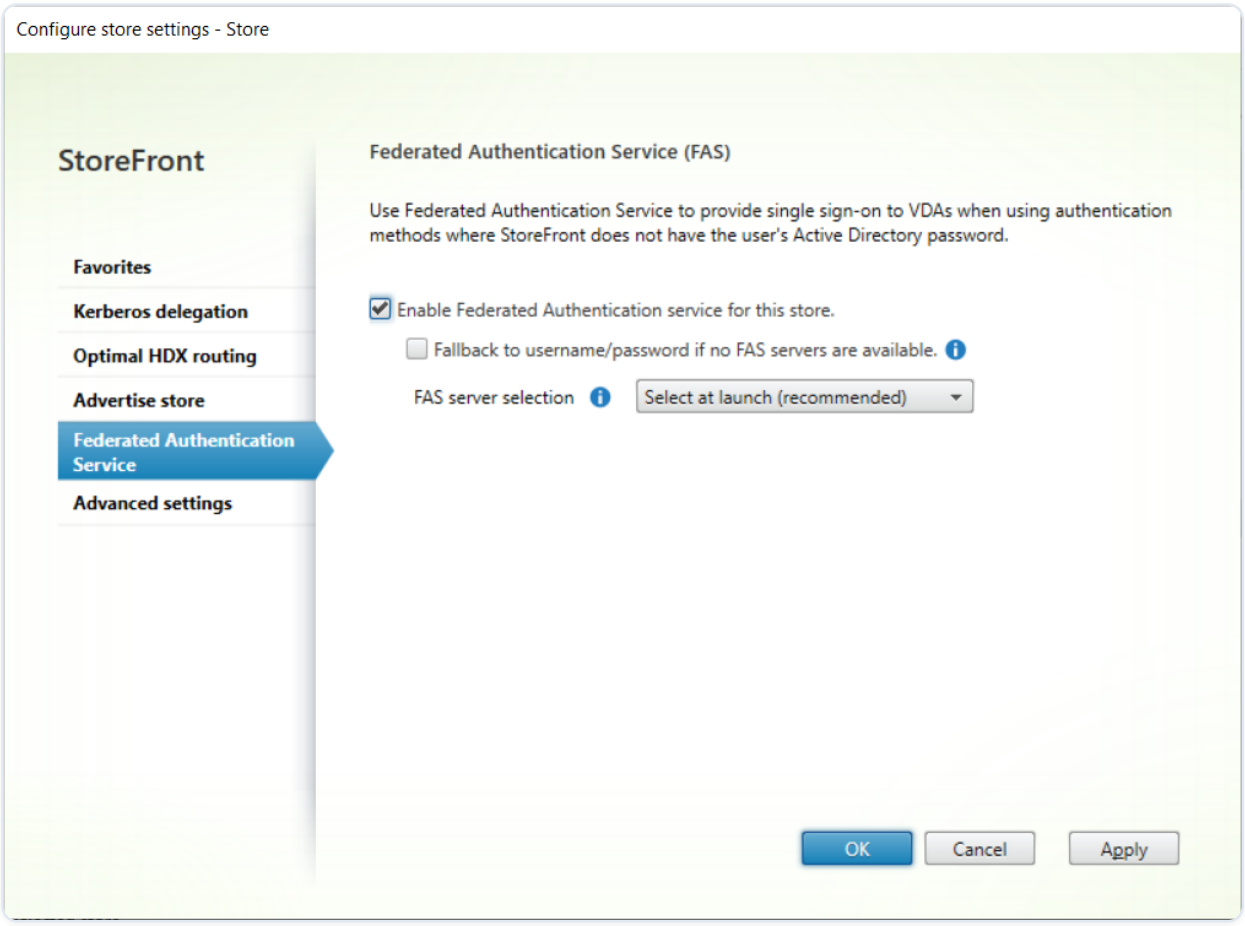
NOTE:

From StoreFront you can configure FAS using the management console. For versions earlier than 2511, the management console does not expose these settings, so you must must configure FAS using PowerShell.

To configure FAS:

1. Configure the list of FAS servers using Group policy. For more details see FAS documentation.
2. Select the Stores node in the left pane of the Citrix StoreFront management console, select a store in the center pane.
3. In the Action pane, select **Configure Store Settings**.
4. On the **Configure Store Settings** page, select the **Federated Authentication Service** tab.
5. To enable single sign-on using FAS, select **Enable Federated Authentication Service for this store**.
6. 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 enable this, tick **Fallback to username/password if no FAS servers are available**.
7. By default, StoreFront selects the FAS server at launch. You can change **FAS server selection** to **Select at logon**. This is not normally required but you can enable this if FAS selection is slow to avoid delays at launch. This setting affects all stores sharing the same authentication service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



8. Click **OK** to save your changes.

Configure FAS using PowerShell

To enable FAS using PowerShell, run the cmdlet Set-STFStoreLaunchOptions to set the VDA logon data logon provider to `FASLogonDataProvider`.

For example to enable FAS for a store:

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider
"FASLogonDataProvider"
```

To disable FAS for a store:

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""
```

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

By default the FAS server is selected at log-in. To configure this, run 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:

```
$store = Get-STFStoreService -VirtualPath [VirtualPath]

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName
"FASClaimsFactory"
```

To enable fallback to username and password authentication, run cmdlet Set-STFStoreLaunchOptions with parameter `FederatedAuthenticationServiceFailover`. For example:

```
$storeService = Get-STFStoreService -VirtualPath [VirtualPath]

Set-STFStoreLaunchOptions $storeService
-FederatedAuthenticationServiceFailover $True
```

Entra ID single sign-on to VDAs

You can enable single sign-on to Entra joined VDAs, so that after users have authenticated to the store using Entra ID, they do not need to re-enter credentials when they launch a virtual app or desktop.

Prerequisites

- StoreFront 2607 or higher.
- Sites where you wish to use Entra SSO are Citrix DaaS or Citrix Virtual Apps and Desktops™ 2607 or higher.
- Users authenticate to their store using a Citrix Gateway configured for Entra ID via OIDC.
- The UI experience is set to **Modern**.
- You have completed all configuration described at
    - Microsoft Entra single sign-on - DaaS.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

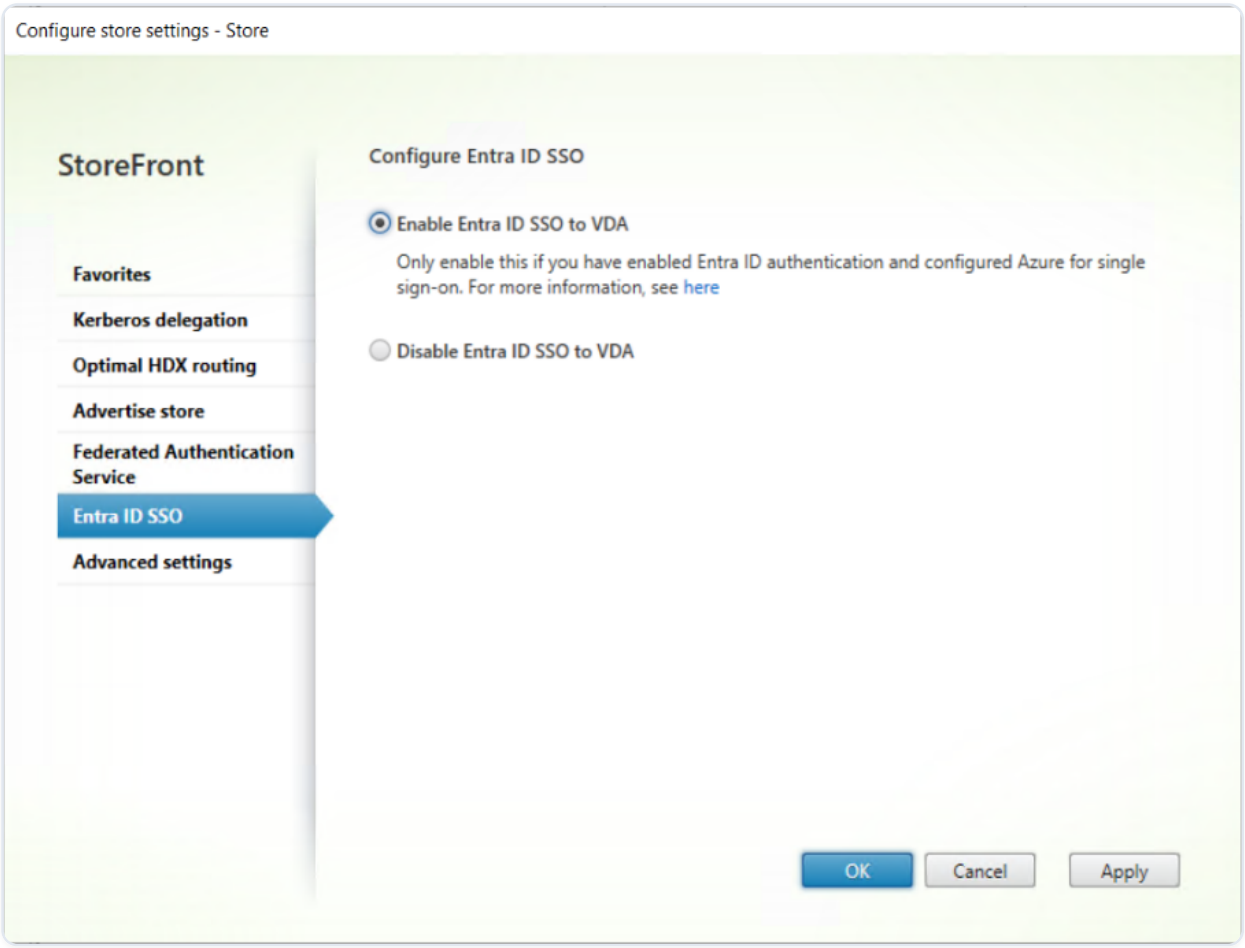
- Microsoft Entra single sign-on - Citrix Virtual Apps and Desktops.

- You have configured DaaS Studio to use your own client application in your Microsoft Entra tenant. In Studio go to **Settings**, **Microsoft Entra single sign-on (SSO)**, **Edit**, **Custom Microsoft Entra settings** and enter the application details. **Citrix Cloud settings** cannot be used with StoreFront.

Configure using management console

To configure Entra ID SSO:

1. Open the Store settings window for the store you wish to configure.
2. In the Action pane, select **Configure Store Settings**.
3. On the **Configure Store Settings** page, select the **Entra SSO** tab.
4. Enable or disable Entra SSO.



5. Select **OK** to save your changes.

This setting only affects machines in delivery groups configured to use log on type of Entra or hybrid. For delivery groups with log on type Active Directory, you may wish to also enable Federated Authentication Service.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configuration using PowerShell

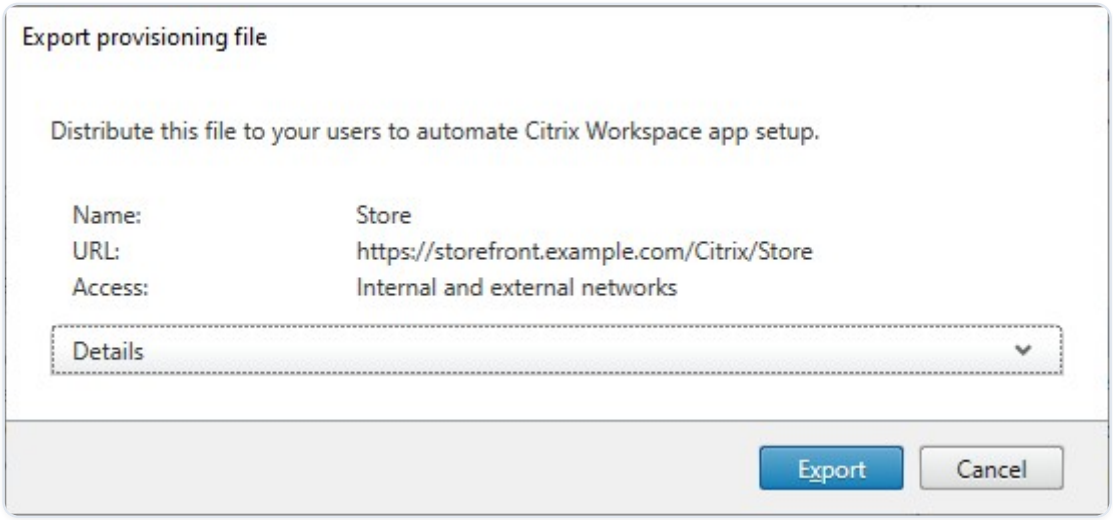
To configure single sign-on using PowerShell, call the Set-STFStoreLaunchOptions cmdlet with parameter `-EntraIdSsoEnabled`.

Export store provisioning files for users

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

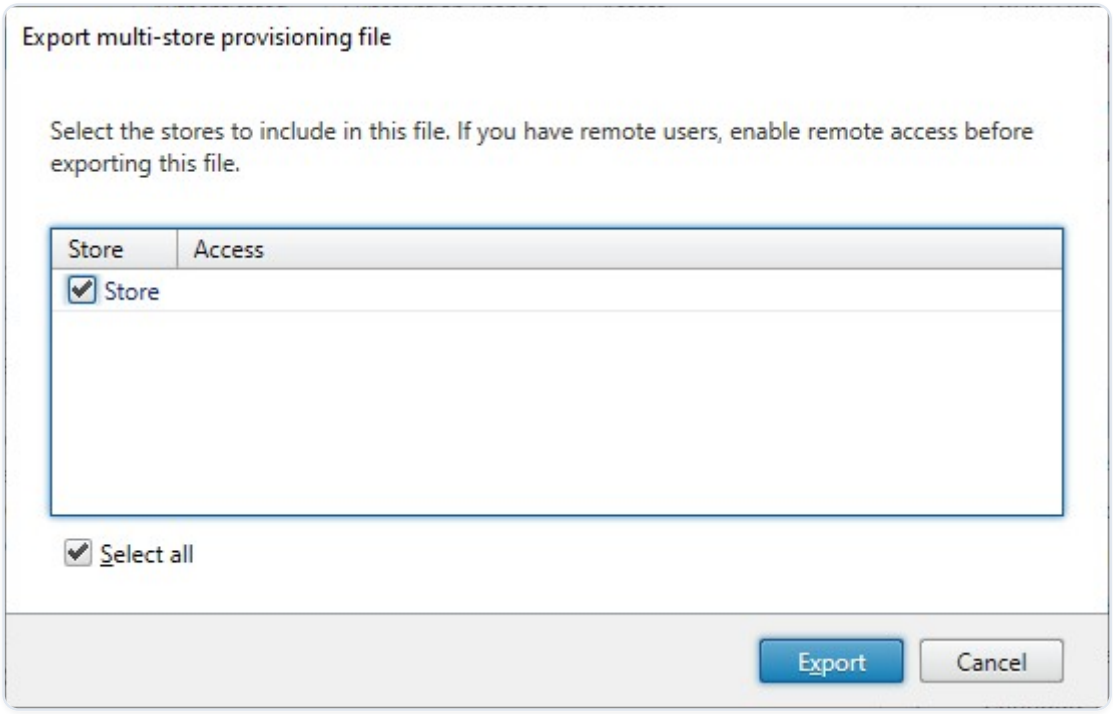
1. In the StoreFront management console select the **Store** node.
2. Select the store for which you wish to export a provisioning file.
3. From the **Actions** pane, select **Export provisioning file**.
4. Select **Export**.
5. Choose a location to save the file and select **Save**.



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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Configure session settings

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

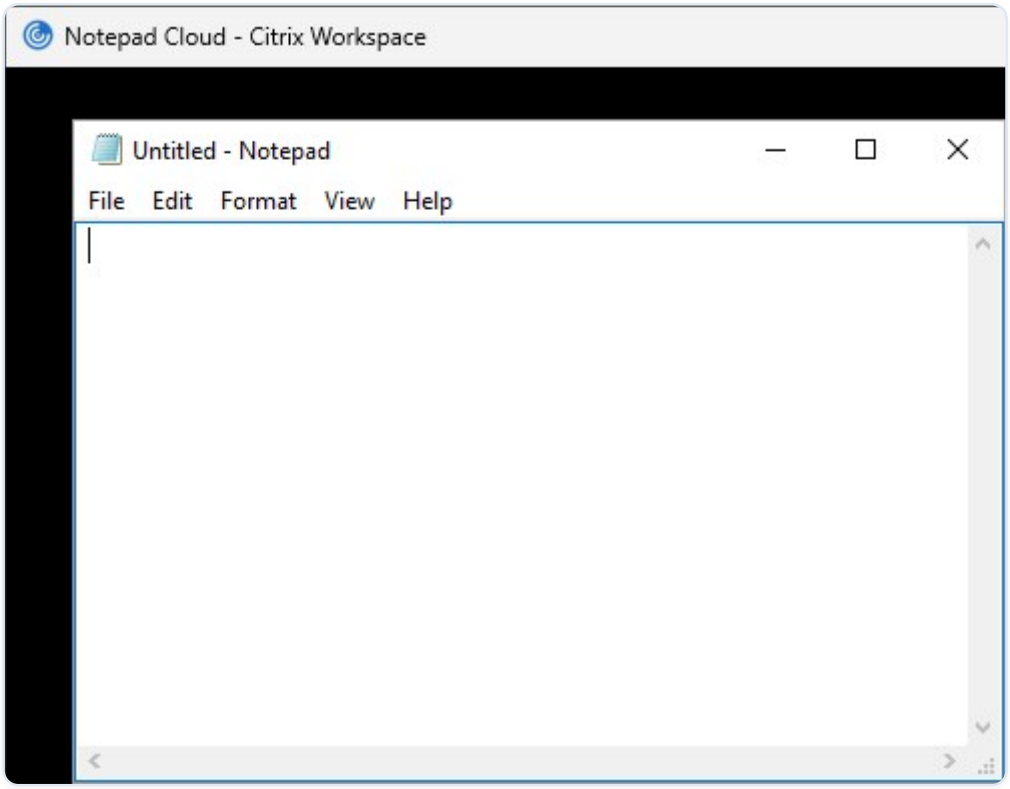
For example:

```
[Notepad]

TWIMode=Off

DesiredHRES=1024

DesiredVRES=768
```



© 1997–2026 Citrix Systems, Inc. All rights reserved.

Citrix Workspace™ app configuration

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:

```
<properties>

    <clear/>

    <property name="PutShortcutsOnDesktop" value="true"/>

    <property name="DesktopDir" value="Citrix Applications"/>

</properties>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Integrate with Citrix Gateway and NetScaler ADC

Use Citrix Gateway with StoreFront to provide secure remote access for users outside the corporate network and NetScaler ADC to provide load balancing.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Configure Citrix Gateways

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.

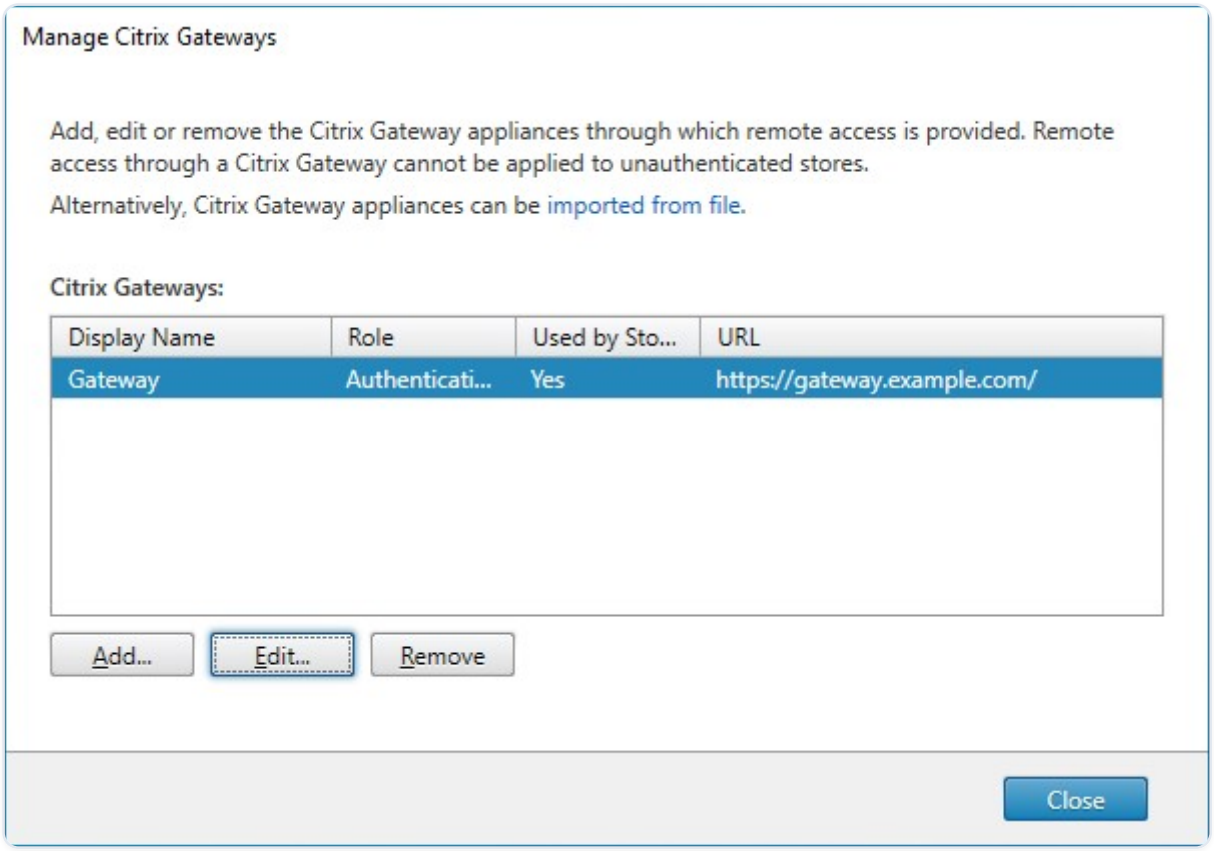
For more information about configuring your Gateway, see Integrate NetScaler Gateway with StoreFront.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

URL to the `X-Citrix-Via` HTTP header. StoreFront uses this header to determine which gateway is in use.

Using the GUI it is only possible to add a single gateway URL. If a gateway can be access by multiple URLs then you need to add the same gateway twice with identical configuration apart from the URL. To simply configuration, you can configure a secondary URL used to access the gateway. This option is not available using the GUI so you must configure this using PowerShell. You should close the management console before running any PowerShell commands. For example if you have multiple gateways behind a global server load balancer, typically it is useful to add both the GSLB URL and a URL that can be used to access each specific regional gateway, for example for testing or troubleshooting purposes. Once you have created the gateway you can add an additional URL using `Set-STFRoamingGateway`, using the `-GSLBurl` parameter for the secondary URL. Although the parameter is called `GSLBurl` this can be used for any situation where you wish to add a second URL. For example:

```
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.

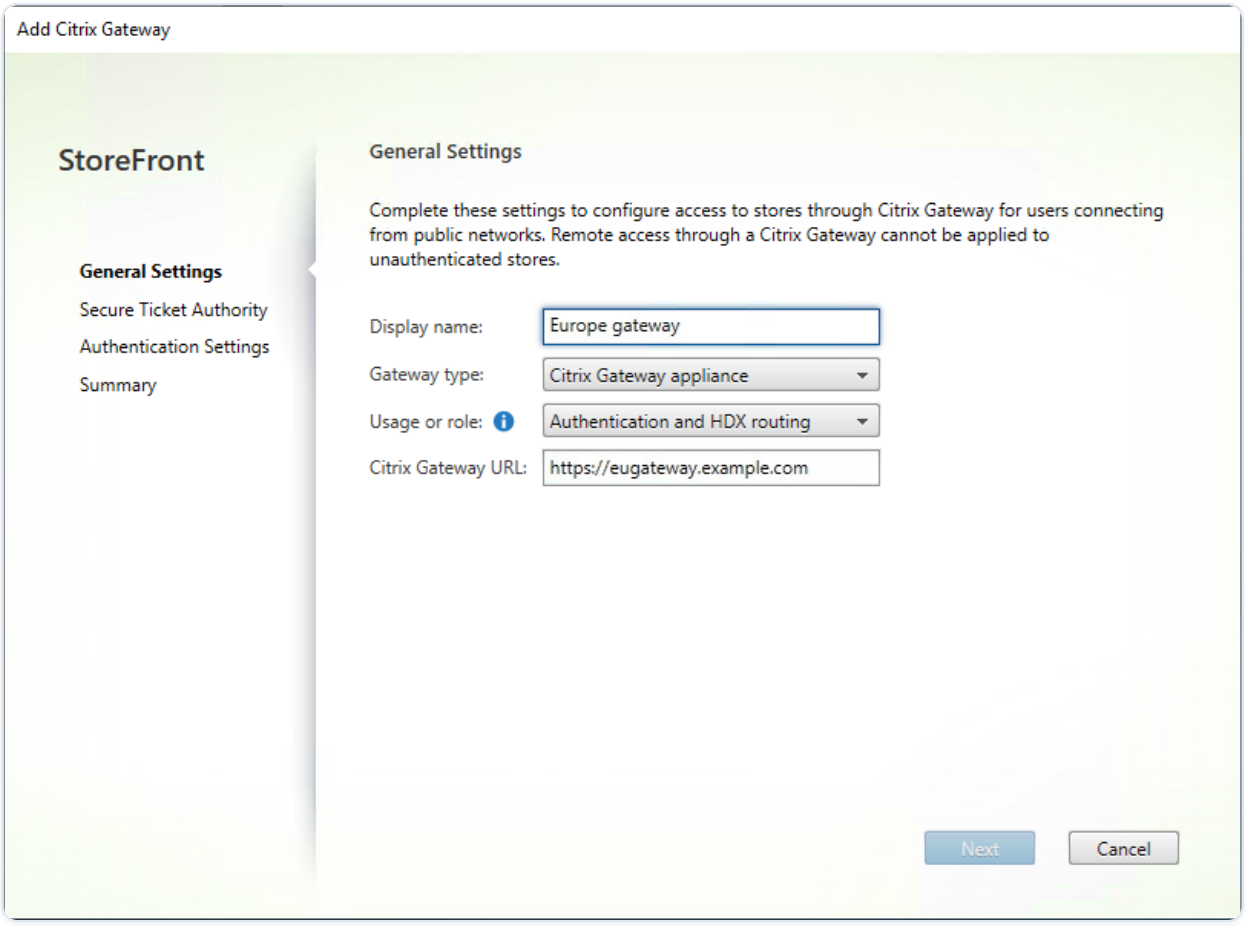
If you need more than two URLs then you will need to configure this as a separate gateway.

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

USAGE OR ROLE	DESCRIPTION
Authentication only	Select this if the gateway is used only for remote access to StoreFront. This option prevents Citrix Workspace launcher from working. Therefore, if you need to use hybrid launches, choose **Authentication and HDX routing** 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.



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.

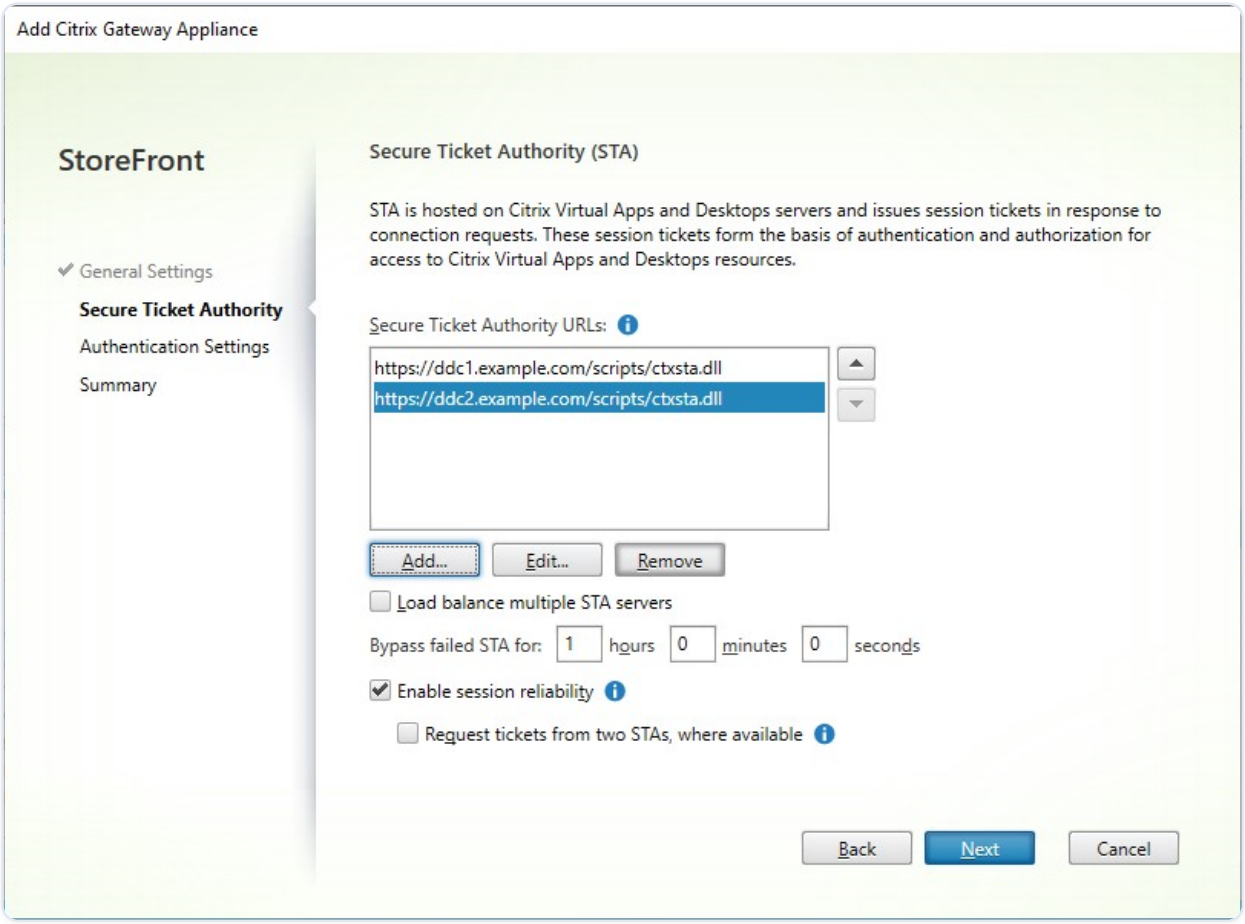
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



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.

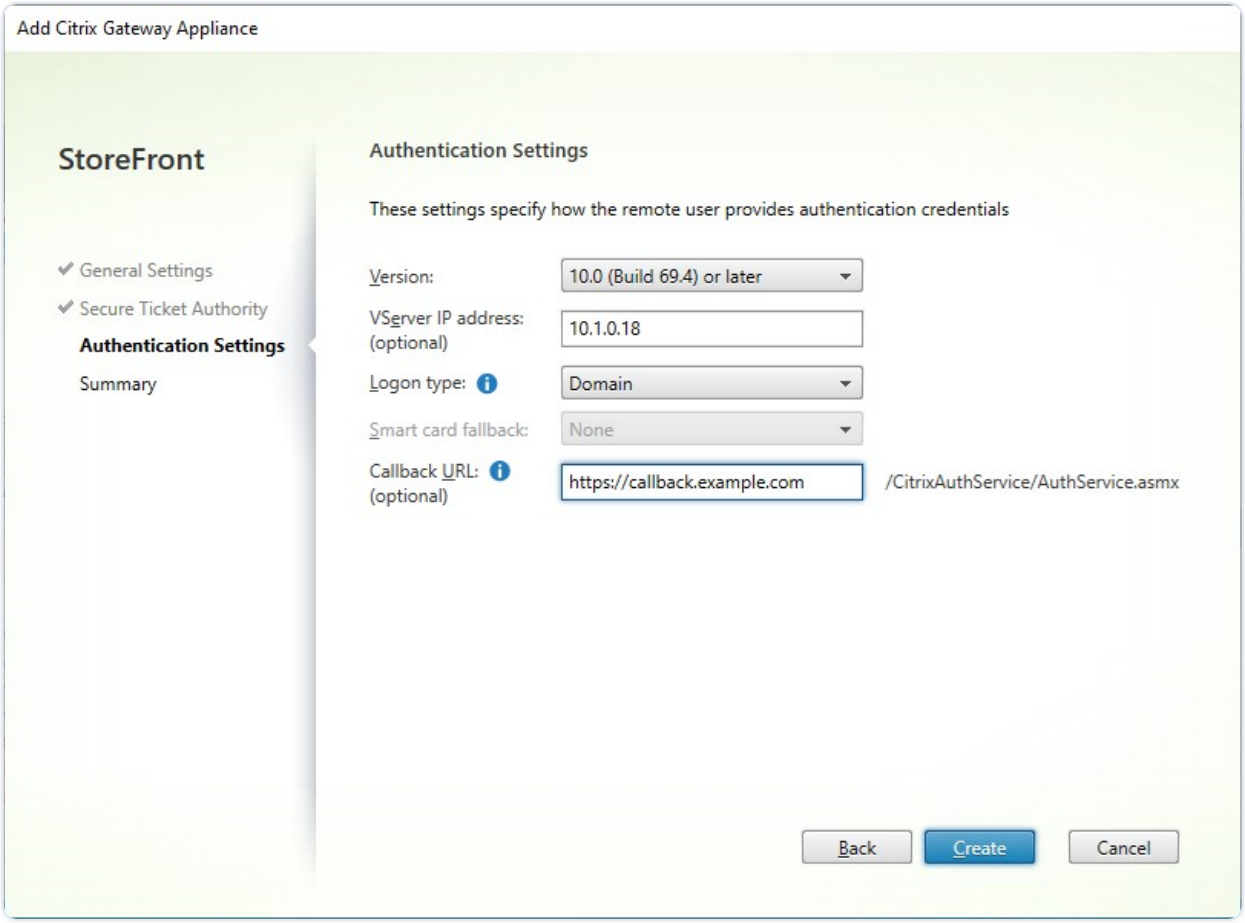
   The information you provide about the configuration of your Citrix Gateway appliance is added to the provisioning file for the store. This enables Citrix Workspace app to send the appropriate connection request when contacting the appliance for the first time.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- For LDAP authentication, select **Domain**.
- For Native OTP authentication, select **Security token**.
- For LDAP plus OTP authentication, select **Domain and security token**.
- For OTP via text message, select **SMS authentication**.
- For certificate authentication, select **Smart card**.
- For SAML authentication, select **Domain**.
- For OIDC authentictation, select **Domain**.

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.

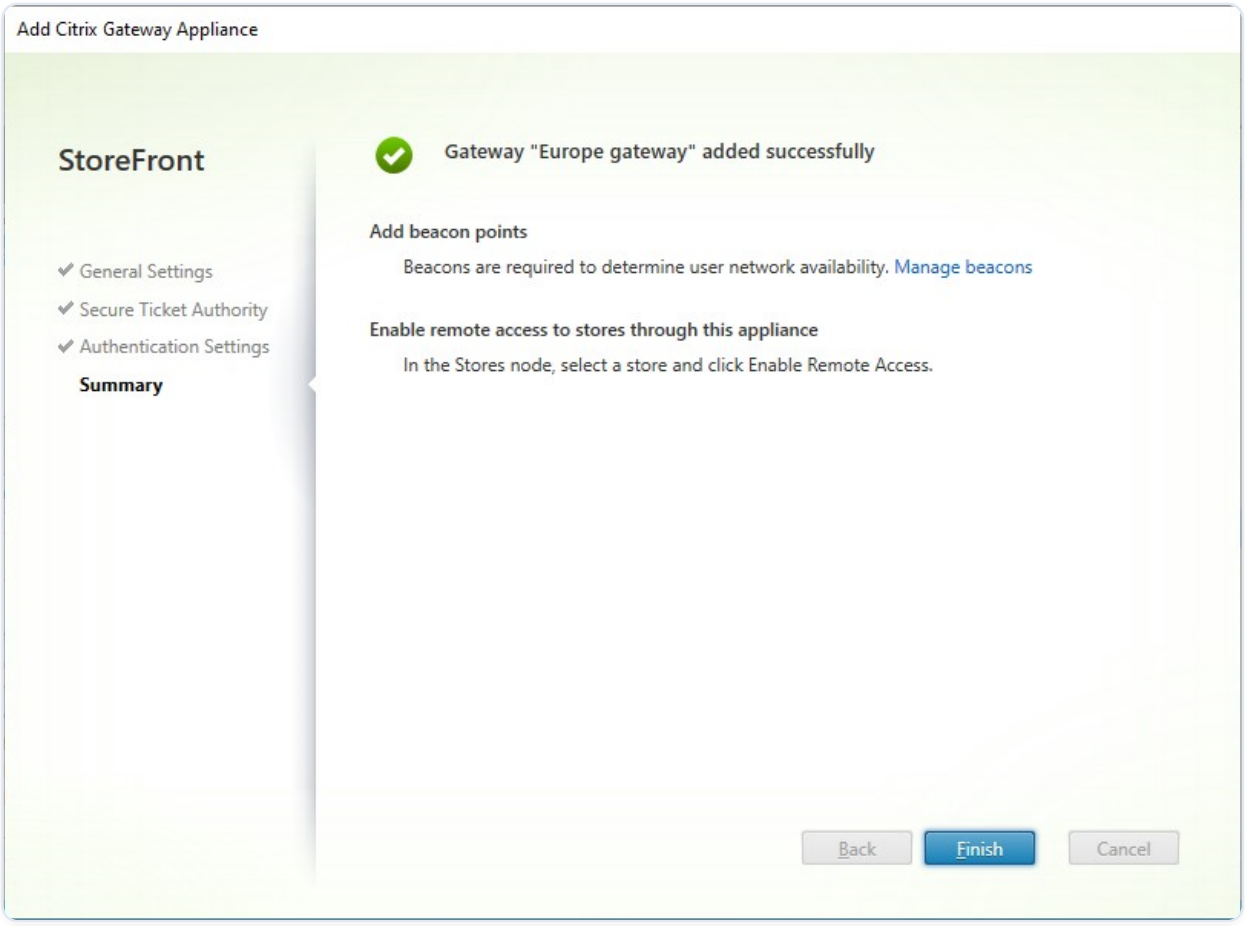
- Optionally, enter the internally accessible URL of the gateway in the Callback URL box. This allows StoreFront to contact the Citrix Gateway authentication service to verify that requests received from Citrix Gateway originate from that appliance. It is required for smart access and for password-less 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.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

Set-STFRoamingGateway -Gateway $gateway -SecureTicketAuthorityObjs
$sta1,$sta2
```

8. To enable users to access your stores through the Gateway, configure remote user access.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

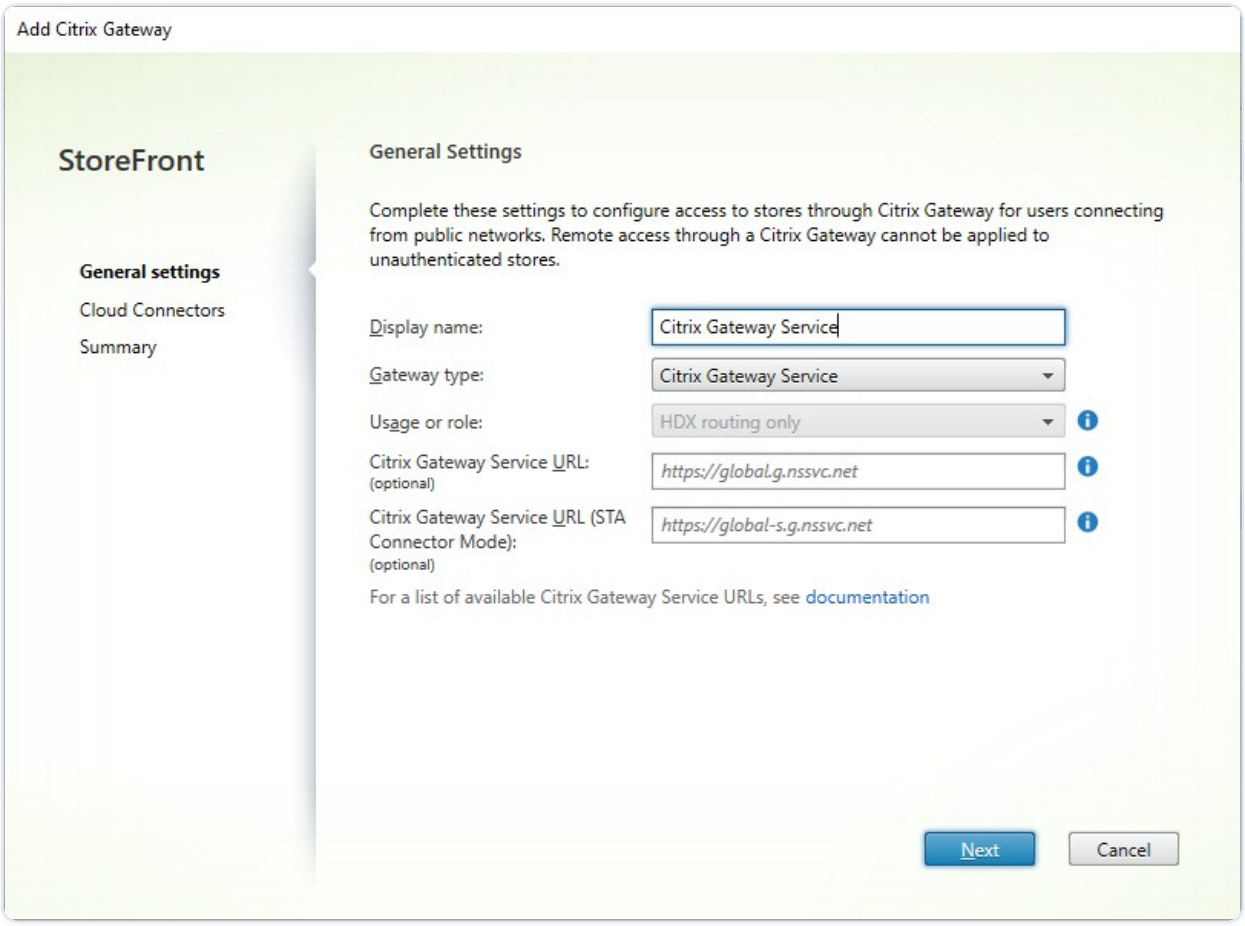
If you have enabled the Citrix Gateway Service for StoreFront in Citrix Cloud then you must configure it as a gateway within StoreFront.

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`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

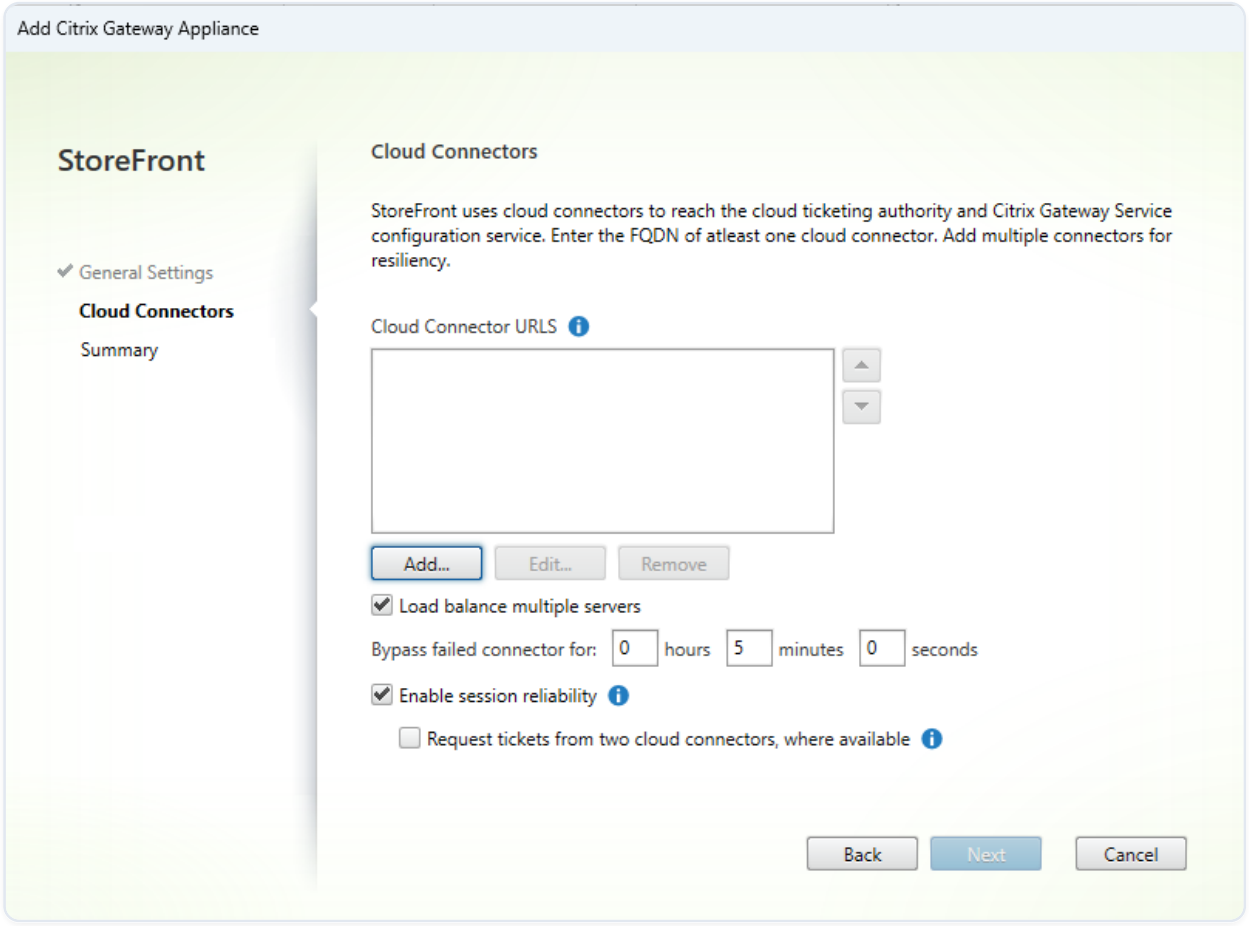
     StoreFront calls these cloud connectors to retrieve STA tickets which Citrix Workspace app can use to authenticate requests through the Citrix Gateway. In normal operation the Cloud Connectors proxy requests to the Citrix Cloud Ticketing Authority, or when in LHC mode generate their own tickets. In the 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.
     - Instead of listing each Cloud Connector in a resource location individually, you can add a load balancer that distributes requests between the Cloud Connectors in that location. However in the Citrix Gateway VServer configuration you must list each connector individually.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- Citrix DaaS 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.

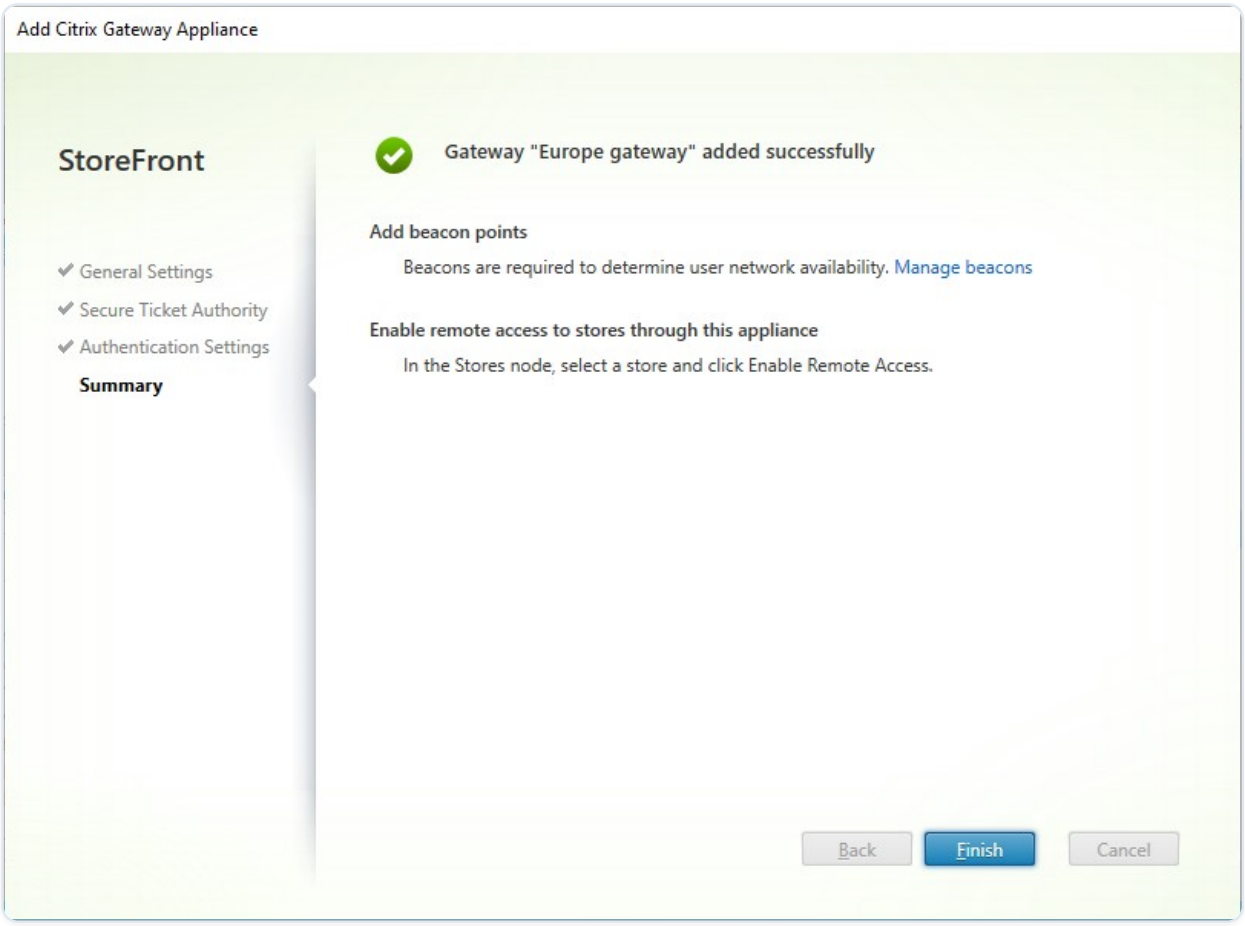
- Select **Load balance multiple servers** to distribute requests between the servers. If cleared then StoreFront will try the servers in the order in which they are listed.
- If StoreFront cannot reach a server then it avoids using that server for a period of time. By default this is 1 hour but you can customize this value.
- Optionally select **Enable session reliability**.
- Optionally select **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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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:

```
$gateway = Get-STFRoamingGateway -Name [Gateway name]

$sta1 = New-STFSecureTicketAuthority -StaUrl [STA1 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

$sta2 = New-STFSecureTicketAuthority -StaUrl [STA2 URL]
-StaValidationEnabled $true -StaValidationSecret [secret]

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

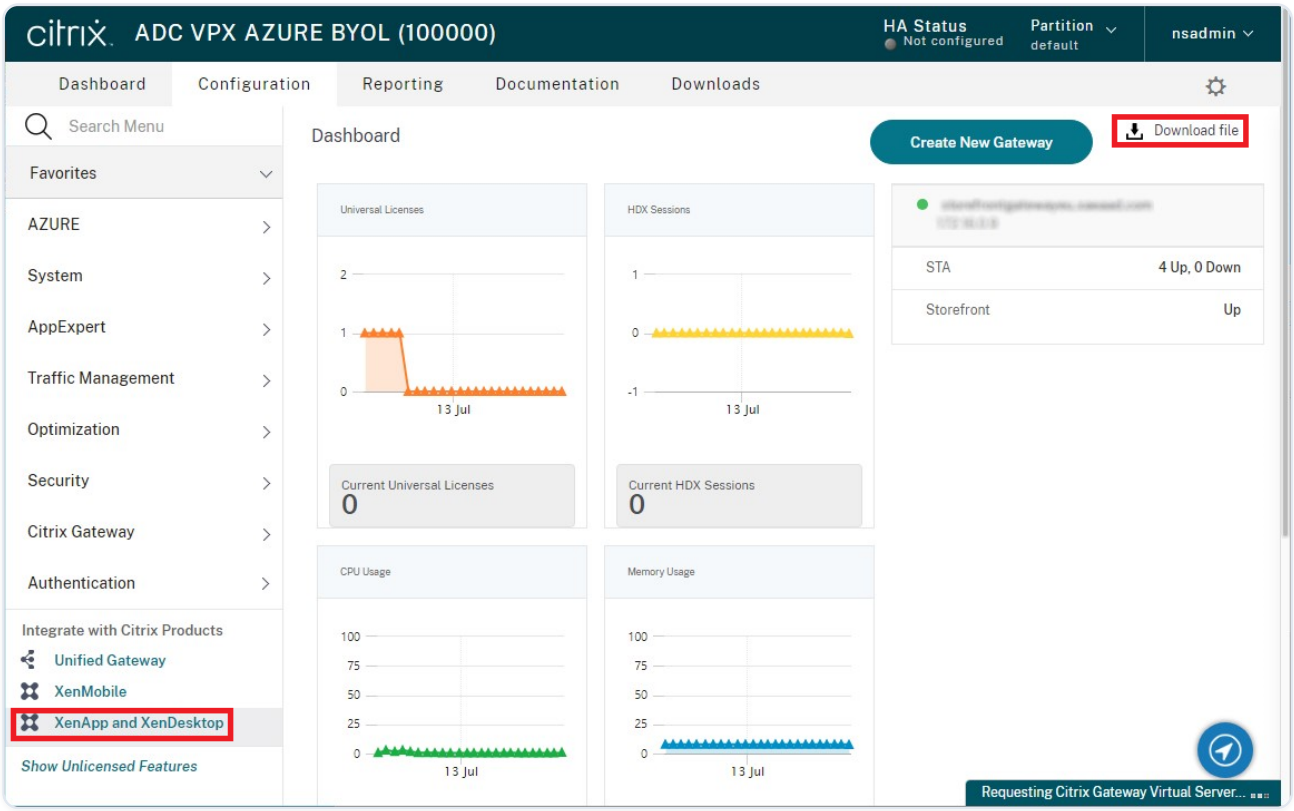
  or

  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".

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. Choose whether you wish to download the configuration for all gateways or a specific gateway.

Import a Citrix Gateway using the console

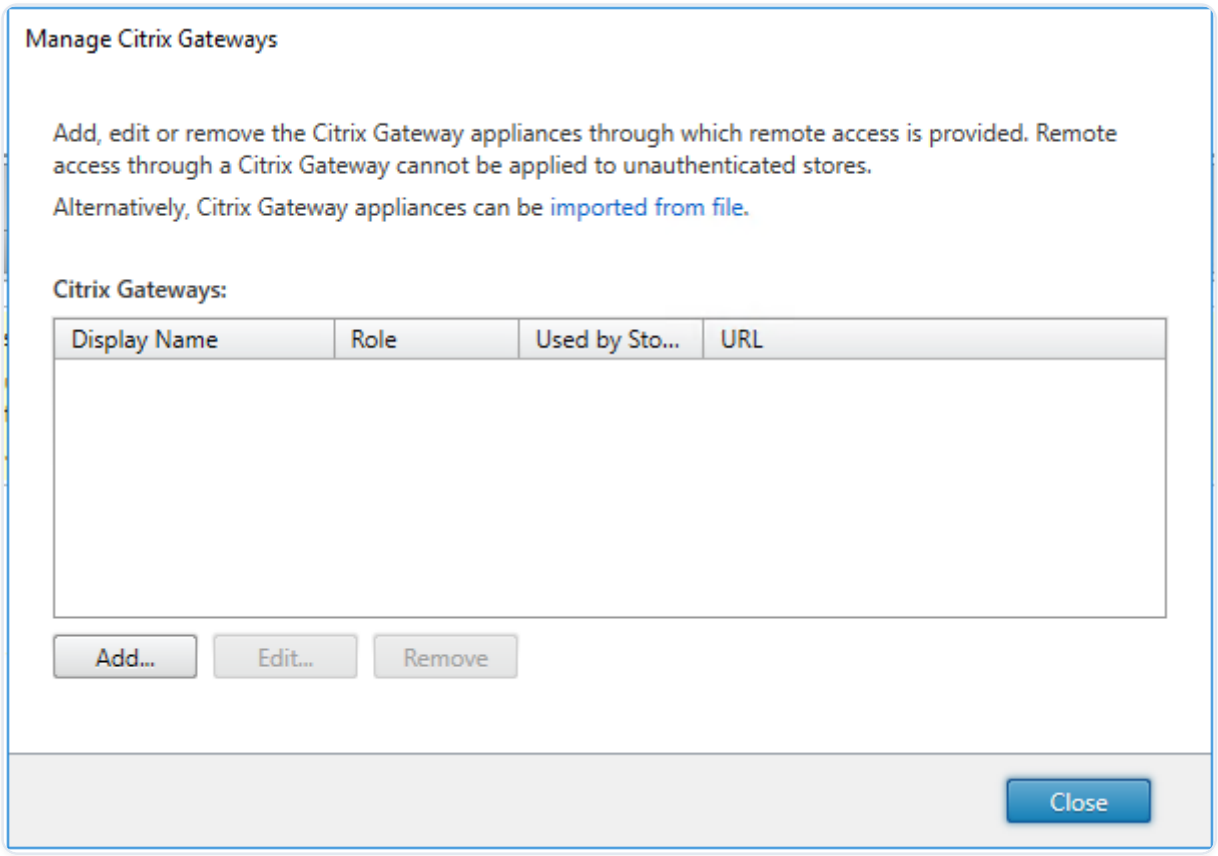
You can import one or more Citrix Gateway virtual server configurations using the same import file. If you have multiple gateway virtual servers from different Citrix Gateway, you must use multiple import files.

Important:

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

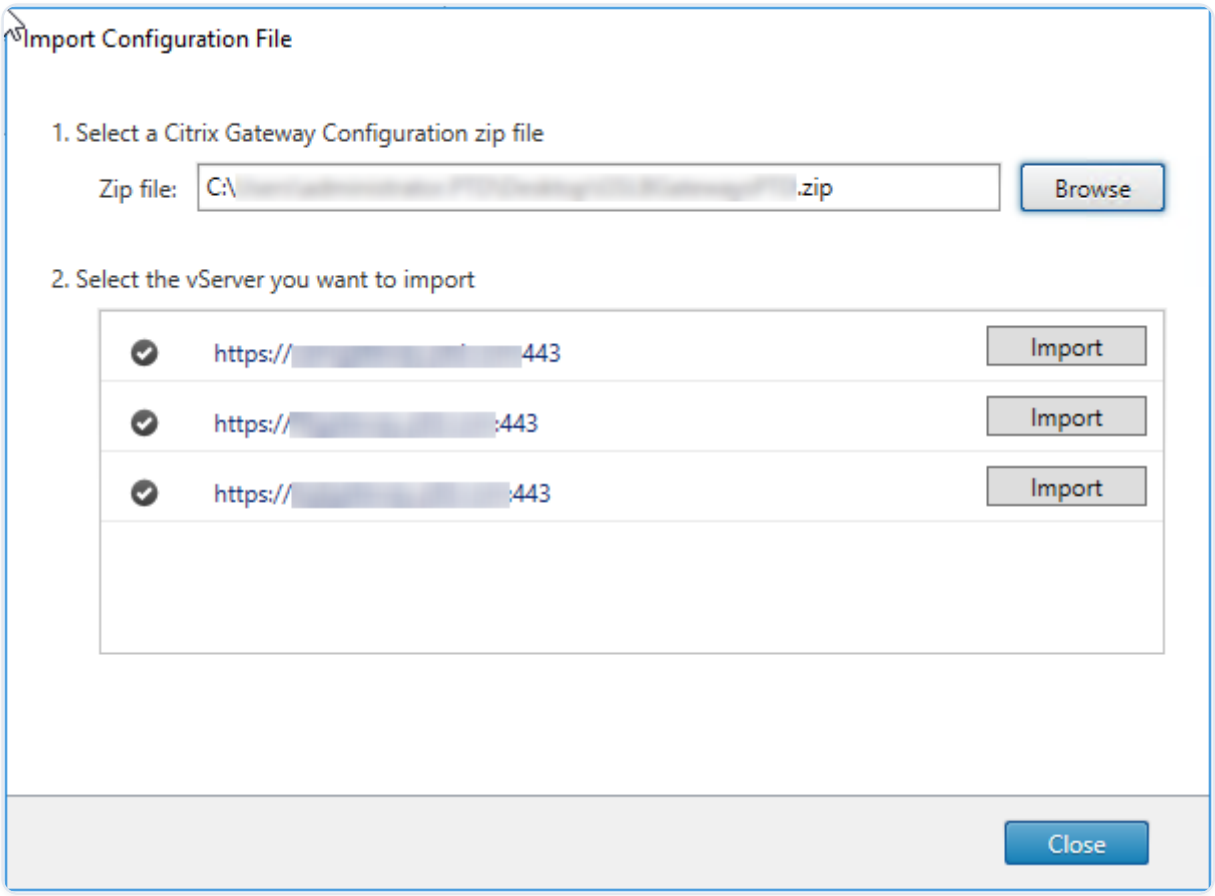
1. Select **Stores** in the left pane of the Citrix StoreFront management console, and in the **Actions** pane, click **Manage Citrix Gateways**.
2. On the Manage Citrix Gateways screen, click the **imported from file** link.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

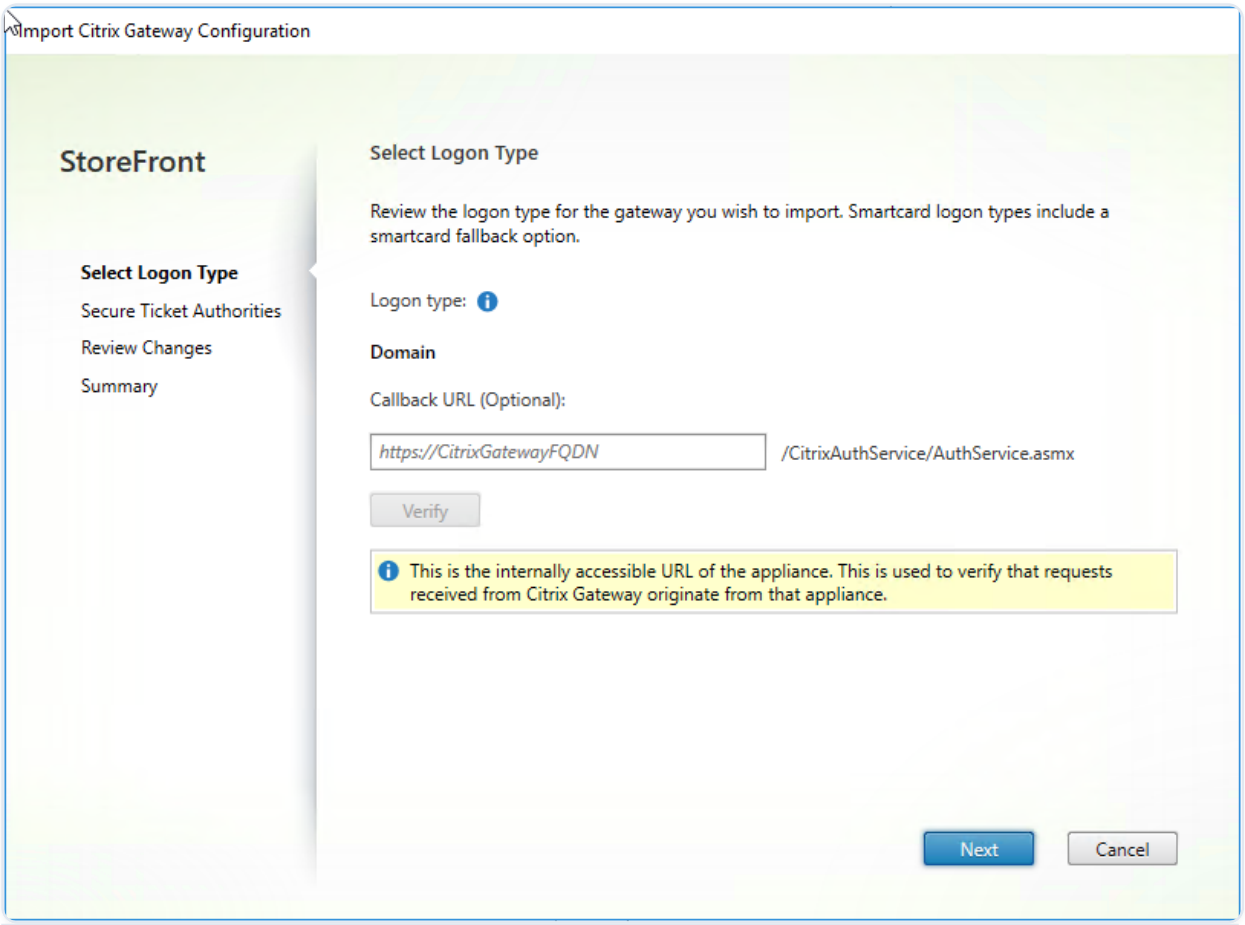
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



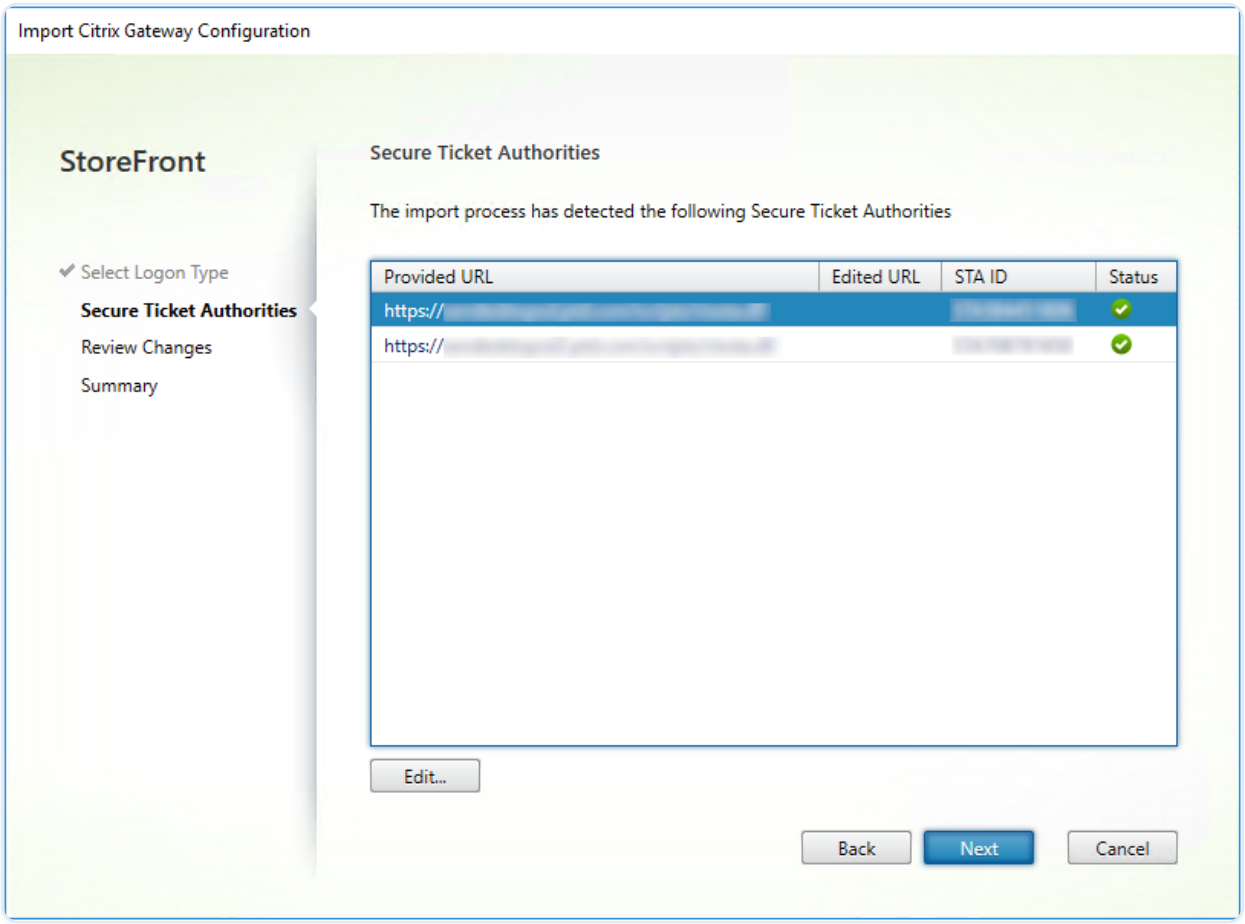
LOGON TYPE IN CONSOLE	LOGONTYPE IN JSON FILE	CALLBACK URL REQUIRED
Domain	Domain	No
Domain and security token	DomainAndRSA	No
Security token	RSA	Yes
Smart card - no fallback	SmartCard	Yes
Smart card - domain	SmartCardDomain	Yes
Smart card - domain and security token	SmartCardDomainAndRSA	Yes
Smart card - security token	SmartCardRSA	Yes
Smart card - SMS authentication	SmartCardSMS	Yes
SMS authentication	SMS	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

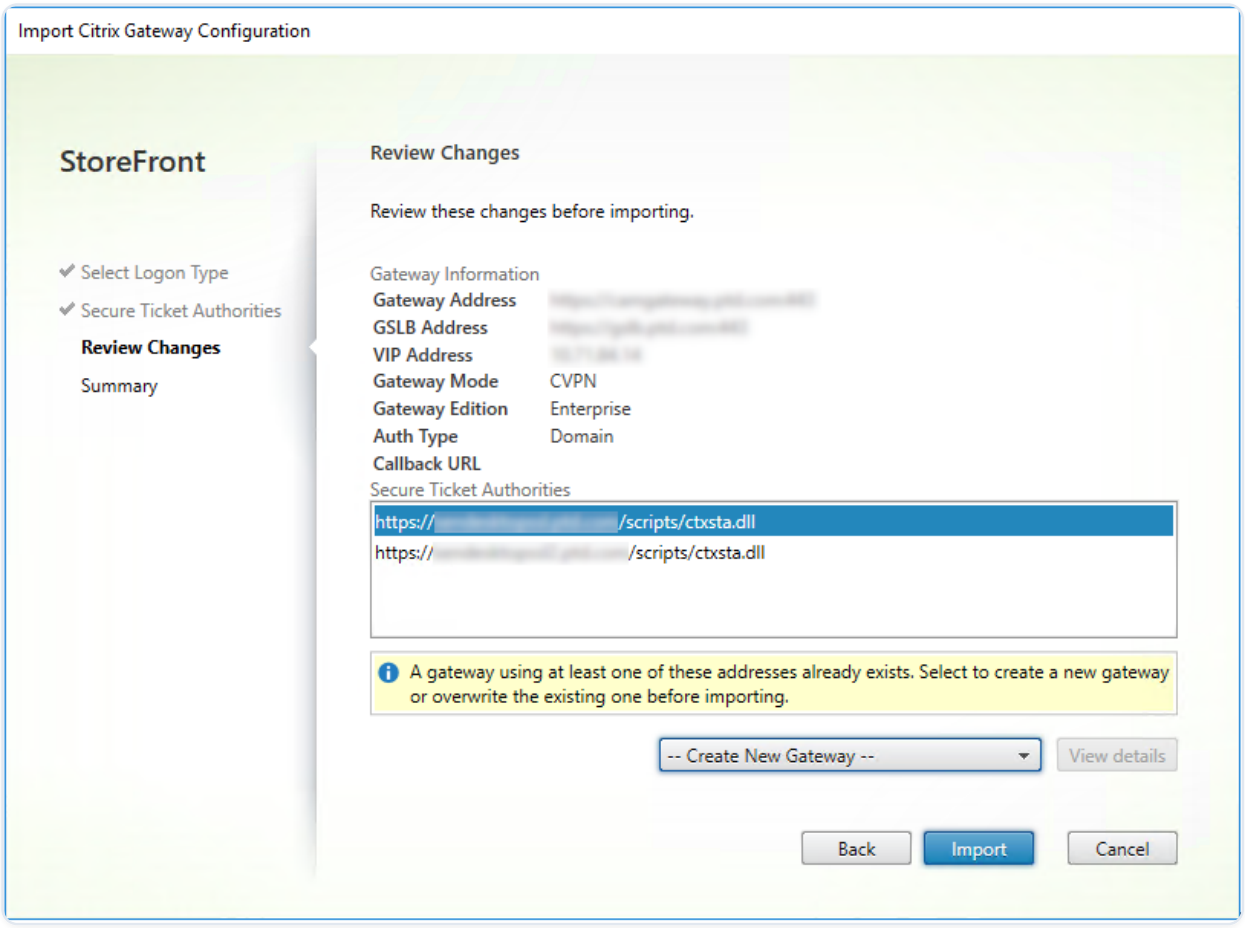
To use Smart Access or password-less authentication, a Callback URL is required.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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
All Logon Types	Yes

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path
"$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.

```
$ImportedGateways.Document.Gateways[0]

$ImportedGateways.Document.Gateways[1]

$ImportedGateways.Document.Gateways[2]



GatewayMode             : CVPN

CallbackUrl             :
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
GslbAddressUri         : https://gslb.example.com/

AddressUri             : https://emeagateway.example.com/

Address                : https://emeagateway.example.com:443

GslbAddress            : https://gslb.example.com:443

VipAddress             : 10.0.0.1

Stas                   : {STA298854503, STA909374257}

StaLoadBalance         : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType        : Domain

GatewayEdition         : Enterprise

ReceiverForWebSites    :
{Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite
}



GatewayMode            : CVPN

CallbackUrl            :

GslbAddressUri         : https://gslb.example.com/

AddressUri             : https://emeagateway.example.com/

Address                : https://emeagateway.example.com:444

GslbAddress            : https://gslb.example.com:443

VipAddress             : 10.0.0.2

Stas                   : {STA298854503, STA909374257}

StaLoadBalance         : True
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType        : DomainAndRSA

GatewayEdition         : Enterprise

ReceiverForWebSites    :
{Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite
}



GatewayMode            : CVPN

CallbackUrl            : https://emeagateway.example.com:445

GslbAddressUri         : https://gslb.example.com/

AddressUri             : https://emeagateway.example.com/

Address                : https://emeagateway.example.com:445

GslbAddress            : https://gslb.example.com:443

VipAddress             : 10.0.0.2

Stas                   : {STA298854503, STA909374257}

StaLoadBalance         : True

CertificateThumbprints : {F549AFAA29EBF61E8709F2316B3981AD503AF387}

GatewayAuthType        :SmartCard

GatewayEdition         : Enterprise

ReceiverForWebSites    :
{Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.ReceiverForWebSite
}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path
"$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.

```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 0 -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 1 -Confirm:$False

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.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path
"$env:USERPROFILE\desktop\GatewayConfig.zip"



Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 0 -CallbackUrl "https://emeagatewaycb.example.com:443
-Confirm:$False



Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.com:444
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-Confirm:$False



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.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path
"$env:USERPROFILE\desktop\GatewayConfig.zip"



Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 0 -LogonType "SmartCard" -CallbackUrl "https://
emeagatewaycb.example.com:443" -Confirm:$False



Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 1 -LogonType "SmartCard" -CallbackUrl "https://
emeagatewaycb.example.com:444" -Confirm:$False



Import-STFNetScalerConfiguration -Configuration $ImportedGateways
-GatewayIndex 2 -LogonType "SmartCard" -CallbackUrl "https://
emeagatewaycb.example.com:445" -Confirm:$False
```

Load balancing with NetScaler® ADC

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
$ServiceUrl = "https://localhost:443/StorefrontMonitor"

Set-STFServiceMonitor -ServiceUrl $ServiceUrl
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
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`

```
<ArrayOfServiceStatus xmlns="http://schemas.datacontract.org/2004/07/
Citrix.DeliveryServices.ServiceMonitor.Contract" xmlns:i="http://
www.w3.org/2001/XMLSchema-instance">

<ServiceStatus>

    <name>Citrix Peer Resolution Service</name>

    <status>running</status>

</ServiceStatus>

<ServiceStatus>

    <name>CitrixConfigurationReplication</name>

    <status>running</status>

</ServiceStatus>

<ServiceStatus>

    <name>CitrixCredentialWallet</name>

    <status>running</status>

</ServiceStatus>

<ServiceStatus>

    <name>CitrixDefaultDomainService</name>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    <status>running</status>
</ServiceStatus>
<ServiceStatus>
    <name>CitrixSubscriptionsStore</name>
    <status>running</status>
</ServiceStatus>
<ServiceStatus>
    <name>NetTcpPortSharing</name>
    <status>running</status>
</ServiceStatus>
<ServiceStatus>
    <name>WAS</name>
    <status>running</status>
</ServiceStatus>
<ServiceStatus>
    <name>W3SVC</name>
    <status>running</status>
</ServiceStatus>
</ArrayOfServiceStatus>
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.:

```
openssl pkcs12 -in cert.pfx -clcerts -nokeys -out cert.cer

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:

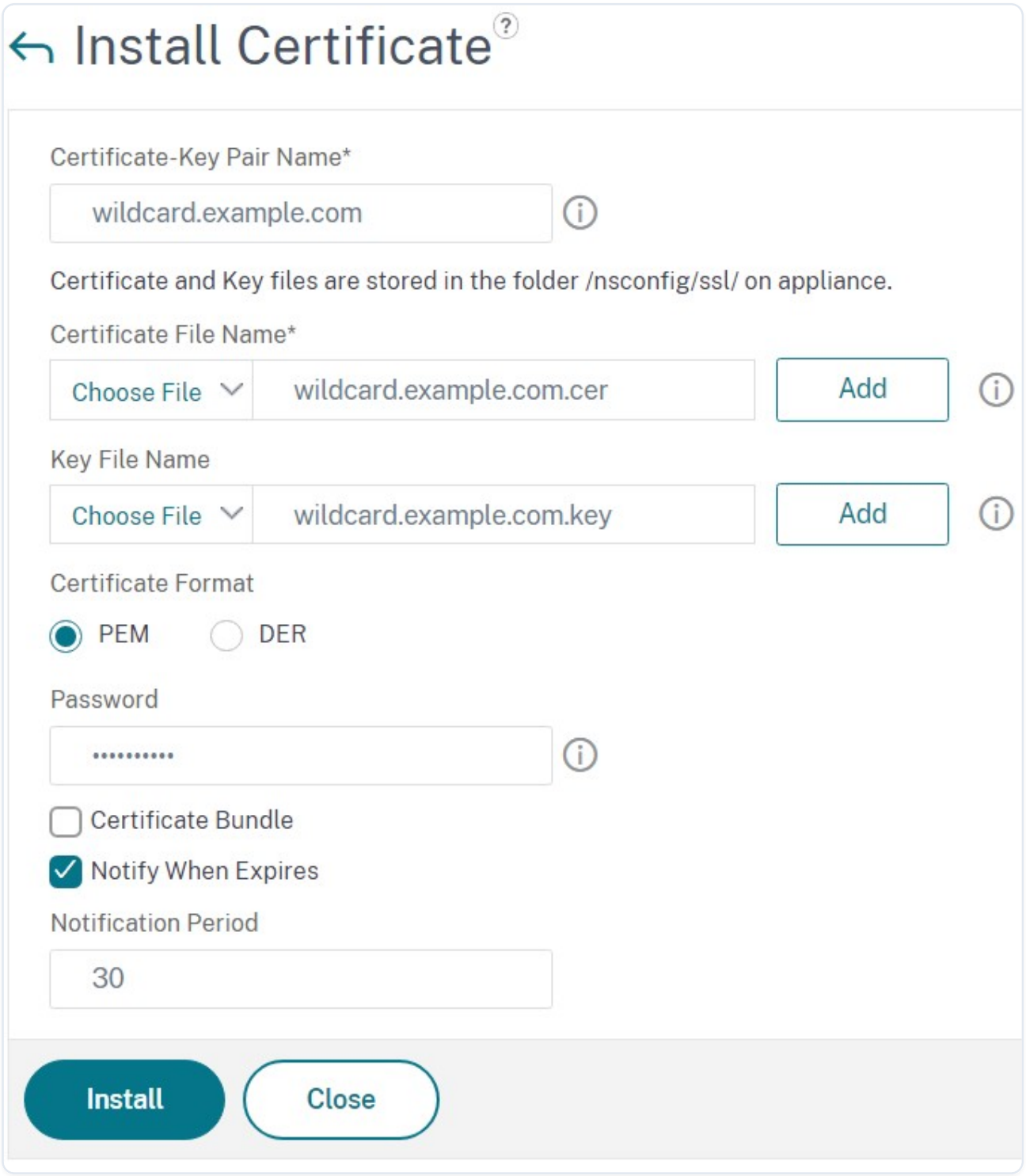
1. Log on to the NetScaler ADC appliance management GUI.
2. Select **Traffic Management** > **SSL** > **Certificates** > **CA Certificates**.
3. Click **Install**.
4. On the **Install CA Certificate** page:
    a. Enter a **Certificate-Key Pair Name**.
    b. Under **Certificate File Name**, click **Choose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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

d. Under **Password** enter the passphrase.

e. Click **Install**.

5. Click **Link** to link the certificate to the root certificate.



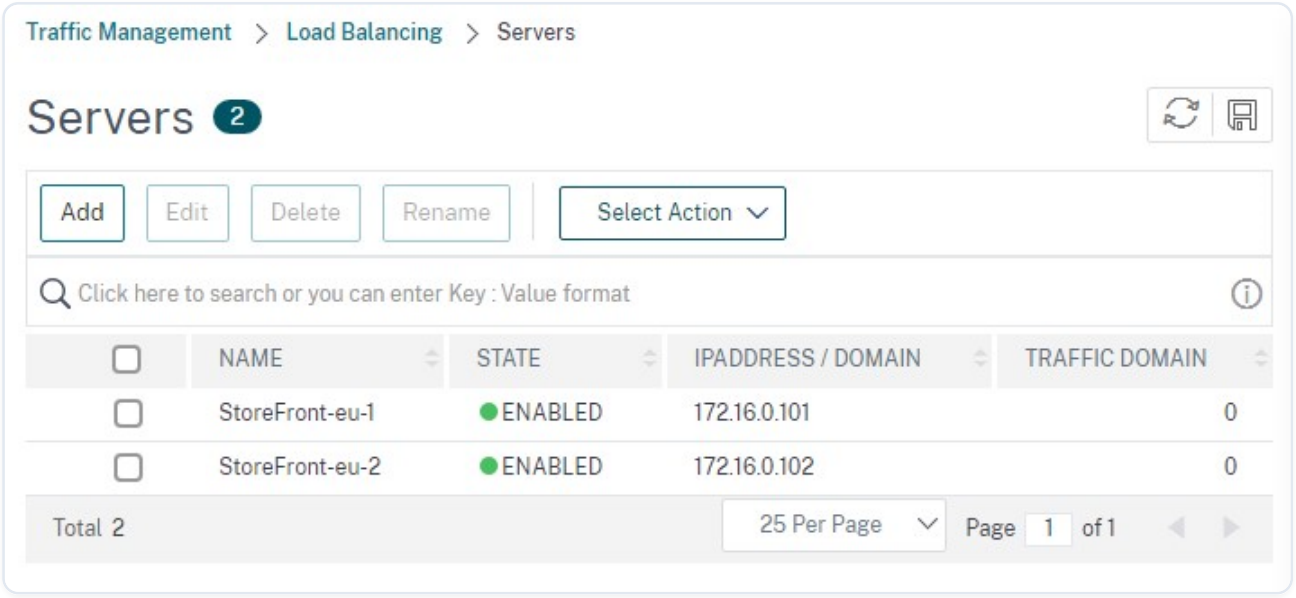
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



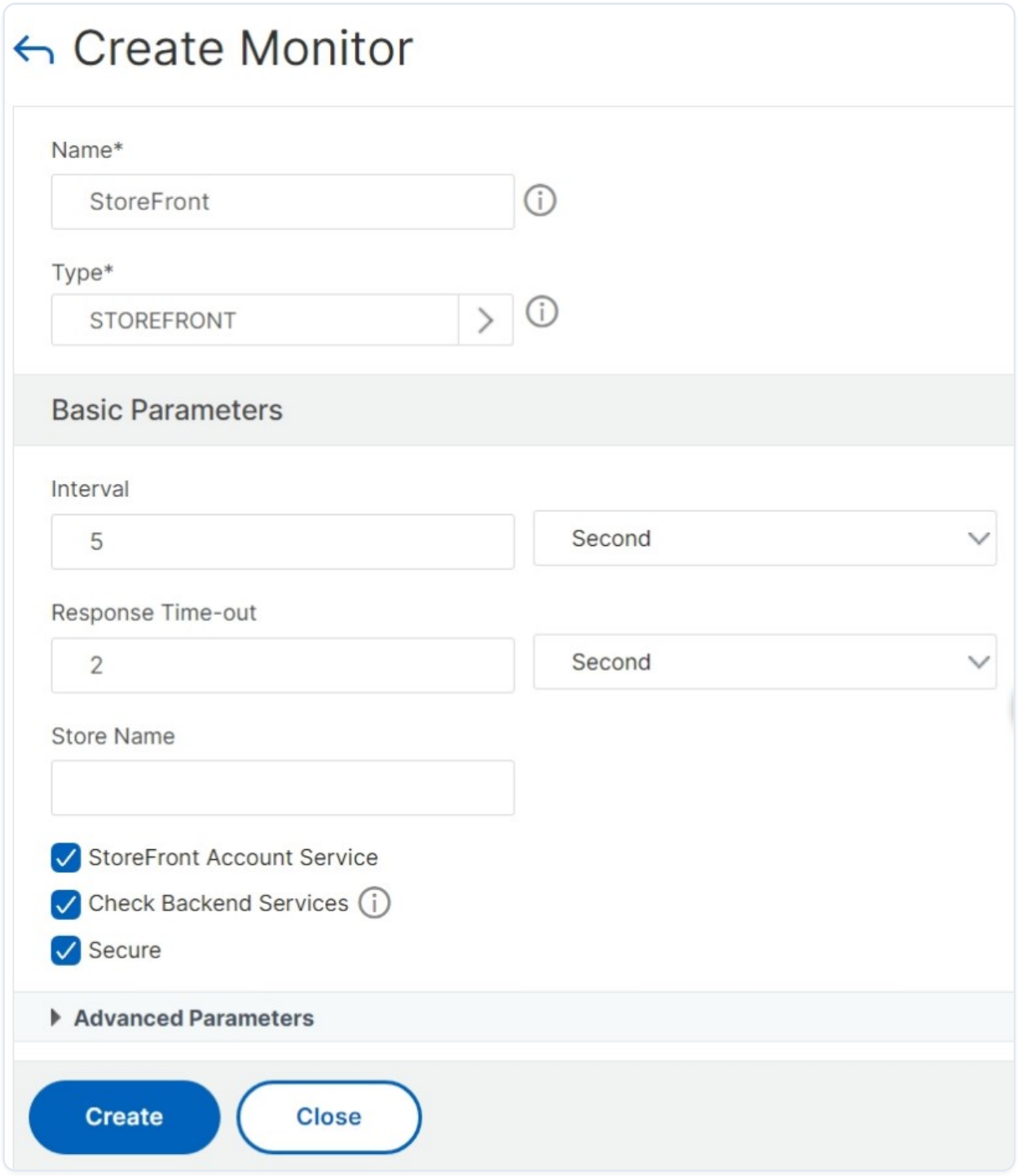
Define a StoreFront monitor to check the status of all StoreFront nodes in the server group

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- CitrixDefaultDomainService



Create a service group containing all of the StoreFront servers

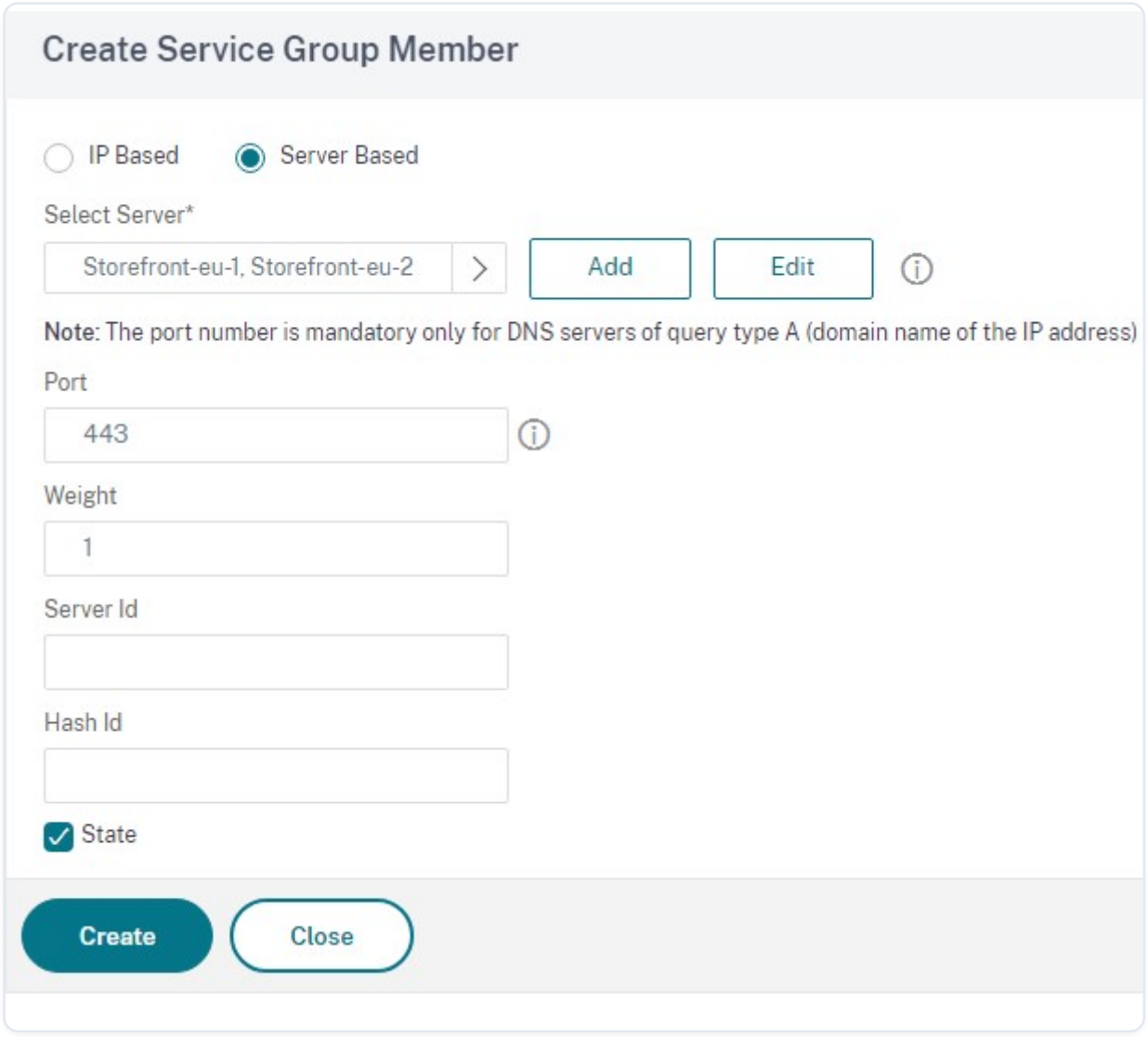
1. Navigate to **Traffic Management > Load Balancing > Service Groups**. Press **Add**. To connect to the StoreFront servers over HTTPS, select a protocol of SSL. Leave other settings as default. Press **OK**.
2. Within your Service Group, under **Service Group Members**, click **No Service Group Member**.

   a. Click **Service Based**.

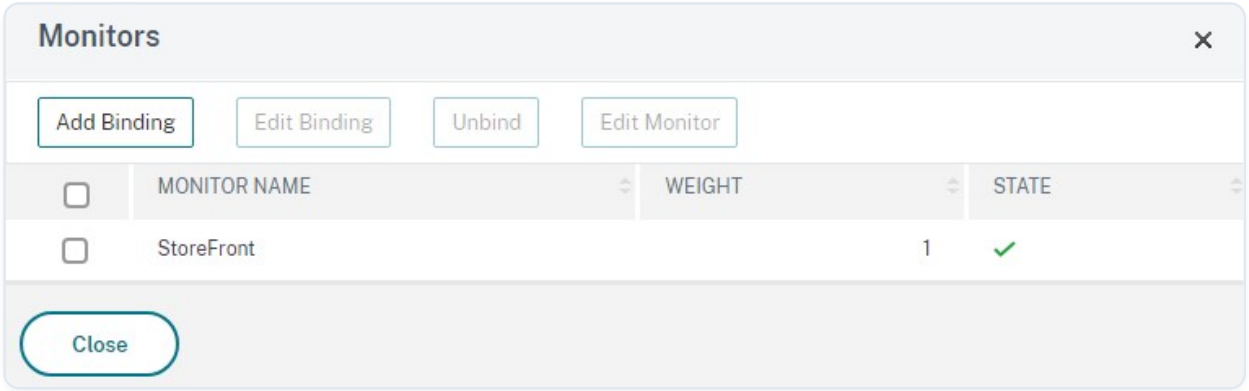
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



3. Add the **Monitors** section and select the StoreFront monitor you created earlier.

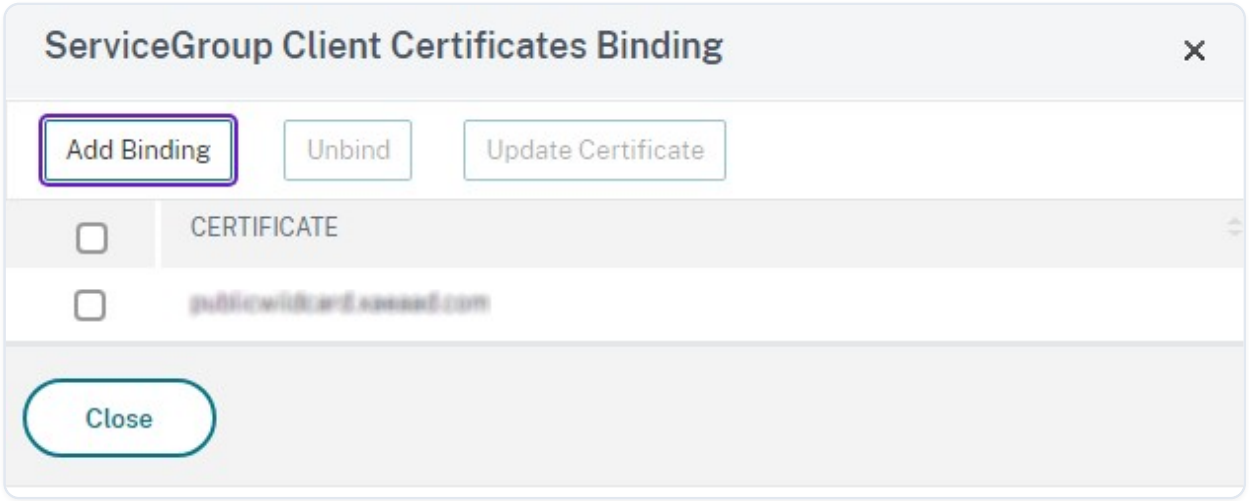


4. Add the **Certificates** section.

a. Bind the client certificate.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

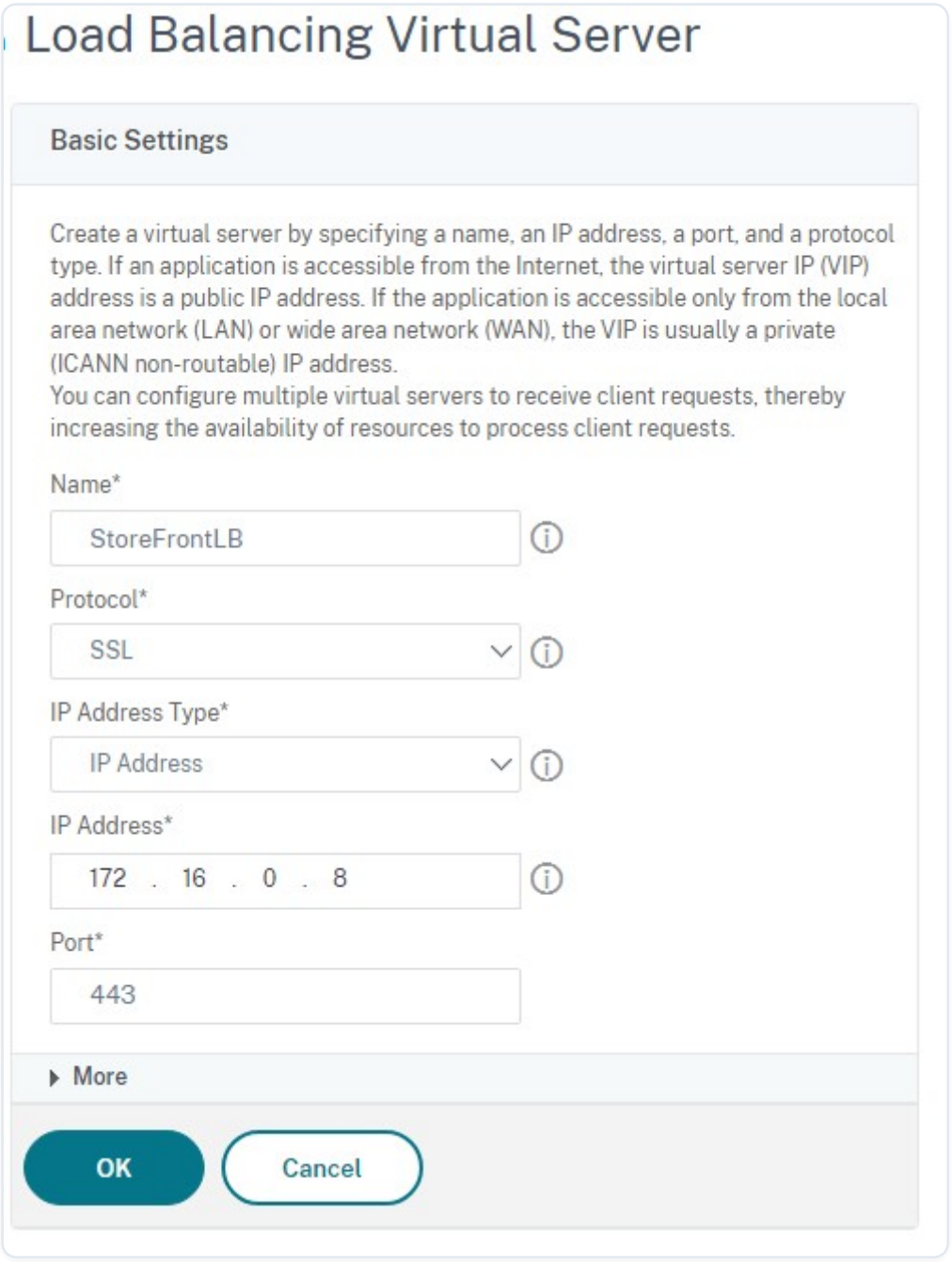


5. Add the **Settings** section. Select **Insert Client IP Header** and enter a header name of **X-Forwarded-For**. This allows the Client IP Address to be used in Citrix Virtual Apps and Desktops Policies.

Create a load balancing virtual server for user traffic

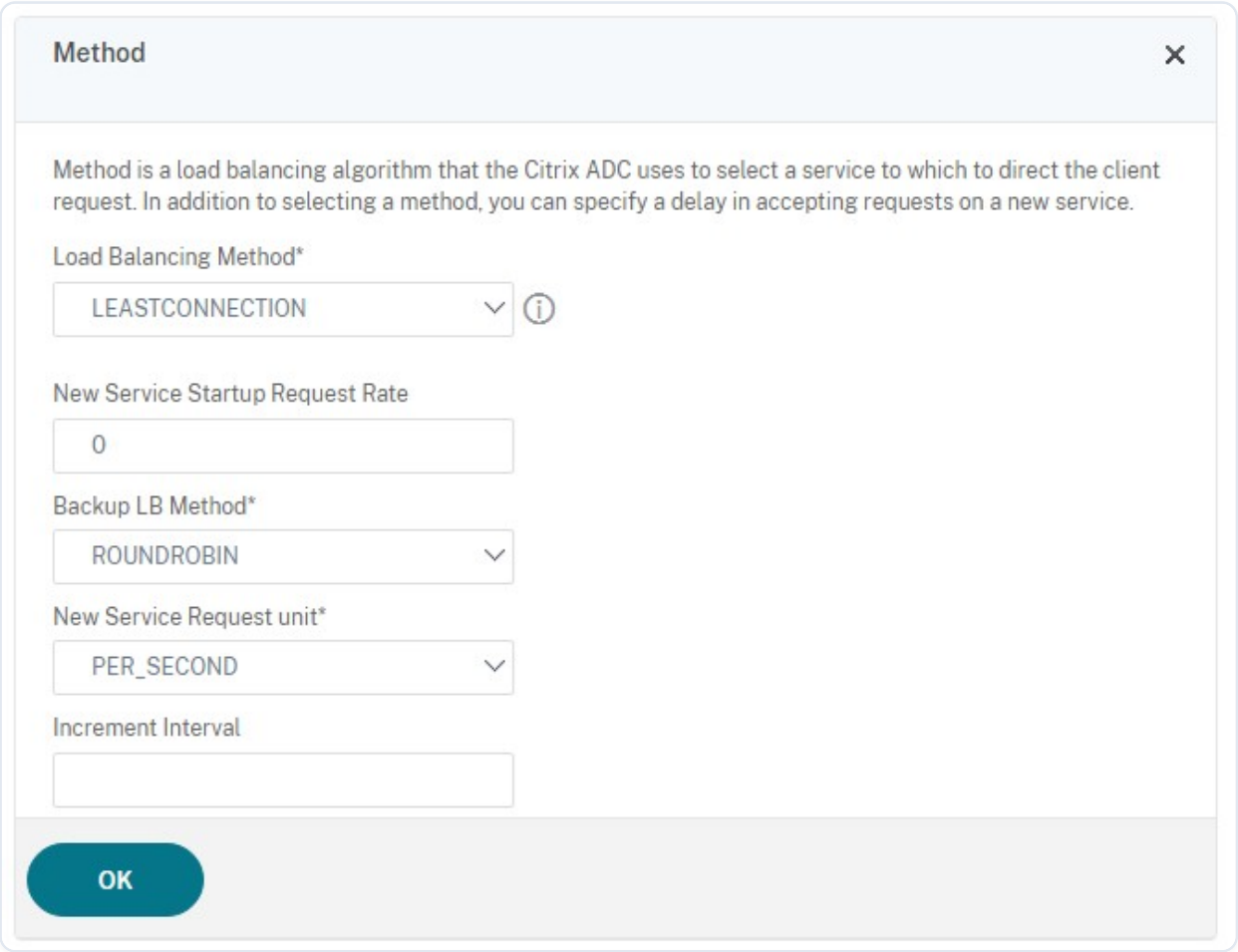
1. Log on to the NetScaler ADC appliance management GUI.
2. Select **Traffic Management > Load Balancing > Virtual Servers > Add** to create a new virtual server.
3. Enter a name, choose a protocol of SSL and enter the **Port**. Click OK to create the Virtual Server.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



7. Add the **Persistance** section.

   a. Set the persistence method to be **COOKIEINSERT**.

   b. Set the time-out to be the same as the Session time out within StoreFront which by default is 20 minutes.

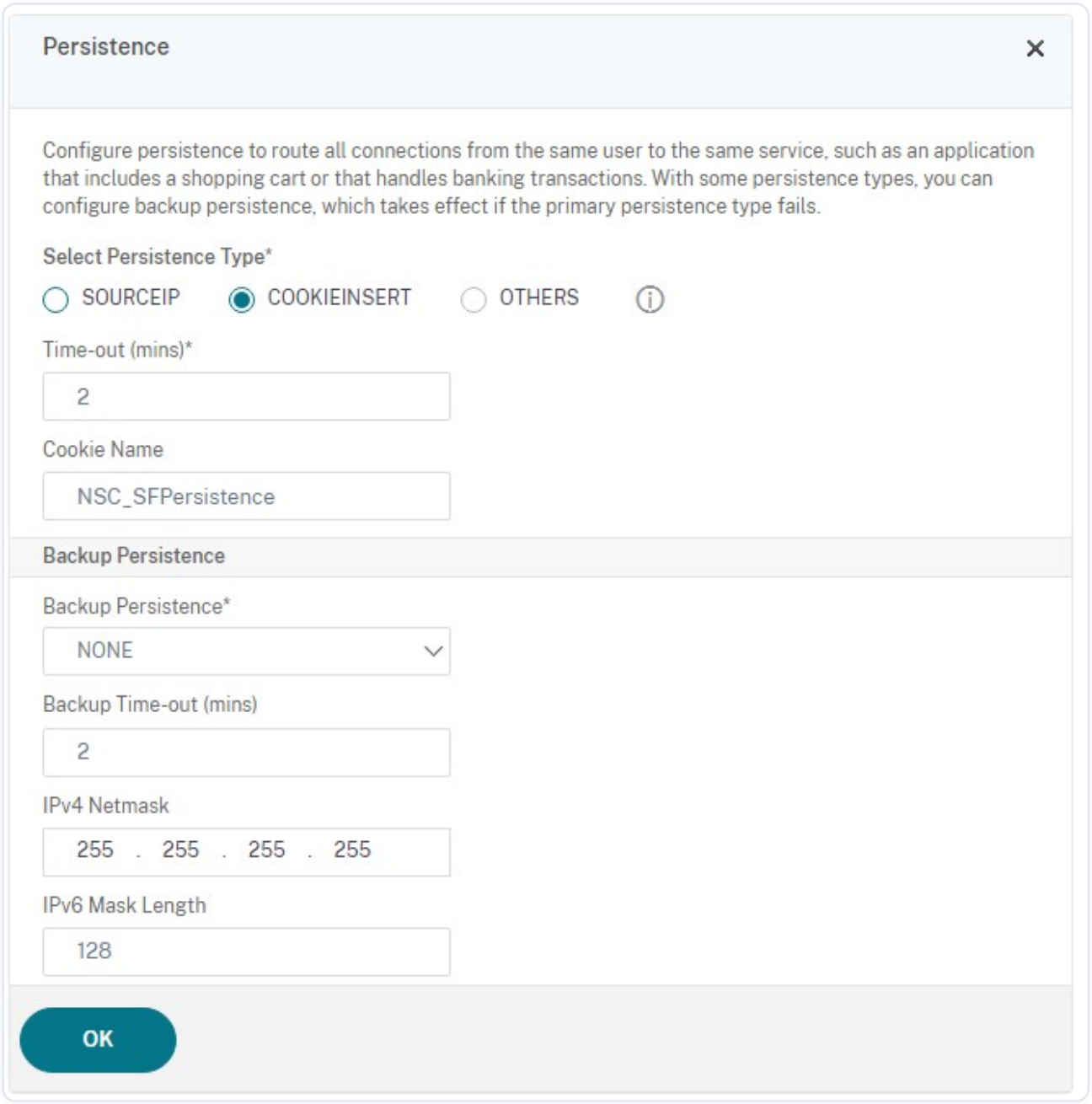
   c. Name the cookie. For example, **NSC_SFPersistence**, as this makes it easy to identify during debugging.

   d. 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

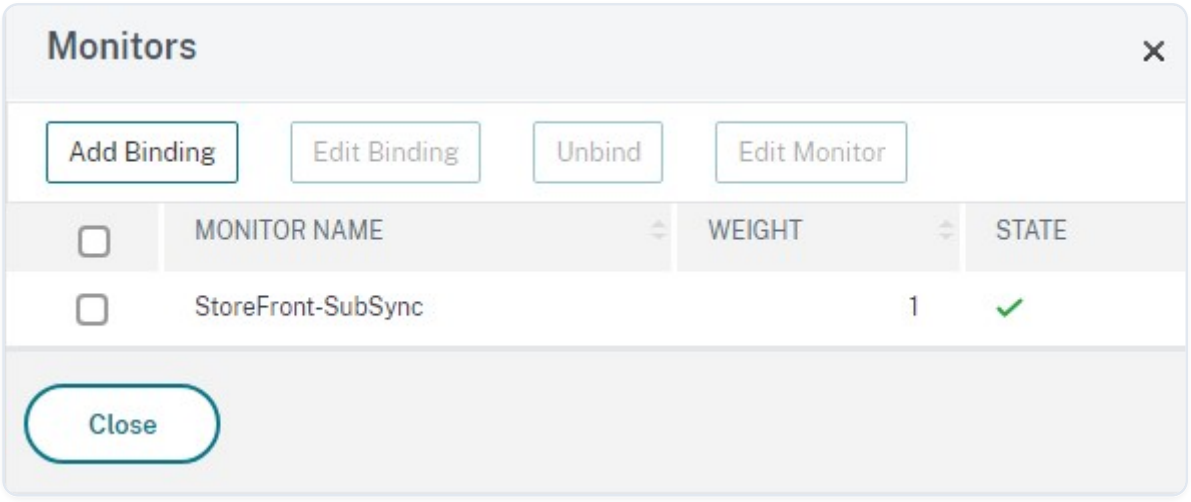
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**.

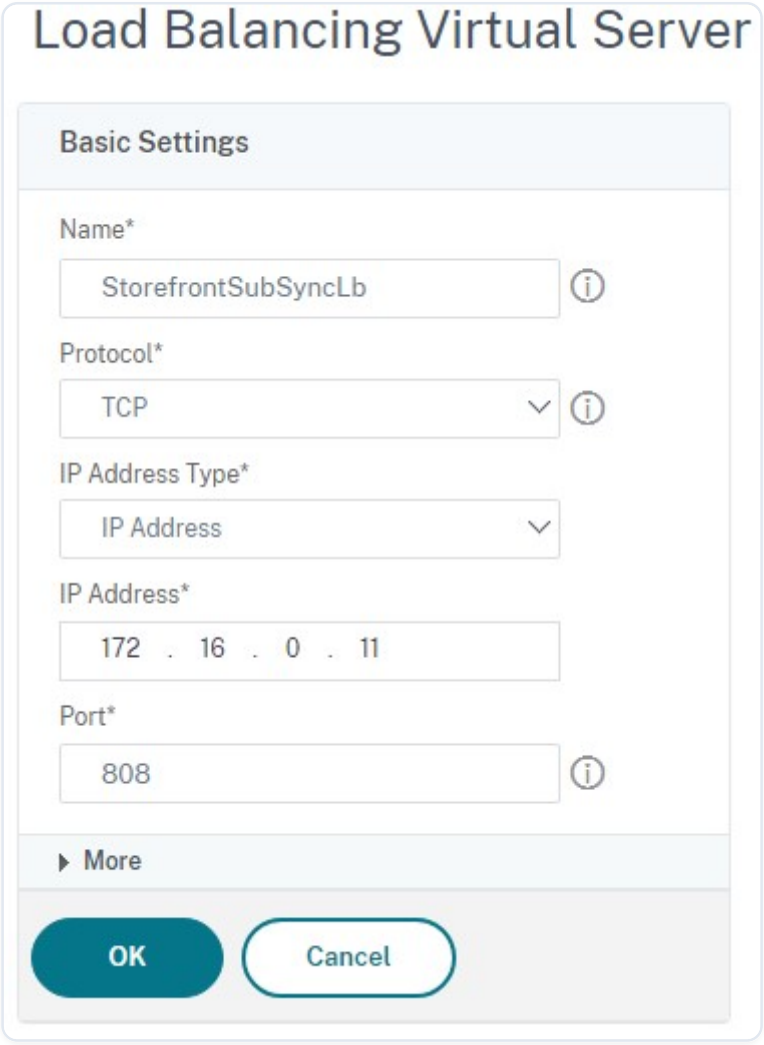


Create a load balancing virtual server for subscription synchronization

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Enter a **Name**
4. Change the protocol to **TCP**.
5. Enter an IP Address.
6. Enter a **Port** of **808**.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure Citrix Gateway and StoreFront for Delegated Forms Authentication (DFA)

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 it 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.

```
PS C:\Users\administrator.PTD.000> cd 'C:\Program Files\Citrix\Receiver
StoreFront\Scripts'

PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> & .
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
\ImportModules.ps1

Adding snapins

Importing modules

Loading 'C:\Program Files\Citrix\Receiver
StoreFront\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'

Loading 'C:\Program Files\Citrix\Receiver
StoreFront\Admin\Citrix.DeliveryServices.ConfigurationProvider.dll'



PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Install-
DSDFAServer

Id                              : bf694fbc-ae0a-4d56-8749-c945559e897a

ClassType                       : e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc

FrameworkController             :
Citrix.DeliveryServices.Framework.FileBased.FrameworkController

ParentInstance                  : 8dd182c7-f970-466c-ad4c-27a5980f716c

RootInstance                    : 5d0cdc75-1dee-4df7-8069-7375d79634b3

TenantId                        : 860e9401-39c8-4f2c-928d-34251102b840

Data                            : {}

ReadOnlyData                    : {[Name, DelegatedFormsServer],
[Cmdlet, Add-DSWebFeature], [Snapin, Citrix.DeliverySer

                                  vices.Web.Commands], [Tenant,
860e9401-39c8-4f2c-928d-34251102b840]}

ParameterData                   : {[FeatureClassId, e1eb3668-9c1c-4ad8-
bbae-c08b2682c1bc], [ParentInstanceId, 8dd182c7-f

                                  970-466c-ad4c-27a5980f716c],
[TenantId, 860e9401-39c8-4f2c-928d-34251102b840]}
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
AdditionalInstanceDependencies : {b1e48ef0-b9e5-4697-af9b-0910062aa2a3}

IsDeployed                     : True

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.

```
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.

```
<example connectorURL="http://Example.connector.url:8080/adapters-sf-
aaconnector-webapp">

      <routeTable order="1000">

        <routes>

          <route name="StartExampleAuthentication" url="Example-Bridge-
Forms/Start">

            <defaults>

              <add param="controller"
value="ExplicitFormsAuthentication" />

              <add param="action" value="AuthenticateStart" />

              <add param="postbackAction" value="Authenticate" />

              <add param="cancelAction" value="CancelAuthenticate" />
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
              <add param="conversationFactory"
value="ExampleBridgeAuthentication" />

              <add param="changePasswordAction"
value="StartChangePassword" />

              <add param="changePasswordController"
value="ChangePassword" />

              <add param="protocol" value="CustomForms" />

            </defaults>

          </route>
```

4. In PowerShell, set the Delegated Forms Authentication conversation factory. In this example, to ExampleBridgeAuthentication.

```
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

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

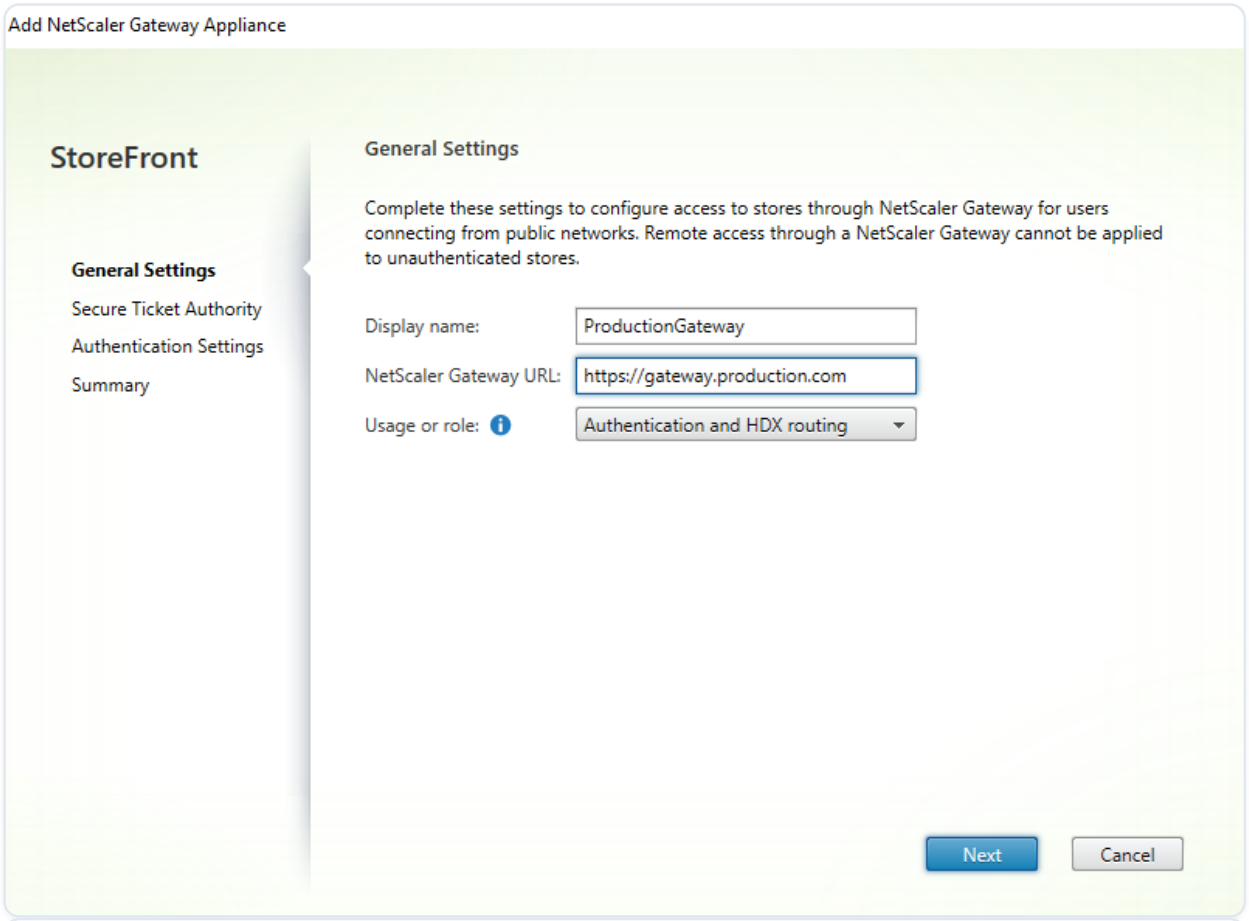
- StoreFront, Citrix Virtual App and Desktops and VDAs are all on the `development.com` domain.
- Authentication to the Citrix Receiver for Web site occurs using a development\testuser1 account and password.
- There is no trust relationship between the two domains.

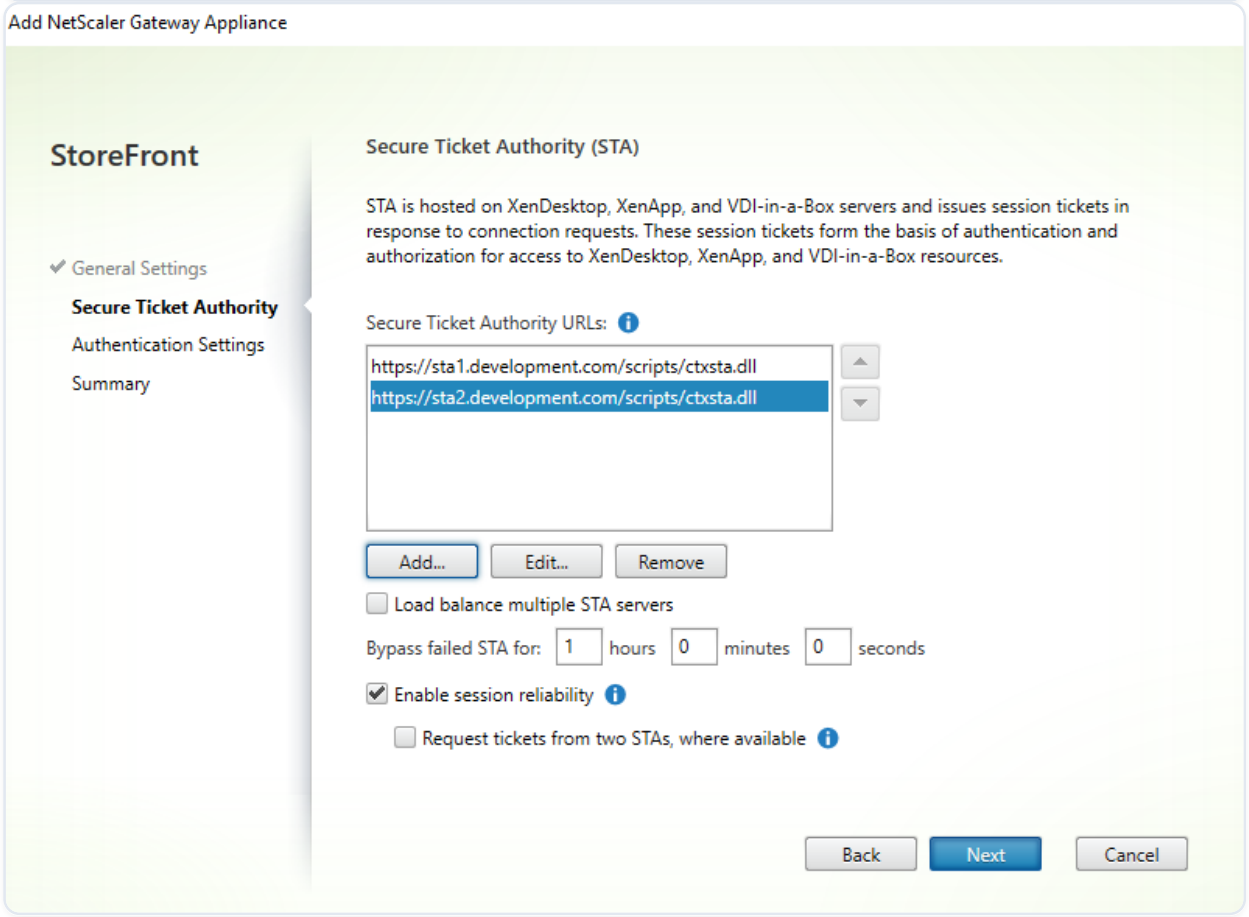
Configure a Citrix Gateway for the store

To configure a Citrix Gateway for the store:

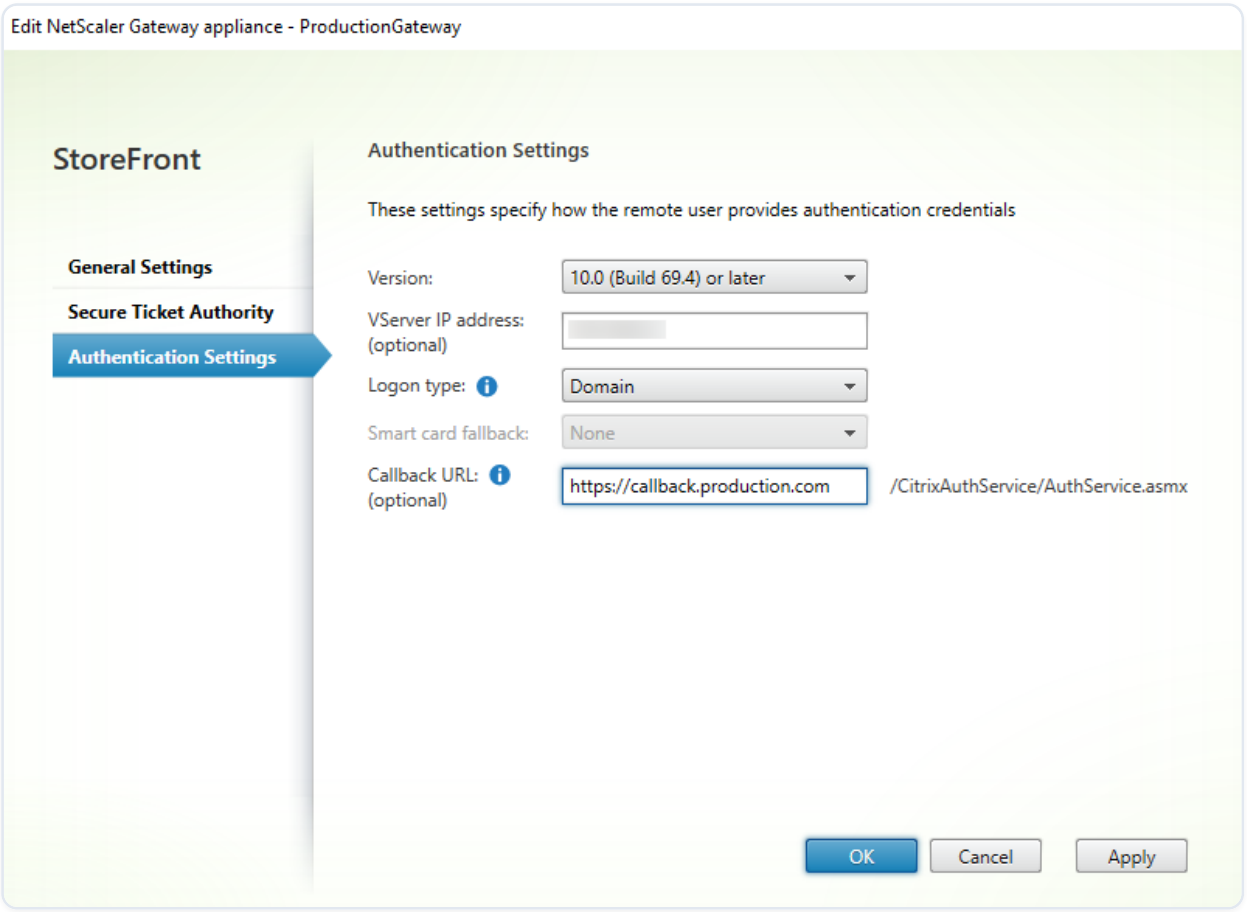
1. Select **Stores** in the left pane of the Citrix StoreFront management console, and in the **Actions** pane, click **Manage Citrix Gateways**.
2. On the Manage Citrix Gateways screen, click **Add**.
3. Complete the General Settings, Secure Ticket Authority, and Authentication steps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.





© 1997–2026 Citrix Systems, Inc. All rights reserved.



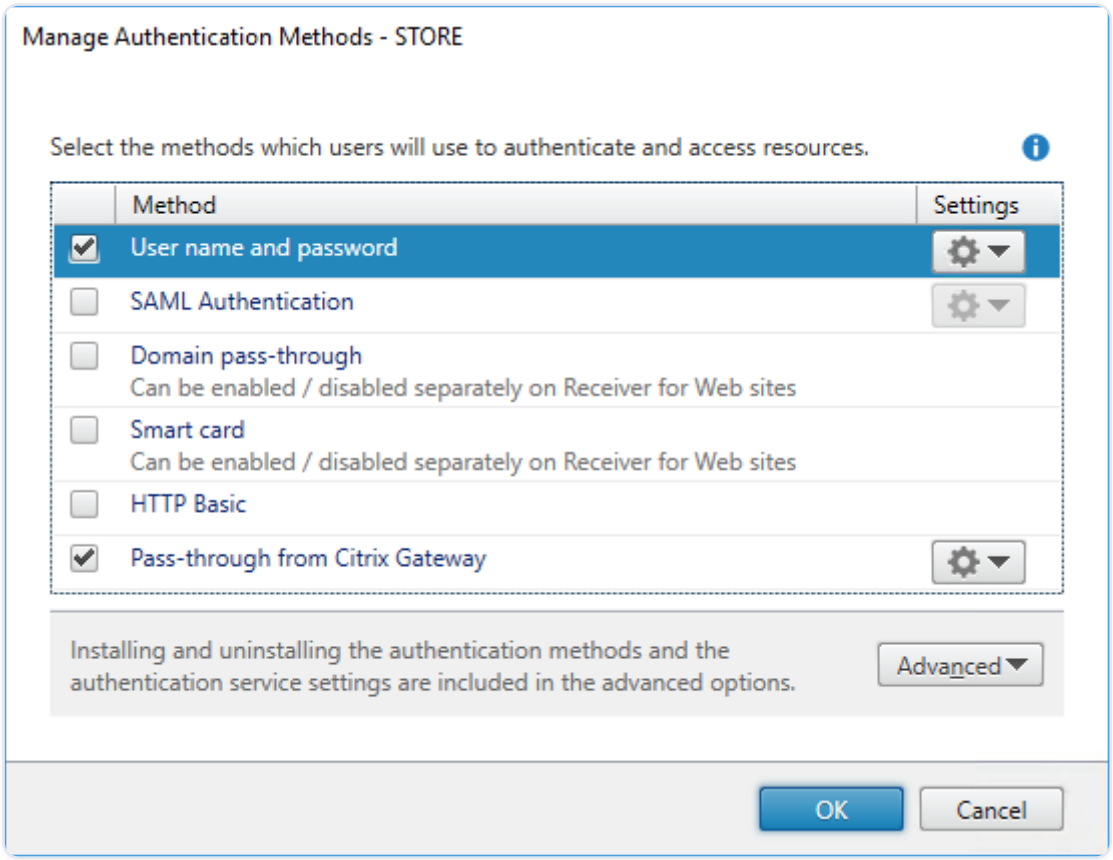
NOTE:

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**.

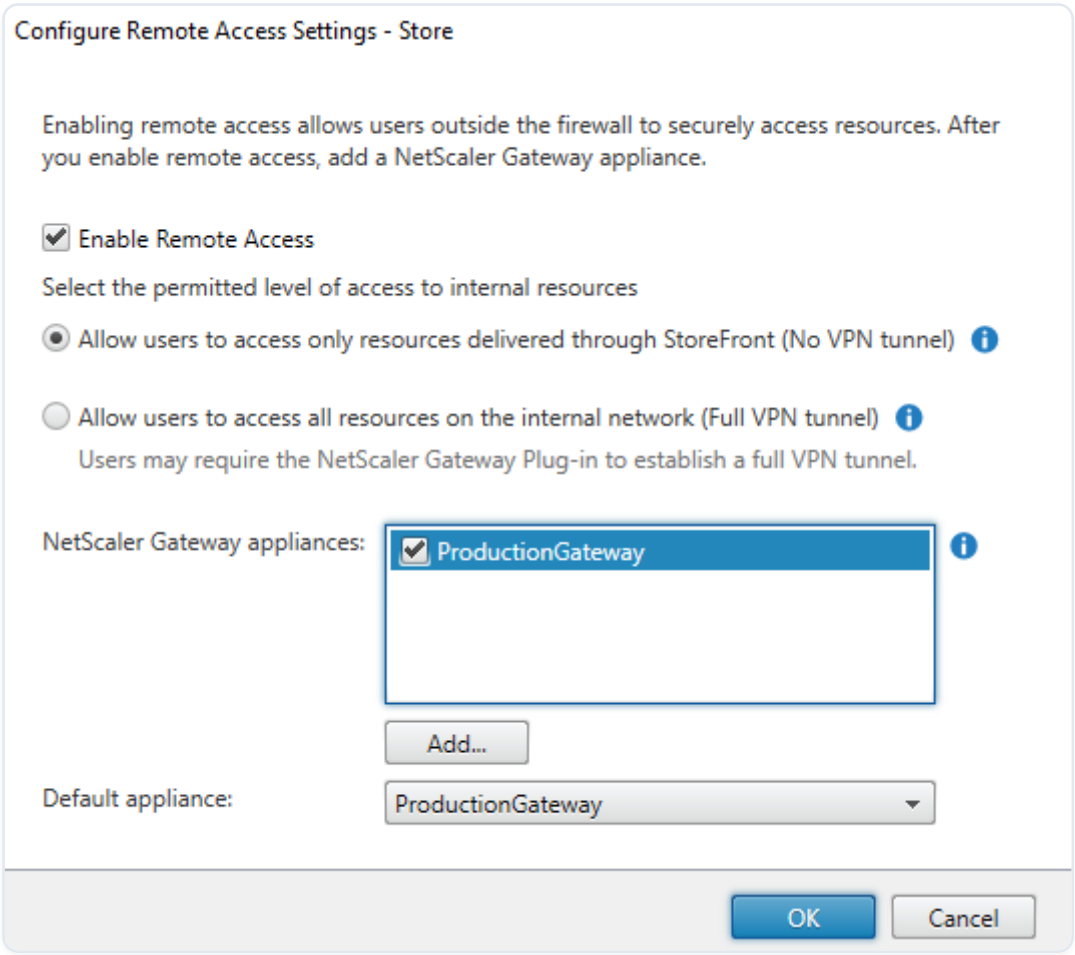
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

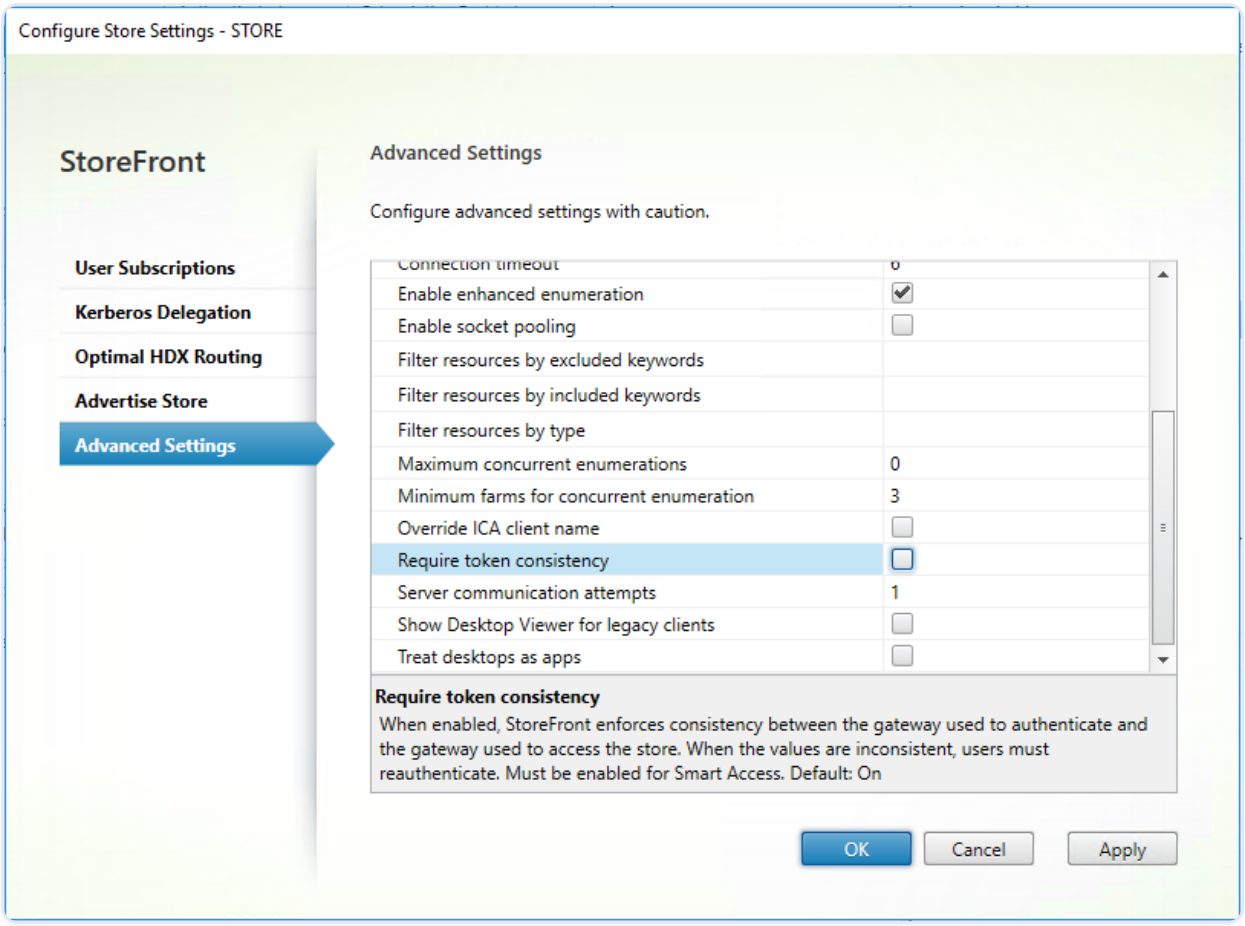
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

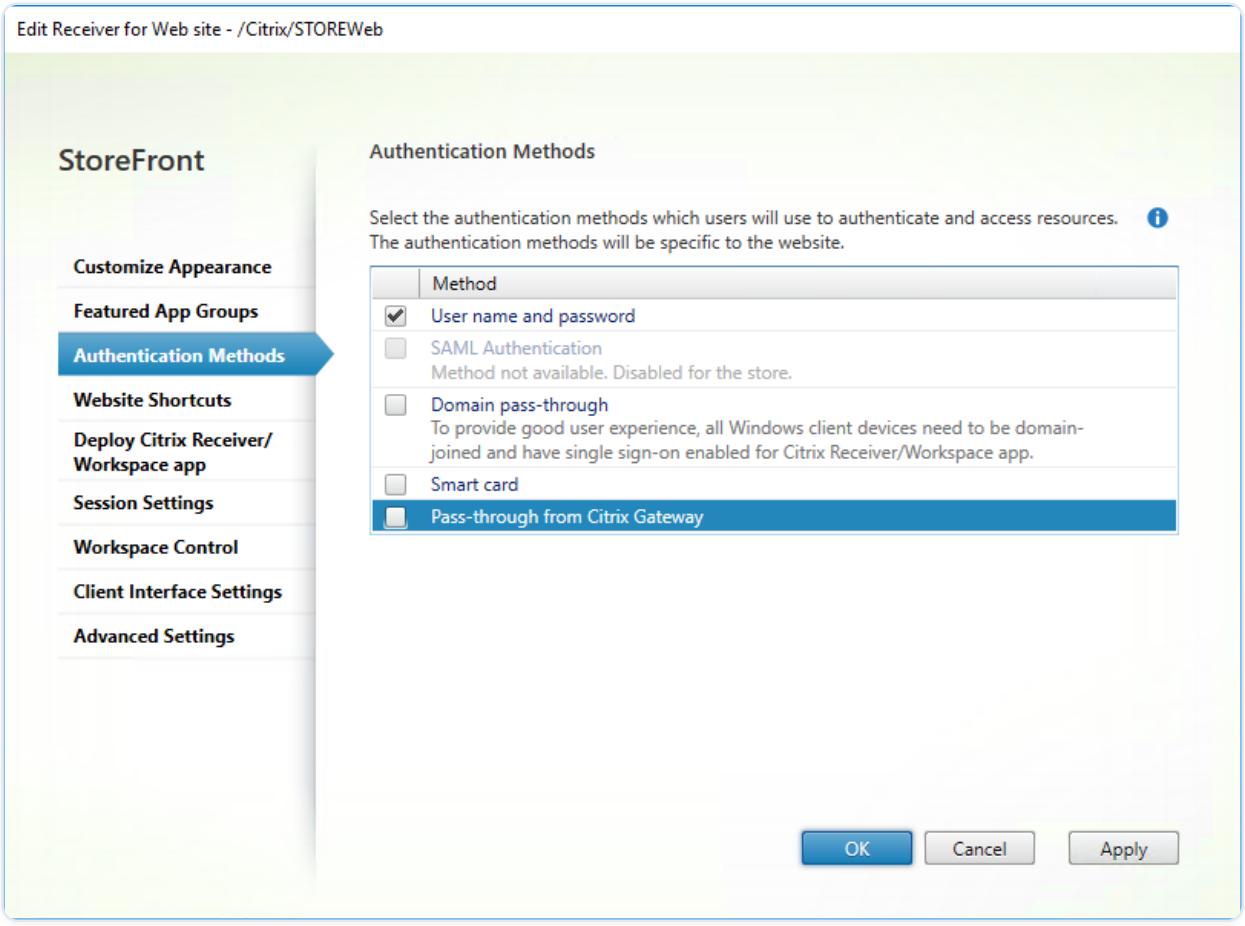
IMPORTANT:

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.

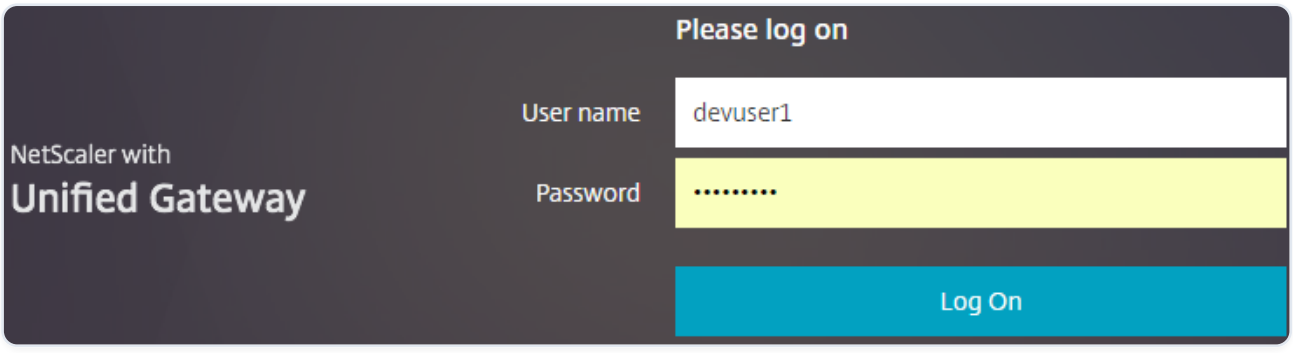
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In the **Actions** pane, click **Manage websites**.
4. In Authentication Methods, clear **Pass-through from Citrix Gateway**.
5. Click **OK**.



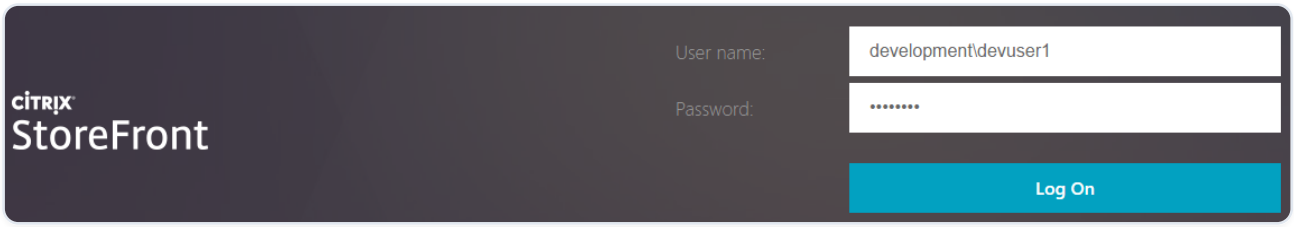
Log on to Gateway using a `production.com` user and credentials

To test, log on to Gateway using a `production.com` user and credentials.



After logon, the user is prompted to enter `development.com` credentials.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

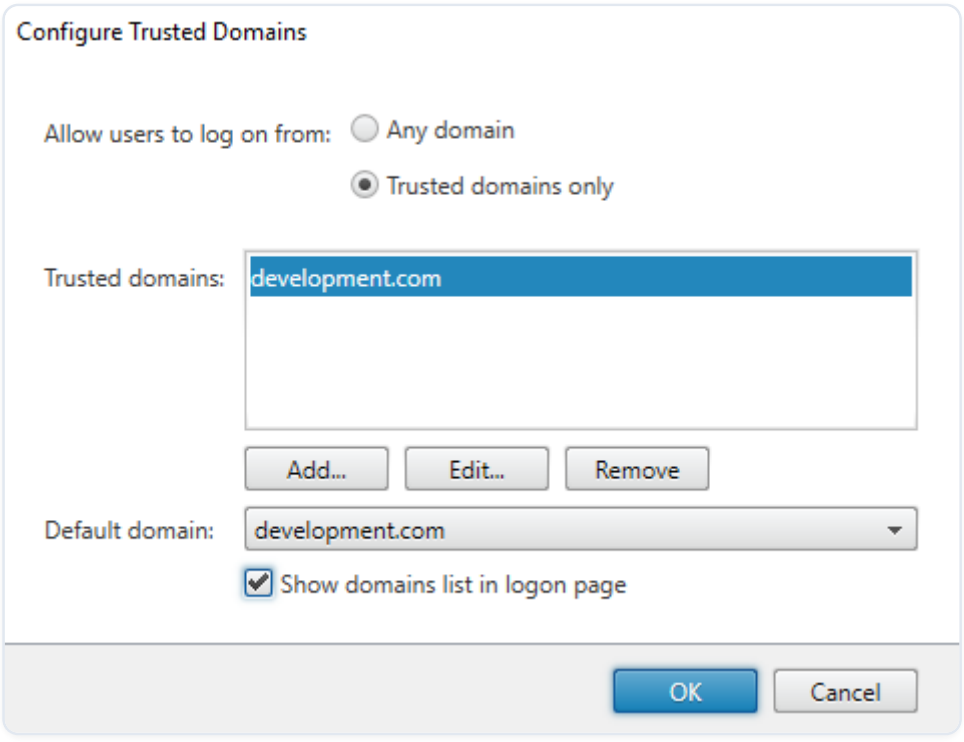


Add a trusted domain drop-down list in StoreFront (optional)

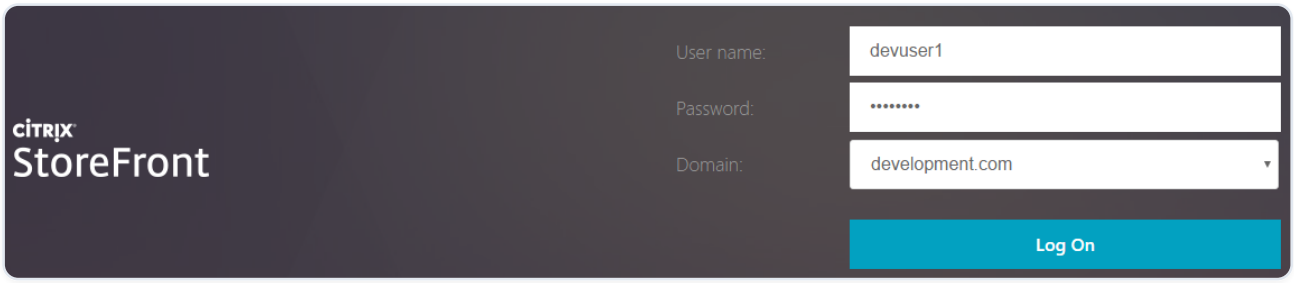
This setting is optional, but it may help prevent the user from accidentally entering the wrong domain to authenticate through the Citrix Gateway.

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**.



© 1997–2026 Citrix Systems, Inc. All rights reserved.



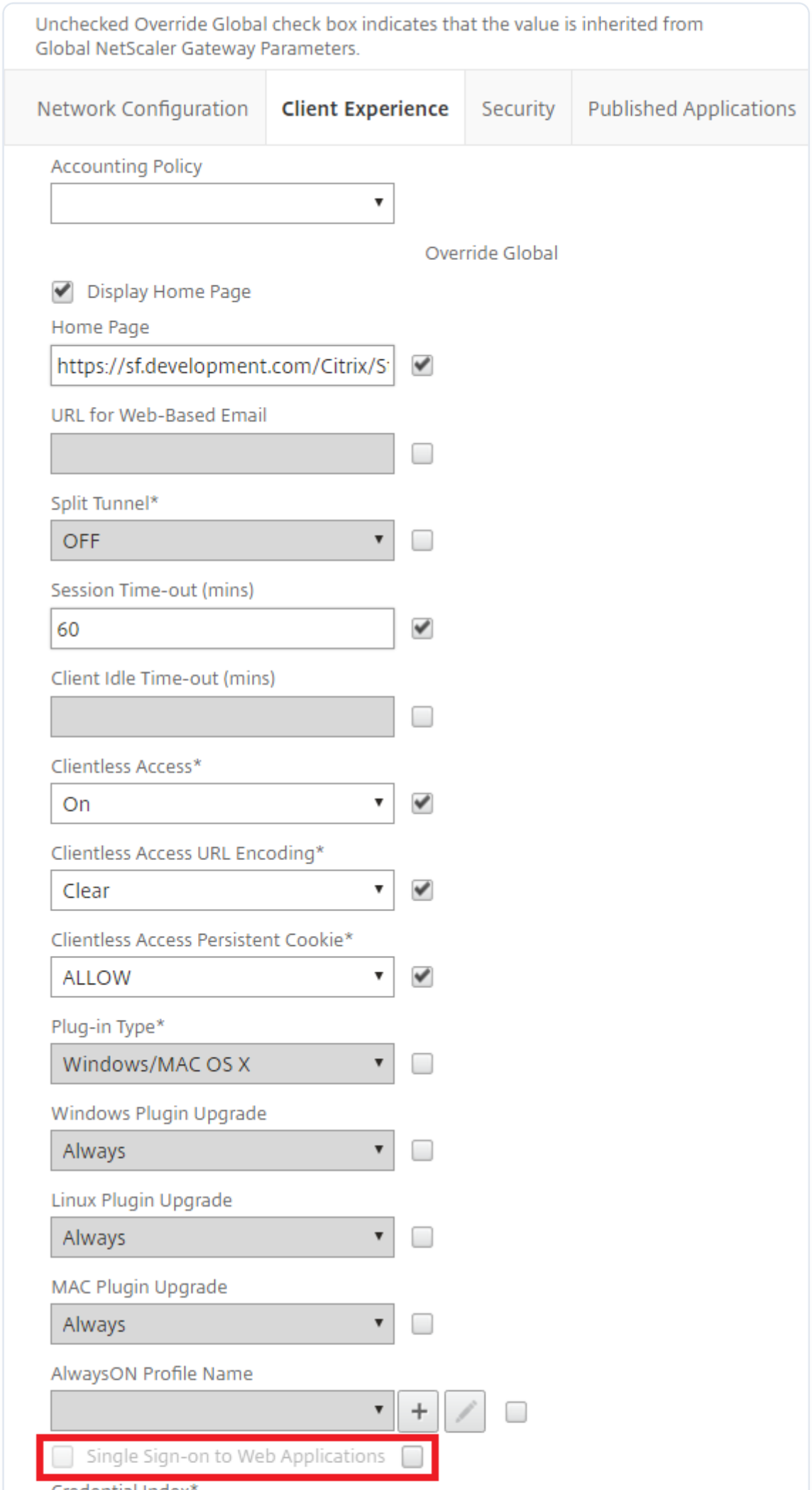
NOTE:

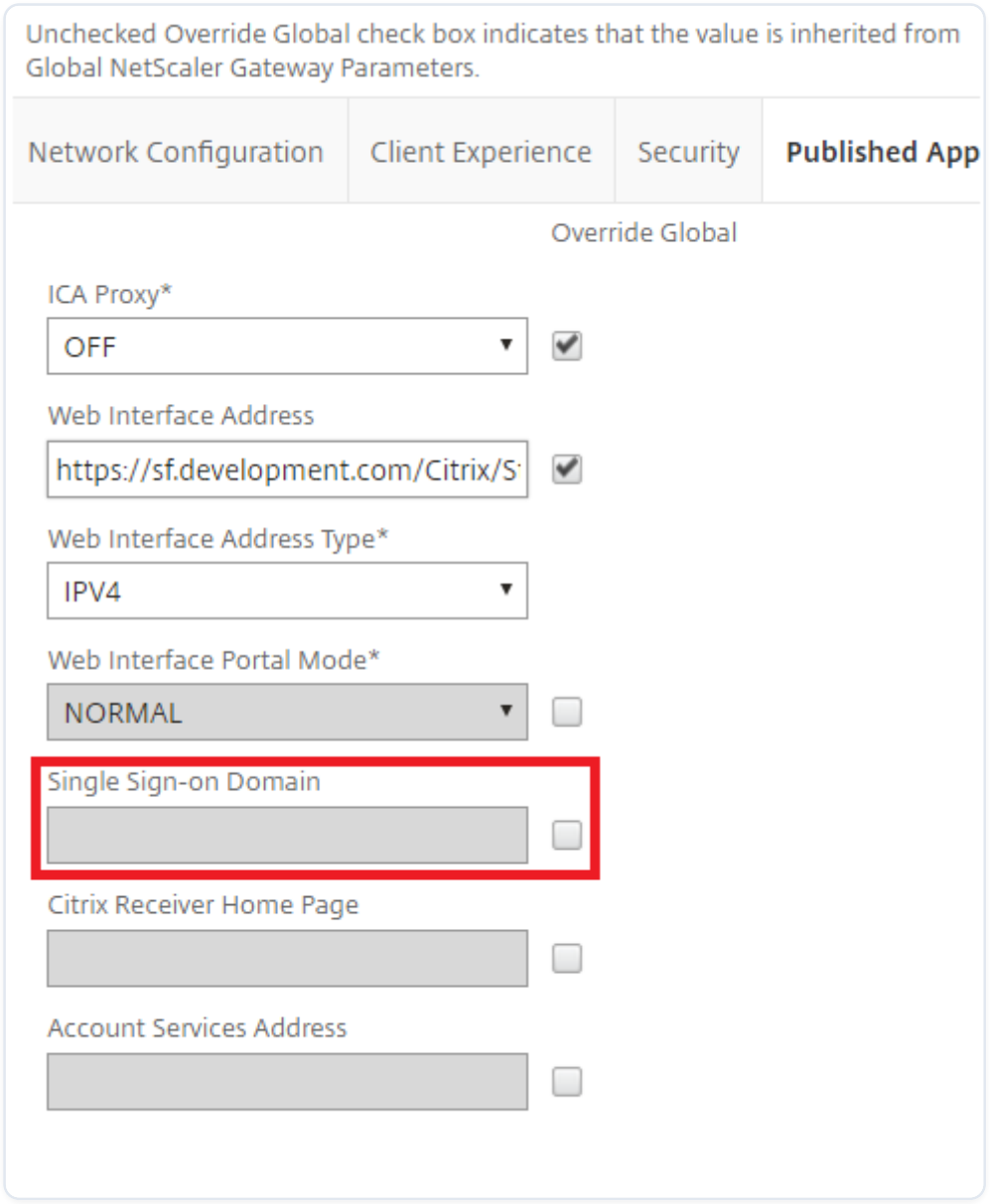
Browser password caching is not recommended in this authentication scenario. If users have different passwords for the two different domain accounts, password caching can lead to a poor experience.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.


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
Override Global
Display Home Page
Home Page
https://sf.development.com/Citrix/S
URL for Web-Based Email
Split Tunnel*
OFF
Session Time-out (mins)
60
Client Idle Time-out (mins)
Clientless Access*
On
Clientless Access URL Encoding*
Clear
Clientless Access Persistent Cookie*
ALLOW
Plug-in Type*
Windows/MAC OS X
Windows Plugin Upgrade
Always
Linux Plugin Upgrade
Always
MAC Plugin Upgrade
Always
AlwaysON Profile Name
Single Sign-on to Web Applications



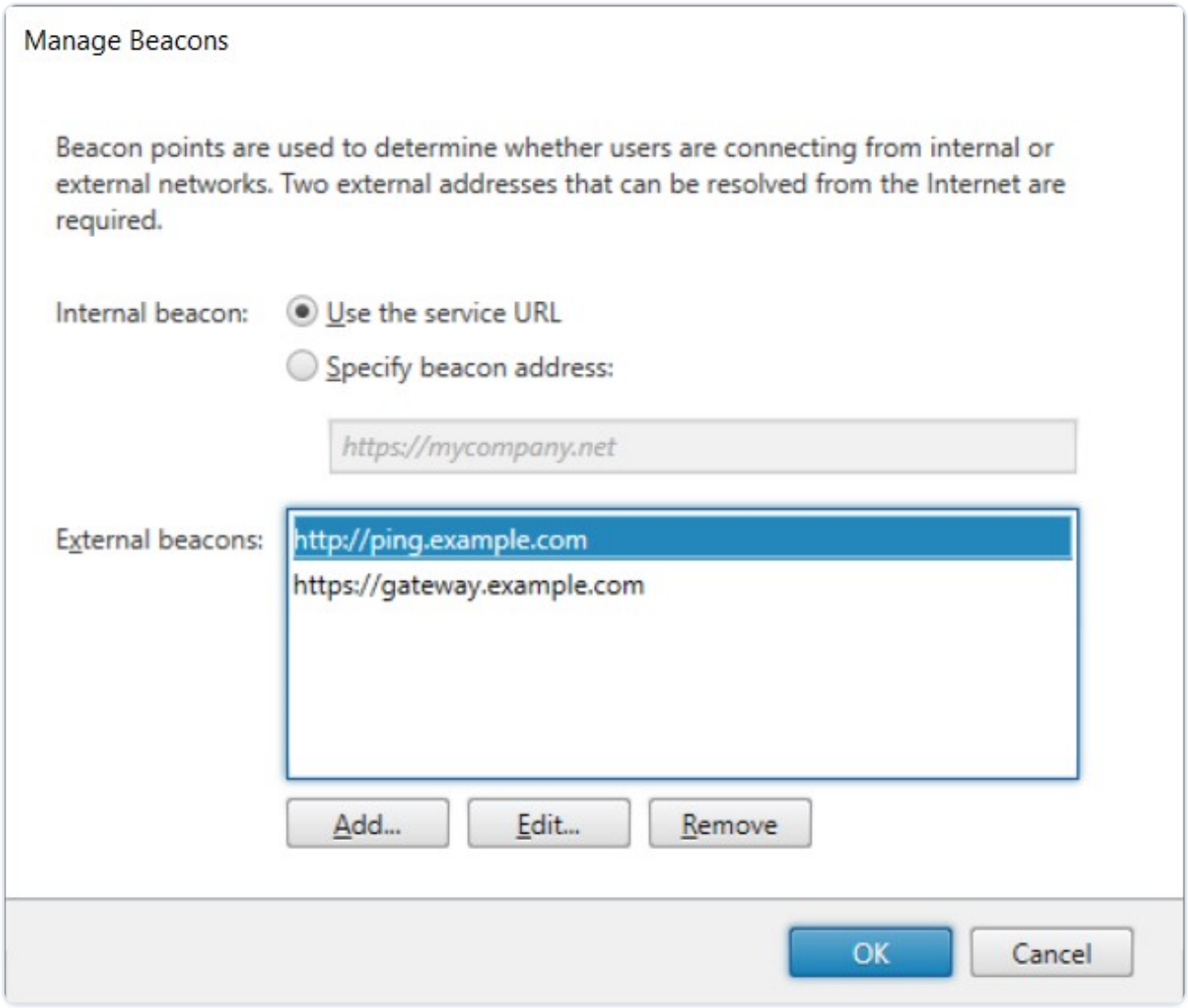
Configure beacon points

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`).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



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 though 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

To set the beacons to their defaults, use Clear-STFRoamingBeacon.

Create a single FQDN used internally and externally

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Require Citrix Workspace™ app when connecting through a gateway

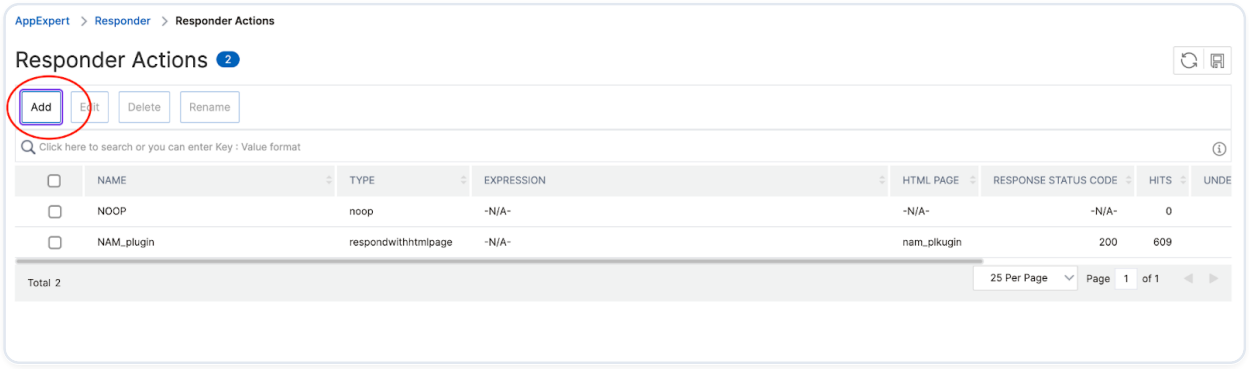
You can require users to use Citrix Workspace app when connecting through a gateway by using a plug-in.

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.



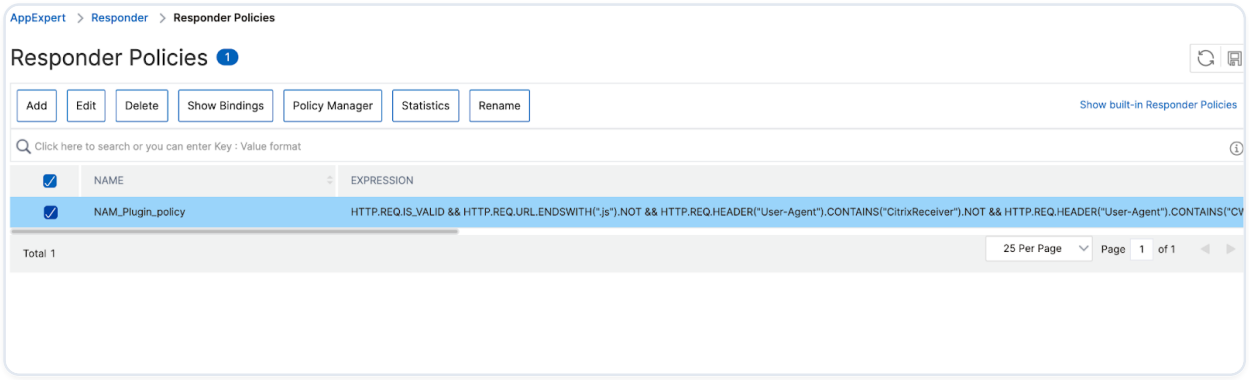
3. Configure the responder action:

   Type: Respond with HTML page

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

4. Create a responder policy.

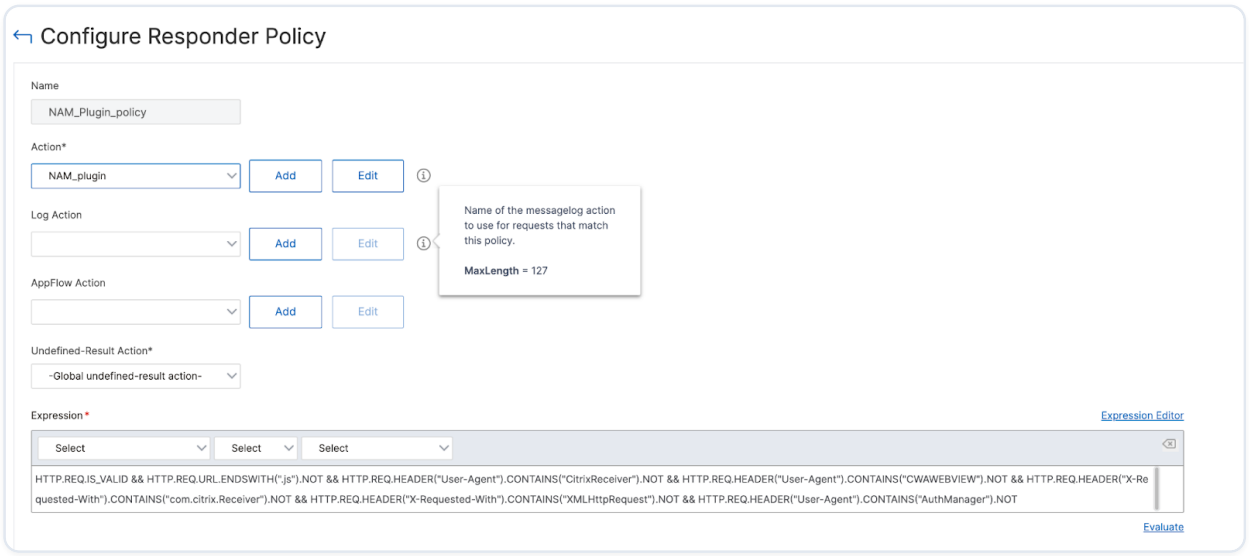
© 1997–2026 Citrix Systems, Inc. All rights reserved.



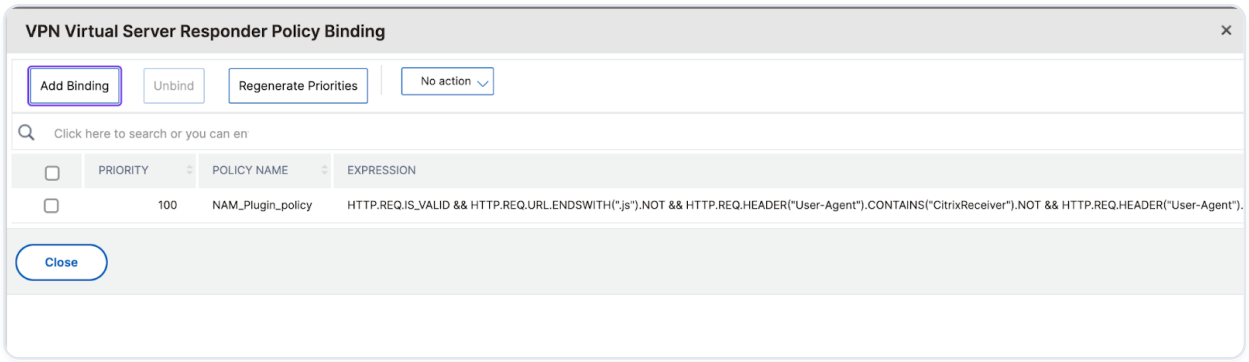
5. Configure the responder policy:

   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("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`

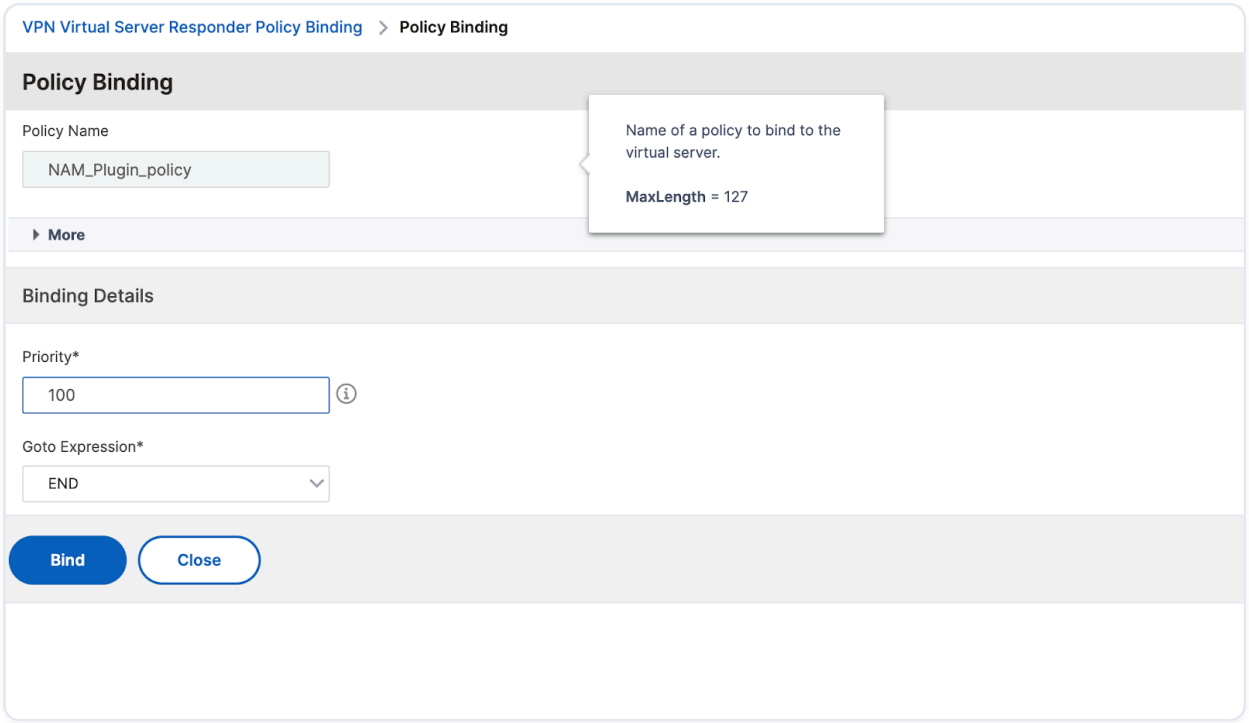


6. Navigate to the virtual server where you want to bind the responder policy.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

7. Bind the policy you created.



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)

```
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.

```
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
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. Bind the policy to the VPN vserver

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

Citrix Gateway OIDC Entra ID authentication

This section describes how to configure NetScaler and StoreFront so users can authenticate using Entra ID. In this configuration, users can either have a hybrid identity, or an Entra only identity without an Active Directory account.

Prerequisites

- NetScaler ADC
- StoreFront 2607 or higher
- Microsoft Entra ID account with one of the following permissions:
  - Cloud Application Administrator
  - Application Administrator
  - Global Administrator

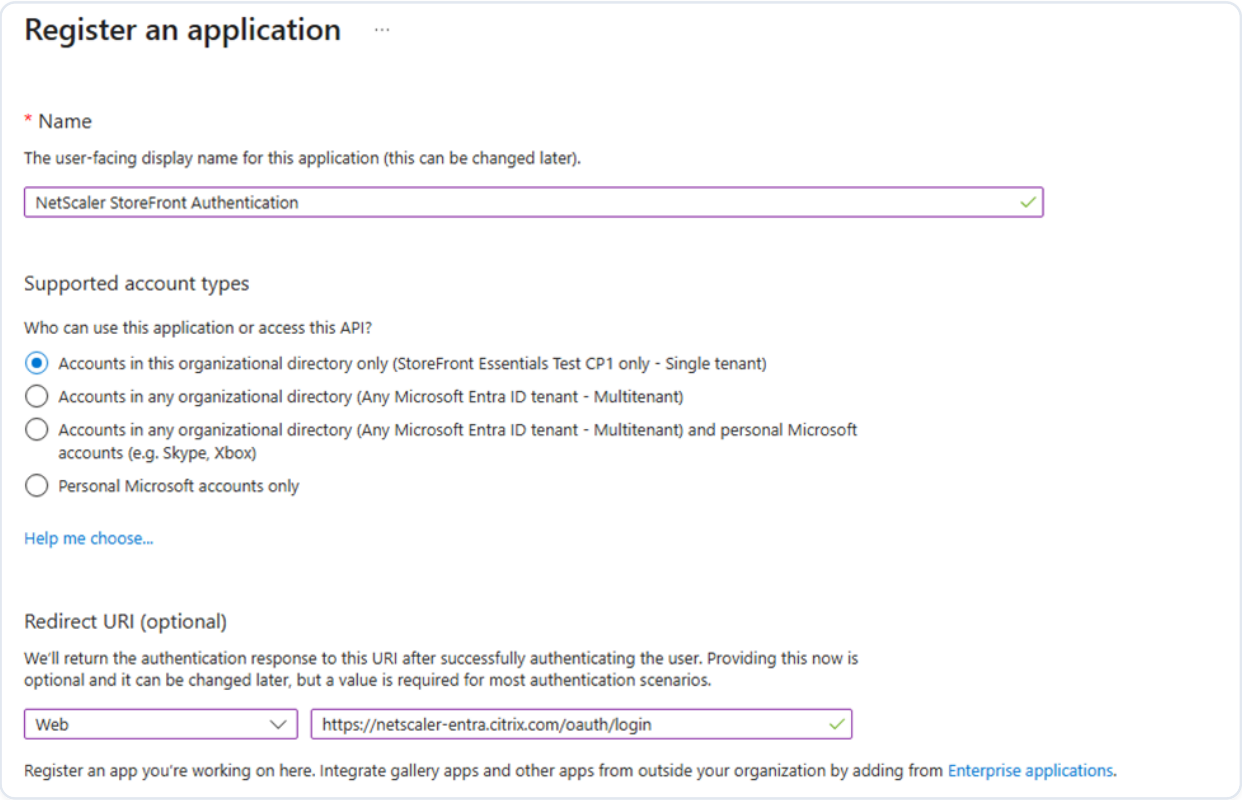
Create a Microsoft Azure Entra ID application

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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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`.

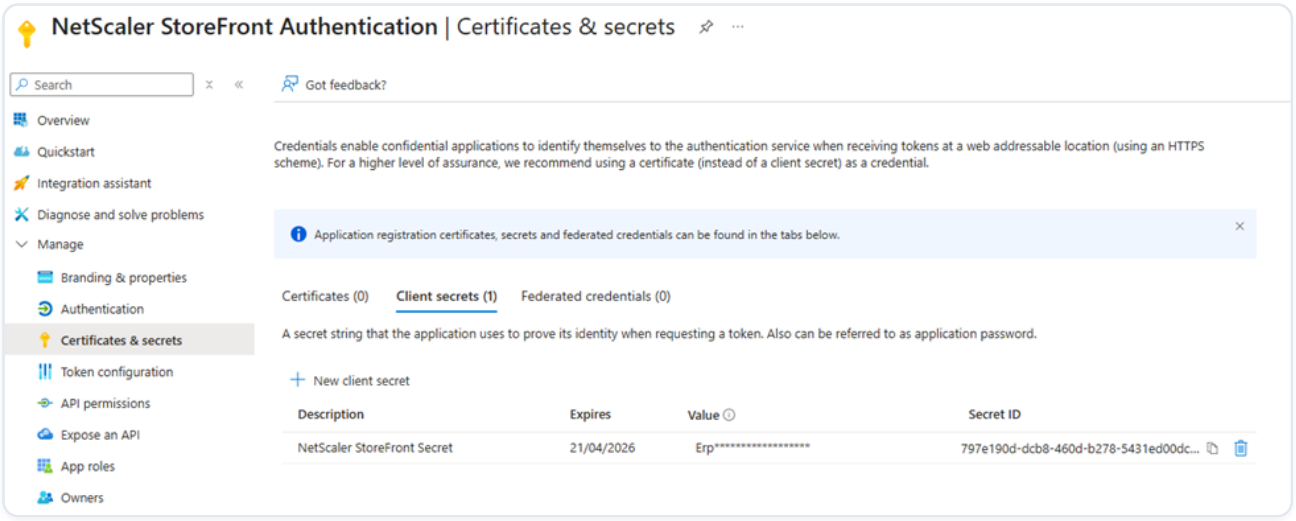


Create client secret

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

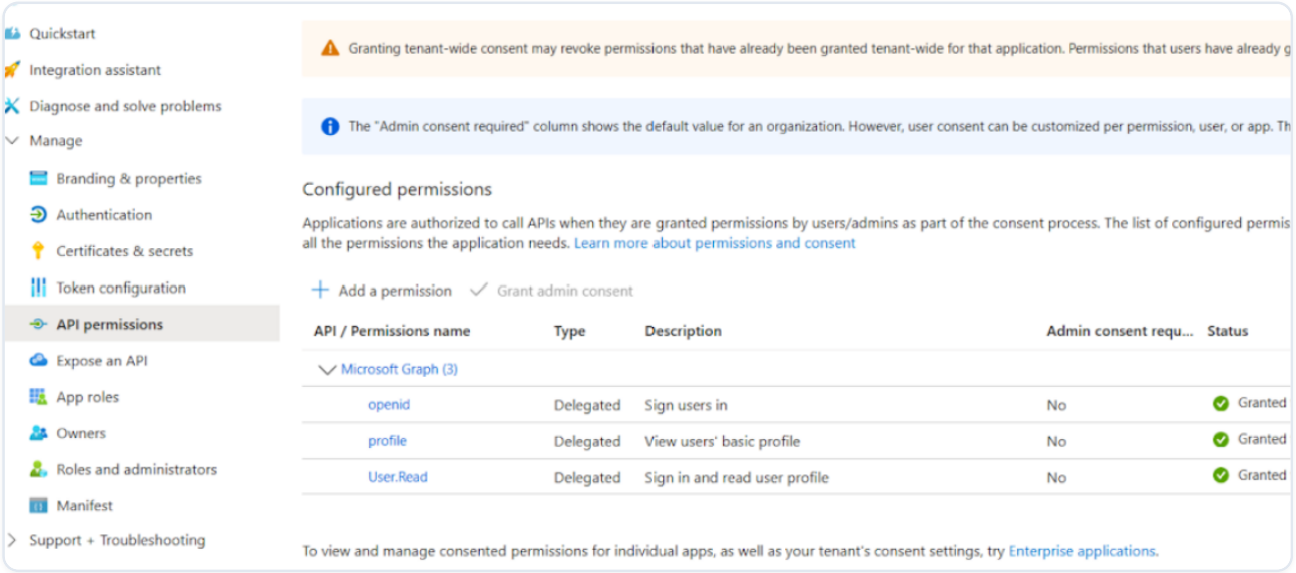


Configure application permissions

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.

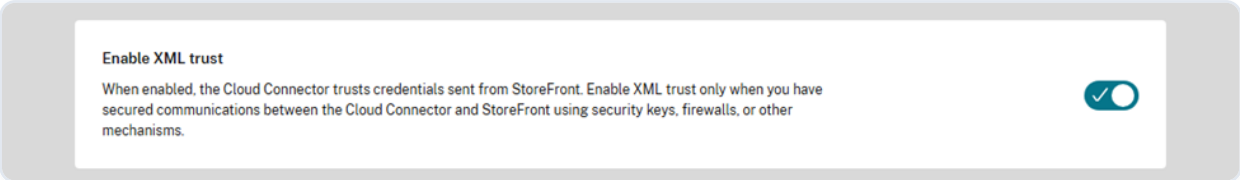


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure Citrix DaaS to enable XML trust

By default Citrix DaaS authenticates requests using the user's Active Directory credentials. With Entra ID authentication, StoreFront does not have the credentials. Therefore you must configure DaaS to trust StoreFront without requiring using authentication. It is strongly recommended that you enable security keys to provide service level authentication instead.

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 NetScaler authentication profile

This section describes how to configure a NetScaler authentication profile that you can bind to your gateway VPN virtual server. 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 user authentication.

```
add authentication vserver EntraId_Authentication_VirtualServer SSL
0.0.0.0 443 \

  -state ENABLED \

  -authentication ON \
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -td 0 -appflowLog ENABLED \

  -noDefaultBindings NO
```

Create OAuth policy and action

The OAuth action specifies how NetScaler ADC interacts with an OAuth IdP such as Microsoft Entra ID. This action allows the Citrix Gateway to redirect users to the IdP for sign-in and handle the OAuth token returned. It sets the `userNameField` to `oid` which causes the gateway to pass the OID as the username when authenticating to StoreFront. StoreFront validates that the oid matches the details it gets from looking up the Entra ID access token, otherwise authentication fails.

You need the Client ID and Client secret from the previous steps.

```
add authentication OAuthAction EntraId_Oauth_Server \

  -authorizationEndpoint "https://login.microsoftonline.com/<TenantId>/
oauth2/v2.0/authorize\?prompt=login" \

  -tokenEndpoint "https://login.microsoftonline.com/<TenantId>/oauth2/
v2.0/token" \

  -clientID <ClientId> \

  -clientSecret <ClientSecret> \

  -Attribute1 email \

  -Attribute2 family_name \

  -Attribute3 given_name \

  -Attribute4 upn \

  -CertEndpoint "https://login.microsoftonline.com/<TenantId>/discovery/
v2.0/keys" \

  -userNameField oid \

  -allowedAlgorithms HS256 RS256 RS512 \
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
  -PKCE ENABLED \

  -tokenEndpointAuthMethod client_secret_post \

  -OAuthType GENERIC \

  -grantType CODE \

  -refreshInterval 1440

add authentication Policy EntraId_Authentication_Policy \

  -rule true \

  -action EntraId_Oauth_Server
```

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.

Bind the authentication policy to the virtual server

```
bind authentication vserver EntraId_Authentication_VirtualServer \

  -policy EntraId_Authentication_Policy \

  -priority 100 \

  -gotoPriorityExpression END
```

Create authentication profile

```
add authentication authnProfile EntraId_Auth_Profile \

  -authnVsName EntraId_Authentication_VirtualServer \

  -AuthenticationLevel 0
```

Create VPN Virtual Server and bind the authentication profile

Complete steps 1, 2 and 4 from Integrate NetScaler Gateway with StoreFront, using the authentication profile created in the previous steps.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Alternatively, if you already have a suitable Citrix Gateway then you can bind the new authentication profile to it. Running this command replaces the existing authentication profile.

```
set vpn vserver <StoreFront ICA Proxy vServer> \

  -authentication ON \

  -authnProfile EntraId_Auth_Profile
```

Entra ID token injection configuration for SSO to StoreFront

After the Citrix gateway authenticates the user, it must pass sufficient information to StoreFront so that it can validate the user is authenticated and look up group membership. By default, the Citrix gateway only sends the Active Directory username and password. In the case of Entra ID authentication, it must pass the Entra ID access token so that StoreFront can look up user information using the Microsoft Graph API. To achieve this you must add a re-write policy that adds the Entra ID token to the call it makes to authenticate the user to StoreFront. If the rewrite Entra ID access token policy does not take effect, login will fail. If the rewrite policy feature is disabled by default and is not already enabled, then you must enable it first.

```
enable ns feature Rewrite

add rewrite action EntraId_Oauth_Insert_AccessToken_Header
insert_http_header X-Citrix-OIDC-Access-Token
"AAA.USER.ATTRIBUTE(\"accesstoken\")" \

  -comment "A rewrite policy to add the OAUTH access_token to subsequent
user authentication requests"

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 \

  -comment "A rewrite policy to add the OAUTH access_token to subsequent
user authentication requests"

bind vpn vserver <StoreFront ICA Proxy vServer> \

  -policy EntraId_Oauth_Insert_AccessToken_Policy \
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
-priority 100 \

-gotoPriorityExpression END \

-type REQUEST
```

Configure Citrix Gateway within StoreFront

1. Add a NetScaler Gateway instance on StoreFront.
2. Configure the Citrix Gateways.
   - Set Login type to **Domain**.
   - Specify a valid callback URL. This is required for Entra ID authentication with StoreFront.
3. Configure the gateway for remote access for the Store aggregating the Citrix DaaS resources.
4. On the Manage Authentication Methods screen:

a. Enable **Pass-through from Citrix Gateway**. b. Configure Entra ID settings. c. Enable delegated authentication.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

End user experience

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.

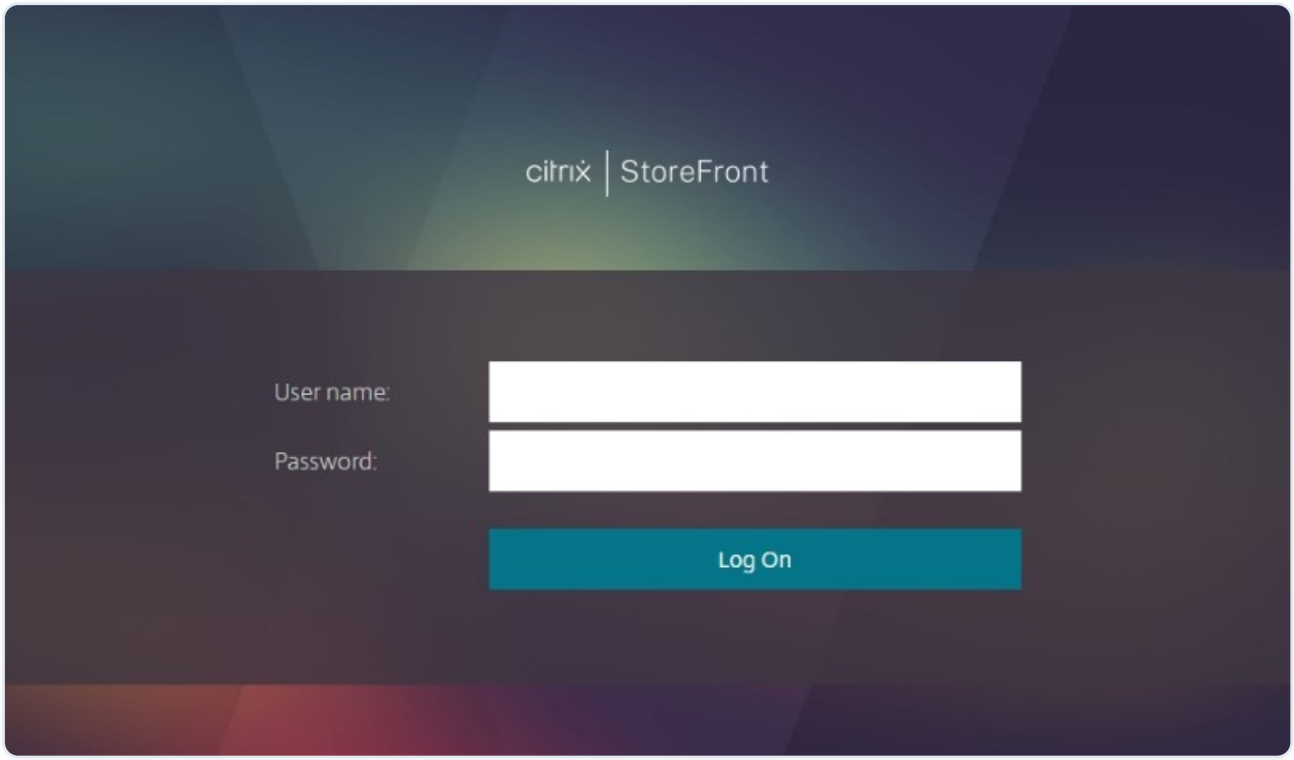
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Classic experience

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

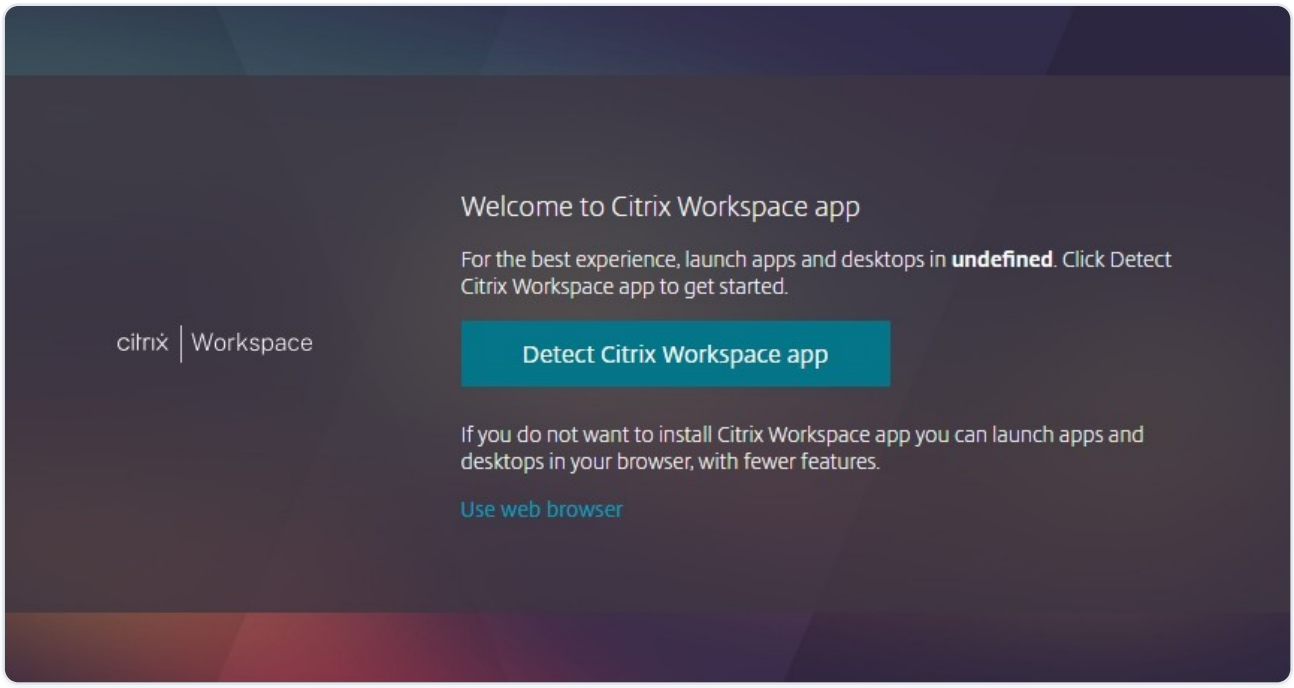
NOTE:

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 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

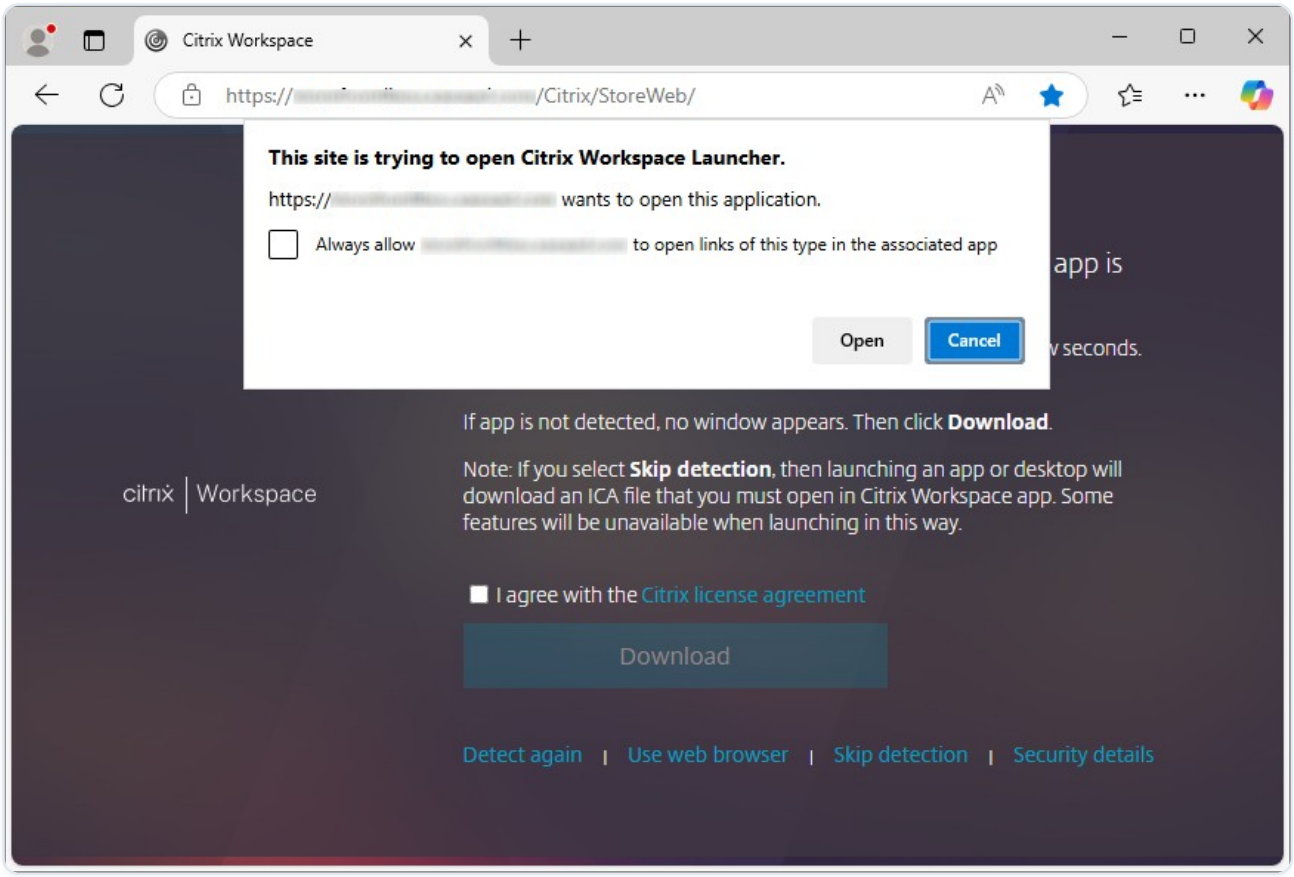


They can either:

- 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**, 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 their browser may display a message prompting the user to open **Citrix Workspace Launcher**. The user must 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. It is possible to configure managed browsers to always open **Citrix Workspace launcher** without any prompts. For more information, see Citrix Workspace launcher.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

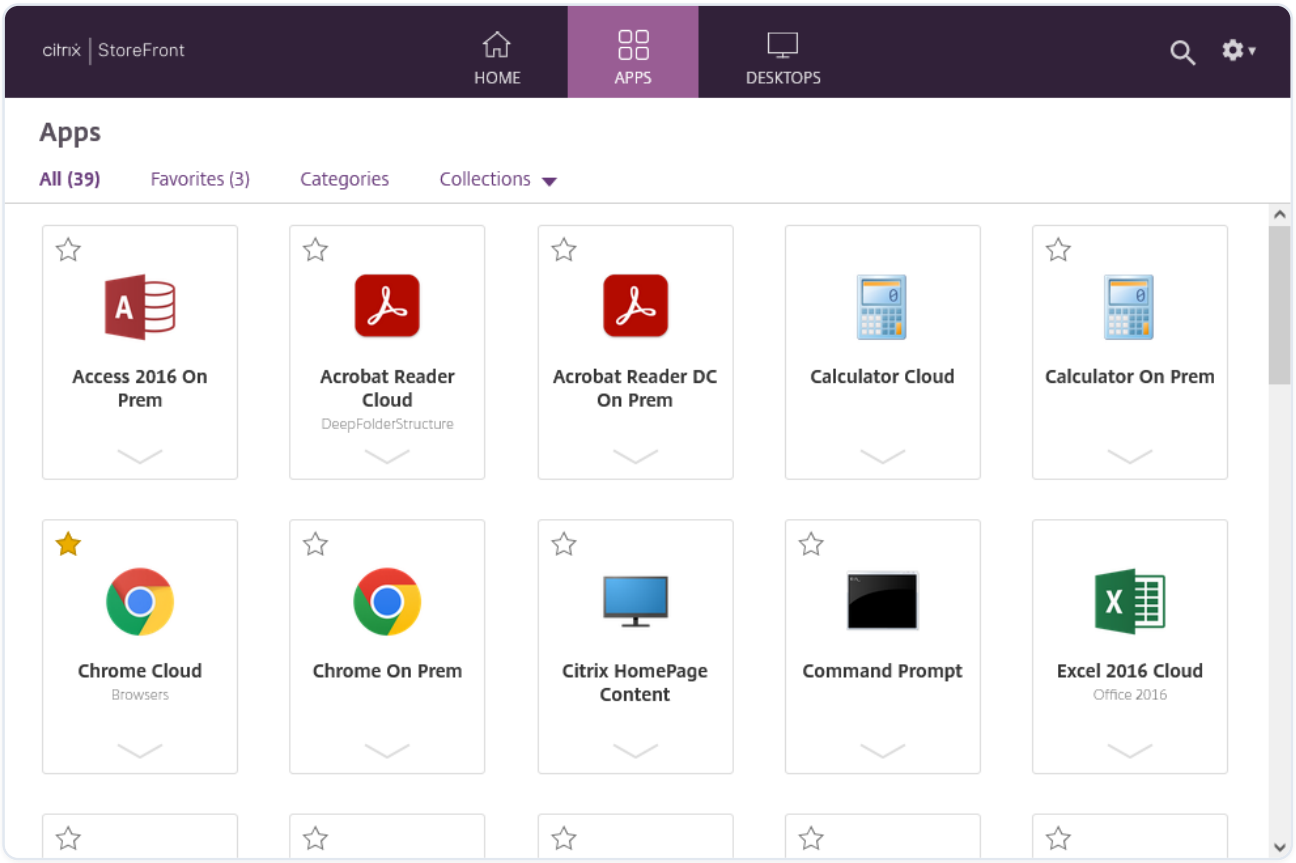


Apps tab

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



.

Desktops tab

The **Desktops** tab has two sub-views:

- **All** - Displays all desktops.
- **Favorites** - Displays the user's favorite desktops.

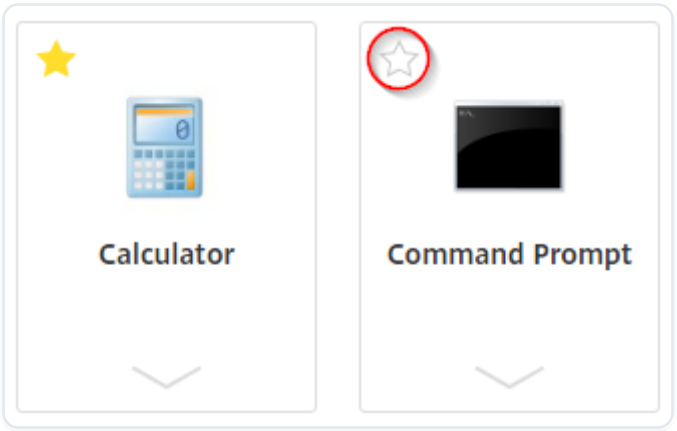
App and desktop tiles

Click on an icon to launch the app or desktop.

Favorites

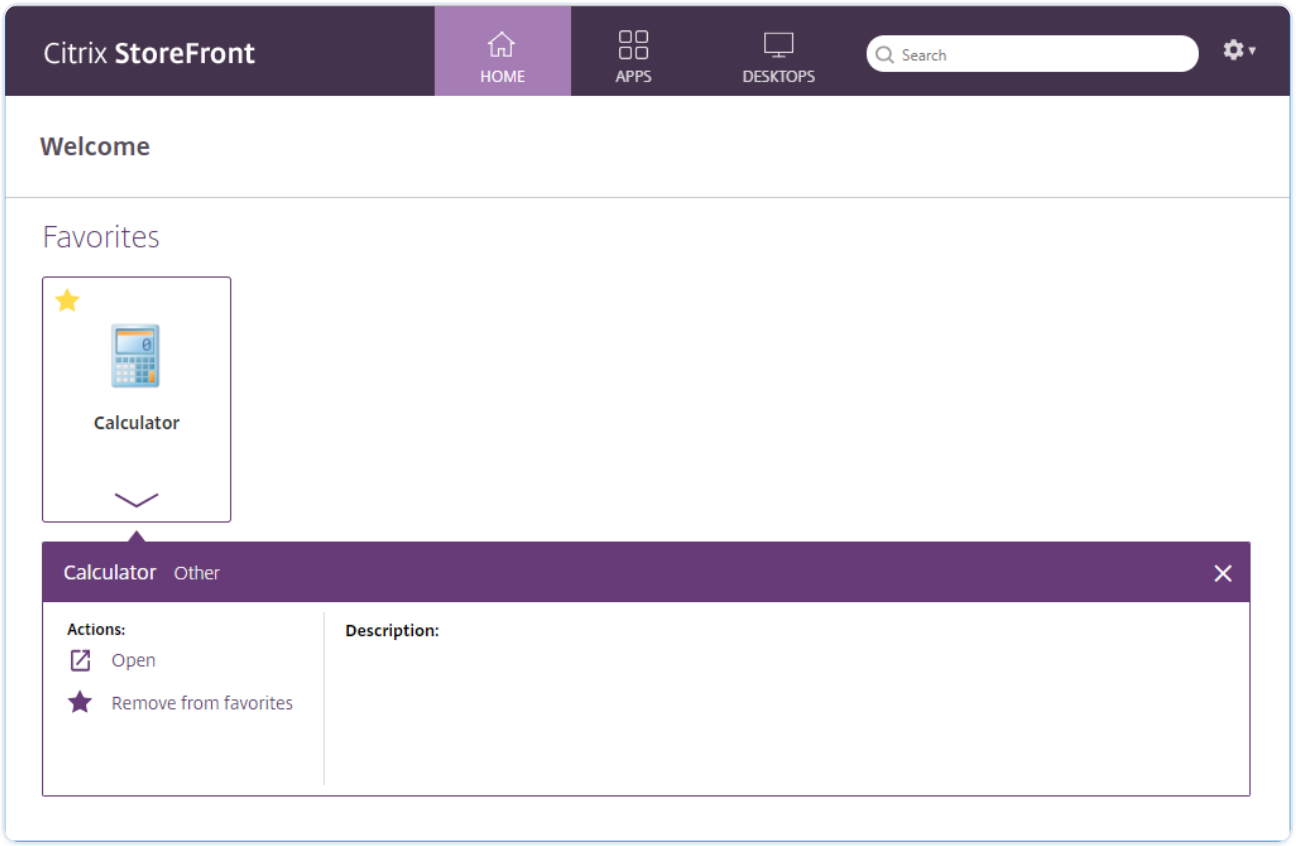
If favorites are enabled then the user can select star on a resource's tile to make it a favorite:

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

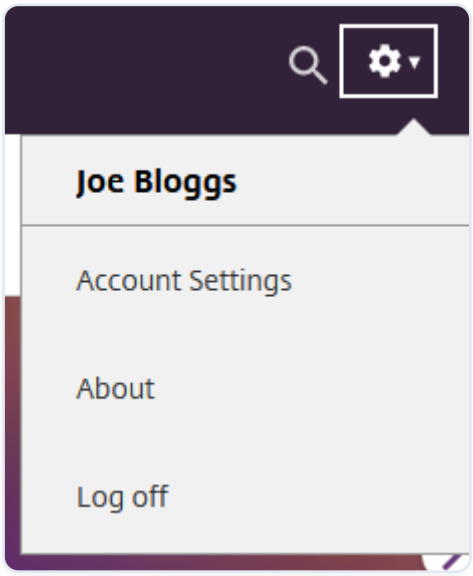
Search

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.

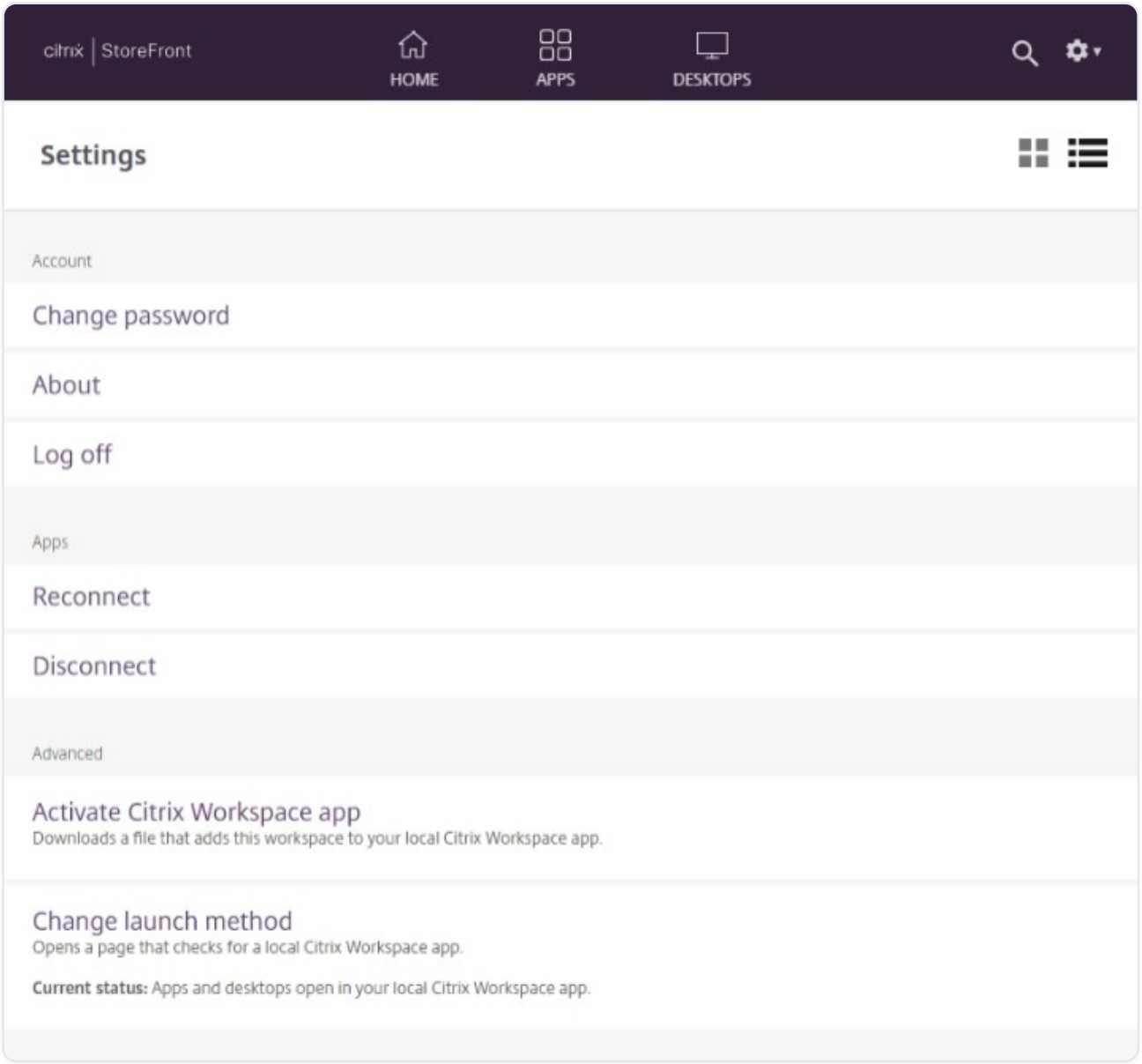


The settings menu has the following options:

- **Account Settings** - opens the settings page.
- **About** - Displays information about the application.
- **Log off** - Logs off the website.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Settings

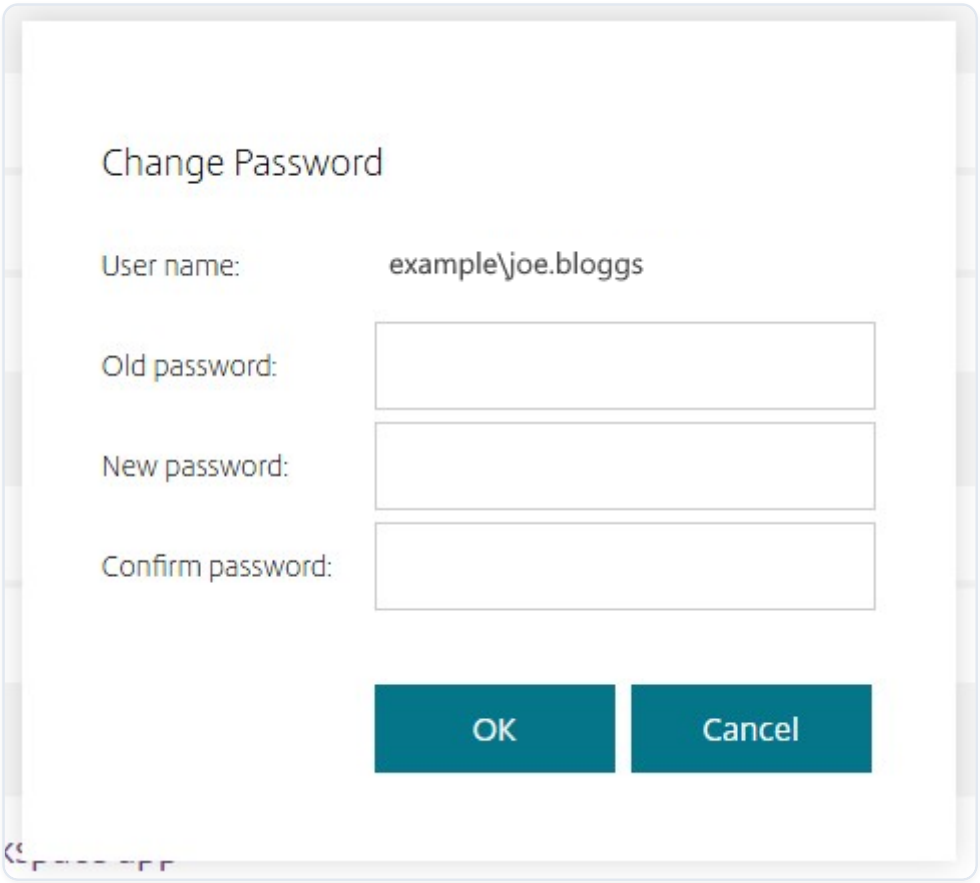


The account settings page may have the following sections.

Account

Change password. Only when using Username and password authentication. To configure whether this option is displayed, see Username and password.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

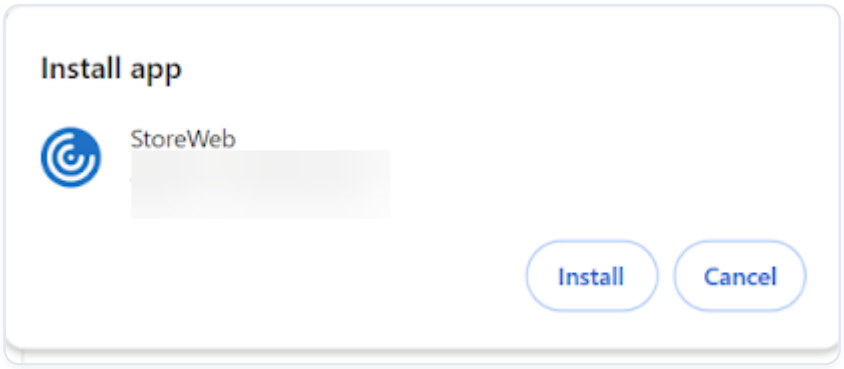
Install Progressive Web App using Google Chrome

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

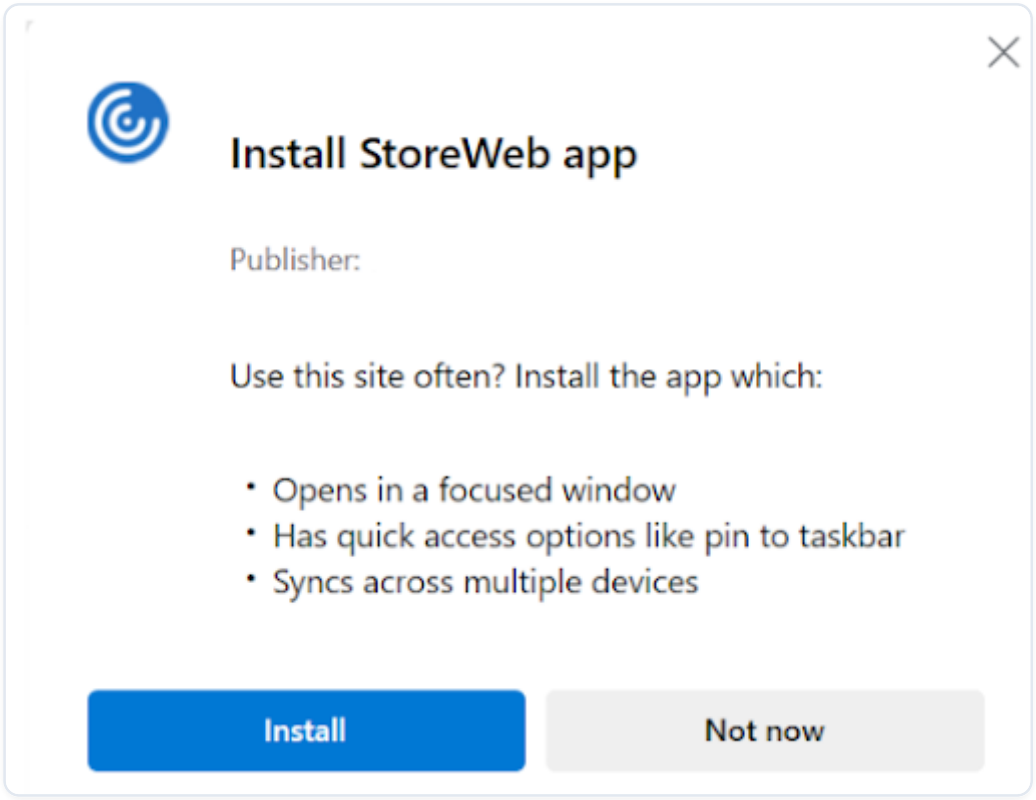
Install Progressive Web App using Microsoft Edge

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

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 detects Citrix Workspace app. This step may occur before or after log in depending configuration. For more information, see Citrix Workspace app detection screen.

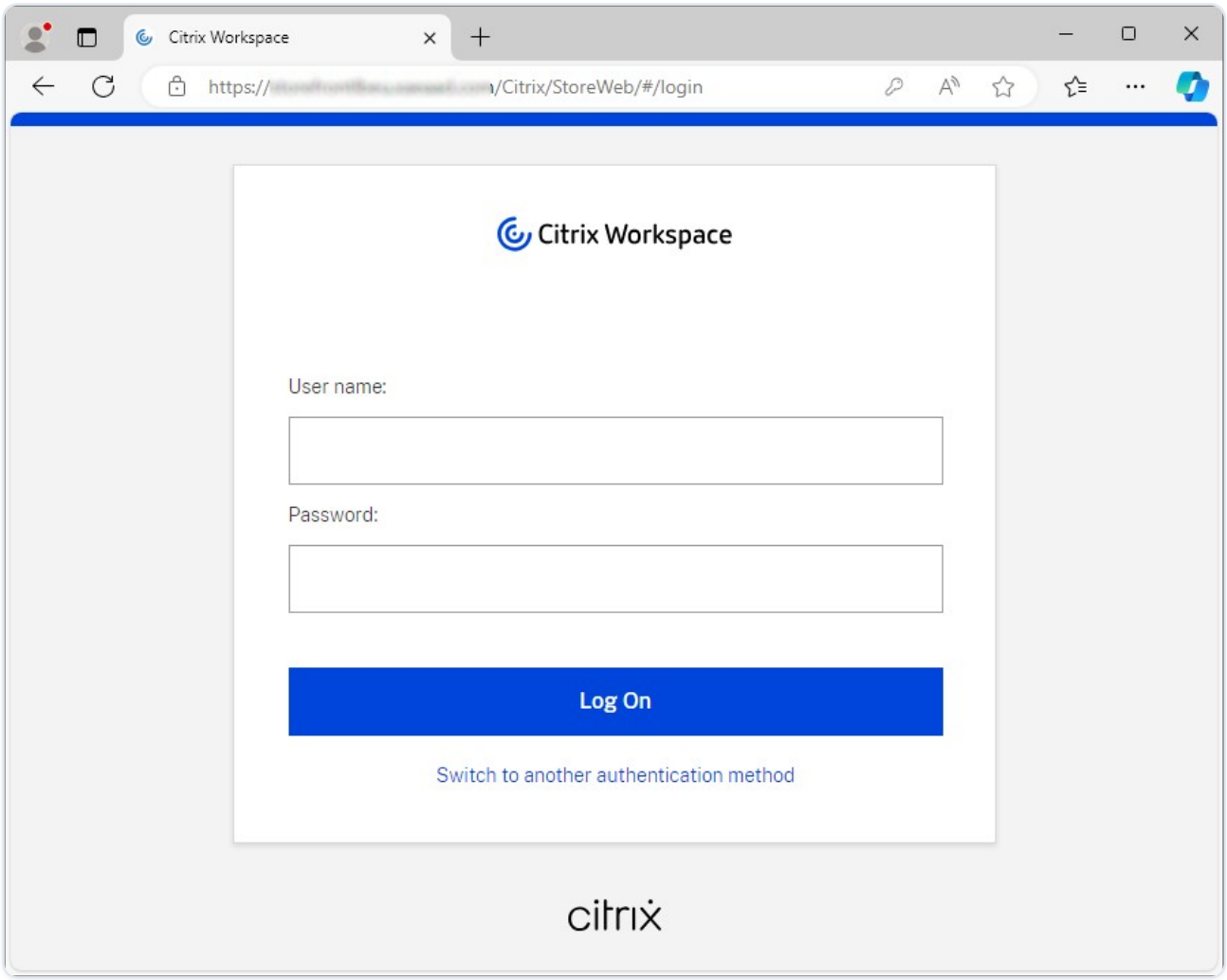
When users Authenticate at the NetScaler Gateway this screen is displayed after authentication. When users authenticate directly to Storefront, normally this screen is displayed before authentication, unless you have configured prompt to install Citrix Workspace app after logon.

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.

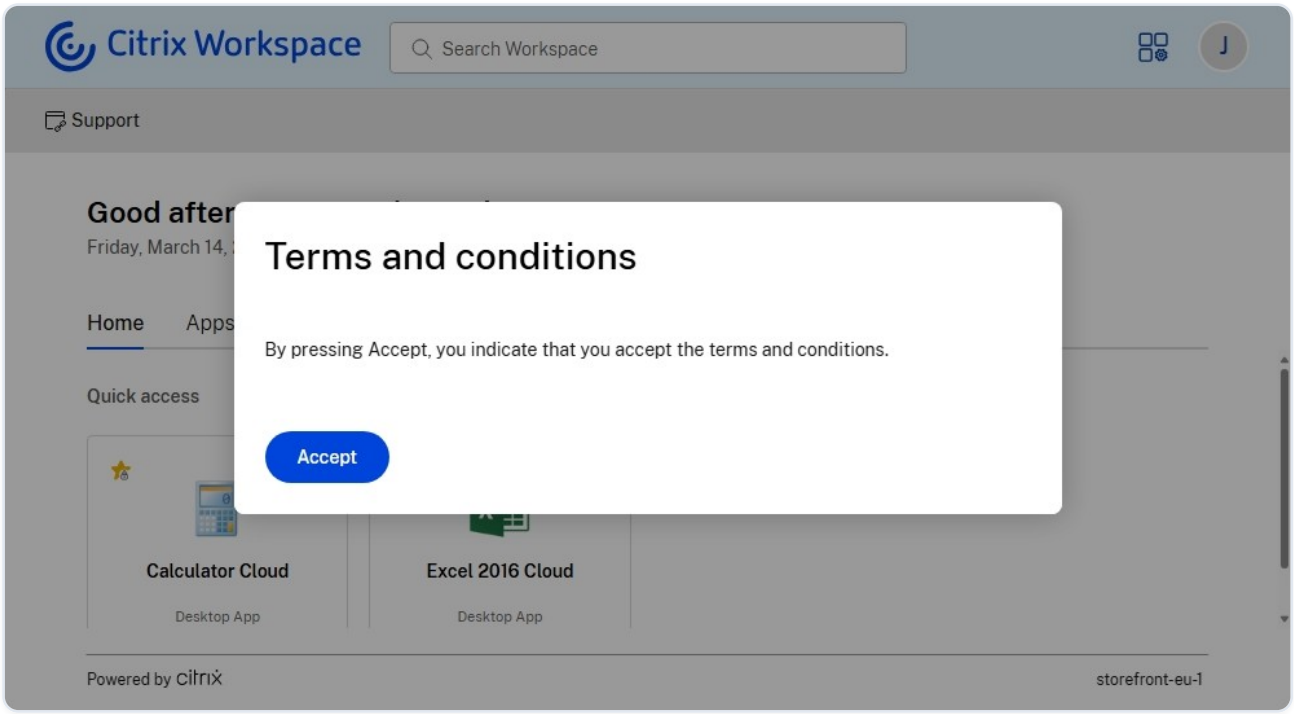
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

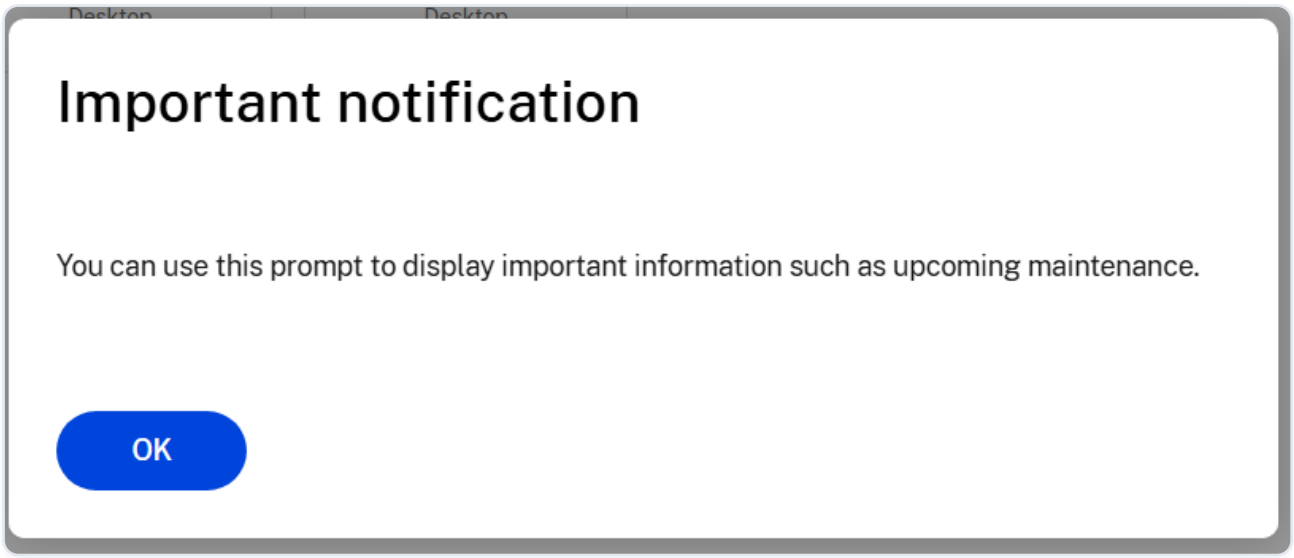
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

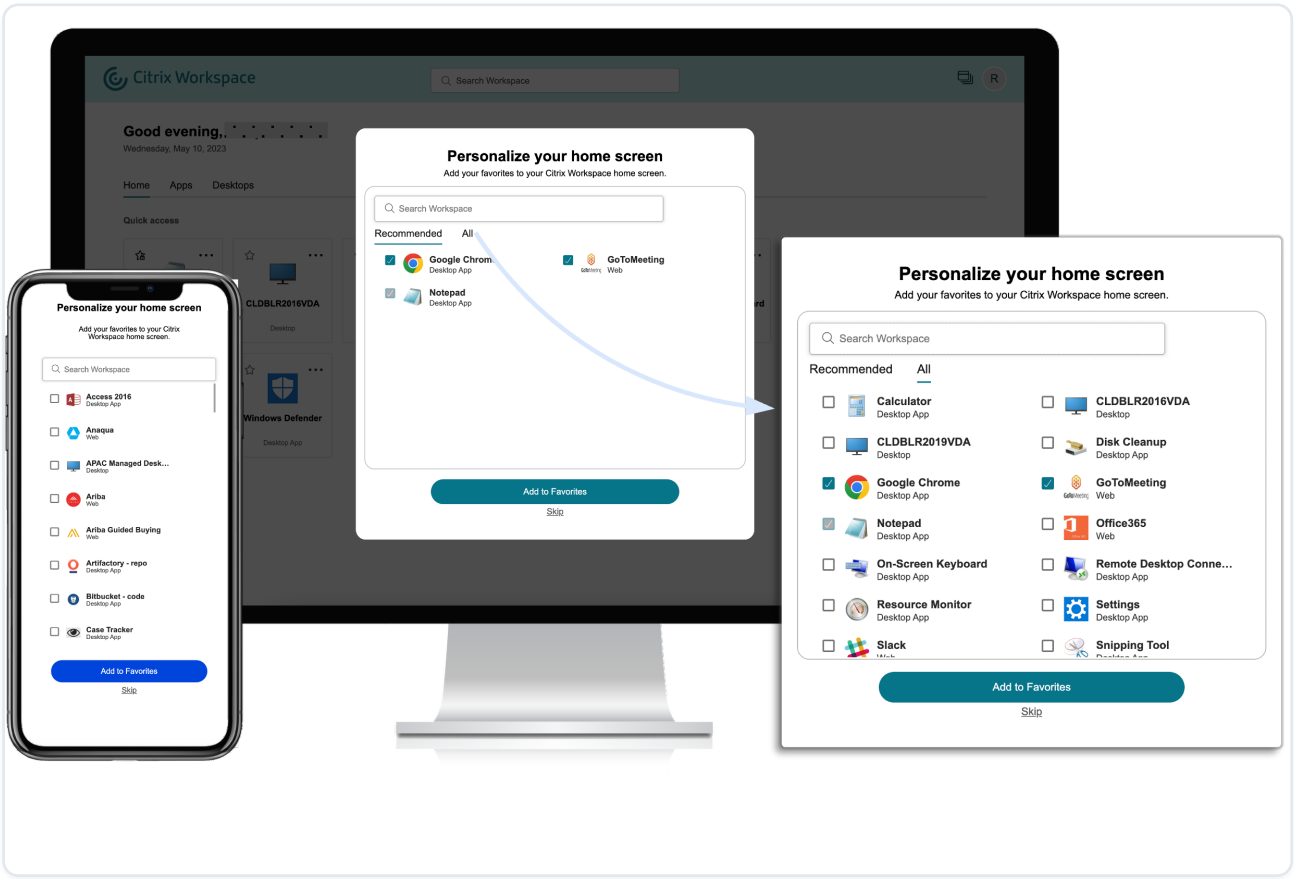
First-time user experience

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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). To configure whether this window appears, see Display Personalize your home screen for first time users.

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 add to Favorites. 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:

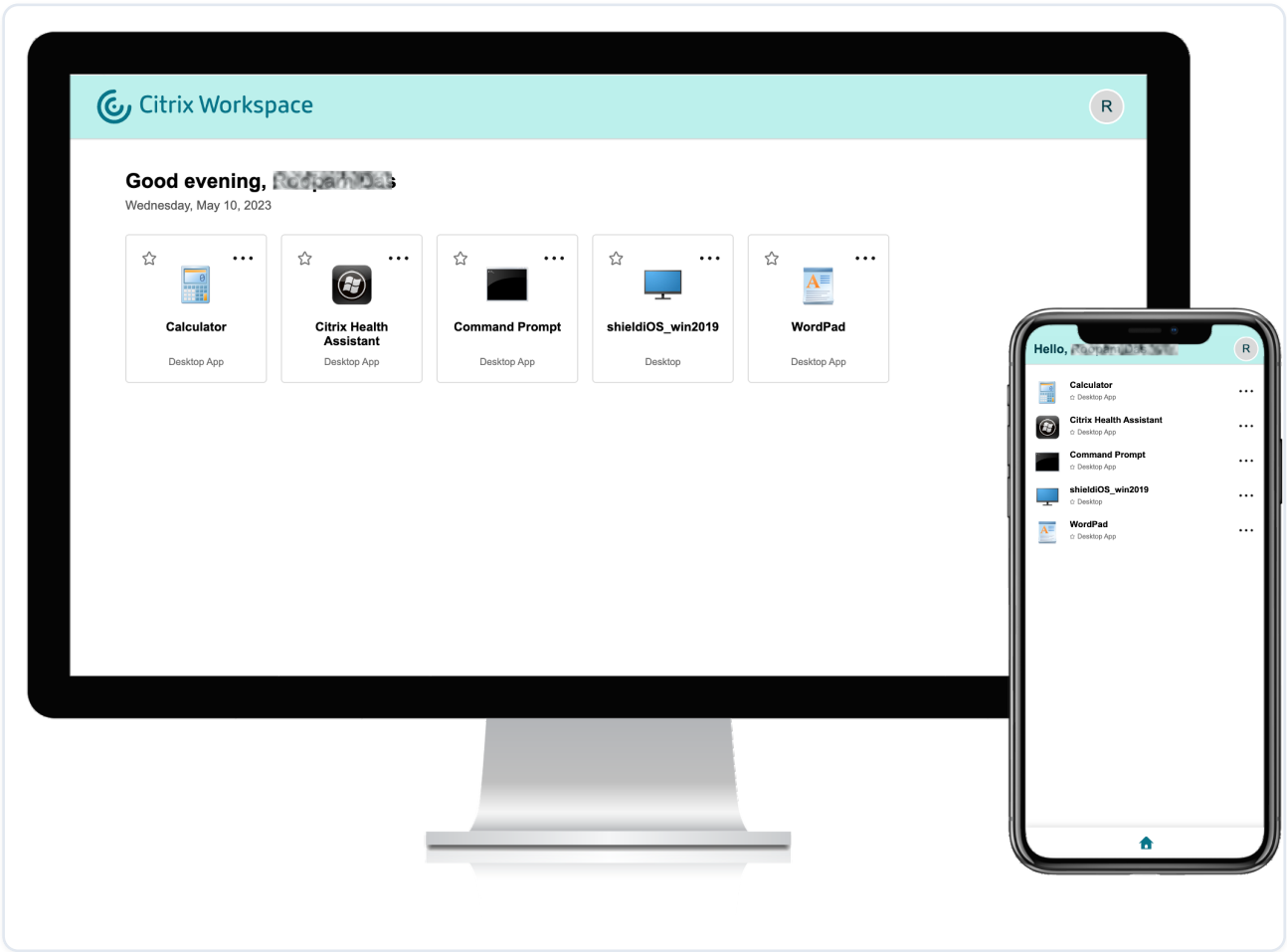
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

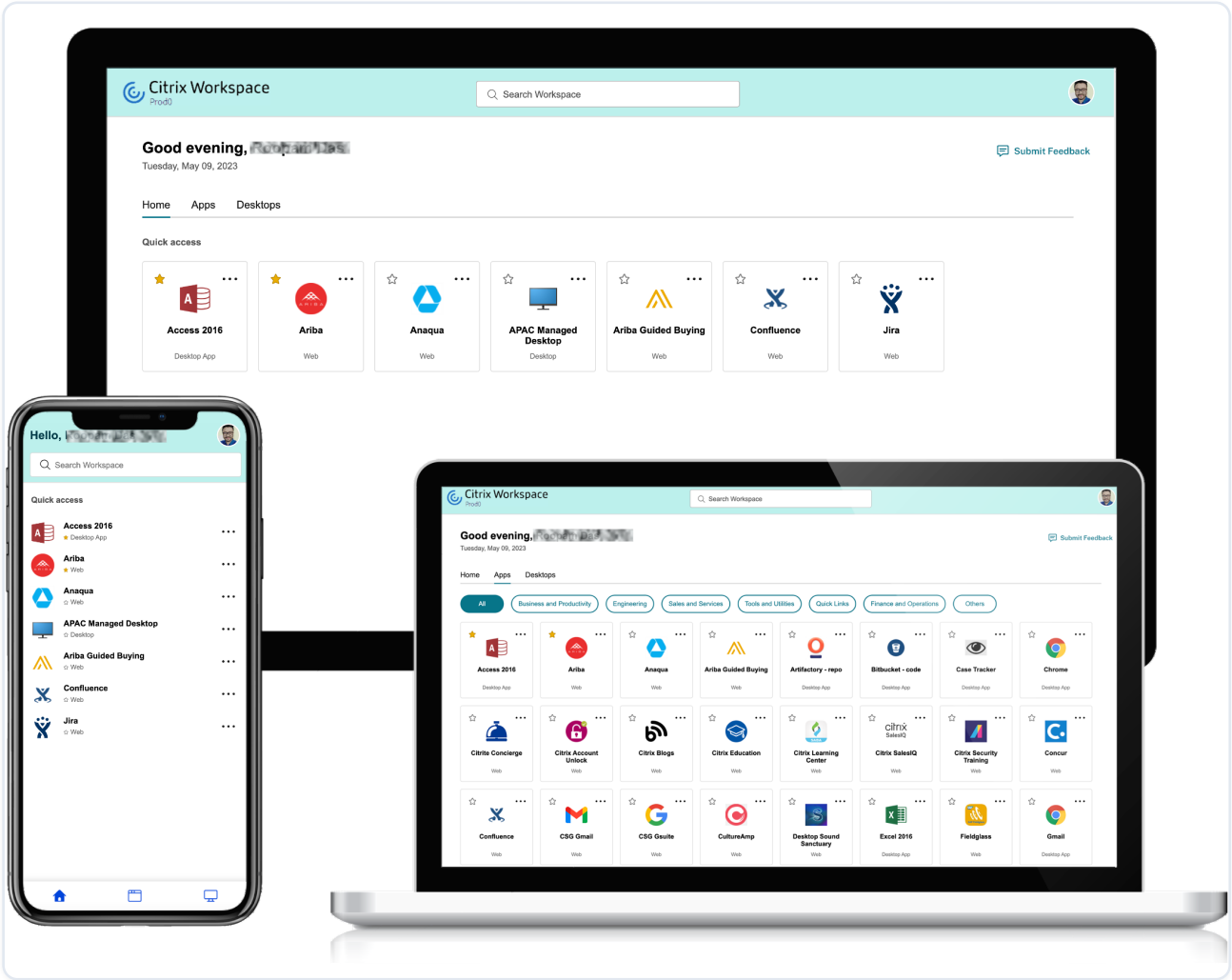
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

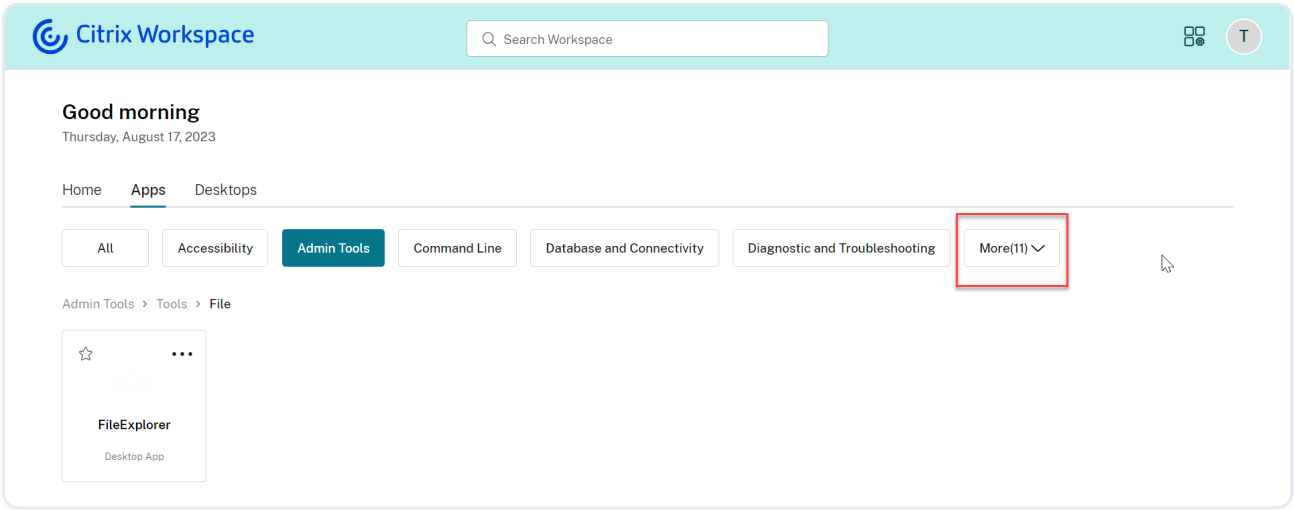
On the **Apps** tab, favorites appear first, followed by all the other apps in an alphabetical order. If the admin has created categories and attached the apps to them, then the various categories appear, and users can select the category of the apps that they want to view.



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.

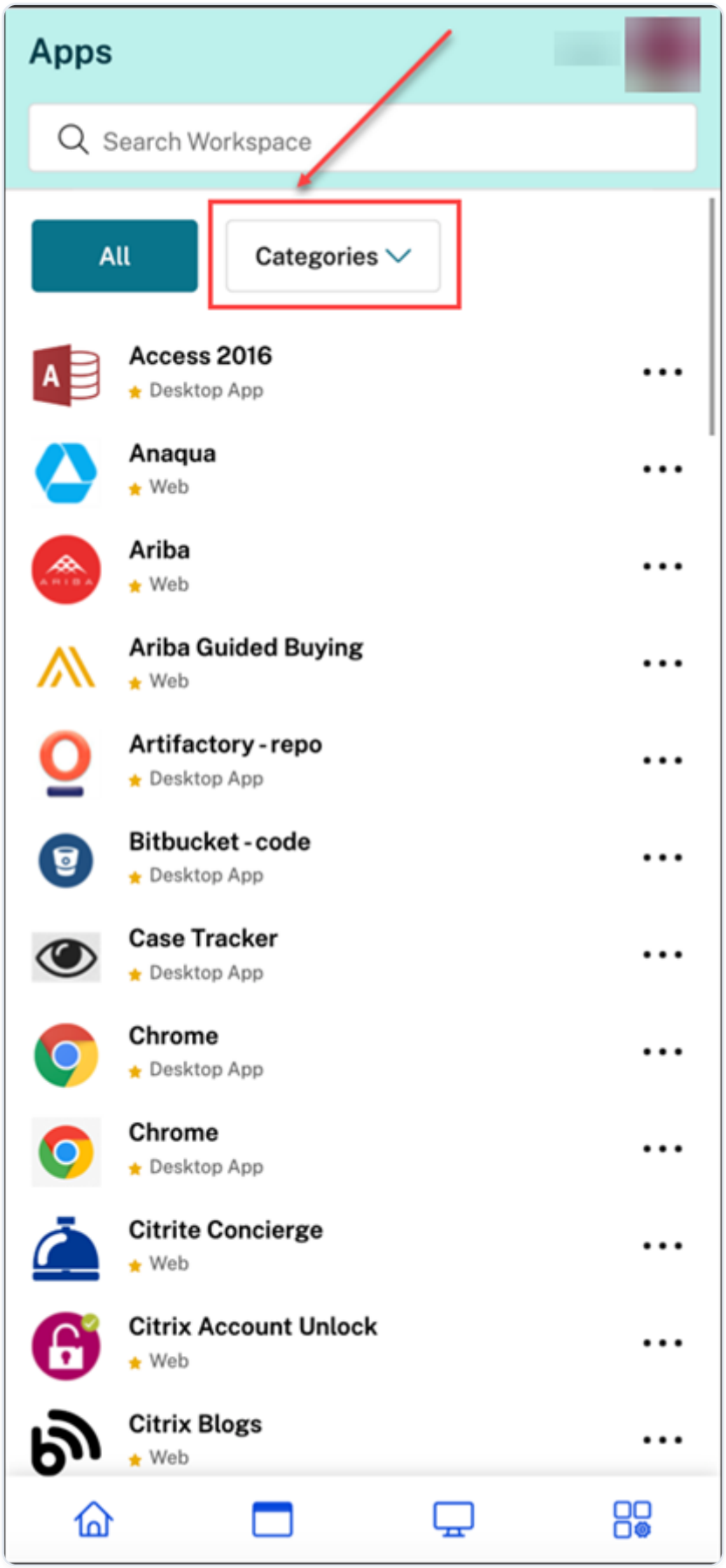
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



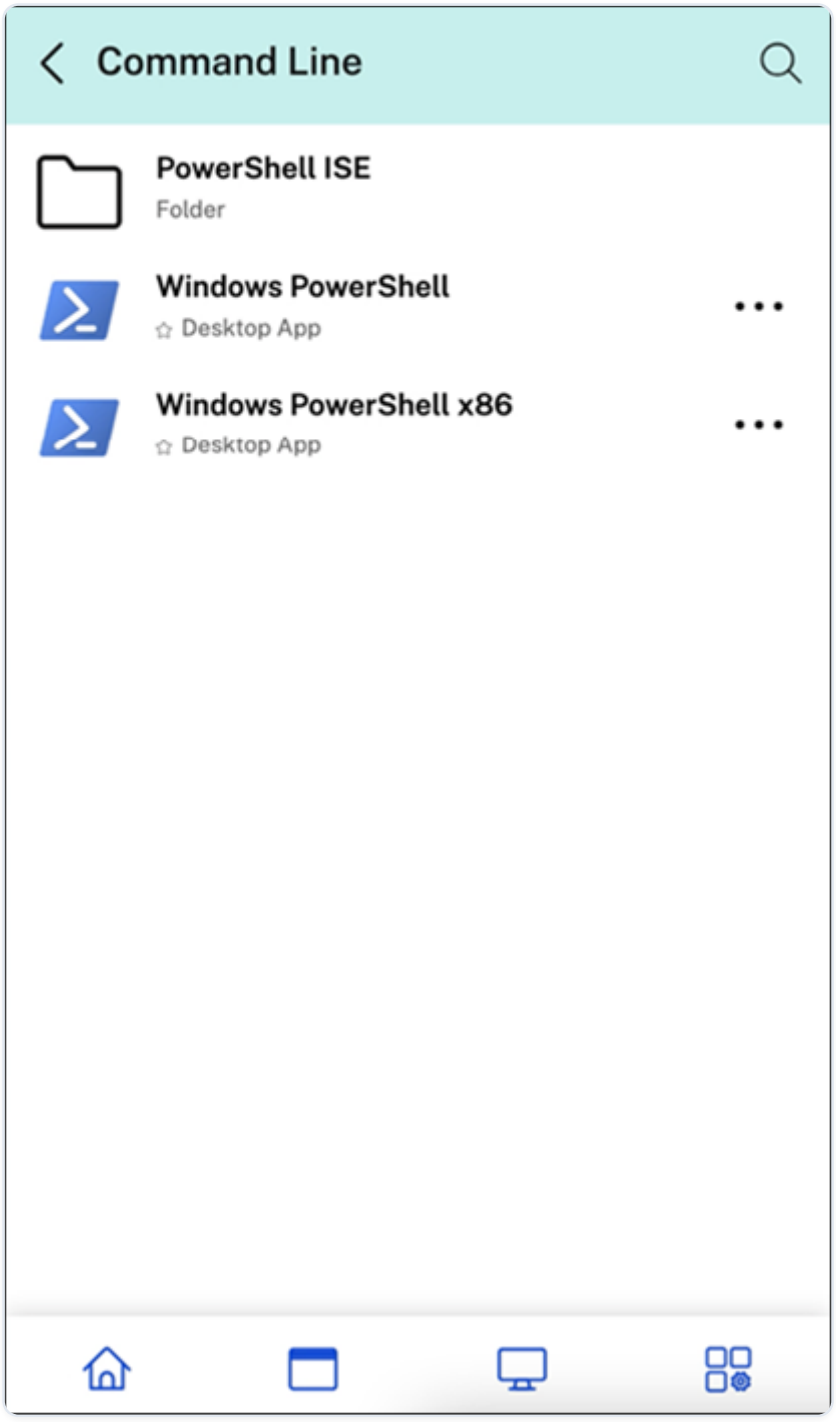
On mobile platforms, navigate to the Apps tab and click the **Categories** dropdown to view a list of available categories. Sub-categories are displayed as folders that might contain further sub-folders or applications as per the admin configuration.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Select the relevant category, a list of available sub-categories and applications is displayed based on the configuration made by the admin.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

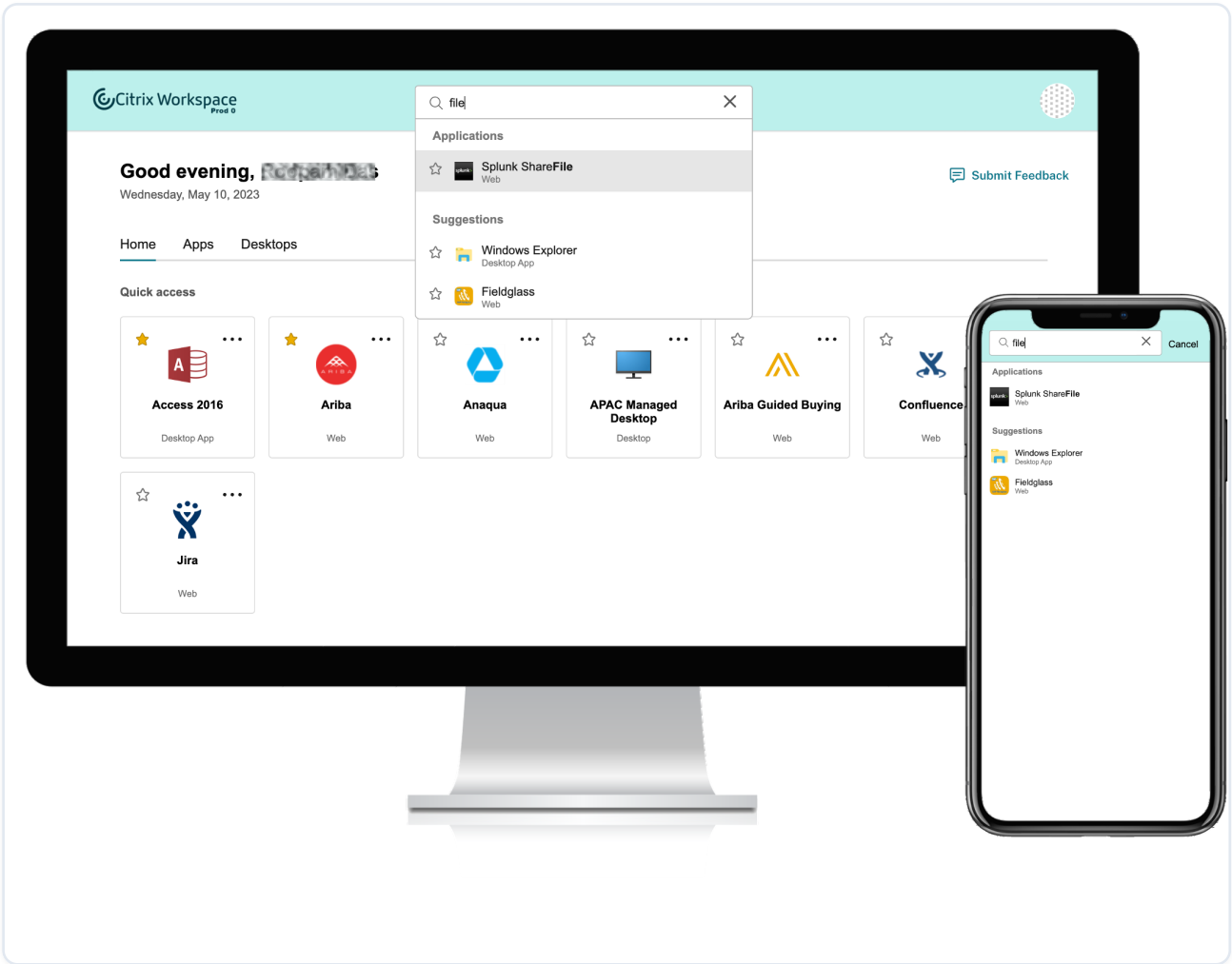
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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 tiles

The tile displays the application name as configured within Studio. Users can click the tile to launch the application.

The **More** options menu (ellipsis icon) displays the following options.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Open App** - Launch or reconnect to the app.
- **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.
- **Remove from favorites** - Shown for apps that are already favorites. This has the same effect as clicking the **Star**.
- **Show Details** - Opens a pop-up window containing the description of the app.

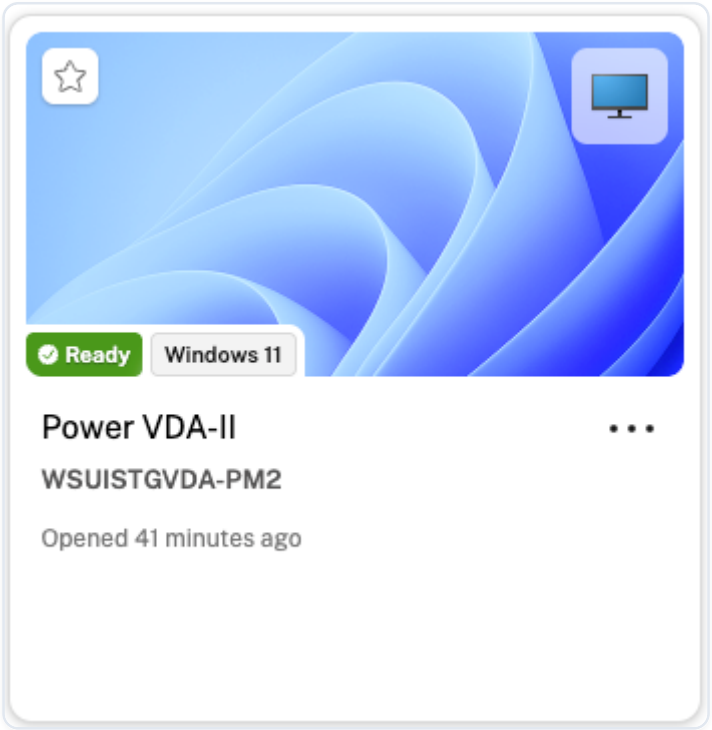
Desktop tiles

The tile displays the desktop name configured within studio.

For assigned desktops, in addition the power state is displayed. For more information, see Power status.

If you have enabled detailed desktop tiles then in addition it displays the following information:

- A larger thumbnail image.
- The desktop's operating system.
- When the user last connected to the desktop.
- Active session duration if a session is currently running on this desktop.



The **More** options menu (ellipsis icon) on the tile provides users with access to relevant actions. The options presented are context-sensitive.

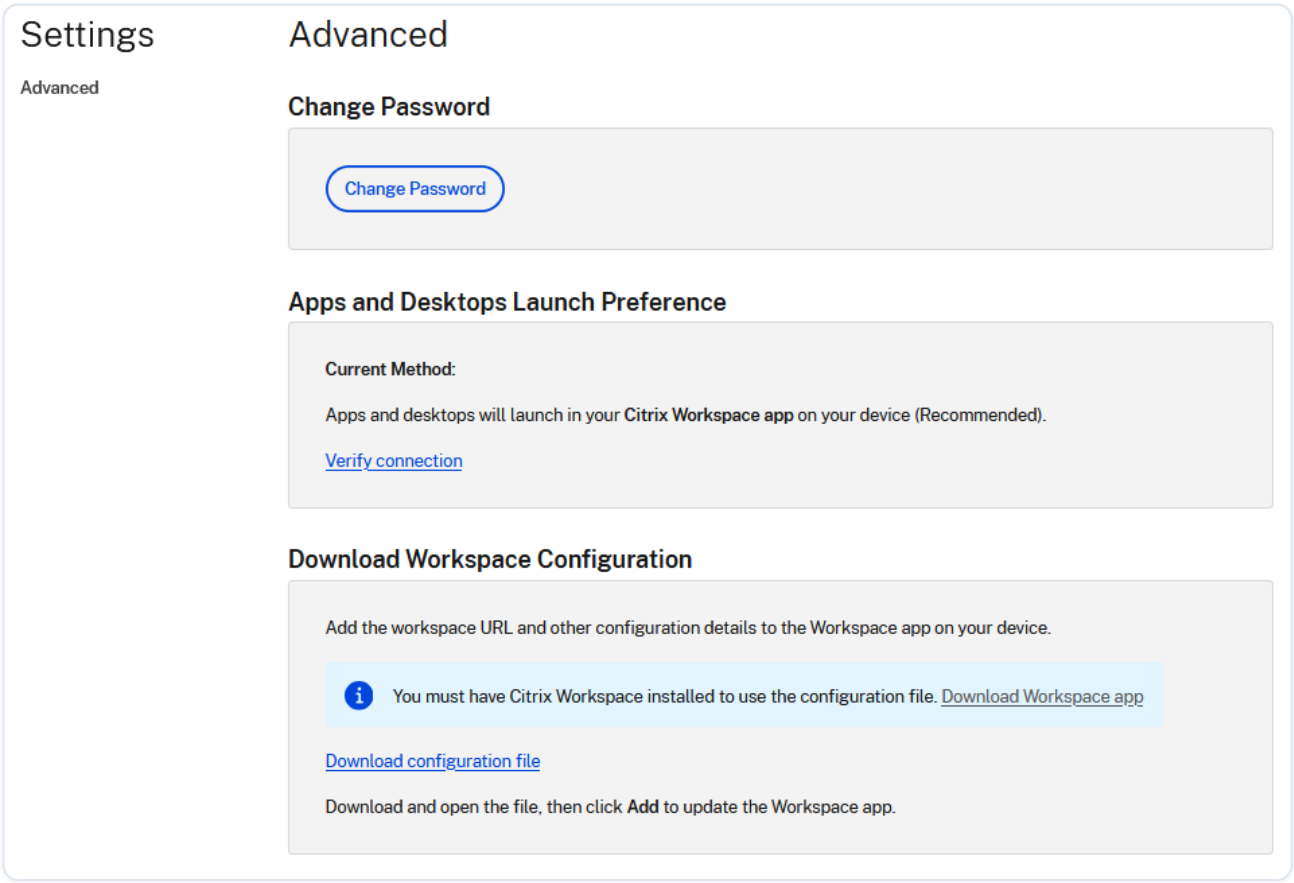
These actions might include:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Open Desktop** - Launch or reconnect to the 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.
- **Remove from favorites** - Shown for desktops that are already favorites. This has the same effect as clicking the **Star**.
- **Show Details** - Opens a pop-up window containing the description of the desktop and, for assigned desktops, the desktop's machine name.
- For assigned desktops, additional power management actions may be available. For more information, see Power actions.

Settings

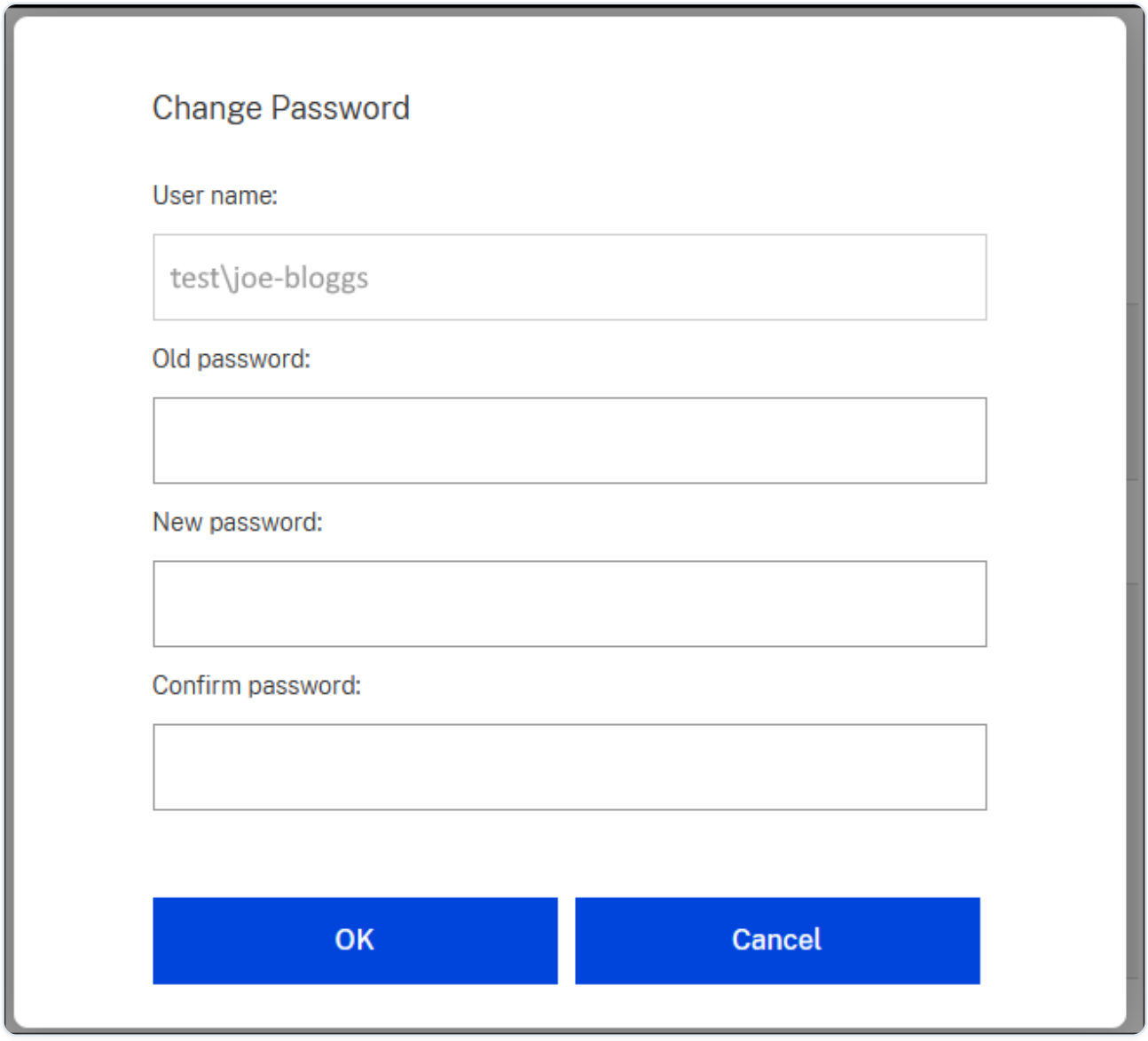
Users access **Account Settings** from a menu that appears when they select their profile icon in the upper-right corner of the UI.



© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

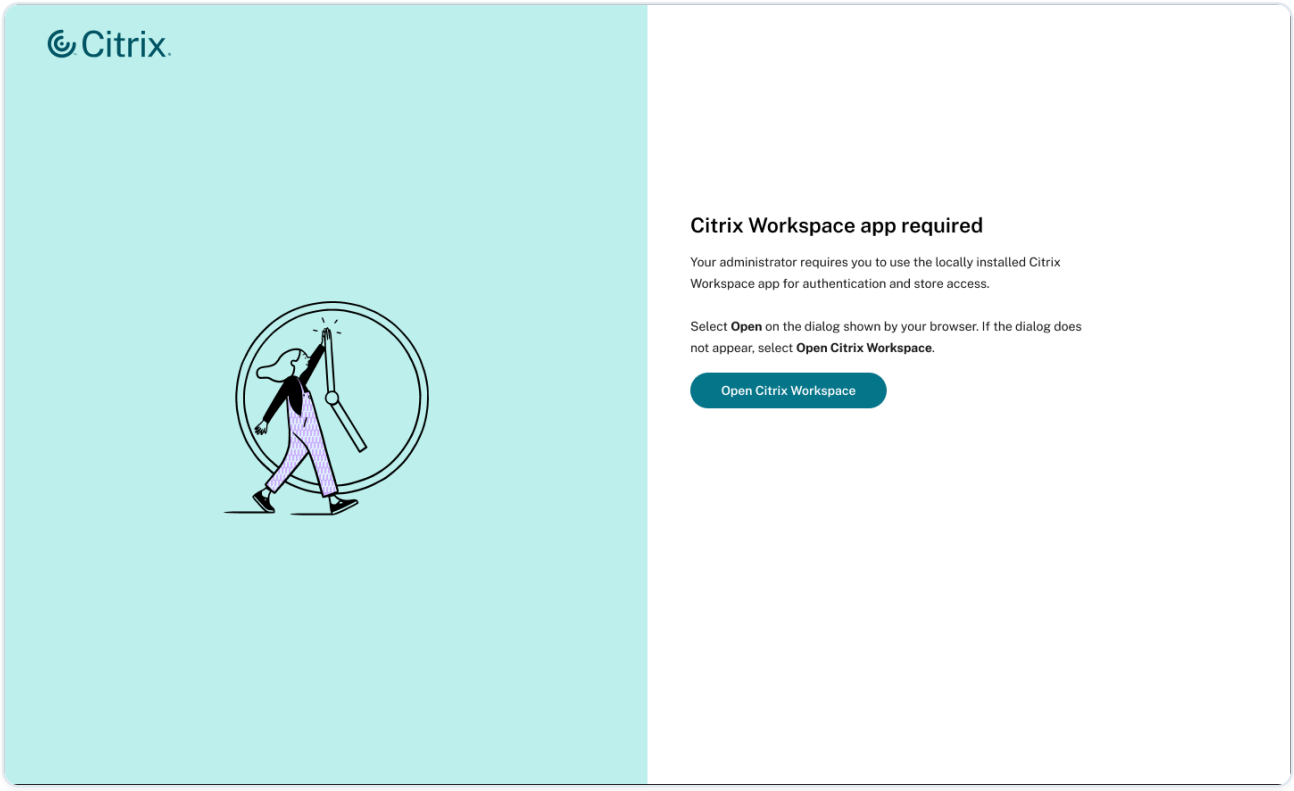
Download Workspace Configuration

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

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.

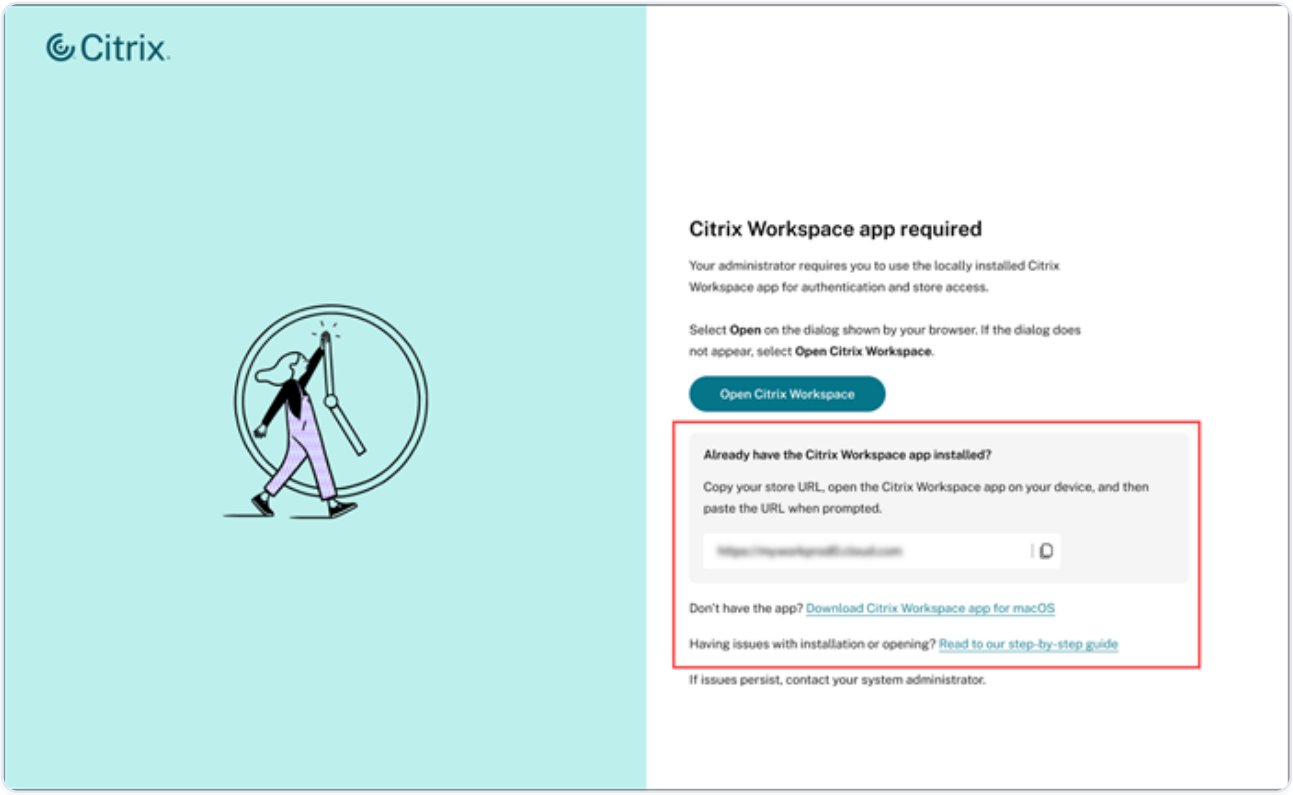
   The **Open Citrix Workspace Launcher** prompt appears asking users to open the native app.
2. Click **Open Citrix Workspace app**.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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

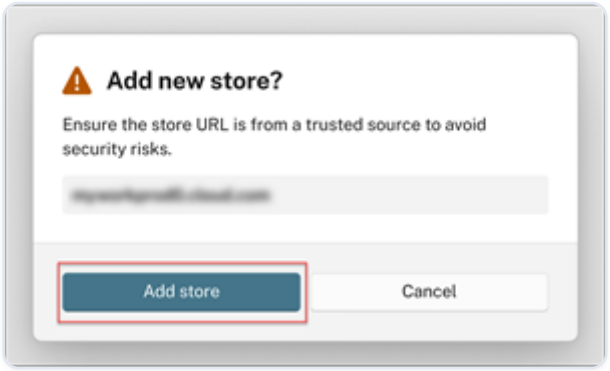
On supported versions of Citrix Workspace app, it automatically adds the store. The minimum versions are as follows:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



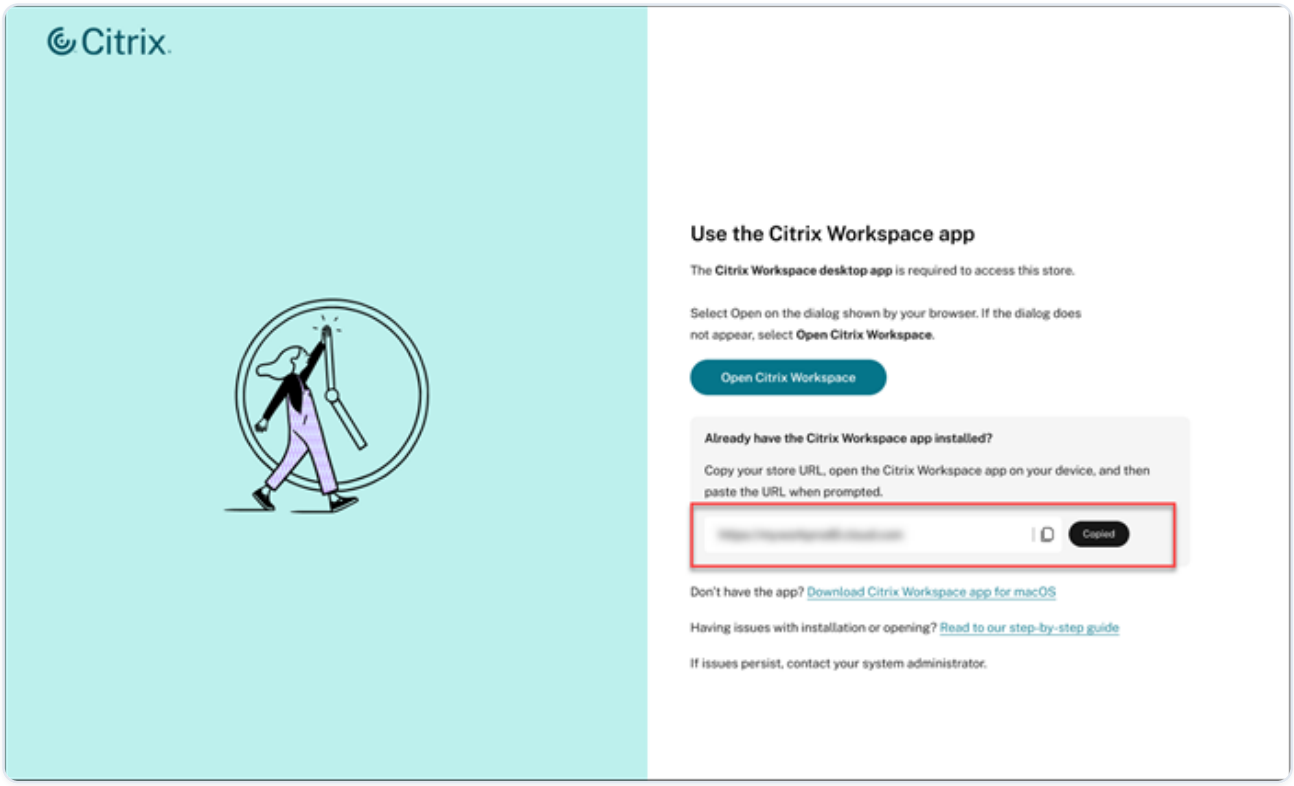
Click **Add store**.

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.

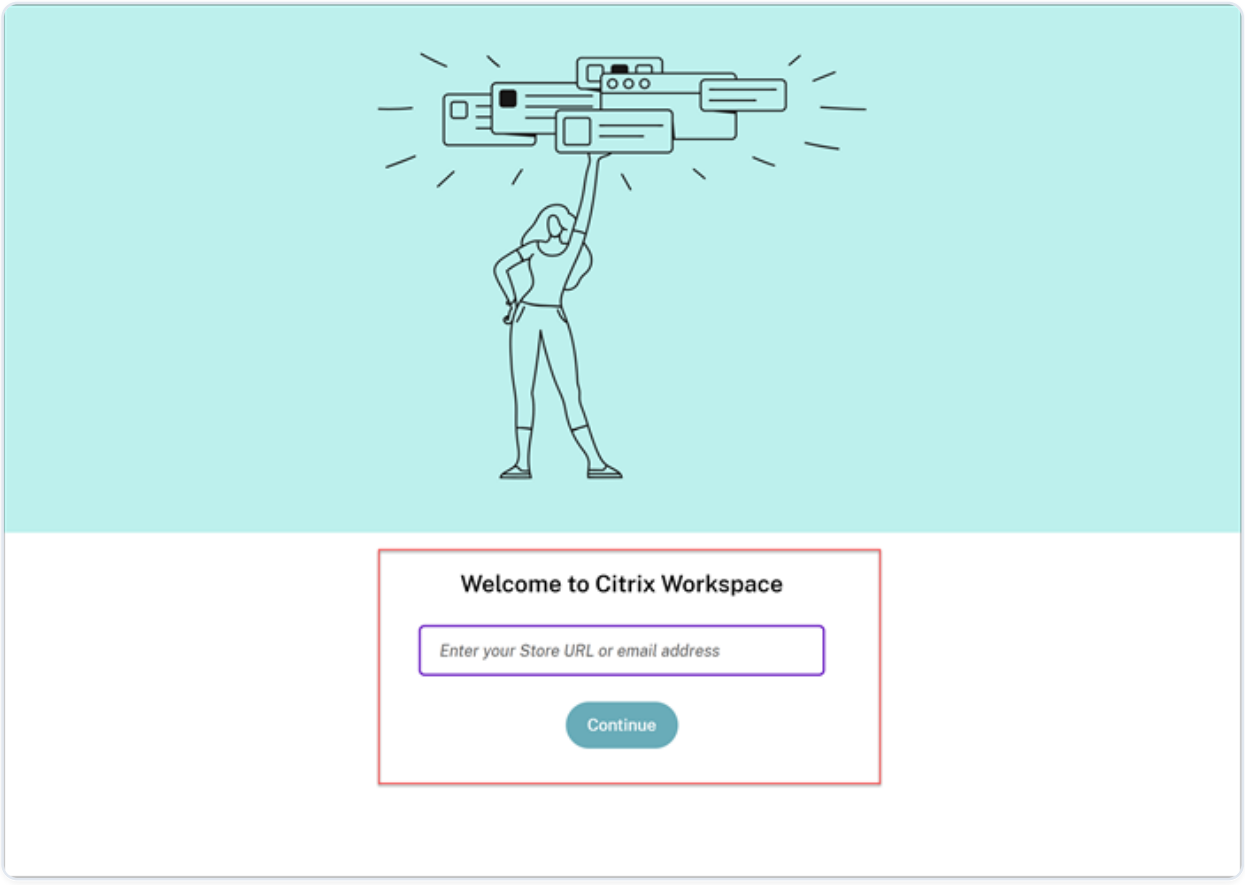
Manual store addition

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



1. Copy the store URL from the native mandate webpage, and paste it into the **Welcome to Citrix Workspace** page.



2. Click **Continue**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

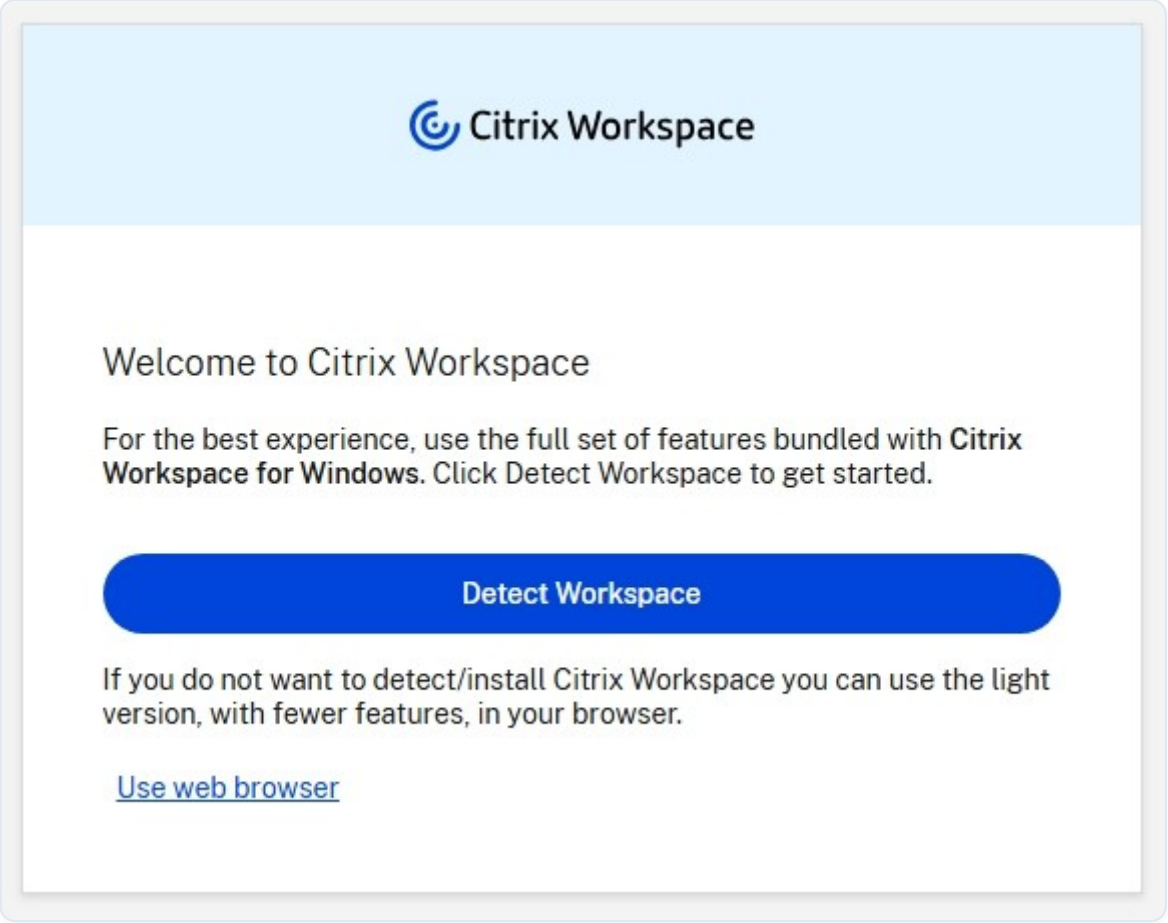
After submitting a valid store URL, Citrix Workspace app displays the authentication page for the user to sign in. After the successful authentication, the user can see the home page of the native Citrix Workspace app.

Citrix Workspace app detection

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.



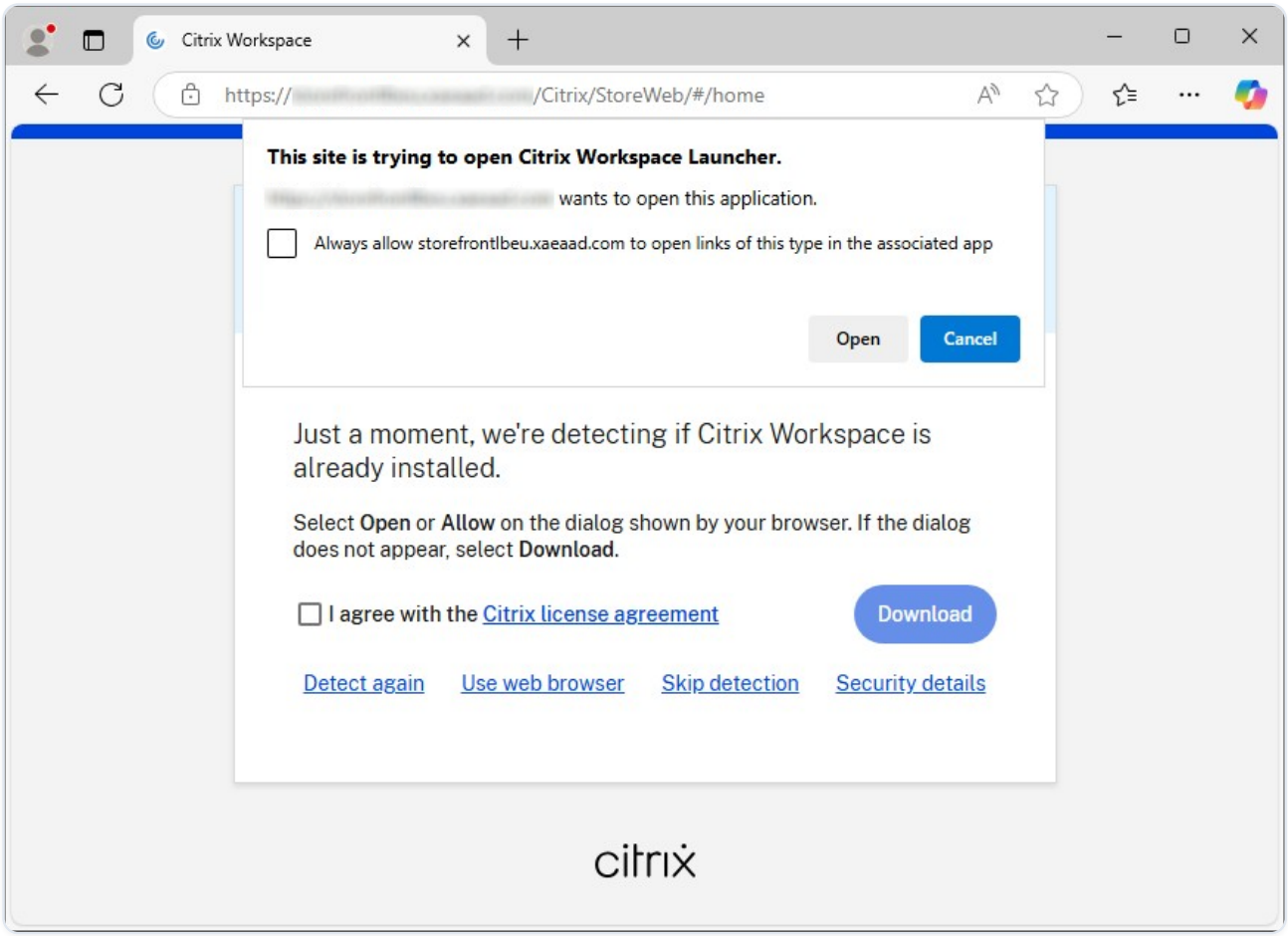
Users can either:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Activity Manager is a simple yet powerful feature 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 Desktop 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.

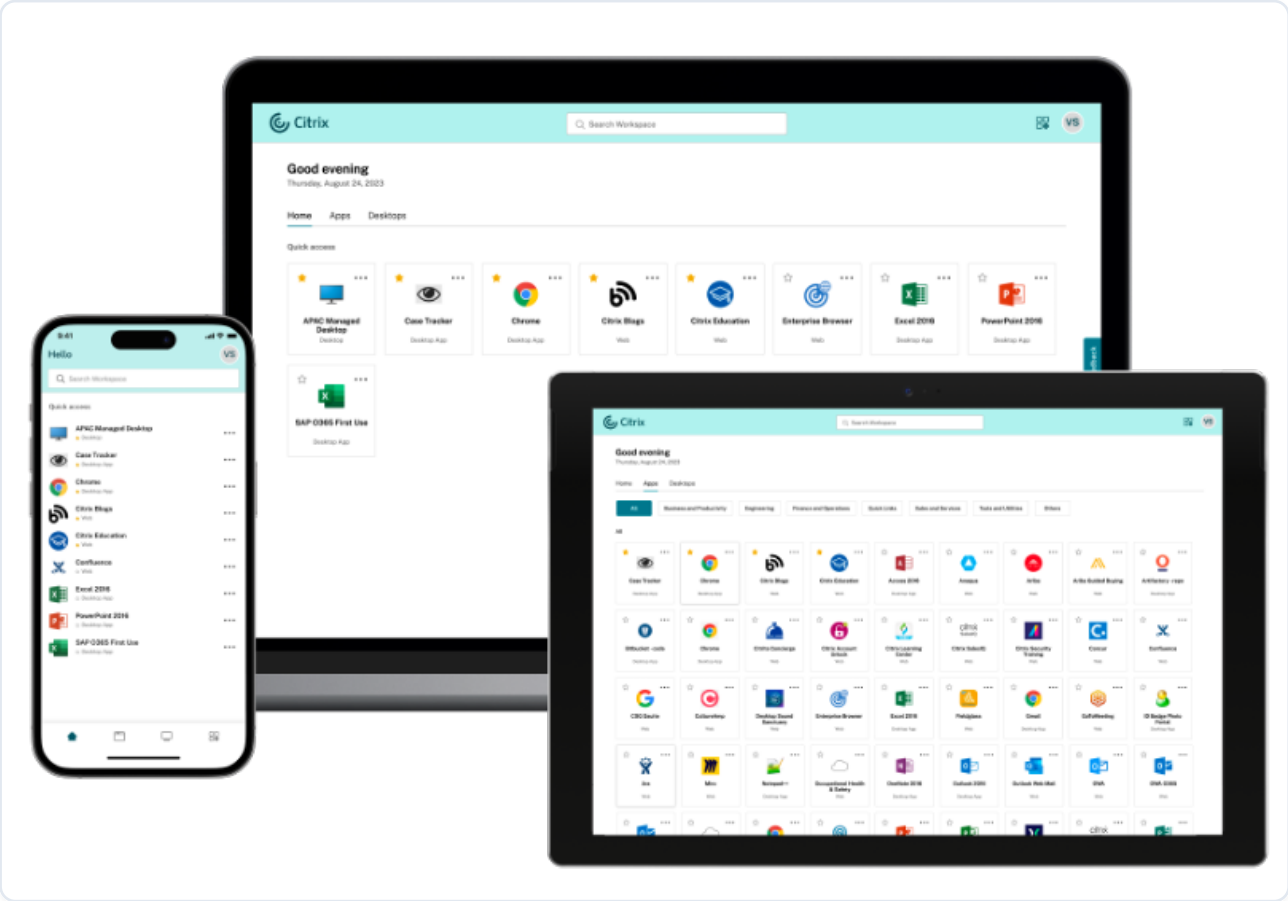
© 1997–2026 Citrix Systems, Inc. All rights reserved.

To control whether the **Activity manager** button is displayed, see Display Activity manager.

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.

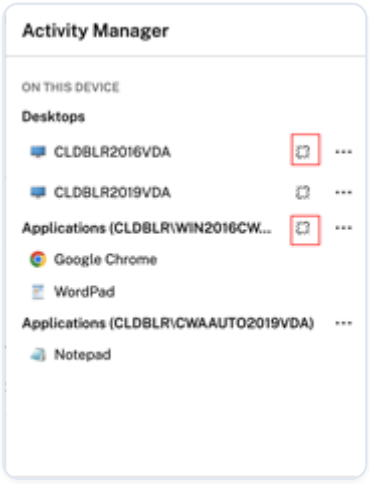
- **Disconnect**: The remote session is disconnected but the apps and desktops are active in the background.
- **Log out**: Logs out from the current session. All the apps in the sessions are closed, and any unsaved files are lost.
- **Shut Down**: Closes your disconnected desktops.
- **Force shutdown**: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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Hibernate**: Saves the current state and powers off the machine.
- **Resume**: Starts and restores the state of a machine in hibernation state.

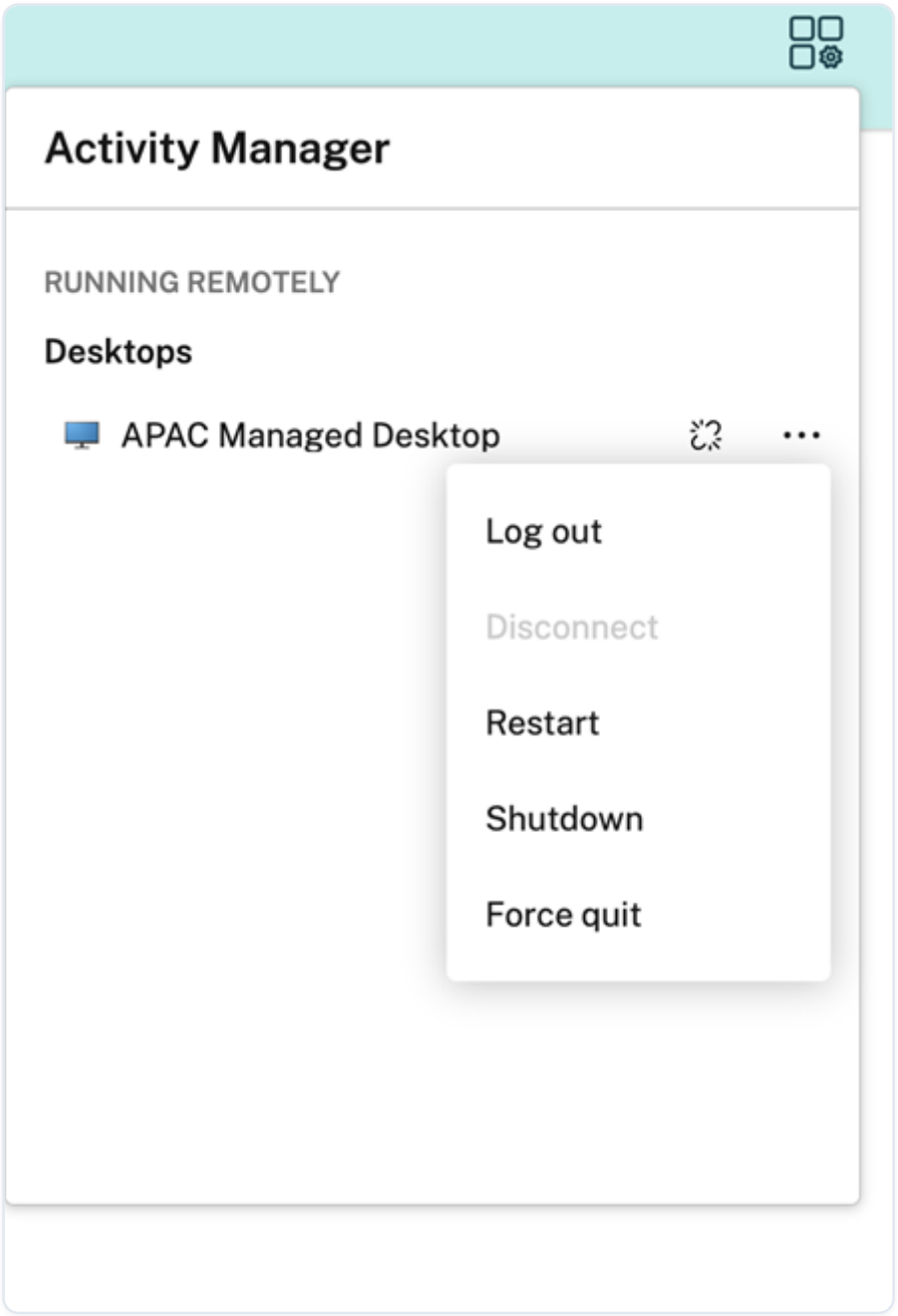
Disconnected apps and desktops

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

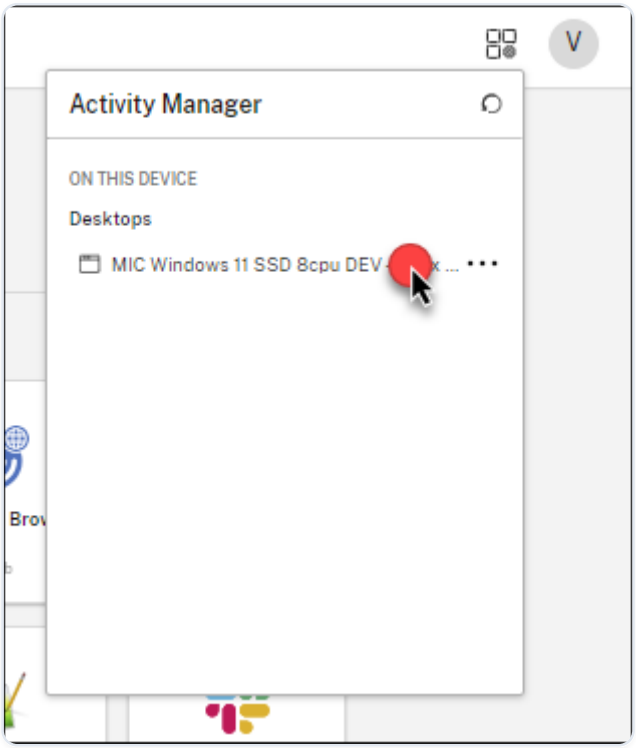
- If the user is signed into Citrix® workspace through a browser, and disconnects a local session, the session is first displayed under **On this device**. However, once the user closes and reopens Activity Manager, the disconnected session is moved under Running Remotely.
- If the user is signed into 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 reopen apps and desktops.

To reconnect to a disconnected app or desktop:

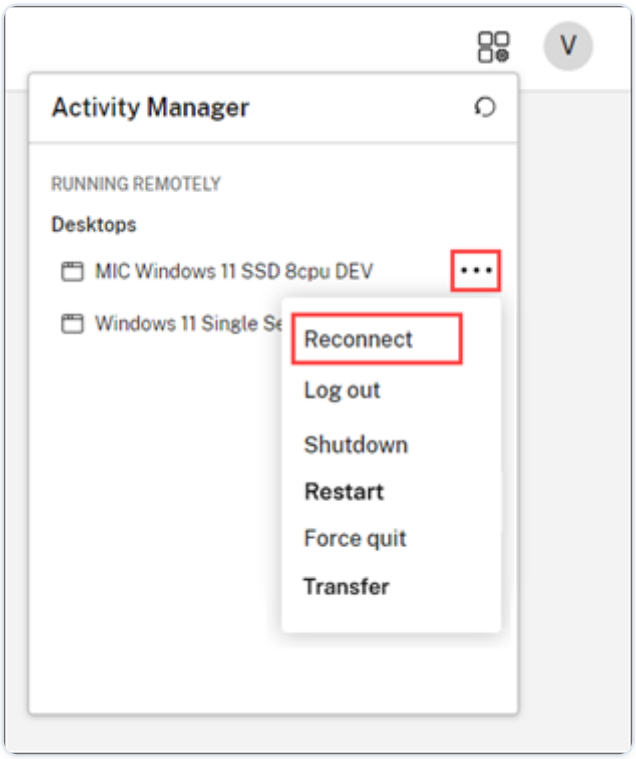
- Open Activity Manager and then click on the resource item.



OR

- Click the ellipsis button (**...**) and then click **Reconnect**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

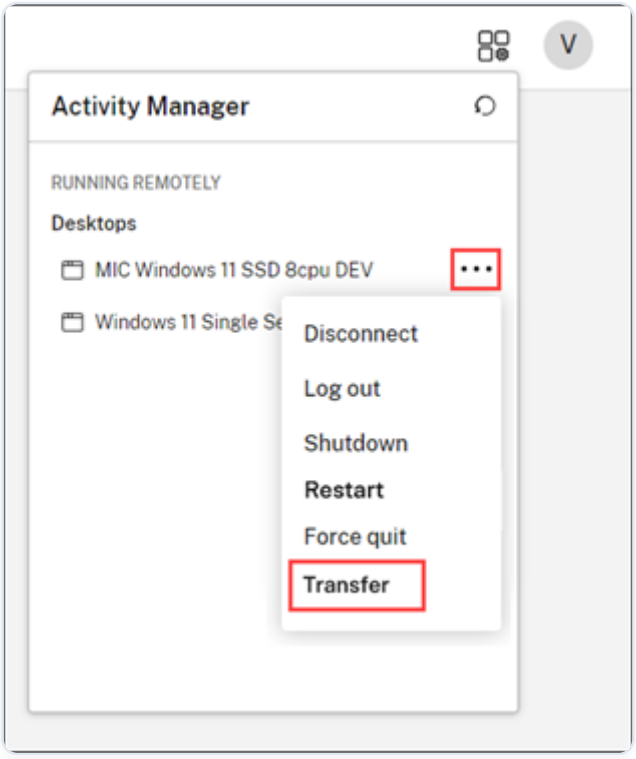


Clicking **Reconnect** reopens the disconnected resource from where you left off.

Transfer your apps and desktops

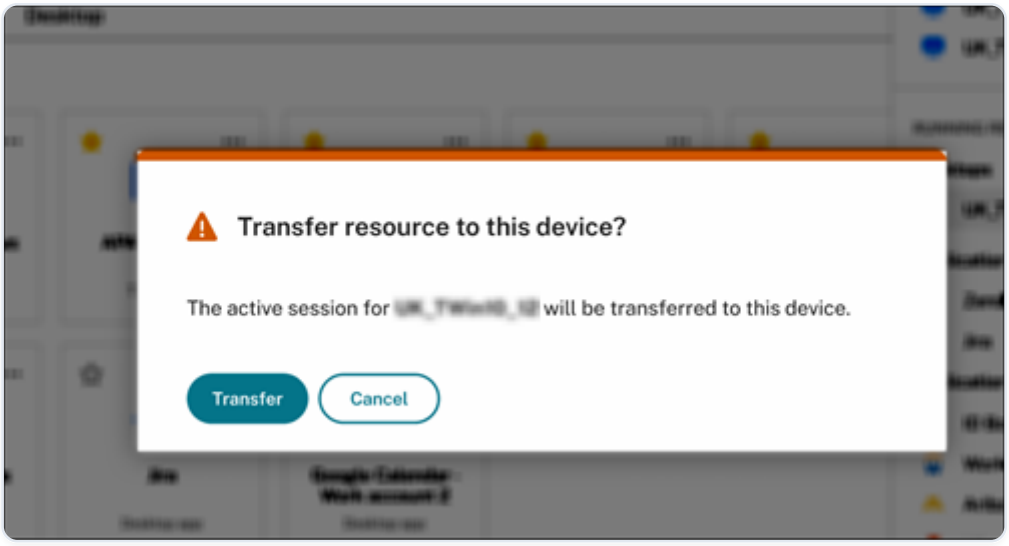
The transfer feature allows end users to transfer their active apps and desktop from other devices to the current device. To transfer the apps and desktops, follow these steps:

1. Click the ellipsis button (**...**) and then click **Transfer**.

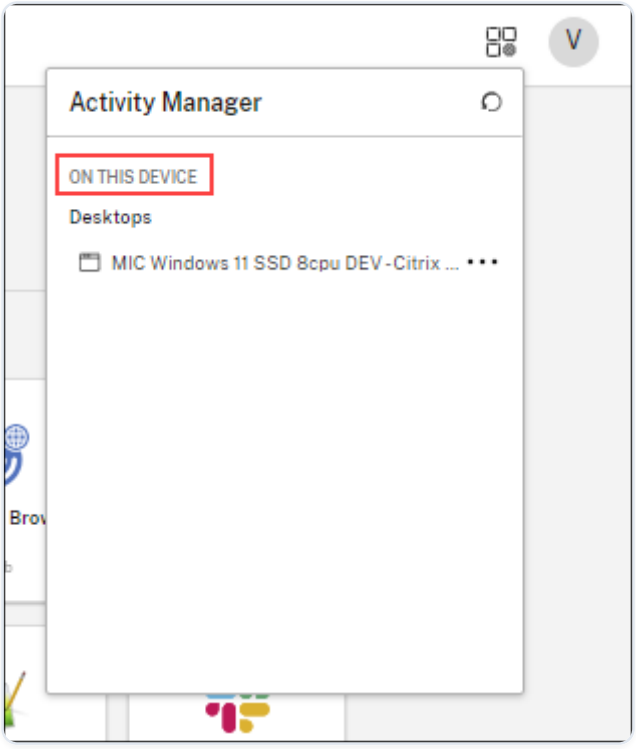


© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

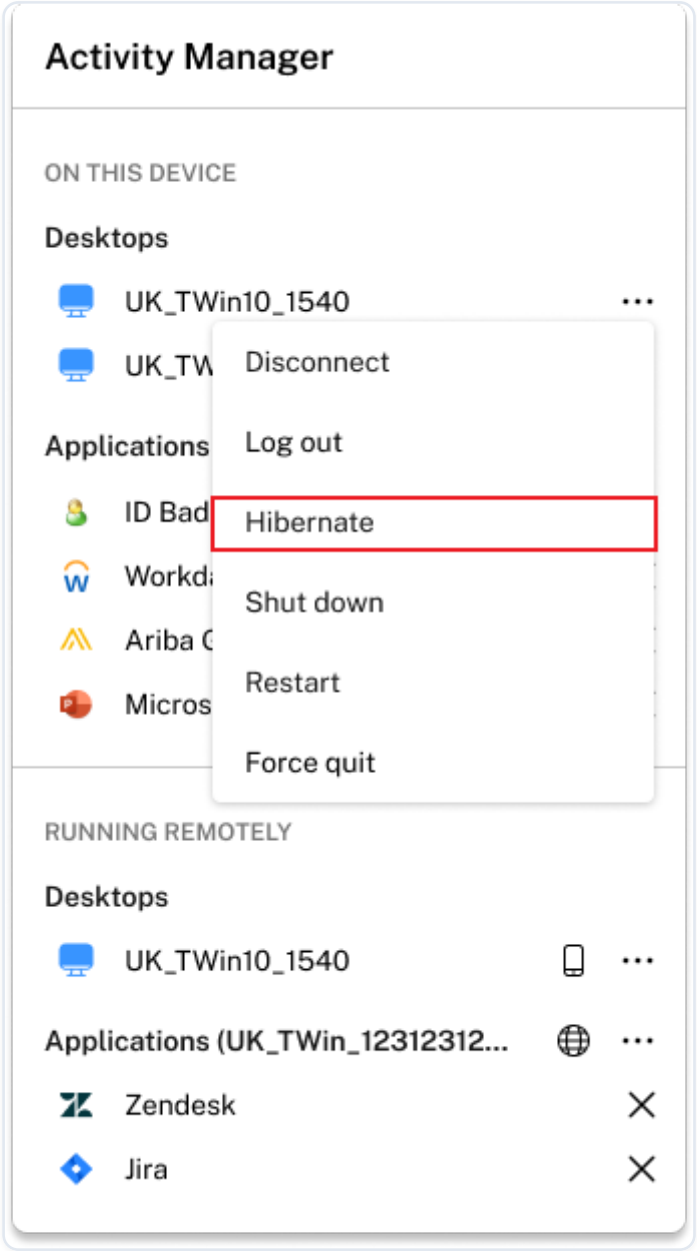
When initiating hibernation, the hypervisor communicates with the guest operating system, triggering a suspend-to-disk action. During this process, the memory (RAM) contents of the virtual

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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).

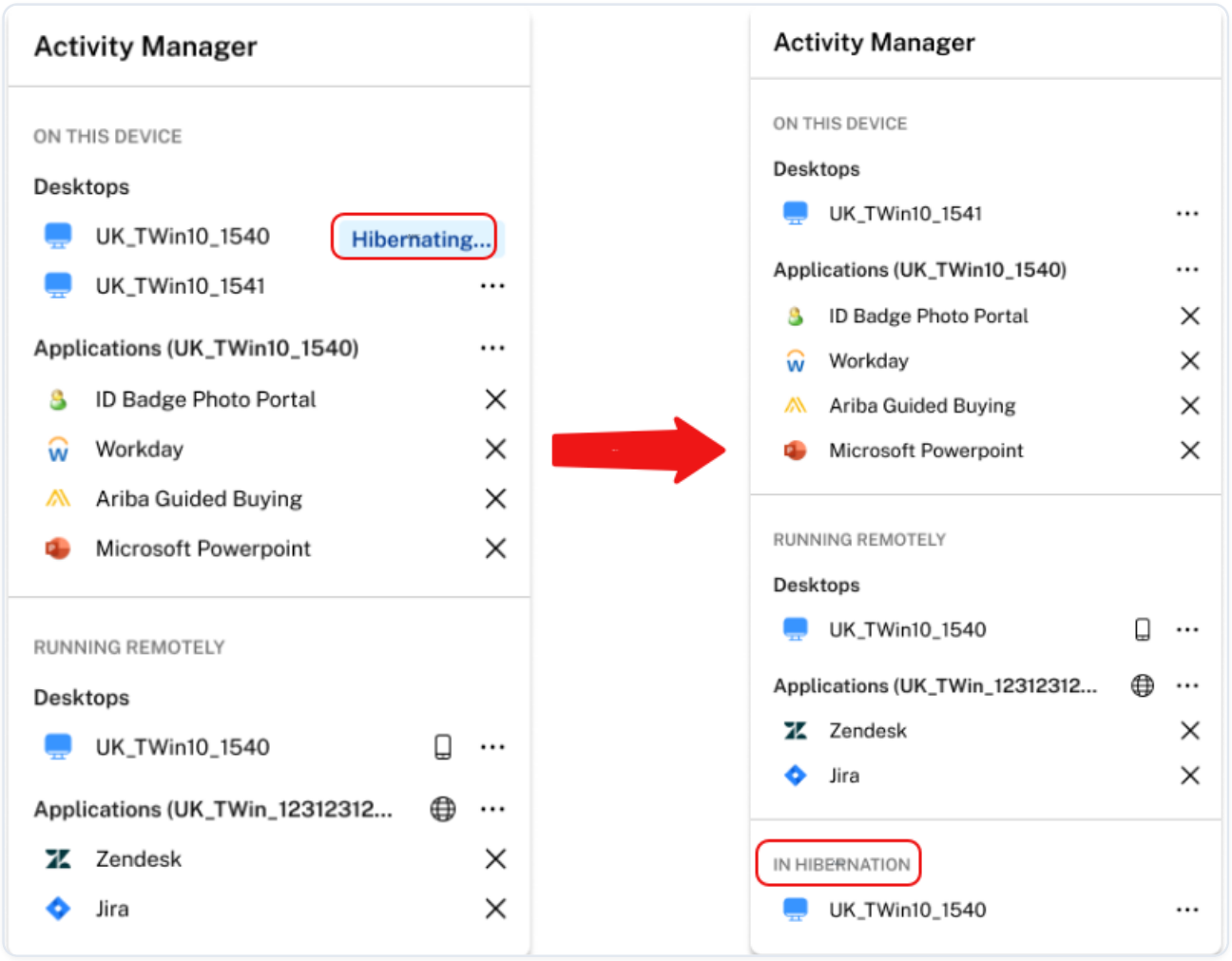
Hibernate a desktop session:



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

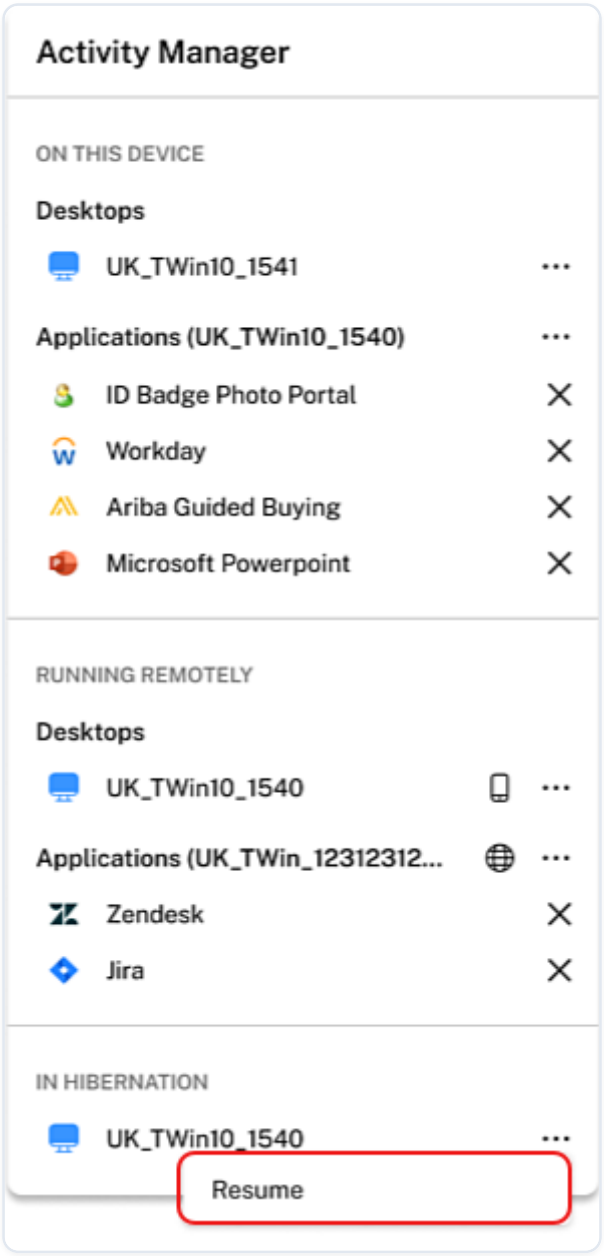
Once the desktop is hibernated, the desktop resource moves to the **In Hibernation** section on **Activity Manager**.



Resume a hibernated desktop session:

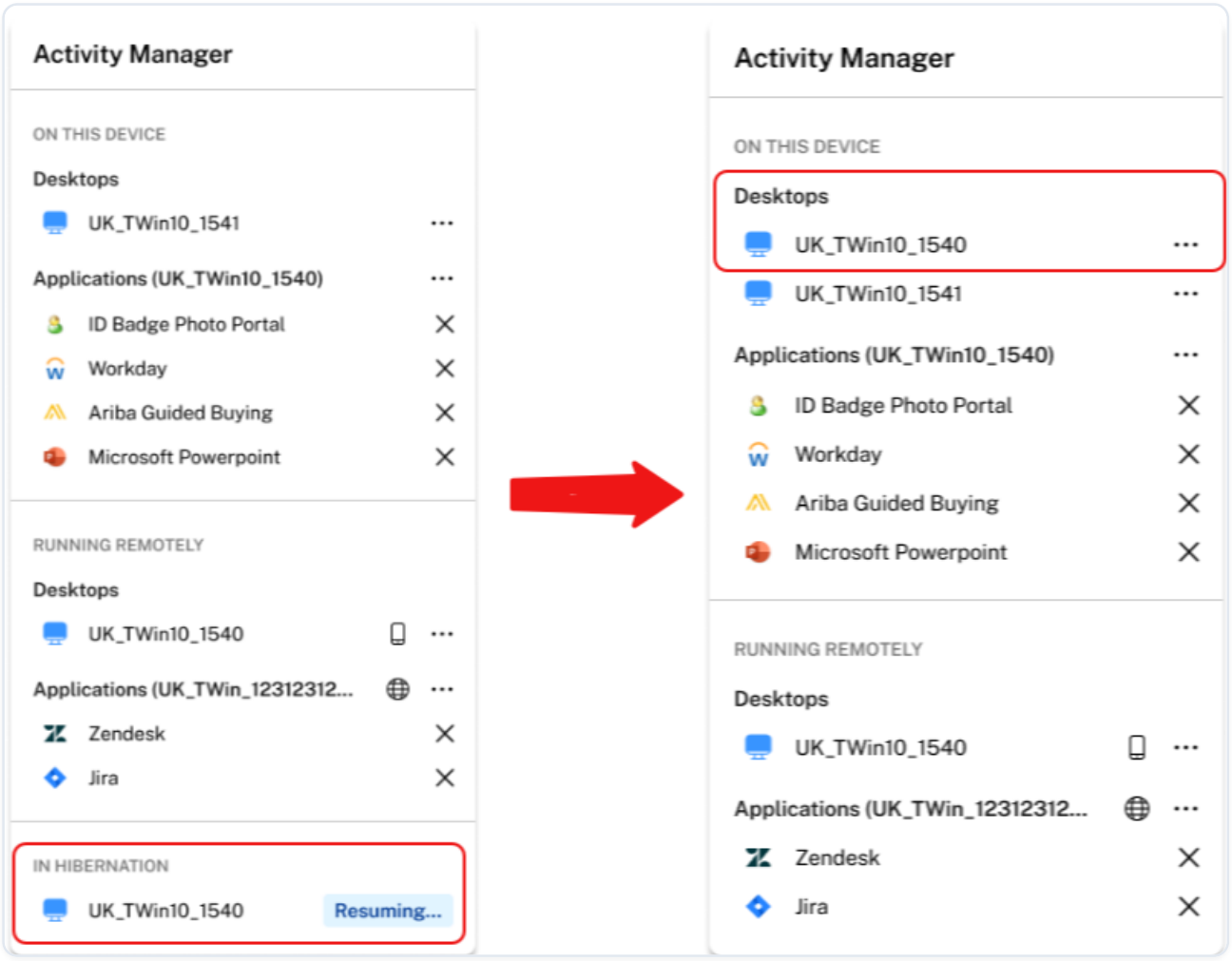
Hibernated desktop sessions are available under the **In Hibernation** section on **Activity Manager**. To resume the hibernated desktop session, users can click the three-dot button (**...**), and then click the **Resume** option.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



Once users click the **Resume** option, the desktop gets restored.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



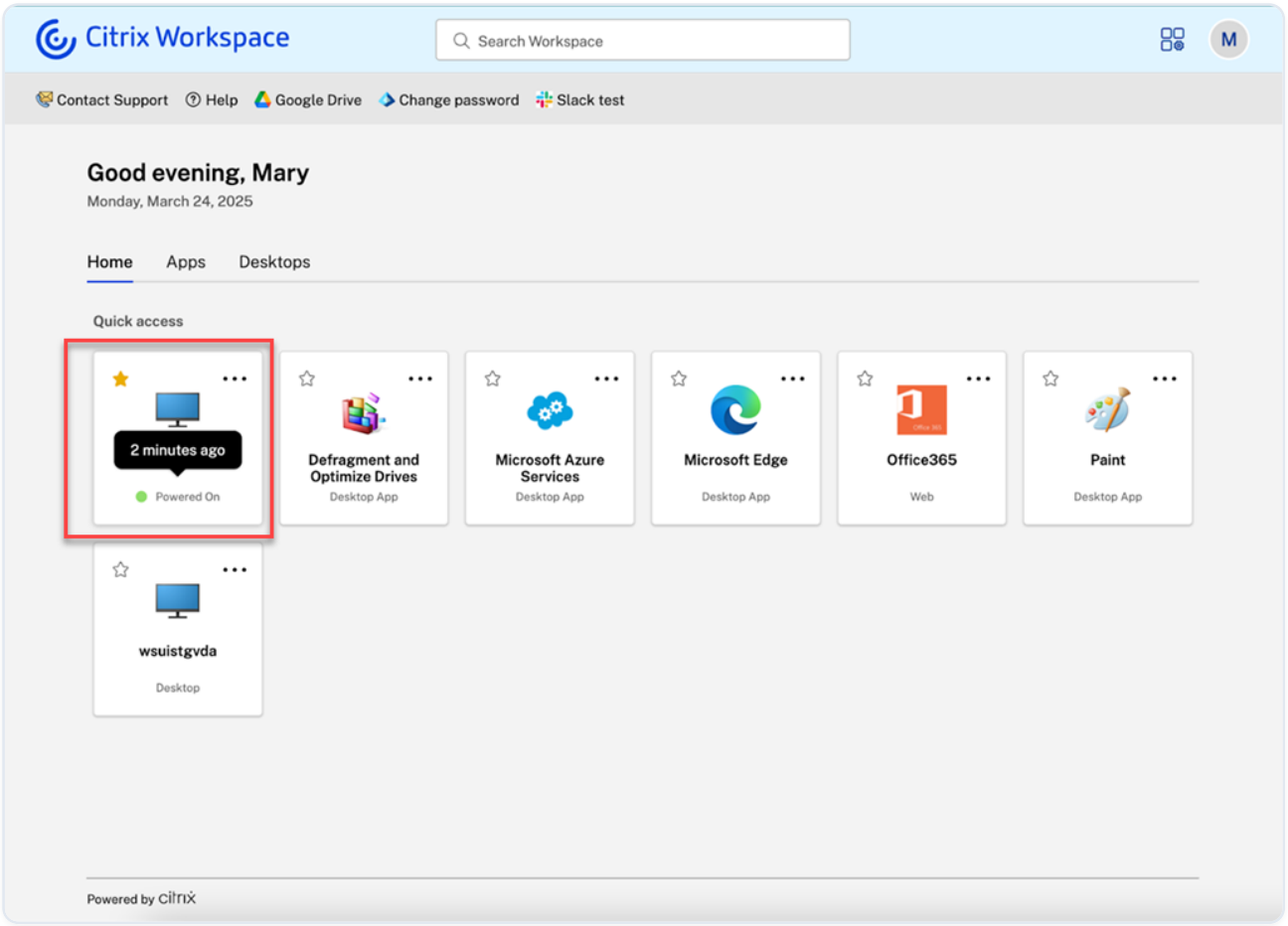
Assigned desktop power management

Power status

The desktop tile may displays 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 or Citrix Virtual Apps™ and Desktops 2511 or higher.

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 running.
- **Ready:** The desktop has registered with the delivery controller and is ready to launch.
- **Shutting down:** The user has initiated a shut down.

If you have enabled the detailed desktop tile then in addition the following states may be displayed:

- **Under Maintenance** — Your desktop is temporarily unavailable due to maintenance scheduled by your IT administrator
- **Unavailable** — Your desktop cannot be accessed at this time
- **Active** - A session is currently running on this desktop.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

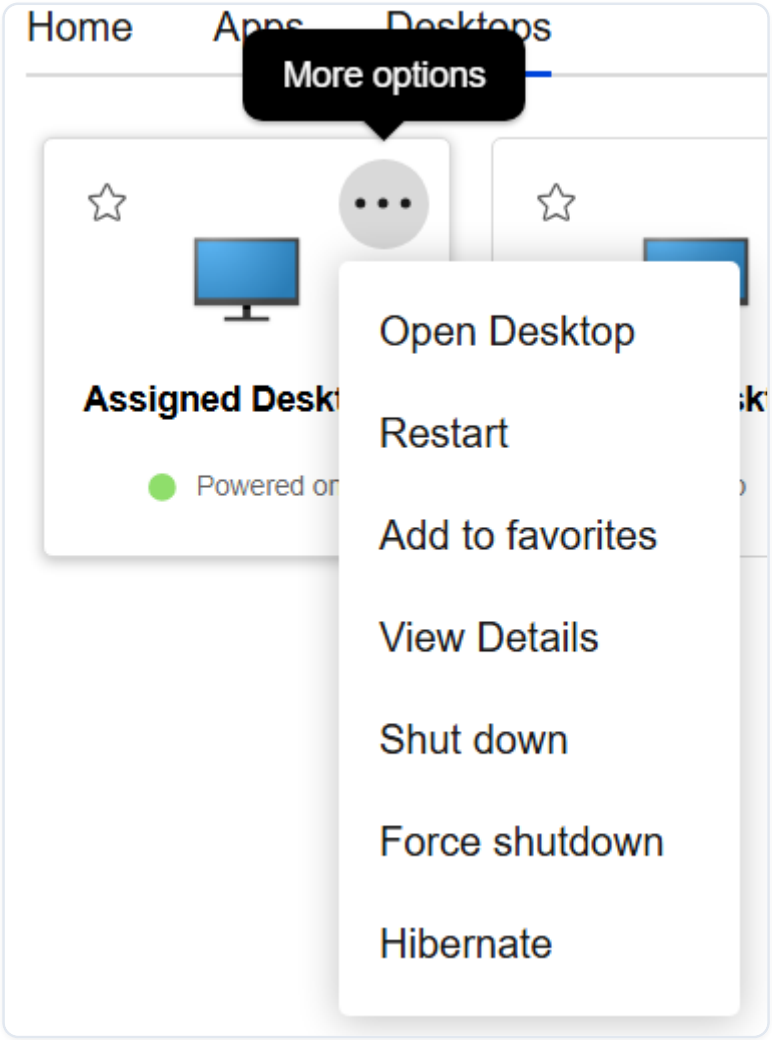
The status is refreshed every two minutes or when the user clicks the ellipsis menu on the desktop tile. When the user hovers over the power state it displays when the last refresh occurred.

Known issues

- When you launch one of multiple power-managed desktops, the store might show inconsistent power statuses for the other desktops until the first desktop completes launching.

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 Desktop** - Launch or reconnect to the desktop.
- **Troubleshoot** - Checks for any issues that could cause launch failures.
- **Restart** - Initiates a force restart. Only available for assigned power managed desktops.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Log out** - Logs out of the desktop. Only available if the user has a logged in session.
- **Disconnect** - Disconnects from desktop. Only available if the user has an active session.
- **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.

You can configure which power actions are available using delivery group access policy rules. To configure the rules, call Set-BrokerAccessPolicyRule with the following parameters:

POWER ACTION	PARAMETER	NOTES
Restart	`-AllowRestart`	
Shutdown	`-AllowShutDown`	Requires CVAD 2607 or higher
Hibernate	`-AllowShutDown`	Requires CVAD 2607 or higher
Force shutdown	`-AllowTurnOff`	Requires CVAD 2607 or higher

NOTE:

If Force Shutdown is disabled for end users, Restart is also disabled.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Secure your StoreFront deployment

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
- .gif
- .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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 includes a header `X-Powered-By` with value `ASP.NET` at the server level. StoreFront removes this header on all StoreFront websites. You can also remove the header at the server level, which applies to all websites on the server, see IIS Custom Headers documentation.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

- 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

If you have favorites enabled using the local ESENT database then StoreFront might use NTLM when synchronizing favorites in a server group. If you disable NTLM then favorites might fail to synchronize. As an alternative you can use a SQL Server database.

If users authenticate using domain pass-through authentication then by default IIS uses kerberos if possible, otherwise falls back to NTLM. If there is a load balancer in front of StoreFront then it always falls back to NTLM.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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
`content-security-policy`	`frame-ancestors 'none'`	This prevents other sites from embedding a StoreFront websites within a frame which avoids click-jacking attacks. In addition the HTML page includes a `meta` tag containing a `content-security-policy` that

© 1997–2026 Citrix Systems, Inc. All rights reserved.

HEADER NAME	VALUE	DESCRIPTION
		restricts script sources to mitigate against XSS attacks.
`X-Content-Type-Options`	`nosniff`	This avoid MIME type sniffing.
`X-Frame-Options`	`deny`	This prevents other sites from embedding StoreFront websites within a frame which avoids click-jacking attacks. It is obsoleted by `content-security-policy` to `frame-ancestors 'none'` but is understood by some older browsers that do not support `content-security-policy`

`Strict-Transport-Security` is not set by default but can be configured. For more information, see HSTS.

Cookies

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

COOKIE	DESCRIPTION
`ASP.NET_SessionId`	Tracks the user's session including authentication status. Has `HttpOnly` set.
`CtxsAuthId`	To prevent session fixation attacks, StoreFront in addition tracks whether the user is authenticated using this cookie. It has `HttpOnly` set.
`CsrfToken`	Used to prevent cross-site request forgery via the standard Cookie-to-header token pattern. The server sets a token in the cookie. The client reads the token from the cookie and

© 1997–2026 Citrix Systems, Inc. All rights reserved.

COOKIE	DESCRIPTION
	includes the token in the query string or a header in subsequent requests. This cookie is required to have `HttpOnly` not set so the client JavaScript can read it.
`CtxsDeviceId`	Identifies the device. Has `HttpOnly` set.

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

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

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:



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**.

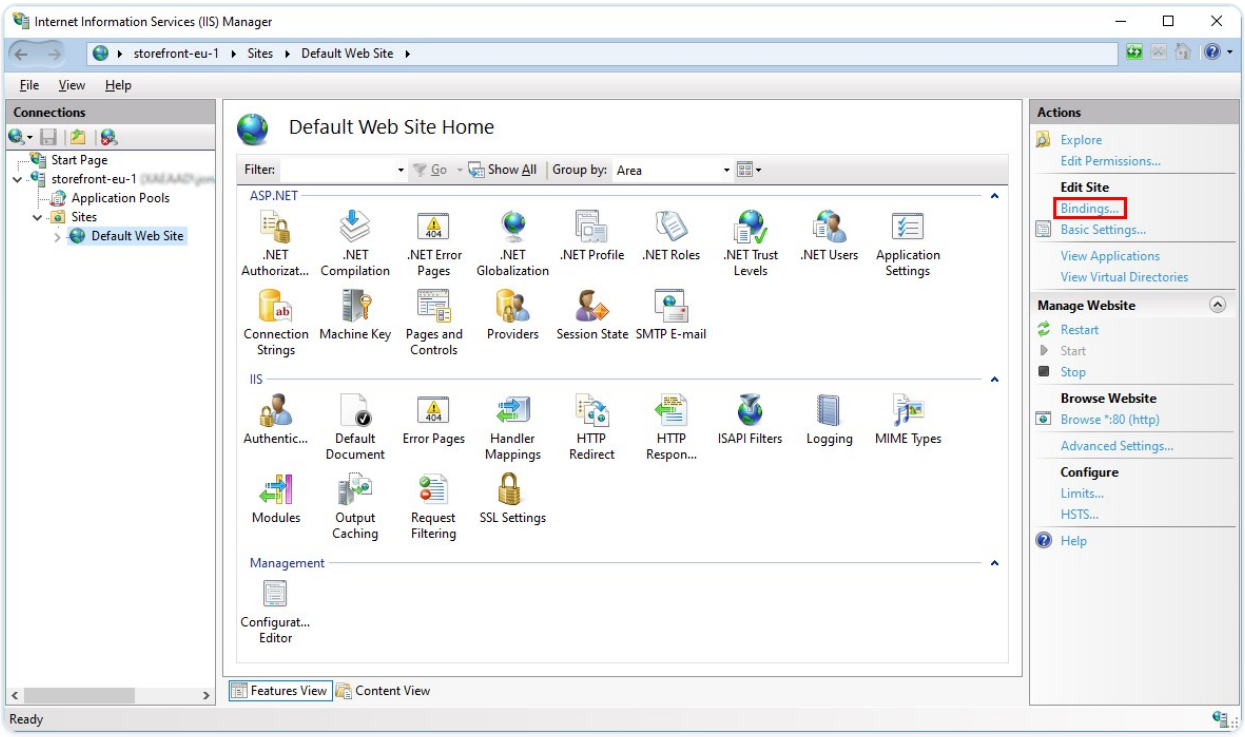
For more information on managing certificates, see Manage certificates.

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...**

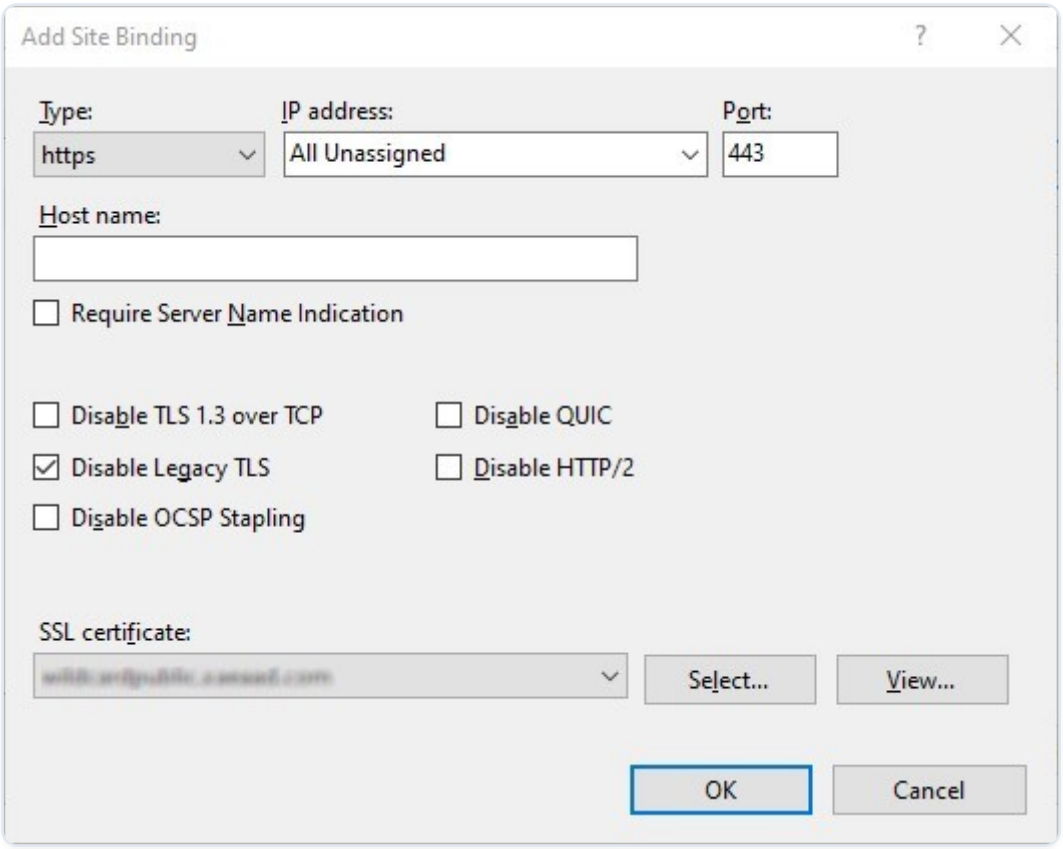
© 1997–2026 Citrix Systems, Inc. All rights reserved.



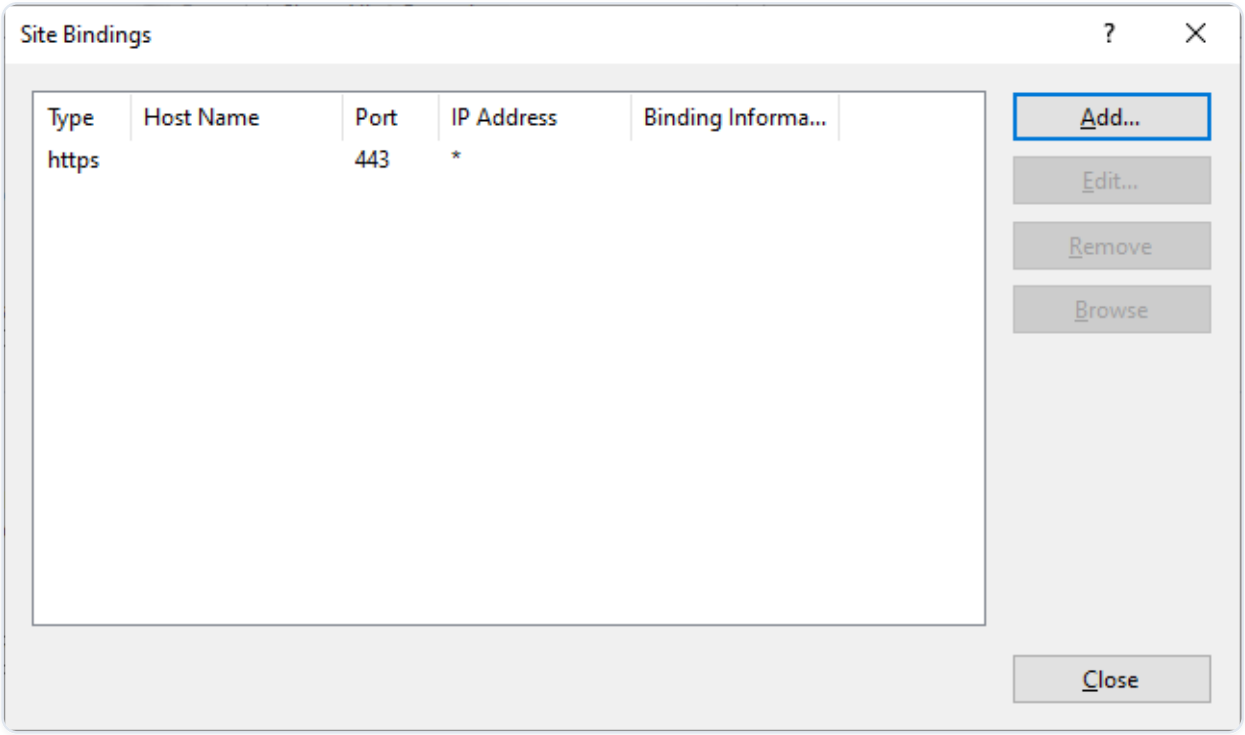
3. In the bindings window click **Add...**
4. In the **Type** drop down select **https**
5. On Windows Server 2022 or above, click **Disable Legacy TLS** to disable TLS older than 1.2.

   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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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



8. Update the base url to use the https protocol.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

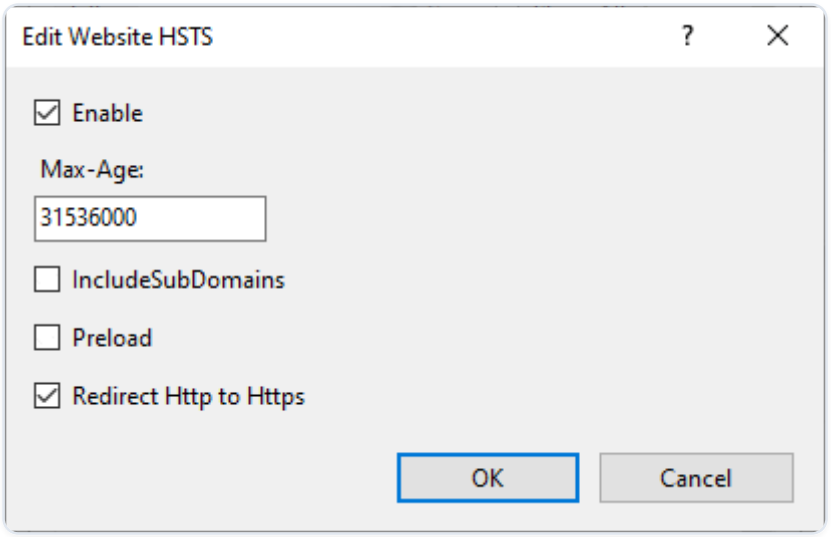
There are a number of options for enabling HSTS. You should choose only one option to avoid setting the same header multiple times.

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**

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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**.
7. Propagate configuration to other servers in the server group.

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.

Option 4 - NetScaler Gateway

If users connect to StoreFront via a NetScaler Gateway then you can configure HSTS on the VPN virtual server. This has the benefit that it also applies to the NetScaler log on form as well as the pages hosted by StoreFront.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Certificate Revocation List (CRL) checking

Introduction

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

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

NOTE:

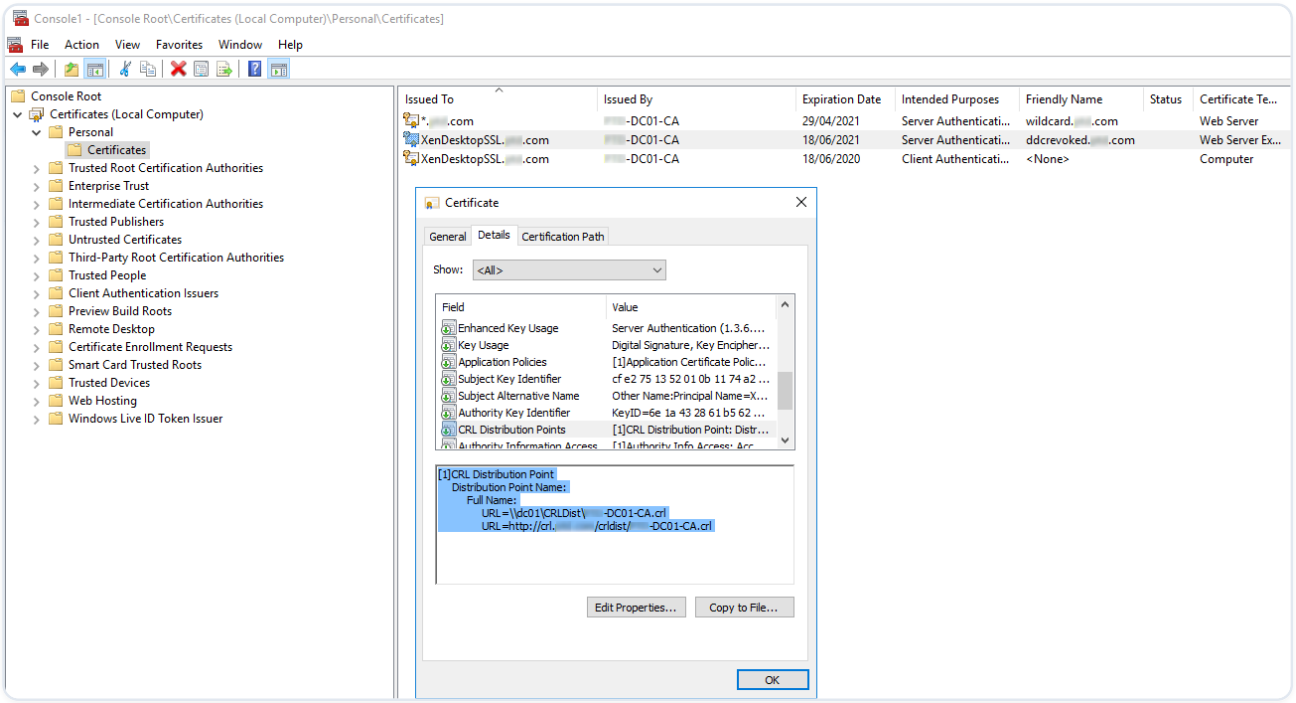
This topic is only relevant when HTTPS connections between StoreFront and Citrix Virtual Apps and Desktops delivery controllers are used. HTTP connections to delivery controllers do not require a certificate, so the -CertRevocationPolicy setting for the Store, described here, has no effect.

StoreFront supports certificate revocation checking using CRL Distribution Point (CDP) certificate extensions and locally installed certificate revocation lists (CRLs). StoreFront supports full CRLs only: delta CLRs are not supported.

CRL Distribution Points (CDP) extensions

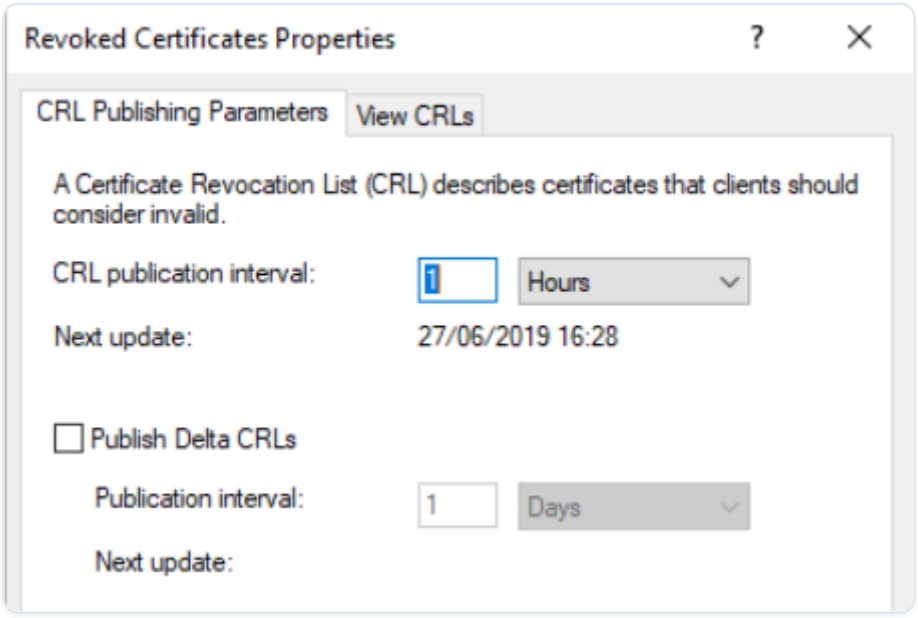
StoreFront does not enumerate resources from Citrix Virtual Apps and Desktops delivery controllers which are using revoked certificates whose serial numbers are listed in the published CRL. To detect which certificates have been revoked, StoreFront must be able to access the published CRL using one of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

© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
$store=Get-STFStoreService -VirtualPath '/Citrix/Store'

(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:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.
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 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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

SETTING	DESCRIPTION
	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:

```
$StoreVirtualPath = "/Citrix/Store"

$StoreObject = Get-STFStoreService -VirtualPath $StoreVirtualPath

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.

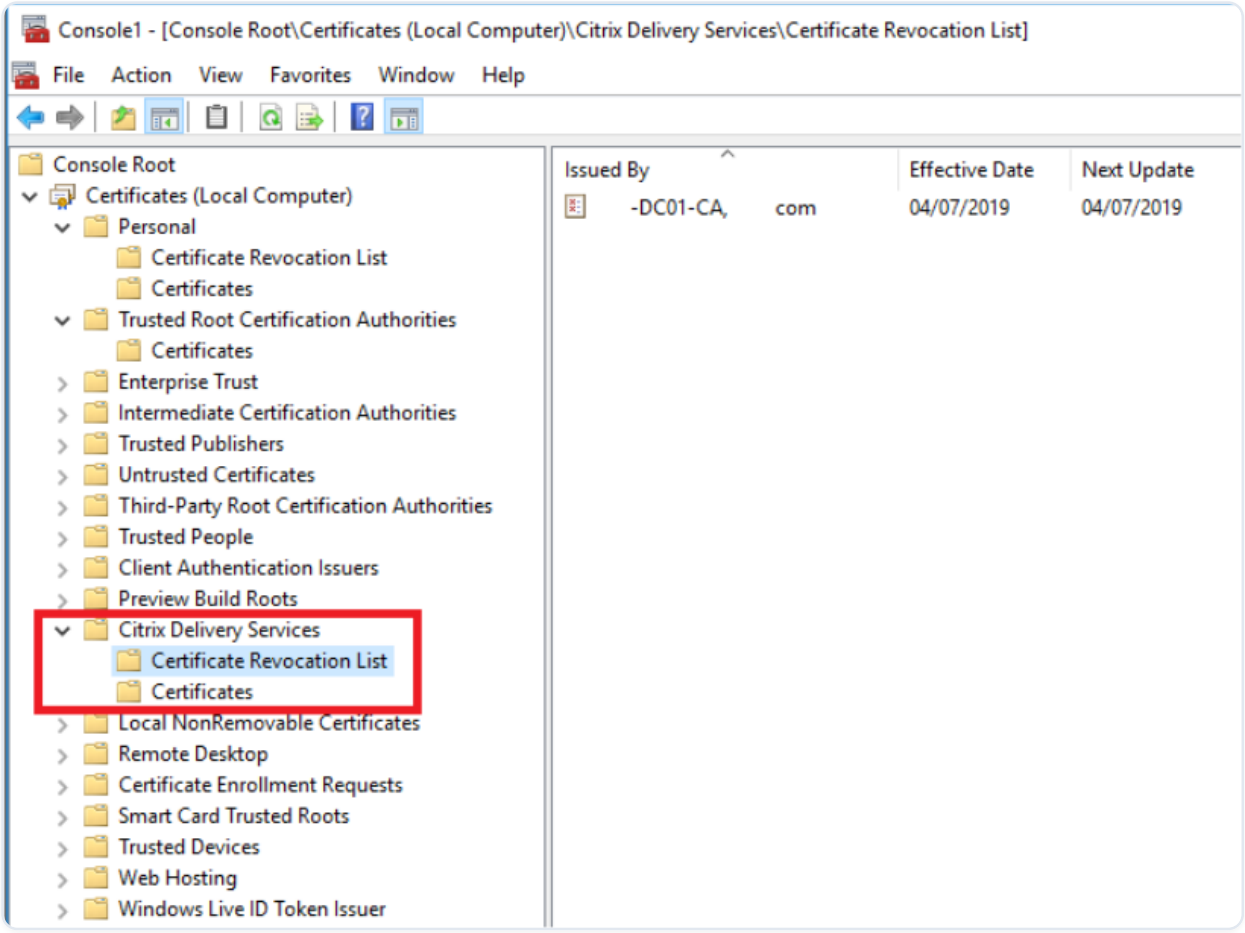
Using locally installed or updated CRLs can be used if -CertRevocationPolicy is set to "NoNetworkAccess", and you have the means to distribute the CRL efficiently to all StoreFront servers.

To use locally imported CLRs

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**.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

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

If successful, the following is returned:

```
Citrix Delivery Services

CRL "CN=Example-DC01-CA, DC=example, DC=com" added to store.

CertUtil: -addstore command completed successfully.
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
```

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 certificate revocation policy.
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

1. Open the PowerShell ISE and select **Run As Admin**.

```
$SiteID = 1

$StoreVirtualPath = "/Citrix/Store"

$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.

```
$StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
$StoreVirtualPath

$FarmObject = Get-STFStoreFarm -StoreService $StoreObject -FarmName
"CVAD"

$AuthObject = Get-STFAuthenticationService -SiteID $SiteID -VirtualPath
$AuthVirtualPath
```

3. Modify the CertRevocationPolicy property of the authentication service directly.

```
$AuthObject.FarmsConfiguration.CertRevocationPolicy = "FullCheck"

$AuthObject.Save()

Enable-STFXmlServiceAuthentication -AuthenticationService $AuthObject
-Farm $FarmObject
```

4. Confirm that you have set the correct certificate revocation mode.

```
$AuthObject = Get-STFAuthenticationService -SiteID 1 -VirtualPath
$AuthVirtualPath

$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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

```
An SSL connection could not be established: An error occurred during SSL
crytography: Access is denied.



This message was reported from the Citrix XML Service at address https://
deliverycontrollerTLS.domain.com/scripts/wpnbr.dll.



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

```
An unexpected response was received during the authentication process.



Citrix.DeliveryServicesClients.Authentication.Exceptions.ExplicitAuthentic
ationFailure,

Citrix.DeliveryServicesClients.Authentication, Version=3.20.0.0,

Culture=neutral, PublicKeyToken=null



General Authentication Failure



ExplicitResult.State: 5
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
AuthenticationControllerRequestUrl:

https://storefront.example.com/Citrix/StoreWeb/ExplicitAuth/LoginAttempt



ActionType: LoginAttempt



at

Citrix.Web.AuthControllers.Controllers.ExplicitAuthController.GetExplicitA
uthResult(ActionType

type, Dictionary`2 postParams)
```

ICA® file signing

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
$storeService = Get-STFStoreService

Set-STFStoreService $storeService -IcaFileSigning $true
-IcaFileSigningCertificateThumbprint [certificatethumbprint]
```

Where 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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Logs and Analytics

StoreFront generates a number of log files and telemetry. See the following topics.

TOPIC	DESCRIPTION
Log files	StoreFront creates various different log files for diagnostic purposes.
Event logs	StoreFront writes significant events and errors to the Windows event log.
Performance counters	StoreFront records performance counters that you can view using Performance Monitor.
Telemetry	StoreFront sends information on your configuration to Citrix Cloud.
Citrix Workspace app analytics	Configure Citrix Workspace app to send data to Citrix Analytics
Citrix Scout	Run Citrix Scout to collect log files and other system information to send to support

Log files

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.

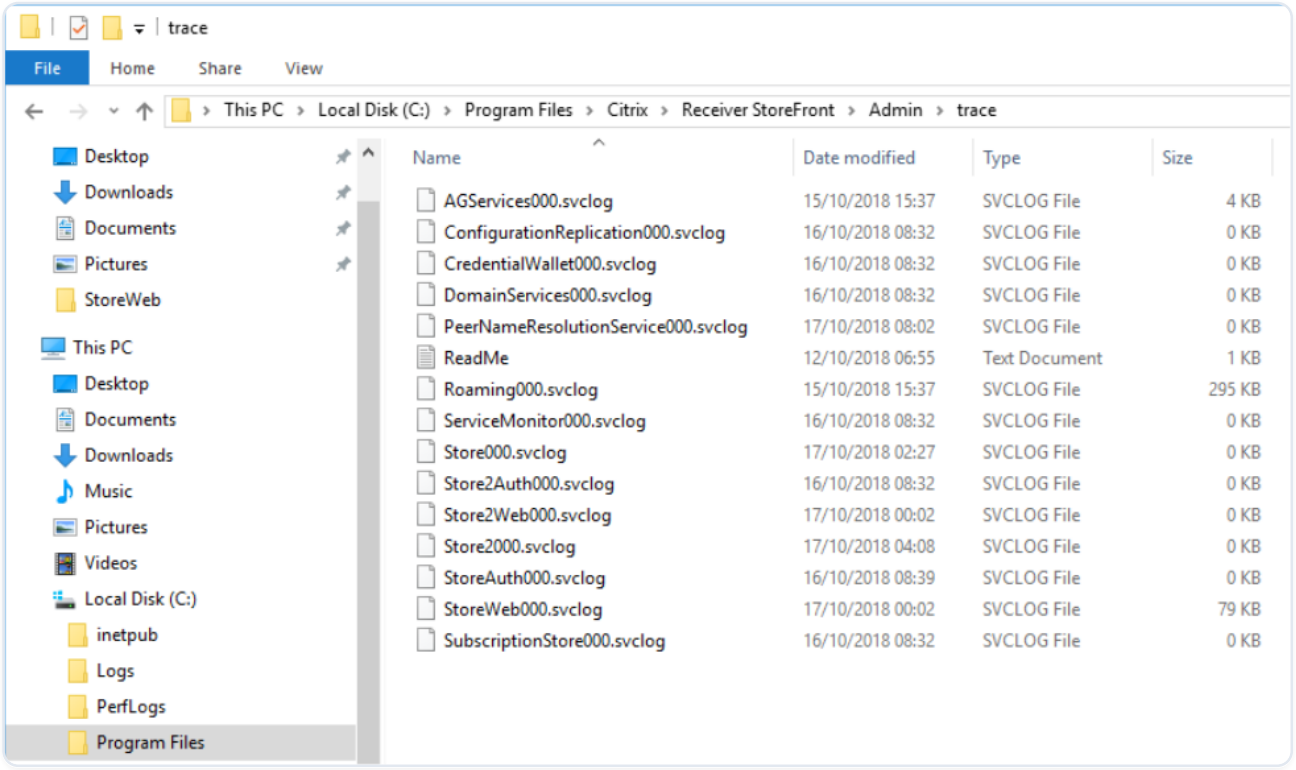
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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`



For StoreFront 2311 version and higher, by default, messages of level **Error**, **Warning**, and **Info** are logged. In most cases this includes sufficient information to diagnose any issues.

NOTE:

In 2308 and earlier versions of StoreFront, by default only messages of level **Error** are logged.

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

   ```
   Set-STFDiagnostics -All -TraceLevel "Verbose" -confirm:$False
   ```

   NOTE:

   If using StoreFront 2311, you must add the parameter `-Override`.

   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 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

   ```
   Set-STFDiagnostics -All -TraceLevel "Info" -confirm:$False
   ```

   NOTE:

   If using StoreFront 2311, you must add the parameter `-Override`.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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 storename is the name specified for the store when it was created.
2. Locate the following element in the file.

   ```
   <logger duplicateInterval="00:01:00" duplicateLimit="10">
   ```

   By default, StoreFront is configured to limit the number of duplicate log entries to 10 per minute.
3. Change the value of the duplicateInterval attribute to 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

StoreFront writes a number of performance counters. To view the counter values:

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Payload

FIELD	DESCRIPTION	EXAMPLE
ver	The version of the payload	1.2
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. **Some values are scrambled**	Example
rfWebSites	The StoreFront website configuration JSON blob. An array of RFWeb Config objects	Example
gateways	The gateway configuration objects as JSON blob. An array of gateway objects	Example
authServices	The Auth service configuration objects as	Example

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FIELD	DESCRIPTION	EXAMPLE
	JSON blob. An array of auth services objects	
IsPiiScrambled	Is the PII in the payload scrambled?	true
baseURLs	An array of the list of base URLs used by this server	["https://storefront.acme.com", "https://storefront.acme2.com"]
serversInGroup	The list of StoreFront servers in the server group	["storefront-a.acme.com", "storefront-b.acme.com", "storefront-c.acme.com"]
osName	The name of the OS	Windows Server 2025
osVersion	The version number of the OS	26100.7178
wasUpgraded	Was the server upgraded from a previous version	true

Example of field stores

```
[{
            "SiteId": 1,
            "BaseURL": "https://storefront.example.com/",
            "VirtualPath": "/Citrix/Store",
            "EnabledFeatures": 21 bit bitmap,
            "DefaultRfWebSite": "/Citrix/StoreWeb",
            "GatewaysUsed": [
                "gatewayId"
            ],
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
            "VdaLogonDataProvider": "",
            "ResourceFeeds": [
                {
                    "FeedName": "CVAD-US",
                    "Type": 1,
                    "LoadBalancingEnabled": true,
                    "Servers": ["ddc-1.acme.com", "ddc-2.acme.com"],
                    "TransportType": "https",
                    "AutoDiscoverServers": false,
                    "UseKeys": false
                }
            ]
}]
```

If no Stores are found, it is an empty array .

Example of field rfWebSites

```
[{
    "SiteId": 1,
    "BaseURL": "https://storefront.example.com/",
    "VirtualPath": "/Citrix/StoreWeb",
    "StorePath": "/Citrix/Store",
    "UiExperience": 0,
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    "EnabledFeatures": 9 bit,
    "AuthMethodsEnabled": [
        "ExplicitForms"
    ],
    "LogoffAction": 0,
    "MultiClickTimeout": 3,
    "DefaultTab": 0
}]
```

If no rfWebSites are found, it is an empty array .

Example of field gateways

```
[{
            "GatewayId": "0bb792c4-37b4-4fbe-a9a6-5ed71baaa603",
            "GatewayURL": "https://sfgw.acme.com",
            "IsCloudGateway": false,
            "StasUseLoadBalancing": true,
            "SessionReliability": true,
            "RequestTicketTwoStas": true,
            "SmartCardFallback": false,
            "Version": 1234,
            "Logon": "domain",
            "StaServers": [
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
                {"url": "sta1.example.com", "useKeys": true},
                {"url": "sta2.example.com", "useKeys": true}
            ]
}]
```

If no gateways are found, it is an empty array .

Example of field authServices

```
[{
    "SiteId": 1,
    "BaseURL": "https://storefront.example.com/",
    "VirtualPath": "/Citrix/Authentication",
    "AuthMethodsEnabled": [
        "CitrixFederation",
        "ExplicitForms"
    ],
    "AllowUserPasswordChange": 2,
    "ShowPasswordExpiryWarning": 1,
    "ValidatePasswordsOnDeliveryControllers": false,
    "DelegateCredentialValidationToGateway": false,
    "IsAuthenticationServiceShared": false,
    "EnabledFeatures": 1,
    "isThirdPartyAuthSdkInUse": false
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
}]
```

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. **The value is scrambled**	fullName: C648FE671A44B3F7 **(always scrambled)** samName:C758LH671A44B3F7

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FIELD	DESCRIPTION	EXAMPLE
		(always scrambled) upn: C7948FE671A44B3F7 **(always scrambled)** userLicenseId:C265FE671A44B3F7 **(always scrambled)** userSid: C097FE671A44B3F7 **(always scrambled)**
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 Linux/ 5.17.15 X1Class CWACapable CWA/ 22.11.0.19

© 1997–2026 Citrix Systems, Inc. All rights reserved.

FIELD	DESCRIPTION	EXAMPLE
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. **The values is scrambled**	john-doe
transactionId	Identifier used to group related events	773aba9e-5b91-4ef9-8782-c4afb75698e7

Citrix Workspace app analytics

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

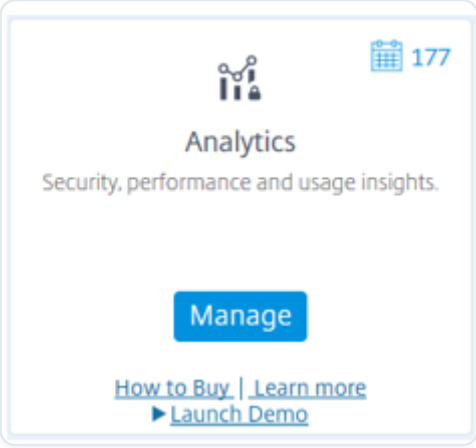
Your StoreFront deployment must be able to contact Citrix API Services. See Analytics network requirements.

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 *StoreFrontConfigurationFile.json* file.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Example configuration file

```
{

  "customerId": "<yourcloudcustomer>",

  "enablementService": " https://api.analytics.cloud.com /casvc/
<yourcloudcustomer>/ctxana/v1/cas/<yourcloudcustomer>/XenDesktop/
<deviceid>/dsconfigdata",

  "cwsServiceKey": "PFJTPn…….. T4=",

  "enablementServiceStatus": " https://api.analytics.cloud.com /casvc/
<yourcloudcustomer>/ctxana/v1/cas/storefront/config",

  "instanceId": "d98f21d0-56e0-11e9-ba52-5136d90862fe",

  "name": "CASSingleTenant"

}
```

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

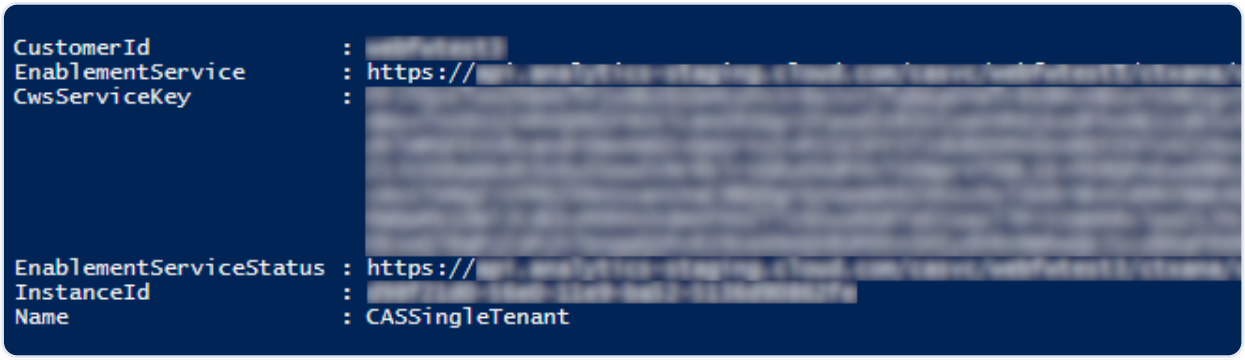
1. Copy the *StoreFrontConfigurationFile.json* file to a suitable folder on the on-premises StoreFront server (or one server in a StoreFront server group). The following commands assume that the file is saved to the Desktop.
2. Open PowerShell ISE and select **Run as Administrator**.
3. Run the following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

```
Import-STFCasConfiguration -Path
"$Env:UserProfile\Desktop\StoreFrontConfigurationFile.json"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
Get-STFCasConfiguration
```

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



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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

```
$WebConfigPath = "C:\Program Files\Citrix\Receiver
StoreFront\Framework\FrameworkData\Framework.xml"

$XMLObject = (Get-Content $WebConfigPath) -as [Xml]

$XMLObject.framework.properties.property
```

For example, these commands generate output like the following:

```
name value

---- -----

ClusterId 8b8ff5c8-44ba-46e4-87f0-2df8cff31432

HostBaseUrl https://storefront.example.com/

SelectedIISWebSiteId 1

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:

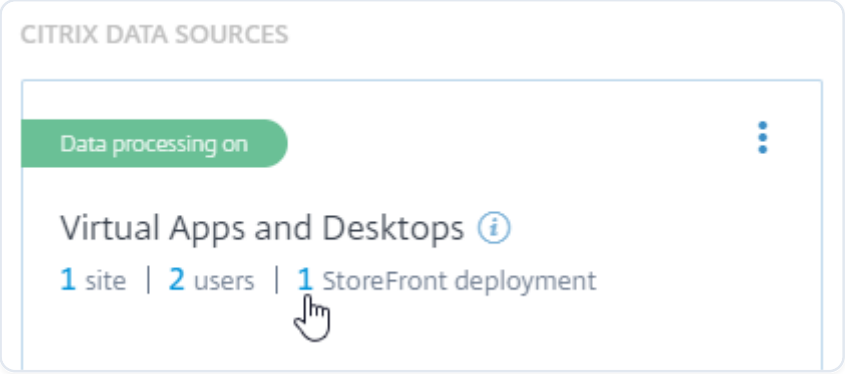
   `Publish-STFServerGroupConfiguration`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

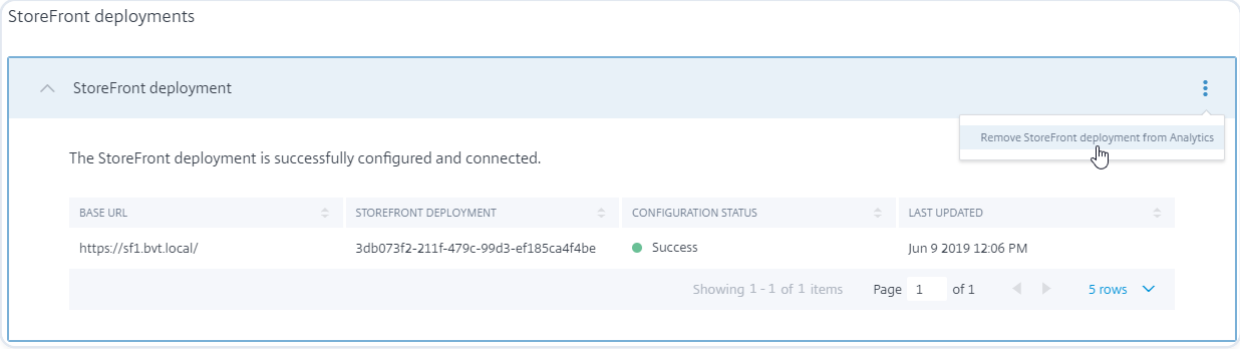
4. On any other server group members, run the following command to confirm that Citrix Analytics configuration has been successfully removed from all servers in the group:

   ```
   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:



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**.



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).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

```
$Stores = @("Store","Store2")

$ProxyIP = "10.0.0.1"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
$ProxyFQDN = "proxyserver.example.com"

$ProxyPort = 8888



# Set this for every Store using Stores array

function Set-StoreProxyServer() # Tested with both IP and FQDN

{

    [CmdletBinding()]

    param([Parameter(Mandatory=$true,ParameterSetName="ProxyIP")]
[Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][array]
$Stores,

        [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")][string]
$ProxyIP,

        [Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")]
[string]$ProxyFQDN,

        [Parameter(Mandatory=$true,ParameterSetName="ProxyIP")]
[Parameter(Mandatory=$true,ParameterSetName="ProxyFQDN")][int]
$ProxyPort)



    foreach($Store in $Stores)

    {

        Write-Host "Backing up the Store web.config file for store
$Store before making changes..." -ForegroundColor "Yellow"

        Write-Host "`n"



        if(!(Test-Path "$env:UserProfile\desktop\$Store\"))
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        {

            Write-Host "Creating $env:UserProfile\desktop\$Store\
directory for backup..." -ForegroundColor "Yellow"

            New-Item -Path "$env:UserProfile\desktop\$Store\" -ItemType
"Directory" | Out-Null

            Write-Host "`n"

        }



        Write-Host "Copying c:\inetpub\wwwroot\Citrix\$Store\web.config
to $env:UserProfile\desktop\$Store\..." -ForegroundColor "Yellow"

        Copy-Item -Path "c:\inetpub\wwwroot\Citrix\$Store\web.config"
-Destination "$env:UserProfile\desktop\$Store\" -Force | Out-Null



        if(Test-Path "$env:UserProfile\desktop\$Store\web.config")

        {

            Write-Host "$env:UserProfile\desktop\$Store\web.config file
backed up" -ForegroundColor "Green"

        }

        else

        {

            Write-Host "$env:UserProfile\desktop\$Store\web.config file
NOT found!" -ForegroundColor "Red"

        }

        Write-Host "`n"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        Write-Host "Setting the proxy server to $ProxyAddress for Store
$Store..." -ForegroundColor "Yellow"

        Write-Host "`n"



        $StoreConfigPath = "c:\inetpub\wwwroot\Citrix\
$Store\web.config"

        $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]



        if([string]::IsNullOrEmpty($ProxyFQDN))

        {

            $ProxyServer = ("HTTP://$ProxyIP"+":"+$ProxyPort)

        }

        else

        {

            $ProxyServer = ("HTTP://$ProxyFQDN"+":"+$ProxyPort)

        }



        $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]



        # Create 3 elements

        $SystemNet = $XMLObject.CreateNode("element","system.net","")

        $DefaultProxy =
$XMLObject.CreateNode("element","defaultProxy","")
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        $Proxy = $XMLObject.CreateNode("element","proxy","")

        $Proxy.SetAttribute("proxyaddress","$ProxyServer")

        $Proxy.SetAttribute("bypassonlocal","true")



        # Move back up the XML tree appending new child items in
reverse order

        $DefaultProxy.AppendChild($Proxy)

        $SystemNet.AppendChild($DefaultProxy)

        $XMLObject.configuration.AppendChild($SystemNet)



        # Save the modified XML document to disk

        $XMLObject.Save($StoreConfigPath)



        Write-Host "Getting the proxy configuration for c:
\inetpub\wwwroot\Citrix\$Store..." -ForegroundColor "Yellow"

        $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]

        $ConfiguredProxyServer =
$XMLObject.configuration.'system.net'.defaultProxy.proxy.proxyaddress |
Out-Null

        Write-Host ("Configured proxy server for Store $Store"+": "+
$ConfiguredProxyServer) -ForegroundColor "Green"

        Write-Host "`n"

    }

    Write-Host "Restarting IIS..." -ForegroundColor "Yellow"
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
    IISReset /RESTART

}



Set-StoreProxyServer -Stores $Stores -ProxyFQDN $ProxyFQDN -ProxyPort
$ProxyPort

# OR

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.

```
        </dependentAssembly>

    </assemblyBinding>

</runtime>

<system.net>

    <defaultProxy>

    <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
bypassonlocal="true" />

    </defaultProxy>

</system.net>

</configuration>
```

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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:

   ```
   <system.net>

       <defaultProxy>

       <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
   bypassonlocal="true" />

       </defaultProxy>

   </system.net>
   ```

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

   ```
   <system.net>

       <defaultProxy>

       <proxy proxyaddress="HTTP://10.0.0.1:8888" bypassonlocal="true" />

       </defaultProxy>

   </system.net>
   ```

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
<runtime>

<gcServer enabled="true" />

<assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">

    <dependentAssembly>

    <assemblyIdentity name="System.Web.MVC"
publicKeyToken="31BF3856AD364E35" culture="neutral" />

    <bindingRedirect oldVersion="0.0.0.0-5.0.0.0"
newVersion="5.0.0.0" />

    </dependentAssembly>

    <dependentAssembly>

    <assemblyIdentity name="Newtonsoft.Json"
publicKeyToken="30ad4fe6b2a6aeed" culture="neutral" />

    <bindingRedirect oldVersion="0.0.0.0-9.0.0.0"
newVersion="9.0.0.0" />

    </dependentAssembly>

</assemblyBinding>

</runtime>



Insert the <system.net> element here



</configuration>
```

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

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Deprecation notices

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	

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ITEM	DEPRECATION ANNOUNCED IN VERSION	REMOVED IN VERSION	ALTERNATIVE
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.
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	3.14	2203	Upgrade Citrix Receivers to a Citrix

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ITEM	DEPRECATION ANNOUNCED IN VERSION	REMOVED IN VERSION	ALTERNATIVE
Citrix Virtual Apps and Desktops and Citrix Workspace app.			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 Desktop Lock for non-domain-joined use cases.
Citrix classic experience (“green bubbles” user interface)	3.12	1903	Use the Unified UI

© 1997–2026 Citrix Systems, Inc. All rights reserved.

ITEM	DEPRECATION ANNOUNCED IN VERSION	REMOVED IN VERSION	ALTERNATIVE
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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Third Party Notices

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Licensed under the Microsoft Public License (MS-PL)

Microsoft .Net Reference Source

Copyright © Microsoft Corporation. Licensed under the MIT license.

ManagedEsent Release 1.9.4

Copyright © Microsoft Corporation.

Licensed under the Microsoft Public License (MS-PL).

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 by Jorik Tangelder <j.tangelder@gmail.com>;

Licensed under the MIT license

jQuery MouseWheel

Copyright (c) 2011 Brandon Aaron (http://brandonaaron.net)

Licensed under the MIT License (LICENSE.txt).

Extended WPF Toolkit 3.8.2

Copyright (C) 2010-2020 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>`

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)

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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 10

The MIT License (MIT)

Copyright (c) .NET Foundation and Contributors

CoreWCF 1.8

Copyright .NET Foundation

License: MIT

Project URL: `<https://github.com/CoreWCF/CoreWCF>`

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Azure SDK for .NET

Copyright (c) 2015 Microsoft. Licensed under the MIT License.

AspNetWebStack

Copyright (c) .NET Foundation. All rights reserved.

Licensed under the Apache License, Version 2.0

Microsoft Graph SDK

Copyright 2019 Microsoft Graph

Licensed under the MIT License.

Microsoft Graph Core SDK

Copyright 2019 Microsoft Graph

Licensed under the MIT License.

AspNet Logging

Copyright (c) .NET Foundation and Contributors

Licensed under the Apache License, Version 2.0

Microsoft AzureAD IdentityModel Extensions for .NET

Copyright (c) Microsoft Corporation. Licensed under the MIT license.

Microsoft .NET Kiota

The MIT License (MIT)

Copyright (c) Microsoft Corporation

Microsoft.Web.Infrastructure 1.0

Copyright (c) Microsoft Corporation. Licensed under the Microsoft Software License (MS-SL).

© 1997–2026 Citrix Systems, Inc. All rights reserved.

Std-UriTemplate

Copyright (c) 2023 std-uritemplate Licensed under the Apache License, Version 2.0

Microsoft .NET Maintenance Packages

Copyright (c) .NET Foundation and Contributors. Licensed under the MIT license.

APPENDIX: Referenced Licenses

MIT License

```
Permission is hereby granted, free of charge, to any person obtaining a
copy

of this software and associated documentation files (the "Software"), to
deal

in the Software without restriction, including without limitation the
rights

to use, copy, modify, merge, publish, distribute, sublicense, and/or sell

copies of the Software, and to permit persons to whom the Software is

furnished to do so, subject to the following conditions:



The above copyright notice and this permission notice shall be included in

all copies or substantial portions of the Software.



THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR

IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY,

FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL
THE
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER

LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING
FROM,

OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN

THE SOFTWARE.
```

Apache License, Version 2.0

```
                                 Apache License

                           Version 2.0, January 2004

                        http://www.apache.org/licenses/



TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION


1. Definitions.


   "License" shall mean the terms and conditions for use, reproduction,

   and distribution as defined by Sections 1 through 9 of this document.


   "Licensor" shall mean the copyright owner or entity authorized by

   the copyright owner that is granting the License.


   "Legal Entity" shall mean the union of the acting entity and all
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
other entities that control, are controlled by, or are under common
control with that entity. For the purposes of this definition,
"control" means (i) the power, direct or indirect, to cause the
direction or management of such entity, whether by contract or
otherwise, or (ii) ownership of fifty percent (50%) or more of the
outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity
exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications,
including but not limited to software source code, documentation
source, and configuration files.

"Object" form shall mean any form resulting from mechanical
transformation or translation of a Source form, including but
not limited to compiled object code, generated documentation,
and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or
Object form, made available under the License, as indicated by a
copyright notice that is included in or attached to the work
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

(an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner 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 excluding communication that is conspicuously marked or otherwise

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   designated in writing by the copyright owner as "Not a Contribution."

   "Contributor" shall mean Licensor and any individual or Legal Entity
   on behalf of whom a Contribution has been received by Licensor and
   subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of
   this License, each Contributor hereby grants to You a perpetual,
   worldwide, non-exclusive, no-charge, royalty-free, irrevocable
   copyright license to reproduce, prepare Derivative Works of,
   publicly display, publicly perform, sublicense, and distribute the
   Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of
   this License, each Contributor hereby grants to You a perpetual,
   worldwide, non-exclusive, no-charge, royalty-free, irrevocable
   (except as stated in this section) patent license to make, have made,
   use, offer to sell, sell, import, and otherwise transfer the Work,
   where such license applies only to those patent claims licensable
   by such Contributor that are necessarily infringed by their
   Contribution(s) alone or by combination of their Contribution(s)
   with the Work to which such Contribution(s) was submitted. If You
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   institute patent litigation against any entity (including a
   cross-claim or counterclaim in a lawsuit) alleging that the Work
   or a Contribution incorporated within the Work constitutes direct
   or contributory patent infringement, then any patent licenses
   granted to You under this License for that Work shall terminate
   as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the
   Work or Derivative Works thereof in any medium, with or without
   modifications, and in Source or Object form, provided that You
   meet the following conditions:

   (a) You must give any other recipients of the Work or
       Derivative Works a copy of this License; and

   (b) You must cause any modified files to carry prominent notices
       stating that You changed the files; and

   (c) You must retain, in the Source form of any Derivative Works
       that You distribute, all copyright, patent, trademark, and
       attribution notices from the Source form of the Work,
       excluding those notices that do not pertain to any part of
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
        the Derivative Works; and


    (d) If the Work includes a "NOTICE" text file as part of its
        distribution, then any Derivative Works that You distribute must
        include a readable copy of the attribution notices contained
        within such NOTICE file, excluding those notices that do not
        pertain to any part of the Derivative Works, in at least one
        of the following places: within a NOTICE text file distributed
        as part of the Derivative Works; within the Source form or
        documentation, if provided along with the Derivative Works; or,
        within a display generated by the Derivative Works, if and
        wherever such third-party notices normally appear. The contents
        of the NOTICE file are for informational purposes only and
        do not modify the License. You may add Your own attribution
        notices within Derivative Works that You distribute, alongside
        or as an addendum to the NOTICE text from the Work, provided
        that such additional attribution notices cannot be construed
        as modifying the License.


    You may add Your own copyright statement to Your modifications and
    may provide additional or different license terms and conditions
    for use, reproduction, or distribution of Your modifications, or
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions

© 1997–2026 Citrix Systems, Inc. All rights reserved.

of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   on Your own behalf and on Your sole responsibility, not on behalf

   of any other Contributor, and only if You agree to indemnify,

   defend, and hold each Contributor harmless for any liability

   incurred by, or claims asserted against, such Contributor by reason

   of your accepting any such warranty or additional liability.



END OF TERMS AND CONDITIONS
```

Microsoft Public License (MS-PL)

```
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.



1. Definitions

   The terms “reproduce,” “reproduction,” “derivative works,” and
“distribution” have the

   same meaning here as under U.S. copyright law.



   A “contribution” is the original software, or any additions or changes
to the software.



   A “contributor” is any person that distributes its contribution under
this license.



   “Licensed patents” are a contributor’s patent claims that read directly
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

on its contribution.

2. Grant of Rights

(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.

(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.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors’ name, logo, or trademarks.

(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.

(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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   (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.



   (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

```
Redistribution and use in source and binary forms, with or without

modification, are permitted provided that the following conditions are
met:



1. Redistributions of source code must retain the above copyright notice,
this

   list of conditions and the following disclaimer.



2. Redistributions in binary form must reproduce the above copyright
notice,

   this list of conditions and the following disclaimer in the
documentation

   and/or other materials provided with the distribution.



3. Neither the name of the copyright holder nor the names of its
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

```
   contributors may be used to endorse or promote products derived from

   this software without specific prior written permission.



THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS
IS"

AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE

IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE
ARE

DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE
LIABLE

FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL

DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR

SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER

CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY,

OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE
USE

OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

Microsoft Reciprocal License (Ms-RL)

```
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.



1. Definitions

The terms "reproduce," "reproduction," "derivative works," and
```

© 1997–2026 Citrix Systems, Inc. All rights reserved.

"distribution" have the same meaning here as under U.S. copyright law.

A "contribution" is the original software, or any additions or changes to the software.

A "contributor" is any person that distributes its contribution under this license.

"Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(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.

(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.

3. Conditions and Limitations

(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.

(B) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

(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.

(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.

(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.

(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.

© 1997–2026 Citrix Systems, Inc. All rights reserved.

StoreFront Document History

The following table describes important changes to the StoreFront product documentation. To receive notifications about these updates, subscribe to the RSS feed.

DATE	CHANGE	DESCRIPTION
18 Aug 2026	Release of StoreFront 2607 LTSR	For details, see What's new.

© 1997–2026 Citrix Systems, Inc. All rights reserved.