Citrix® StoreFront 2402

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

Contents

StoreFront 2402 Long Term Service Release Overview 25
- What's new 25
- Earlier releases 25
- Support lifecycle 26

What's new 27
- Cumulative Update 4 (CU4) 27
  - About this release 27
    - Citrix Workspace app for HTML5 27
  - What's new in 2402 LTSR CU4 27
  - Fixed issues in 2402 LTSR CU4 27
- Cumulative Update 3 (CU3) 28
  - About this release 29
  - System requirements 29
  - Citrix Workspace app for HTML5 29
  - What's new in 2402 LTSR CU3 29
    - Citrix Licensing Telemetry 29
  - Fixed issues in 2402 LTSR CU3 29
- Cumulative Update 2 (CU2) 30
  - About this release 30
  - Citrix Workspace app for HTML5 30
  - What's new in 2402 LTSR CU2 31
    - Modern experience - General availability 31
  - Fixed issues in 2402 LTSR CU2 32
- Cumulative Update 1 (CU1) 33
  - About this release 33
  - Citrix Workspace app for HTML5 33

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

What's new in 2402 LTSR CU1 33
Enable advanced health check for all stores 34
Fixed issues 34
What's new in 2402 (initial release) 35
Prevent .ica® file downloads during Hybrid launch 35
Enable advanced health check for all stores 36
Deprecation announcement for Windows server 2016 37
Citrix Secure Private Access on StoreFront 37
Uninterrupted VDA launch in case of FAS server unavailability 37
Improved user-journey logs 37
Citrix® web extensions - General Availability 37
New UI for on-premises stores (Technical Preview) 38
Citrix Workspace app for HTML5 39
App Protection for hybrid launches 39
Advanced health check enabled by default 39
Deprecation of XenApp® Services 39
Removal of ability to add XenApp 6.5 delivery controllers 40
Removal of ability to open resources within Internet Explorer 11 40
Fixed Issues 40
Known issues in 2402 41
2402 LTSR Cumulative Update 4 (CU4) 41
2402 LTSR Cumulative Update 3 (CU3) 41
2402 LTSR Cumulative Update 2 (CU2) 41
2402 LTSR Cumulative Update 1 (CU1) 42
2402 initial release 42
Install, set up, upgrade, and uninstall 43
Plan your StoreFront deployment 44
Active Directory 44

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

StoreFront Server groups 45
Load balancing 45
Citrix Gateway for remote access 45
Global Server Load Balancer 46
User access 47
User access 47
Citrix Workspace™ app 48
Beacons 48
Require use of Citrix Workspace app 48
Add Store to Citrix Workspace App 49
Global App Config Service 50
Web browser 50
Requirements for opening resources in your browser 51
Hybrid Launch 51
Citrix web extensions 51
Citrix Workspace launcher 52
Internet Explorer 54
ICA file downloads 54
Resource shortcuts 55
XenApp Services URLs 55
Important considerations 56
System requirements 56
StoreFront server requirements 56
Software 56
Hardware 58
Network 59
Active directory 60
Storing subscription data using Microsoft SQL Server 60

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

Infrastructure requirements 60
Citrix Virtual Apps and Desktops™ 60
Citrix Gateway 61
User device requirements 61
Locally installed Citrix Workspace app 61
Web browsers 61
Legacy devices 62
Smart card requirements 63
Using Citrix Workspace app with smart cards 63
Citrix Analytics service requirements 63
Install StoreFront 63
Before installing and configuring 63
Install StoreFront 64
To install StoreFront at a command prompt 65
.Net Framework 4.8 reboot step with Windows Server 2019 66
Installing as part of Citrix Virtual Apps and Desktops™ 67
Installation logs 67
Configure StoreFront 67
Citrix Customer Experience Improvement Program 68
CEIP data collected from StoreFront 69
Citrix Analytics service 70
Download the configuration file from Citrix Analytics 71
Example configuration file 71
Import Citrix Analytics data into your StoreFront™ deployment 72
Propagate Citrix Analytics data to a StoreFront server group 73
Check StoreFront server group ID 73
Stop sending data to Citrix Analytics from StoreFront 74
Configure StoreFront to use a web proxy to contact monitor and register with Citrix Analytics 76

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

Method 1: Set the store proxy configuration via PowerShell for one or more stores (recommended) 76

Method 2: Manually add a `<system.net>` section to the store web.config file 82

Securing StoreFront with HTTPS 84

Create or import certificate 84

Create certificate using Windows Certification Authority 84

Import existing certificate 86

Configure IIS for HTTPS 87

Change StoreFront server base URL from HTTP to HTTPS 89

HSTS 90

Secure your StoreFront deployment 91

End user authentication 92

Communication with end-users 92

Communication with Delivery Controllers 92

Communication with Cloud Connectors 93

Communication with Federated Authentication Service 93

Remote access 93

Microsoft Internet Information Services (IIS) hardening 93

Filename extensions 93

Verbs 94

Non-Ascii characters in URLs 95

MIME Types 95

Remove X-Powered-By Header 95

Remove Server header with IIS version 95

Move the StoreFront website to a separate partition 95

IIS features 95

Handler Mappings 96

ISAPI filters 96

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

.NET Authorization Rules 96
Retail mode 96
Application Pools 96
Default IIS landing page 97
Required settings 97
Services 97
User rights assignment 97
Configure group memberships 98
NTLM 99
Certificates in StoreFront 100
Server certificates 100
Token management certificates 100
Citrix Delivery Services certificates 100
Code signing certificates 100
StoreFront security separation 101
ICA downloads 101
ICA file signing 101
App protection 101
User change password 101
Customizations 102
Security Headers 102
Cookies 103
Additional security information 104
Email-based account discovery 104
Global App Config Service 104
DNS SRV records records 104
DNS discoverReceiver record 105
Create a new deployment 105

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

Create a new deployment using the PowerShell SDK 107
Multiple Internet Information Services (IIS) websites 107
Join an existing server group 108
Upgrade StoreFront™ 110
Supported upgrade paths 110
Good to know 110
Get ready to upgrade 111
Upgrade a single StoreFront server 111
Upgrade a StoreFront server group during scheduled maintenance downtime 112
Upgrade a StoreFront server group without scheduled downtime 112
Troubleshoot upgrade issues 114
Reset a server to factory defaults 114
Uninstall StoreFront 115
To manually remove StoreFront 116
Installation logs 116
Authentication 117
Authentication methods 117
Single sign-on to VDAs 118
Authentication method customizations 118
Configure authentication 118
Select authentication methods 118
Select authentication methods using PowerShell SDK 119
Authentication method settings 119
Shared authentication service settings 119
Install or uninstall authentication methods 120
Smart card authentication 120
Prerequisites 121
Configure StoreFront 121

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

Configure Delivery Controller™ to trust StoreFront 121
Remote access via Citrix Gateway 122
Single sign-on to VDAs 122
Important considerations 123
Domain pass-through authentication 124
StoreFront Configuration 124
Configure Delivery Controller™ to trust StoreFront 124
Web browser configuration 125
Internet Explorer, Edge and Chrome 125
FireFox 125
Single sign-on to VDAs 126
Pass-through from Citrix Gateway 126
Enable Gateway pass-through 127
Configure trusted user domains 127
Delegated authentication 128
PowerShell SDK 129
Password validation 129
Allow users to change expired passwords at logon 129
Allow users to change passwords after logon 130
PowerShell SDK 130
Configure Delivery Controller™ to trust StoreFront 131
Single sign-on to VDAs using Federated Authentication Service 131
SAML authentication 131
StoreFront™ SAML Endpoints 132
Configure using Metadata exchange 133
Configure Identity Provider 134
Configure Service Provider 136
PowerShell SDK 136

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

Testing 136
Configure Delivery Controller™ to trust StoreFront 137
Single sign-on to VDAs using Federated Authentication Service 137
User name and password authentication 137
Configure trusted user domains 138
PowerShell 139
Enable users to change their passwords 139
PowerShell 142
Password validation 142
PowerShell 145
Single sign-on to VDAs 145
Customize the logon screen 145
Title Text 145
Prevent Citrix Workspace app for Windows from caching passwords and usernames 146
Remote access via Citrix Gateway 147
Federated Authentication Service Configuration 147
Enable FAS for a Store 147
FAS server unavailability 148
Configure and manage stores 150
View Stores 150
Create a store 151
Store actions 151
Advanced configuration 152
Create store 153
PowerShell SDK 158
Configure a Store 159
Remove a store 160
Export store provisioning files for users 160

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

Advertise and hide stores to users 161
Kerberos delegation 162
PowerShell SDK 163
Manage sites and delivery controllers 163
View sites 163
View sites using the PowerShell SDK 163
Add sites 164
Add sites for Citrix Virtual Apps and Desktops™ 164
Add sites for Citrix Desktops as a Service 166
Add sites for Citrix Secure Private Access 168
Create a site using the PowerShell SDK 169
Modify a site 169
Modify a site using the PowerShell SDK 169
Delete a site 169
Delete a site using the PowerShell SDK 169
Health check and server bypass behavior 169
To change the bypass parameters 170
Map users to site 170
Map users to sites using PowerShell SDK 175
Multi-Site Aggregation 176
Advanced configurations using PowerShell SDK 182
Zone preference 184
Manage remote access to stores through Citrix Gateway 185
Certificate Revocation List (CRL) checking 187
Introduction 187
CRL Distribution Points (CDP) extensions 188
CRL publishing interval 188
Client CRL caching 189

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

StoreFront’s access to certificate revocation lists (CRLs) 189
View certificate revocation policy 190
Configure certificate revocation policy 190
Using locally imported CRLs on the StoreFront server 192
To use locally imported CLRs 192
To add the CRL to the Citrix Delivery Services certificate store via PowerShell or the command line 193
XML authentication using delivery controllers 194
To delegate user authentication to delivery controllers 194
Configure an XML authentication service for certificate revocation checking 194
Windows Event Viewer errors to expect 195
Example Error: Store cannot contact a delivery controller with a revoked certificate 196
Example Error: From Receiver for Web if user cannot log in due to failing XML authentication 196
Configure two StoreFront stores to share a common subscription datastore 197
StoreFront subscription datastore endpoints 198
Manage favorites for a store 199
Purge subscription data 199
Export subscription data 201
Restore subscription data 201
Restoring Data on a Single StoreFront Server 202
Restoring Data on a StoreFront Server Group 202
Import subscription data 203
Subscription data file details 203
Example 204
Size of subscription data on the StoreFront server disk 204
Size of import and export .txt files 204
Store Subscription Counters 205

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

View the Subscription Counters using PowerShell 205
Store subscription data using Microsoft SQL Server 206
Introduction 206
Advantages of ESENT and SQL server 207
Disadvantages of ESENT and SQL server 207
Deployment scenarios 208
Resources 211
Configure the StoreFront server's local security group on the SQL Server 212
Scenario 2: Single StoreFront Server and a local Microsoft SQL server instance installed 212
Scenario 3: StoreFront server group and a dedicated Microsoft SQL server instance 215
Configure the subscription database schema within Microsoft SQL Server for each store 218
Configure the SQL Server Connection String for each StoreFront store 221
Scenario 1 221
Scenarios 2, 3 and 4 222
Migrate existing data from ESENT into Microsoft SQL Server 223
Example: four SQL subscriptions for the same domain user 223
Update or delete existing subscription records using T-SQL 228
Enable or disable favorites 231
Citrix Virtual Apps and Desktops™ configuration 232
Keywords 232
Smart Access Tags 233
Advanced store settings 234
Address resolution type 235
Allow font smoothing 236
Allow session reconnect 236
Allow special folder redirection 236
Advanced health check 236
Background health check polling period 237

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

Communication time-out duration 237
Connection timeout 237
Enable enhanced enumeration 237
Enable socket pooling 238
File type association 238
Filter resources by excluded keywords 238
Filter resources by included keywords 239
Filter resources by type 240
Maximum concurrent enumerations 240
Minimum farms for concurrent enumeration 240
Override ICA® client name 240
Require token consistency 241
Server communication attempts 241
Show Desktop Viewer for legacy clients 241
Treat desktops as apps 241
Configure optimal HDX™ routing for a store 241
Example scenario using farms 242
Example scenario using zones 243
Configure Optimal HDX routing 245
Use PowerShell to configure optimal Citrix Gateway routing for a store 245
Subscription synchronization 246
Configure session settings 249
Example: Launch Notepad in windowed mode 250
ICA® file signing 251
Citrix Workspace™ app configuration 253
Global App Config service 253
Store account settings 253
Workspace app website 254

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

Manage a website 255
PowerShell 256
Create a website 256
Create a website using the PowerShell SDK 259
Configure website 259
UI Experience 261
PowerShell 262
Category Settings 263
Category view 264
Uncategorized apps 266
Hide categories view 266
Configure category settings using PowerShell SDK 267
Customize appearance 267
Edit logo and colors 267
Edit logo and colors using PowerShell SDK 268
Reset appearance to default 268
Reset appearance to default using PowerShell SDK 268
Customization using Javascript and CSS 268
Featured app groups 269
Create featured app group 269
Create featured app group using the PowerShell SDK 272
Edit featured app group 272
Edit featured app group using the PowerShell SDK 272
Delete featured app group 272
Delete featured app group using the PowerShell SDK 273
Authentication methods 273
Configure using PowerShell SDK 275
Website shortcuts 275

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

Add trusted websites using the management console 275
Add trusted websites using PowerShell SDK 277
Citrix Workspace app deployment 277
Require use of Citrix Workspace™ app 278
Supported platforms 278
Configure on StoreFront using classic experience 279
Configure using a Citrix Gateway 279
Deployment option 279
Launch applications in the same tab 280
Show the 'Already installed' link on the client detection page 280
Prevent Ica downloads on all platforms 282
Allow users to download Citrix Workspace app 282
Upgrade Workspace app on logon 282
Download source 282
PowerShell SDK 282
Configure session settings 283
Server communication attempts 283
Communication timeout duration 283
Session inactivity timeout 284
PowerShell 284
Sign in timeout 284
Authentication token lifetime 284
Citrix Gateway timeouts 285
Session time-out 285
Forced time-out 285
Maximum token lifetime of Authentication Service 286
Workspace control 287
Configure Workspace Control in a web browser 287

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

Configure Workspace Control using PowerShell SDK 289
Configure Workspace Control on Workspace app for Windows 289
Configure Workspace Control on Workspace app for Mac 289
Disable Workspace Control across all apps 289
Client Interface Settings 289
Auto launch desktop 290
Show Desktop Viewer 290
Multi-click duration 291
Enable Receiver/Workspace app configuration 291
Application and desktops view 291
Display Personalize your home screen for first time users 292
Show Activity manager 292
App Protection 293
App Protection for launches from Citrix Workspace app 293
App Protection for hybrid launch 293
Enable App Protection for hybrid launch 294
View whether App Protection for hybrid launch is enabled 295
Remove website 295
Configure Workspace app website 295
Advanced settings 296
Enable Fiddler tracing 296
Enable Folder view 296
Enable loopback communication 296
Enable Protocol Handler 297
Enable strict transport security 297
ICA® file cache expiry 297
Icon resolution 297
Loopback port when using HTTP 297

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

Prompt for untrusted shortcuts 297
Prompt to install Citrix Workspace™ app after Logon 298
Resource details 298
Strict transport security policy duration 298
Configure server groups 299
View server group 299
Add a server to a server group 299
Remove servers from a server group 299
Propagate local changes to a server group 300
Change the base URL for a deployment 301
Integrate with Citrix Gateway and NetScaler ADC 302
Configure Citrix Gateways 303
View Gateways 303
PowerShell 303
Add Citrix Gateway 303
PowerShell SDK 311
Edit Citrix Gateway 311
PowerShell SDK 311
Remove Citrix Gateway 311
PowerShell SDK 311
Import a Citrix Gateway 311
Requirements 311
Export configuration from Citrix Gateway 312
Import a Citrix Gateway using the console 313
Import multiple Citrix Gateways using PowerShell 319
Read-STFNetScalerConfiguration 319
Import-STFNetScalerConfiguration without specifying a CallbackURL 322
Import-STFNetScalerConfiguration specifying your own CallbackURL 322

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

Import-STFNetScalerConfiguration override the authentication method stored in the import file and specify your own CallbackURL 323

Load balancing with NetScaler® ADC 323

Create DNS records for the StoreFront server group load balancer 324

Configure StoreFront Servers 324

Optionally Configure Citrix Service monitor for HTTPS 324

Configure NetScaler Load Balancer 327

Install Root certificate 327

Install the server certificate 327

Add individual StoreFront server nodes to the NetScaler ADC appliance load balancer 329

Define a StoreFront monitor to check the status of all StoreFront nodes in the server group 329

Create a service group containing all of the StoreFront servers 330

Create a load balancing virtual server for user traffic 332

Configure StoreFront Loopback 335

Configure NetScaler ADC load balancer for subscription synchronization between server groups 336

Configure a service group for subscription synchronization 336

Create a load balancing virtual server for subscription synchronization 336

Configure StoreFront to pull subscription data via load balancer 337

Configure Citrix Gateway and StoreFront for Delegated Forms Authentication (DFA) 338

Installation recommendations 338

StoreFront cluster installation considerations 338

Enable Delegated Forms Authentication 338

Uninstall StoreFront 341

Authenticate using different domains 341

Set up a test environment 342

`production.com` domain 342

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

`development.com` domain 342
Configure a Citrix Gateway for the store 342
Enable pass-through from Citrix Gateway 344
Configure the store for remote access using the Gateway 345
Disable token consistency 346
Disable pass-through from Citrix Gateway for the website 347
Log on to Gateway using a `production.com` user and credentials 348
Add a trusted domain drop-down list in StoreFront (optional) 349
NetScaler® session action policy 350
Configure beacon points 352
PowerShell SDK 354
Create a single FQDN used internally and externally 354
Server Group base URL 355
StoreFront beacons for locally installed Citrix Workspace app 355
External DNS 355
Internal DNS 355
Require Citrix Workspace™ app to connect through a gateway 355
Configure using the Management GUI 356
Configure using the CLI 358
Export and import the StoreFront configuration 360
Scenarios where configuration export and import can be used 360
Things to consider when exporting and importing a StoreFront configuration 361
PowerShell cmdlets 361
Export-STFConfiguration 361
Import-STFConfiguration 362
Unprotect-STFConfigurationBackup 363
Configuration export and import examples 363

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

Import the StoreFront cmdlets into the current PowerShell session 363

Single server scenarios 364

Create an unencrypted backup of an existing configuration on Server A and restore it onto the same deployment 364

Back up an existing configuration on Server A and restore it onto Server B to create a clone of an existing server 364

StoreFront is already deployed onto a custom website in IIS. Restore the configuration onto another custom website deployment 365

Server group scenarios 366

Scenario 1: Backup an existing server group configuration and restore it later onto the same server group deployment 366

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 367

Scenario 3: Backup an existing configuration from Server Group A and use it to overwrite the existing Server Group B configuration 368

Create an encrypted backup of your server configuration 368

Unprotect an existing encrypted backup archive 369

User experience 371

Modern user experience 371

Classic user experience 371

Citrix Gateway cVPN 371

Classic experience 372

Log On 372

Citrix Workspace app detection 372

Home tab 375

Apps tab 375

Desktops tab 376

App and desktop tiles 376

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

Favorites 376
View details and actions 377
Search 378
Settings menu 378
Settings 379
Account 379
Apps 380
Advanced 380
Log off 381
Modern experience 381
Citrix Workspace™ app detection 381
Log In 384
First-time user experience for Workspace app 384
Limitations 385
Navigation tabs 386
Simple view 386
Full view 386
Home tab 386
Apps tab 387
Desktops tab 390
Favorite and mandatory apps 390
Search feature 391
Activity Manager 391
Account Settings 391
Apps and Desktops Launch Preference 392
Download Workspace Configuration 392
Activity Manager 392
Prerequisites 392

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

Using Activity Manager 393
Disconnected apps and desktops 394
StoreFront SDK 397
Use the SDK 397
Get started with the SDK 397
Examples 398
Example: Create a simple deployment 398
Understand the script 399
Example: Create a remote access deployment 404
Understand the script 405
Example: Create a remote access deployment with optimal launch Gateway 409
Understand the script 409
Troubleshoot StoreFront 413
Installation Logs 413
Event Logs 413
Log throttling 413
PowerShell and management console logs 414
Diagnostics logging 414
Launch.ica file logging 415
Third Party Notices 417
Castle Windsor 3.3.0 417
Microsoft Unity Application Block (Unity) 2.1 417
Microsoft Patterns and Practices: Prism 2.2 417
Microsoft patterns & practices: Common Service Locator 1.0 417
Microsoft .Net Reference Source 418
ManagedEsent Release 1.9.4 418
jQuery UI - v1.10.4 - 2014-03-12 418
jQuery JavaScript Library v1.12.4 418

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

jQuery jScrollPane v2.0.0beta11 418
jquery.contextmenu.js 419
jQuery plugin for Hammer.JS - v1.0.0 - 2014-01-02 419
jQuery MouseWheel 419
WPF Toolkit 3.5 419
Extended WPF Toolkit 3.0 419
WiX Toolset 419
CLR Security 420
Stack Exchange Redis 1.1 420
Newtonsoft JSON 420
jQuery JavaScript Library v3.7.0 420
jQuery UI - v1.13.2 - 2022-07-14 420
Hammer.JS - v2.0.4 - 2014-09-28 420
VelocityJS.org (1.5.0) 421
slick.js - 1.8.0 421
jQuery UI Touch Punch 0.2.3 421
Microsoft .NET 8 421
APPENDIX: Referenced Licenses 421
MIT License 421
Apache License, Version 2.0 422
Microsoft Public License (MS-PL) 430
Common Public License Version 1.0 432
Microsoft Limited Permissive License (MS-LPL) 437
Microsoft Limited Public License (Ms-LPL) 437
StoreFront™ Document History 439

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

StoreFront 2402 Long Term Service Release Overview

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

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 list of resource feeds that StoreFront queries to enumerate the apps and desktops available to the user.
- The appearance of the store.
- What authentication methods users use to log on.
- Whether the store can be remotely accessed through a NetScaler gateway..

Users can use locally installed Citrix Workspace app or a web browser to access StoreFront stores. For more information see User access options.

To get started, Plan your StoreFront deployment, view the System requirements and Install StoreFront.

What's new

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

What's new

Earlier releases

To know more about earlier releases, refer here.

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

© 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. Additional Lifecycle Information for StoreFront is provided in CTX200356.

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

What's new

The 2402 LTSR includes the following releases.

- 2402 LTSR CU4
- 2402 LTSR CU3
- 2402 LTSR CU2
- 2402 LTSR CU1
- 2402 initial release
- Known issues

Cumulative Update 4 (CU4)

Release date: May 08, 2026

About this release

Known issues in this release

Citrix Product Subscription Advantage Eligibility Dates

Citrix Workspace app for HTML5

This release includes Citrix Workspace app for HTML5 26.3.0.49.

What's new in 2402 LTSR CU4

This release addresses areas that improve overall performance and stability.

Fixed issues in 2402 LTSR CU4

StoreFront™ 2402 LTSR CU4 contains all fixes included in CU3, and the following are the new fixes:

- When using Citrix Gateway Service and **Request tickets from two cloud connectors, where available** is selected, the system issues only one ticket.

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

- StoreFront might fail to resources from some sites intermittently. The diagnostics log file contains error `ENUMERATION: Exception encountered while enumerating resources : System.ObjectDisposedException: Cannot access a disposed object. Object name: 'SslStream'`
- The PowerShell command `Set-STFWebReceiverSiteStyle` might fail with error `Value cannot be null`.
- Citrix Session Remote Start incorrectly attempts to reconnect to an existing DaaS-brokered session.
- When **Launch option** is set to **Let the user choose** and Citrix web extension is installed and has detected Citrix Workspace™ app, users can't change the launch method to open resources in a web browser. The fix applies to the Classic UI experience.
- After disabling Allow users to skip Citrix Workspace app detection, users who previously skipped Citrix Workspace app detection are not affected. With this fix, the next time such users open the store website they are required to complete Citrix Workspace app detection.
- The UI hangs if Citrix web extension is disabled or removed after detecting Citrix Workspace app
- When you change the Launch option to Open in Citrix Workspace app and save the changes, StoreFront might display an error. The error occurs when the HTML5 HDX™ version installed on the server differs from the version installed by default by the current version of StoreFront.
- When you change the launch option from **Open in Citrix Workspace app** to **Let the user choose** or **Open in a web browser** and select **OK**, the following error might appear:

  "An error occurred while saving changes on the 'Launch preferences' property dialog. Please check the log in the Event viewer and try again."

  The issue occurs if the HTML5 HDX client is unexpectedly already installed.
- Users encounter a **Cannot start app** error when they attempt to access certain applications through the internal StoreFront URL.
- When Citrix Workspace app has been successfully detected by Citrix web extension, the link to Download Citrix Workspace app should be hidden from the settings page.
- When performing machine control actions, StoreFront doesn't pass the client name and address to the DDC, causing them to be missing from the log files.

Cumulative Update 3 (CU3)

Release date: August 26, 2025

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

About this release

Known issues in this release

Citrix Product Subscription Advantage Eligibility Dates

System requirements

StoreFront™ 2402 LTSR CU3 requires .NET 8. If it is not already installed then the installer automatically installs .NET 8.

For more information, see System requirements

Citrix Workspace app for HTML5

This release includes Citrix Workspace app for HTML5 25.5.0.19.

What's new in 2402 LTSR CU3

Citrix Licensing Telemetry

StoreFront collects telemetry on user log-ins and your configuration. For more information, see Telemetry.

Fixed issues in 2402 LTSR CU3

StoreFront 2402 LTSR CU3 contains all fixes included in CU2, and the following are the new fixes:

- When HDX™ Direct is enabled, StoreFront includes unnecessary VDA host details in the ICA file when a client initiates an HDX connection through a gateway.
- The Citrix Subscription Synchronization Service might experience high memory usage on StoreFront servers or encounter port exhaustion.
- The auto desktop launch feature might not work if more than one year has passed since the client's initial access to the Receiver for Web site from the client.
- A malformed URL might cause an Internal Server Error with a binary response body.
- The Content Security Policy defined in the `http-equiv` tag of the HTML file has been updated to block inline scripts.

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

NOTE:

StoreFront customizations that use *eval or insert* inline scripts into the DOM no longer function due to this update.

- The **Citrix Cluster Service** firewall rule created following the execution of the Start-STFServerGroupJoin command might prevent the configuration of StoreFront server groups.
- When multi-site aggregation is enabled, it is not possible to reconnect to sessions using Activity Manager. Instead, click the icon to reconnect.
- Enable PNA (XenApp® Services) for a non-default Store using `Enable-STFStorePna -DefaultPnaService:$false` cmdlet only works after first running `Disable-STFStorePna cmdlet` to Disable PNA (XenApp Services) for a Store
- The modern experience does not load on Citrix Workspace™ app for Linux
- In the StoreFront management console, Next Generation Experience is renamed to Modern experience, and Unified Experience has been renamed to Classic experience.
- When Cloud Connectors operate in LHC mode and a user attempts to launch a resource that is accessible from multiple locations, the session might fail to start if the resource isn't immediately available. The issue occurs because, after checking the resource's readiness, StoreFront might send the request to a different connector than the one initially used to launch the resource.
- StoreFront **Favorites** do not synchronize between StoreFront servers when NTLM authentication is disabled.

Cumulative Update 2 (CU2)

Release date: January 31, 2025

About this release

Known issues in this release

Citrix Product Subscription Advantage Eligibility Dates

Citrix Workspace app for HTML5

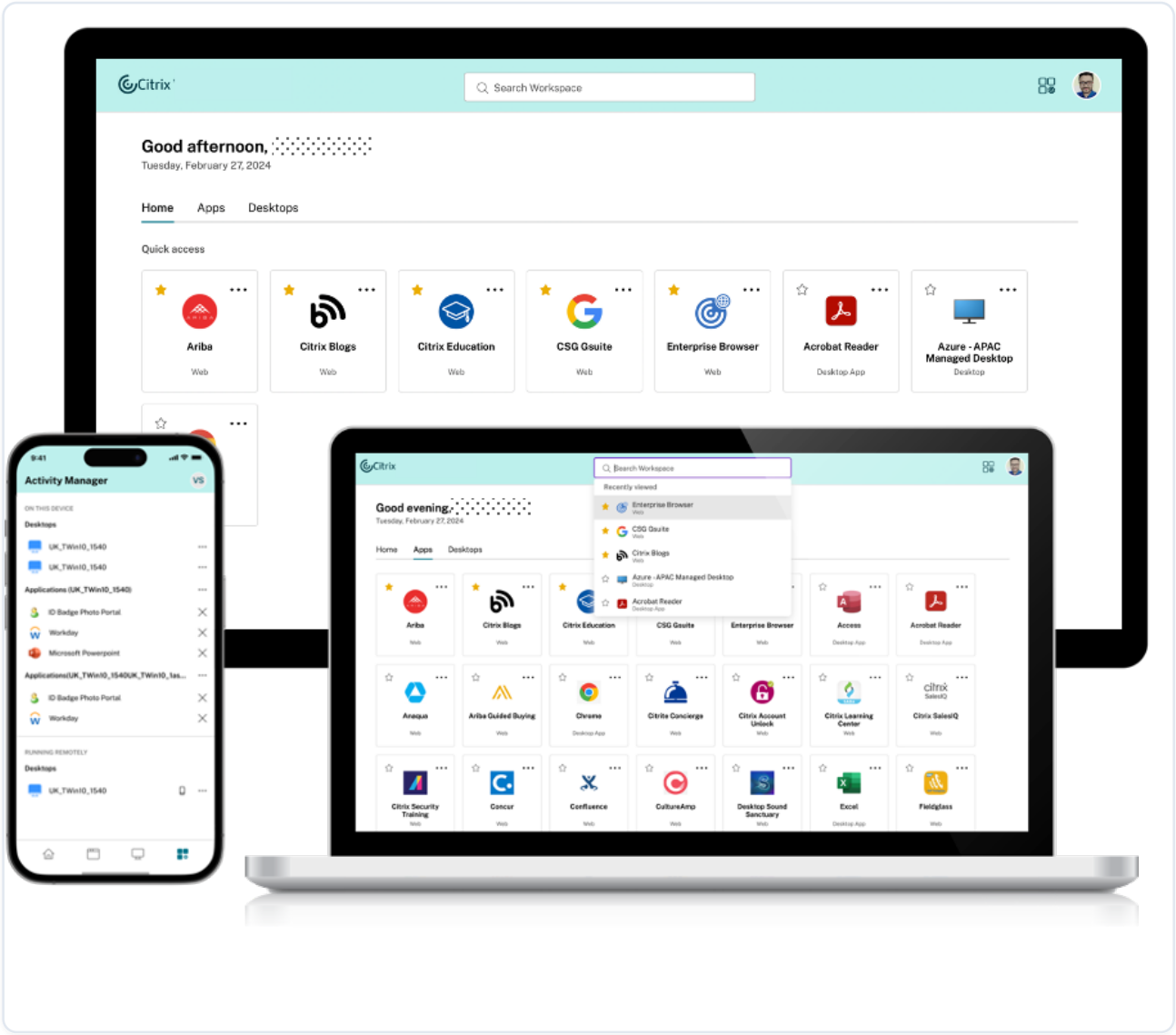
This release includes Citrix Workspace app for HTML5 24.11.0.51.

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

What's new in 2402 LTSR CU2

Modern experience - General availability

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



The new user interface is designed to enhance and simplify the end-user experience to access Citrix® apps and desktops. It reduces visual complexity, provides easy access to essential features, and refines the StoreFront™ app experience. It supports new features, such as Activity Manager that facilitate effective management of your virtual apps and desktop resources. Note: In this article, the current UI experience has been referred to as the classic experience.

To enable the modern experience, see User Experience.

The modern experience brings the following key improvements:

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

- Activity Manager: Enables quick actions on active virtual apps and desktops, saving resources and optimizing performance. For more information, see Activity Manager.
- Enhanced categorization of apps: Multi-level folder structures that are responsive to the user's screen size. For more information, see categorization of apps.
- Improved Search capabilities: New search capabilities provide for better and faster results. For more information, see Search feature.

For more information, see Modern experience.

Fixed issues since the technical preview

- When you change the UI experience for an existing store, users connecting through locally installed Citrix Workspace app aren't updated. They must remove the store and add it back to their app.
- Activity Manager operations such as Logout, Disconnect, and more aren't supported for applications that have App Protection policies enabled.
- Citrix web extensions are not supported.
- Direct SAML authentication using a web browser is not supported.
- App protection for hybrid launches are now supported. Apps requiring App Protection are never displayed.
- On {Citrix Workspace app for iOS, the user's initials aren't displayed on the avatar.
- On Citrix Workspace app for Windows, Mac and Linux when connecting via a gateway, after logging off, the **Back to sign in** option does not work. , ,
- Activity manager cannot retrieve sessions from more resource feeds than can be enumerated concurrently.
- In the **Edit Receiver for Web Site** screen, when **Next generation experience** is selected, settings are displayed that are not relevant to the experience.
- Settings to hide the **Already Installed** option and prevent ICA® downloads are ignored.

Fixed issues in 2402 LTSR CU2

StoreFront 2402 LTSR CU2 contains all fixes included in CU1, and the following are the new fixes:

- Adding custom footers to Receiver for Web site by inserting content with the customBottom ID of the StoreFront customization API might result in unexpected customization behavior.

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

- After upgrading StoreFront 2402 to 2402 CU1, German-language device users might be unable to sign in to the Citrix Workspace™ app and Citrix Workspace web client on browsers. The sign-in page might load with no result.

  For more information, see CTX691873.

  Note that any Citrix Workspace app client that encounters this issue and goes into a bad state must be removed and re-added to the store.
- When enabling ICA signing using the PowerShell command `Set-STFStoreService $storeService -IcaFileSigning $true`, the command doesn't set the necessary permissions on the certificate, causing ICA signing to fail.
- End users can't launch the desktop if the published name contains non-English characters. The issue occurs after Citrix web extension is enabled.
- During an outage, when the connectors go into Local Host Cache mode, StoreFront needs to send launch requests to the connector in the same zone as the resource. When a resource is available in multiple zones, previously, StoreFront would only try to launch the resource in one zone.

  With this enhancement, if the attempt to start a resource in one zone fails, in some cases StoreFront server tries to make another attempt to start the resource using connectors in other available zones to improve resilience.

Cumulative Update 1 (CU1)

Release date: August 20, 2024

About this release

StoreFront (initial release)

Known issues in this release

Citrix Product Subscription Advantage Eligibility Dates

Citrix Workspace app for HTML5

This release includes Citrix Workspace app for HTML5 2404.1.

What's new in 2402 LTSR CU1

Cumulative Update 1 (CU1) is the latest release of the StoreFront 2402 LTSR. See What's new.

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

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

Enable advanced health check for all stores

Advanced health check is enabled for all existing stores on upgrade to 2402 LTSR CU1 to improve resiliency. With the advanced health check feature, StoreFront can more reliably check for any issues in the delivery controller. When used with Citrix Desktops as a Service, the advanced health check provides additional information about the connectors present at the resource locations. This feature is useful during an outage. When a user launches a resource, an appropriate connector to launch the resource is selected automatically using Local Host Cache.

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

```
foreach ($store in Get-STFStoreService)

{

    Set-STFStoreFarmConfiguration -StoreService $store
-AdvancedHealthCheck $False

}
```

Fixed issues

StoreFront 2402 LTSR CU1 contains the following fixes:

- When you start an app or a desktop session, the following error message might appear even though the resource starts successfully:

  "Cannot start Desktop".

  The issue occurs when you upgrade StoreFront to 2203 CU4 Update 1 and Citrix Workspace app for Windows supports opening a custom web portal.
- This fix corrects the typo appearing in the German language error message.
- When you upgrade StoreFront, you might notice duplicate copies of customization files, which were placed in the custom folder (`\StoreWeb\custom`), can also be found in the root of the website folder (`\StoreWeb`) after the upgrade process is complete.

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

- An upgrade to a newer version of StoreFront fails and the logs contain text "VersionData:Load Failed due to exception: System.IndexOutOfRangeException".

  The issue occurs when a user group created by StoreFront has an empty description.

- Intermittently, StoreFront™ upgrade fails. The installer either fails silently before the wizard appears, or the wizard becomes unresponsive, or after clicking through the wizard the upgrade fails.

  The issue occurs because the installation files are deleted before they are needed.

- Upgrade fails with message "There was an error adding user accounts in the Administrators local group to the CitrixStorefrontAdministrators local group" or similar. This occurs when a user group used by StoreFront contains a deleted user.

What's new in 2402 (initial release)

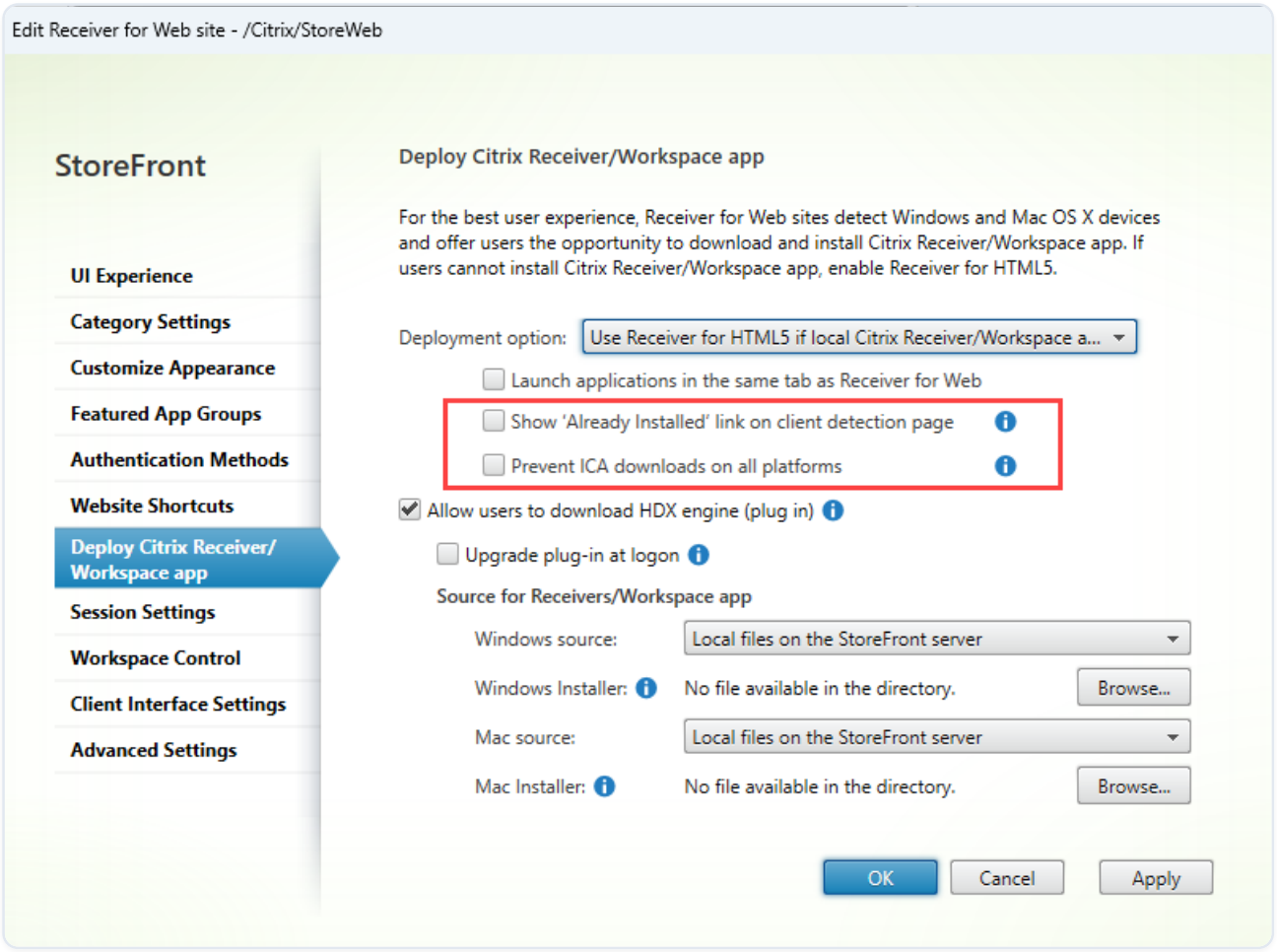
StoreFront 2402 LTSR includes the following new features and enhancements since StoreFront 2203 LTSR:

Prevent .ica® file downloads during Hybrid launch

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

- Show **Already installed** link on client detection page
- Prevent ICA downloads on all platforms

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



For more information, see Prevent ICA file download.

Enable advanced health check for all stores

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

It is possible to disable advanced health check but this is not recommended as it would reduce resiliency. To disable advanced health check for all stores, you can use the following PowerShell script:

```
foreach ($store in Get-STFStoreService)

{

    Set-STFStoreFarmConfiguration -StoreService $store
-AdvancedHealthCheck $False
```

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

```
}
```

Deprecation announcement for Windows server 2016

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

Citrix Secure Private Access on StoreFront

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

Uninterrupted VDA launch in case of FAS server unavailability

You can now configure StoreFront so that a VDA launch is successful even if the FAS server is unavailable. In such cases, the end users can sign in using their username and password. Previously, the VDA launch would fail if the FAS servers were unreachable. This feature is disabled by default and can be enabled using the following PowerShell command.

`Set-STFStoreLaunchOptions` with parameter `FederatedAuthenticationServiceFailover`

You can use the same command to disable this feature, if required. For more information, see FAS.

Improved user-journey logs

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

Citrix® web extensions - General Availability

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

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

Workspace launcher or downloading an `.ica` file, making your experience safer and more reliable. For more information, see Citrix Web Extensions.

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

NOTE:

Citrix web extension is not enabled automatically during a StoreFront version upgrade. Unless the feature feature was turned on before the upgrade, it remains disabled by default. It will be enabled for all deployments in a future release.

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

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

WARNING

When using the classic experience, users who have not installed Citrix web extensions may see a delay of 6s when opening the store website for the first time. This delay does not occur again unless users clear their cookies, or they select **Change Citrix Workspace™ app** from the settings page. This delay is because the webpage makes 2 attempts to detect Citrix web extension, each with a 3s timeout for a total of 6s. If you have not deployed Citrix web extension to your users then consider disabling it.

To disable Citrix web extensions run the PowerShell command:

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

New UI for on-premises stores (Technical Preview)

The new UI, previously available only for cloud stores, is now available as a tech preview for on-premises stores. Upgrade to CU2 or higher before using this in production. It brings the following key improvements:

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

- A consistent look and feel between cloud and on-premises stores.
- **Activity Manager**: Facilitates quick actions on active virtual apps and desktops, saving resources and optimizing performance. For more information, see Activity Manager.
- **Enhanced categorization of apps**: Multi-level folder structure that is responsive to your end user's screen size. For more information, see categorization of apps.
- **Improved Search capabilities**: New search capabilities provide for better and faster results. For more information, see Search options.

For detailed information on this preview, see New UI.

Citrix Workspace app for HTML5

This release includes Citrix Workspace app for HTML5 2402.

App Protection for hybrid launches

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

For more information see App Protection.

Advanced health check enabled by default

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

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

Deprecation of XenApp® Services

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

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

Removal of ability to add XenApp 6.5 delivery controllers

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

```
$store = Get-STFStoreService

Add-STFStoreFarm -StoreService $store -FarmName "XenApp" -FarmType XenApp
-Port 80 -TransportType HTTP -Servers Xen1
```

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

NOTE:

XenApp 6.5 is not supported by Citrix. The ability to use XenApp 6.5 delivery controllers will be removed in a future release.

Removal of ability to open resources within Internet Explorer 11

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

Fixed Issues

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

- App enumeration on StoreFront servers might fail intermittently.
- Names containing special characters might appear corrupted in the Home tab and Settings dropdown menu.
- The first time a user opens a store website in their browser on ChromeOS, it prompts the user to perform client detection but Citrix Workspace app for ChromeOS does not support client detection. As a result, the client detection fails and the users would need to click "already installed" to continue. With this fix, the website skips client detection on ChromeOS.
- Citrix Workspace app for Mac might freeze after waking up from Sleep mode when connected to a StoreFront Store.
- A race condition can cause the Citrix Subscriptions Store service to exit unexpectedly on the StoreFront server with warning messages.

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

- A year after detecting that the user has Citrix Workspace app installed, apps are launched in a browser rather than Citrix Workspace app.
- When using the StoreFront Store Service API to launch an app, overriding settings such as audio quality and disabling printers, the settings may affect all subsequent requests rather than just the current request.

Known issues in 2402

2402 LTSR Cumulative Update 4 (CU4)

There are no new known issues in Cumulative Update 4.

2402 LTSR Cumulative Update 3 (CU3)

There are no new known issues in Cumulative Update 3.

2402 LTSR Cumulative Update 2 (CU2)

- The modern experience does not load on Citrix Workspace app for Linux. For more information and how to install a patch, see CTX692858
- When using the modern experience, the setting to enable/disable Workspace app download is ignored and the download link is always displayed.
- When using the modern experience, if there are multiple authentication methods then when the user logs out they are not given the option whether or not to remember the authentication method.
- When using the modern experience, and multi-site aggregation is enabled, it is not possible to reconnect to sessions using Activity Manager. Instead, click the app or desktop's tile to reconnect.
- When using the modern experience, when a user is notified that their password will expire soon, if they select **Change Now** the **Change Password** screen is displayed without any text input or buttons.
- Upgrades from 2402 CU2 to 2407 or 2411 fail. This is resolved with 2503.
- The PowerShell command `Get-STFWebReceiverSiteStyle` might fail with error `Value cannot be null`.
- The PowerShell command `Set-STFWebReceiverSiteStyle` might fail with error `Value cannot be null`.
- On the first time user screen, favorites are not saved.

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

2402 LTSR Cumulative Update 1 (CU1)

- After upgrading StoreFront 2402 to 2402 CU1, German-language device users might not be able to sign in to the Citrix Workspace app and Citrix Workspace web client on browsers.
- The sign-in page might load with no result. For more information, see CTX691873.

2402 initial release

- When Citrix Workspace app for Windows 2309 or higher is connected to StoreFront using a XenApp Services URL, launching a resource may cause an additional notification to be displayed. This is resolved in 2402 CU1.
- When using a custom Store plug-in, any Access Policies on a delivery group in Studio are evaluated as if the connection is through a gateway.
- When Citrix® web extensions is enabled but not installed on the user's, users experience a 6s delay the first time they open the store in a web browser. This does not apply when using the modern experience or web browsers other than Chrome and Edge.

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

Install, set up, upgrade, and uninstall

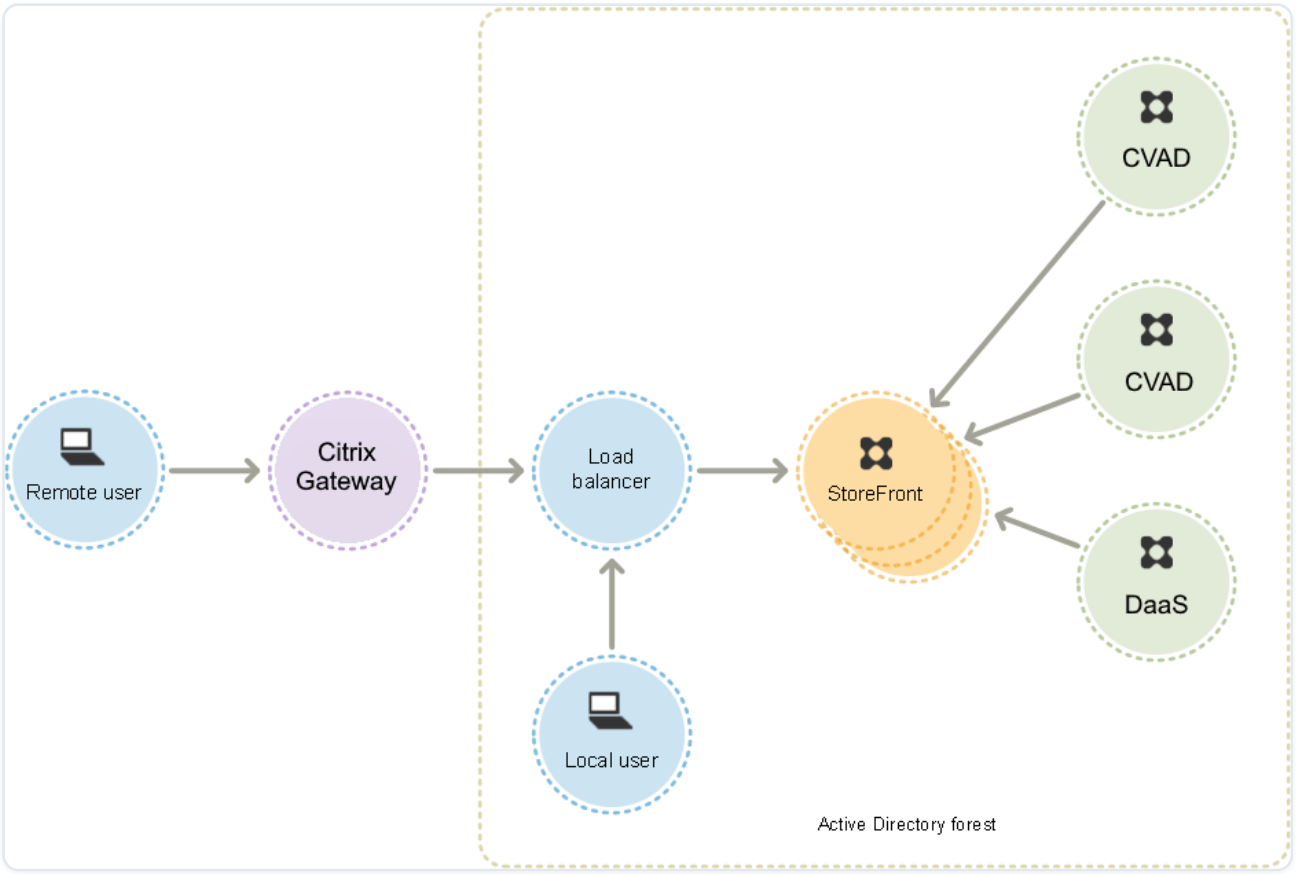
TASK	DETAIL
Plan your StoreFront deployment	An overview of the components involved in a StoreFront deployment
User access	An overview of the ways users can access your stores
System Requirements	Ensure that you have the prerequisites to install StoreFront
Install StoreFront	Install StoreFront onto a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

© 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.

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

StoreFront Server groups

StoreFront can be configured either on a single server or as a multiple server deployment called a StoreFront server group. Server groups not only provide additional capacity, but also greater availability. StoreFront ensures that configuration information and details of users' application subscriptions are stored on and replicated between all the servers in a server group. This means that if a StoreFront server becomes unavailable for any reason, users can continue to access their stores using the remaining servers. Meanwhile, the configuration and subscription data on the failed server are automatically updated when it reconnects to the server group. Subscription data is updated when the server comes back online but you must propagate configuration changes if any were missed by the server while offline. In the event of a hardware failure that requires replacement of the server, you can install StoreFront on a new server and add it to the existing server group. The new server is automatically configured and updated with users' application subscriptions when it joins the server group.

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

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

Load balancing

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

Citrix Gateway for remote access

If you plan to enable access to StoreFront from outside the corporate network, a Citrix Gateway is required to provide secure connections for remote users. Deploy Citrix Gateway outside the corporate network, with firewalls separating Citrix Gateway from both the public and internal

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

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 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:

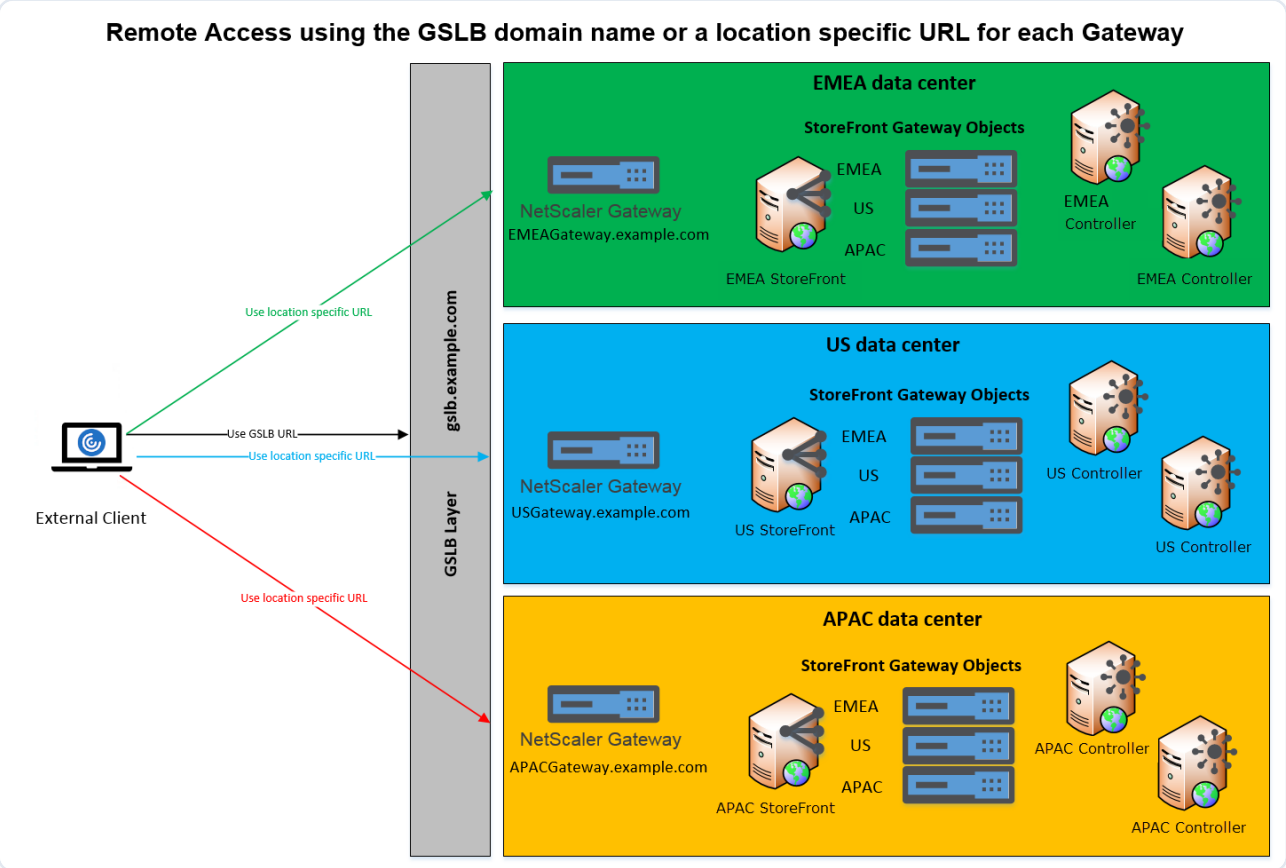
`emeagateway.example.com` - Europe gateway

`usgateway.example.com` - US gateway

`apacgateway.example.com` - Asia Pacific gateway

Along with a GSLB:

`gslb.example.com`



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

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

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

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

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

NOTE:

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

User access

See User access options.

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.

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

- 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.
- **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

When using the classic experience, you can install a plug-in 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

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

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 make the configuration process easier for your users by providing them with the required information in one of the following ways.

IMPORTANT:

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

Manual configuration

Users can connect Citrix Workspace app to their store by entering the store URL or Citrix Gateway URL into Citrix Workspace app. If the user enters the base URL then Citrix Workspace app provides a list of stores to choose from. For more information, see the Citrix Workspace app documentation.

Provisioning files

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

Auto-generated setup URLs

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

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

Email-based account discovery

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

Global App Config Service

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

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.

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.

When users come to launch their resources there are two possibilities:

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

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

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

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

Requirements for opening resources in your browser

For users on the internal network, access through 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:

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

The first time a user goes to a store website on a supported platform, it prompts the user to detect the locally installed Workspace app. It first tries to use the web extension and if this fails then it tries Citrix Workspace Launcher. Existing users who have already completed Workspace app

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

detection can go to **Account Settings**, click **Change Citrix Workspace app** to re-detect workspace app.

NOTE:

Citrix web extension is not enabled automatically during a StoreFront version upgrade. Unless the feature feature was turned on before the upgrade, it remains disabled by default. It will be enabled for all deployments in a future release.

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

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

WARNING

When using the classic experience, users who have not installed Citrix web extensions may see a delay of 6s when opening the store website for the first time. This delay does not occur again unless users clear their cookies, or they select **Change Citrix Workspace app** from the settings page. This delay is because the webpage makes 2 attempts to detect Citrix web extension, each with a 3s timeout for a total of 6s. If you have not deployed Citrix web extension to your users then consider disabling it.

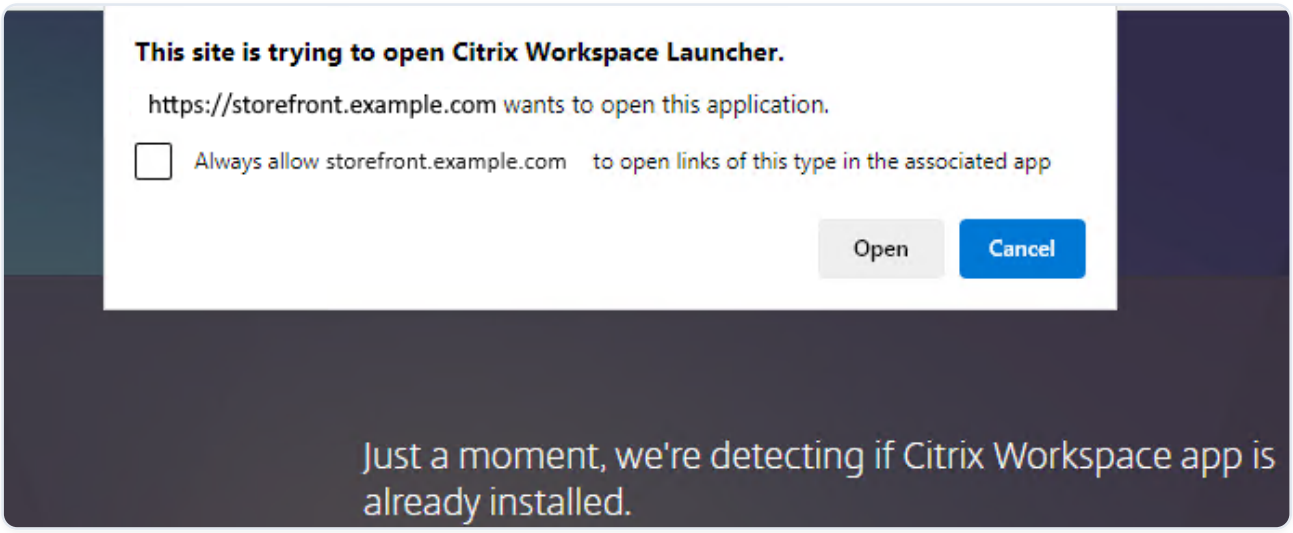
To disable Citrix web extensions, run the PowerShell command:

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

Citrix Workspace launcher

When the user first goes to a StoreFront web site with a supported operating system and browser and Citrix web extensions are not installed, it attempts to invoke the Citrix Workspace Launcher. The browser might prompt the user for confirmation, for example:

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



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

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

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

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

- Receiver for Windows 4.3 or higher with the WebHelper component (this is installed by default)
- Receiver for Mac 12.0 or higher
- Workspace app for Linux 2003 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

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

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

This launch method can be disabled. On the store website Advanced settings screen, clear Enable protocol handler

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 **Already Installed**, 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 Deploy Citrix Workspace app.

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

Resource shortcuts

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

When you create an application shortcut, ensure that no other applications available from the store have the same name. Shortcuts cannot distinguish between multiple instances of an application with the same name. Similarly, if you make multiple instances of a desktop from a single desktop group available from the store, you cannot create separate shortcuts for each instance. Shortcuts cannot pass command-line parameters to applications.

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

XenApp Services URLs

NOTE:

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

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

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

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

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

Important considerations

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

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

System requirements

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:

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

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

NOTE:

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

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

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

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

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

If the version of .NET Framework installed is older than 4.8.0 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 2402 CU3 and higher requires .NET 8. If it is not already installed then the installer automatically installs .NET 8.

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

- Web-Server
  - Web-WebServer
    - Web-Common-Http
      - Web-Default-Doc

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

        - Web-Http-Errors
        - Web-Static-Content
        - Web-Http-Redirect
    - Web-Health
        - Web-Http-Logging
    - Web-Security
        - Web-Filtering
        - Web-Basic-Auth
        - Web-Windows-Auth
    - Web-App-Dev
        - Web-Net-Ext45
        - Web-AppInit
        - Web-Asp-Net45
        - Web-ISAPI-Ext
        - Web-ISAPI-Filter
    - Web-Mgmt-Tools
        - Web-Mgmt-Console
    - Web-Scripting-Tools
- NET-Framework-45-Features
    - NET-Framework-45-ASPNET
    - NET-WCF-Services45
        - NET-WCF-TCP-PortSharing45

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

Hardware

Storefront™ servers must meet the following requirements:

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

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

Network

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

- 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 favorites 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.
  - Synchronizing credentials within a server group.
- A TCP port randomly selected from all unreserved ports is used for communications between the StoreFront servers in a server group.
- 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.

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

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 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 2402 LTSR

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

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

Citrix Gateway

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

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

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

User device requirements

StoreFront provides various options for users to access their desktops and applications. Citrix users can either access stores through locally installed Citrix Workspace app, or within their browser. For more information, see User access options.

Locally installed Citrix Workspace app

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

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

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.

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

On Windows:

- Microsoft Edge
- Google Chrome
- Mozilla Firefox
- Internet Explorer 11*

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

On Mac:

- Safari
- Google Chrome
- Mozilla Firefox

On Linux:

- Google Chrome
- Mozilla Firefox

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

Citrix web extensions

For an improved experience, it is recommended that users add Citrix web extension to their web browser. For requirements, see Citrix web extension.

Legacy devices

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

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

Smart card requirements

Using Citrix Workspace app with smart cards

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

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

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

Citrix Analytics service requirements

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

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

Install StoreFront

Before installing and configuring

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

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

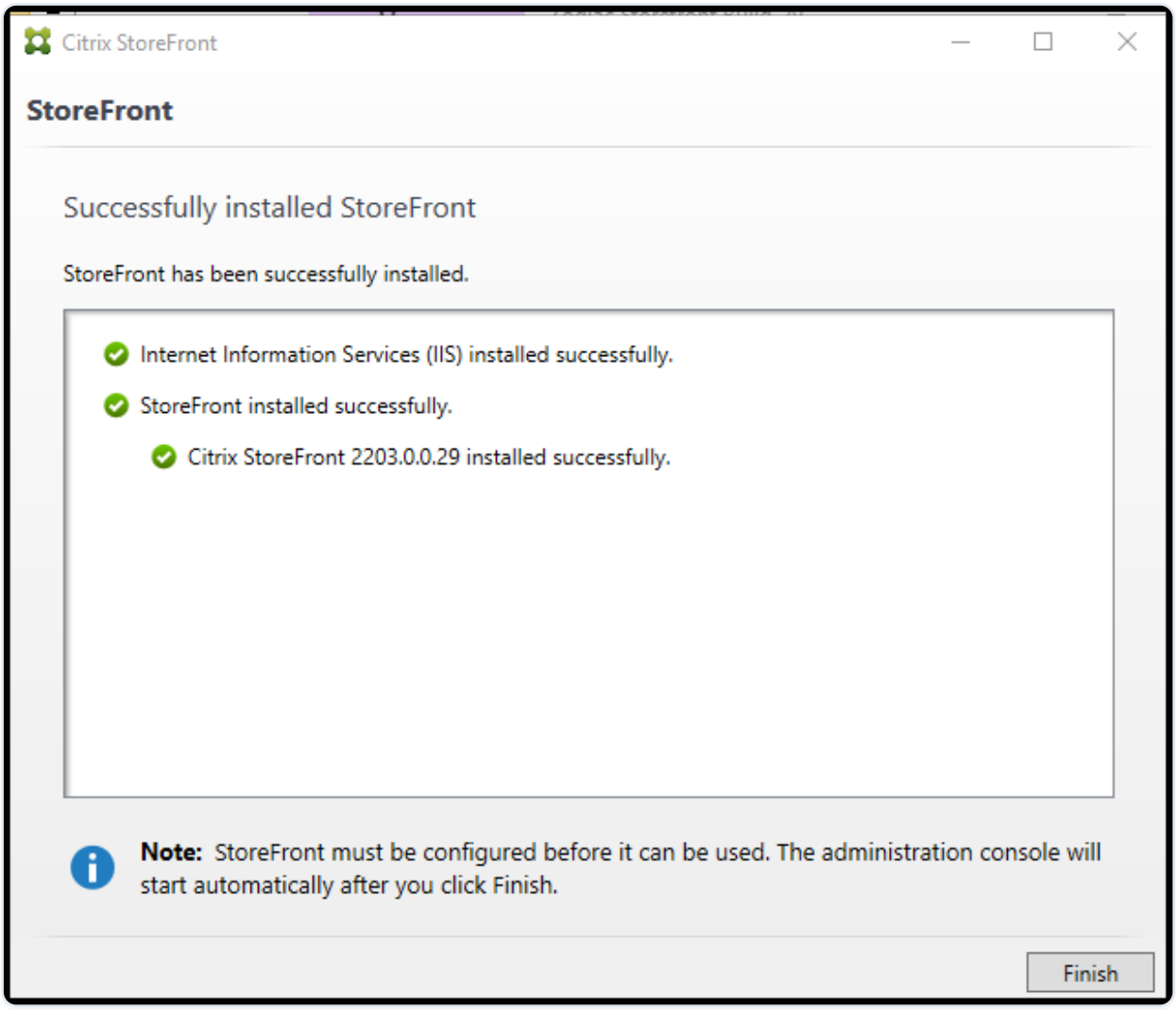
Install StoreFront

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™

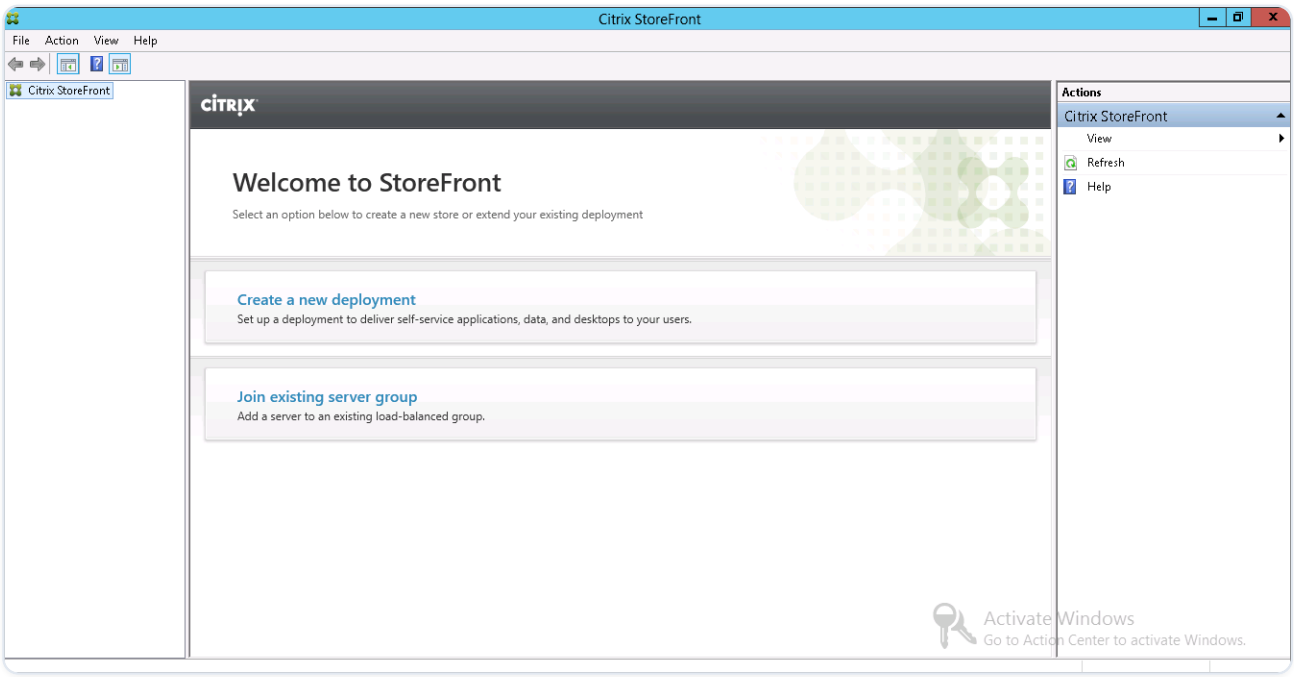
You can install StoreFront on the same server as Citrix Virtual Apps and Desktops. Run the Citrix Virtual Apps and Desktops installer and under **Extend Deployment** choose **Citrix StoreFront**.

Installation logs

For more details of logs files, see Installation Logs.

Configure StoreFront

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



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

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

Your store is now available for users to access through a browser or Citrix Workspace app. See the User experience.

Citrix Customer Experience Improvement Program

IMPORTANT:

The Citrix Customer Experience Improvement Program for StoreFront has been discontinued. StoreFront 2402 LTSR CU3 and later versions don't send data to CEIP. If you are using a version prior to CU3, StoreFront sends data to the service but the data isn't retained.

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

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

WARNING:

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

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

```
Location: HKLM:\Software\Citrix\Telemetry\CEIP

Name: Enabled

Type: REG_DWORD

Value: 0 = disabled, 1 = enabled
```

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

By default, the **Enabled** property does not exist. When it remains unspecified, the automatic upload feature is enabled.

Using PowerShell, the following cmdlet disables enrollment in CEIP:

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

NOTE:

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

CEIP data collected from StoreFront

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

DATA	DESCRIPTION
StoreFront version	String denoting the installed version of StoreFront. For example, "3.8.0.0"
Stores count	A counter for the number of stores in the deployment.
Server Count in server group	A counter for the number of Servers in the Server group.
Delivery Controller™ Count per store	List of numeric values indicating the number of Delivery Controllers available for each store in the Deployment.
HTTPS enabled	String denoting whether HTTPS is enabled ("True" or "False") for the deployment.
HTML5 setting for Citrix Receiver™ for Web	List of Strings denoting the HTML5 Receiver setting ("Always", "Fallback", or "Off") for each Receiver for Web site.

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

DATA	DESCRIPTION
Workspace control enabled for Citrix Receiver/ Workspace app	List of Booleans denoting whether "Workspace Control" is enabled ("True" or "False") for each Receiver for Web site.
Remote Access enabled for store	List of Strings denoting whether "Remote Access" is enabled ("ENABLED" or "DISABLED") for each store in the Deployment.
Gateways count	A counter for the number of Citrix Gateways configured in the deployment.

Citrix Analytics service

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

To configure this behavior:

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

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

IMPORTANT:

Your StoreFront deployment must be able to contact Citrix API Services. See Analytics network requirements.

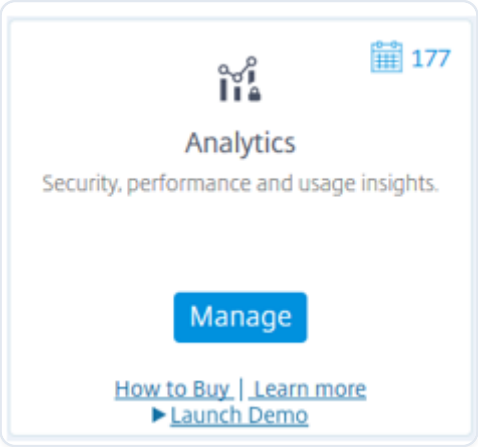
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

Example configuration file

```
{

  "customerId": "<yourcloudcustomer>",

  "enablementService": " https://api.analytics.cloud.com /casvc/
<yourcloudcustomer>/ctxana/v1/cas/<yourcloudcustomer>/XenDesktop/
<deviceid>/dsconfigdata",
```

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

```
  "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

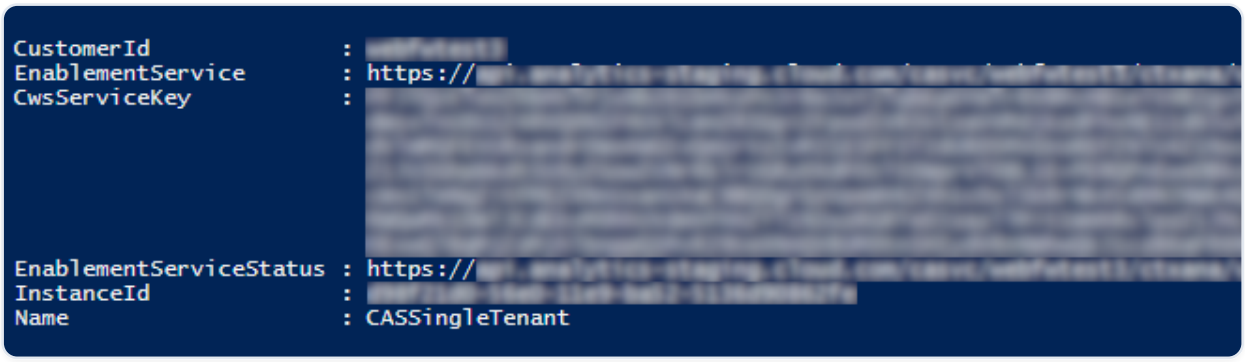
1. Copy the *StoreFrontConfigurationFile.json* file to a suitable folder on the on-premises StoreFront server (or one server in a StoreFront server group). The following commands assume that the file is saved to the Desktop.
2. Open PowerShell ISE and select **Run as Administrator**.
3. Run the following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

   ```
   Import-STFCasConfiguration -Path
   "$Env:UserProfile\Desktop\StoreFrontConfigurationFile.json"

   Get-STFCasConfiguration
   ```

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

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



NOTE:

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

Propagate Citrix Analytics data to a StoreFront server group

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

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

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

Check StoreFront server group ID

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

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

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

```
$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`

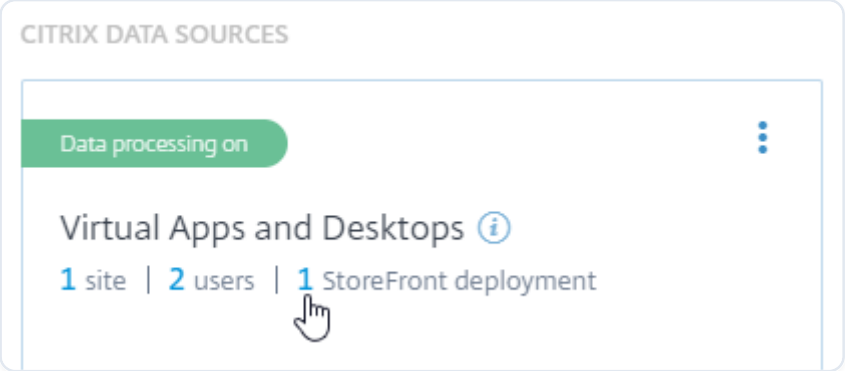
   Get-STFCasConfiguration returns nothing if the previously imported Citrix Analytics data has been successfully removed.
3. If you are performing these actions on a StoreFront server group, propagate the change and remove the imported Citrix Analytics data from all members of the server group. On one server in the server group, run the following command:

   `Publish-STFServerGroupConfiguration`
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:

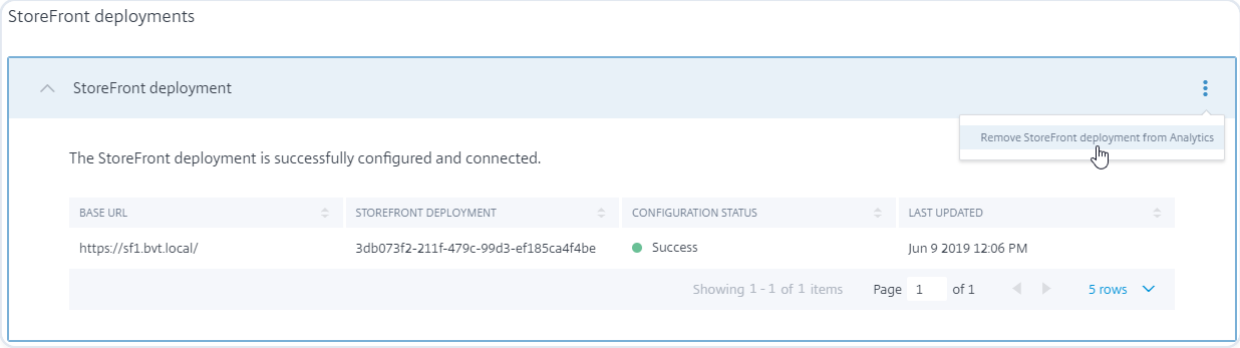
© 1997–2026 Citrix Systems, Inc. All rights reserved.

`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.

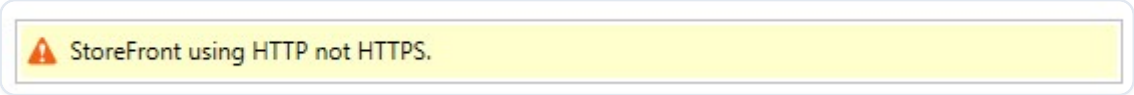
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

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 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 base URL FQDN used to access StoreFront is included in the DNS field as Subject Alternative Name (SANs). When using a load balancer in front of your StoreFront servers, the base URL is the load balancer FQDN rather than the StoreFront server FQDN. The **Create Domain Certificate...** option in IIS does not set the SAN so should not be used.
- Sign the certificate using a third party CA such as Verisign or an enterprise root CA for your organization.
- If using an internal certificate authority and devices connect directly to the StoreFront server, you must ensure that you install the root certificate on those devices. If users access StoreFront via a load balancer or gateway, then the root certificate only needs to be installed on that load balancer or gateway.

Create certificate using Windows Certification Authority

If you have an Active Directory Certificate Services server on your domain, you can use it to create certificates from your StoreFront server or another computer on the domain.

1. Press Start and in the search field type **Manage Computer Certificates**.
2. Expand **Personal > Certificates**.

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

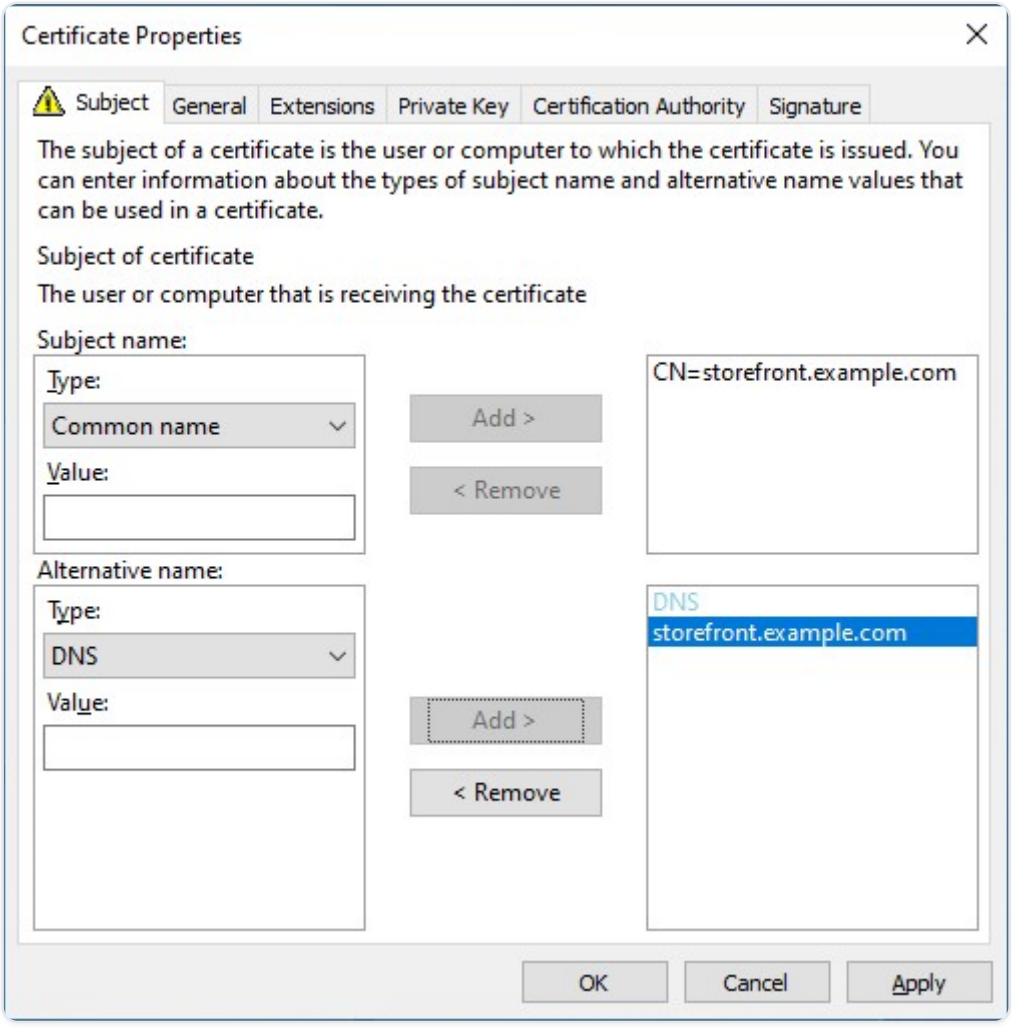
3. Right-click on **Certificates** and from the menu choose **All Tasks** > **Request new certificate**.
4. On the **Select Certificate Enrolment Policy** screen, choose **Active Directory Enrollment Policy**.
5. Choose template **Web server exportable**, or another suitable template.
6. Click on **More information is require to enroll this certificate. Click here to configure settings.**
7. On the **Certificate Properties** screen:

    a. Under **Subject name** choose **Common name** and enter the FQDN.

    b. Under **Alternative name** choose **DNS** and enter the FQDN.

    c. Optionally go to the **General** tab and enter a friendly name.

    d. Press **OK**.



8. Press **Enroll**.

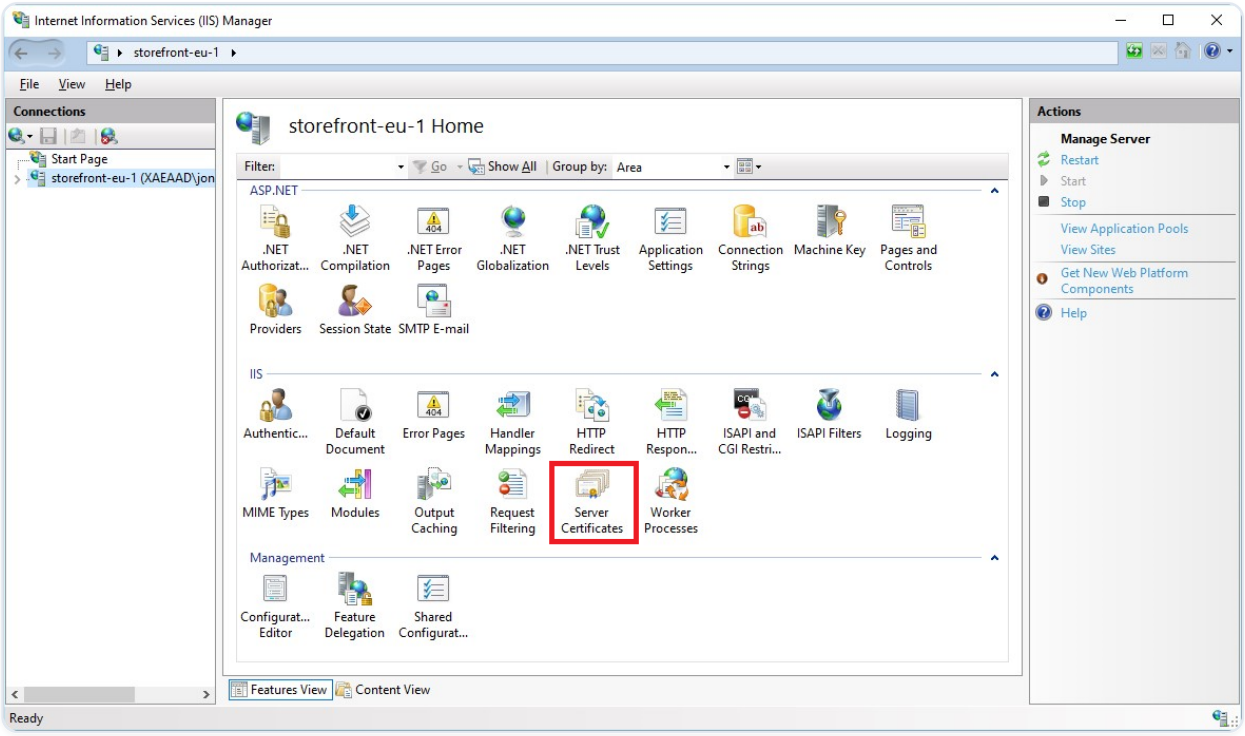
If you created the certificate on your StoreFront server then it is now available to use in IIS. If you created it on another machine then you must export it and import it to the StoreFront server.

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

Import existing certificate

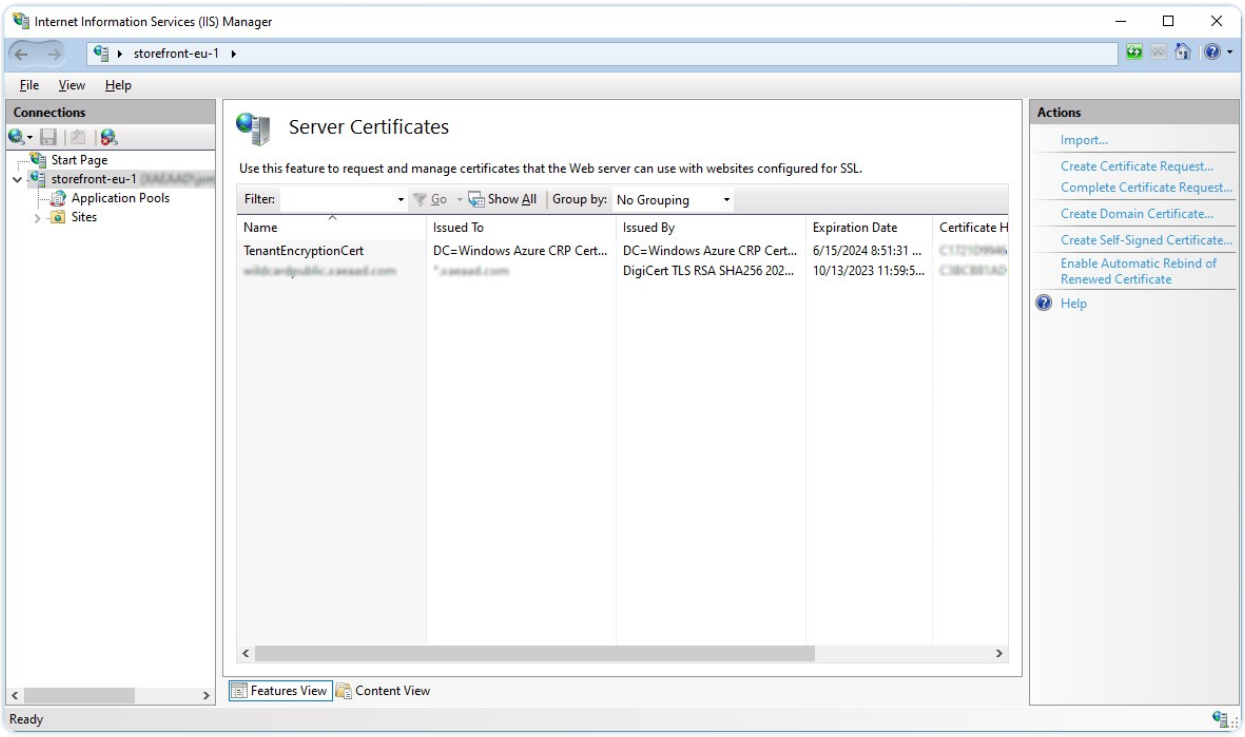
You can import a certificate created in another system. The certificate must be in PFX format and contain the private key.

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



4. From the Server Certificates screen press **Import...** and choose a certificate file.

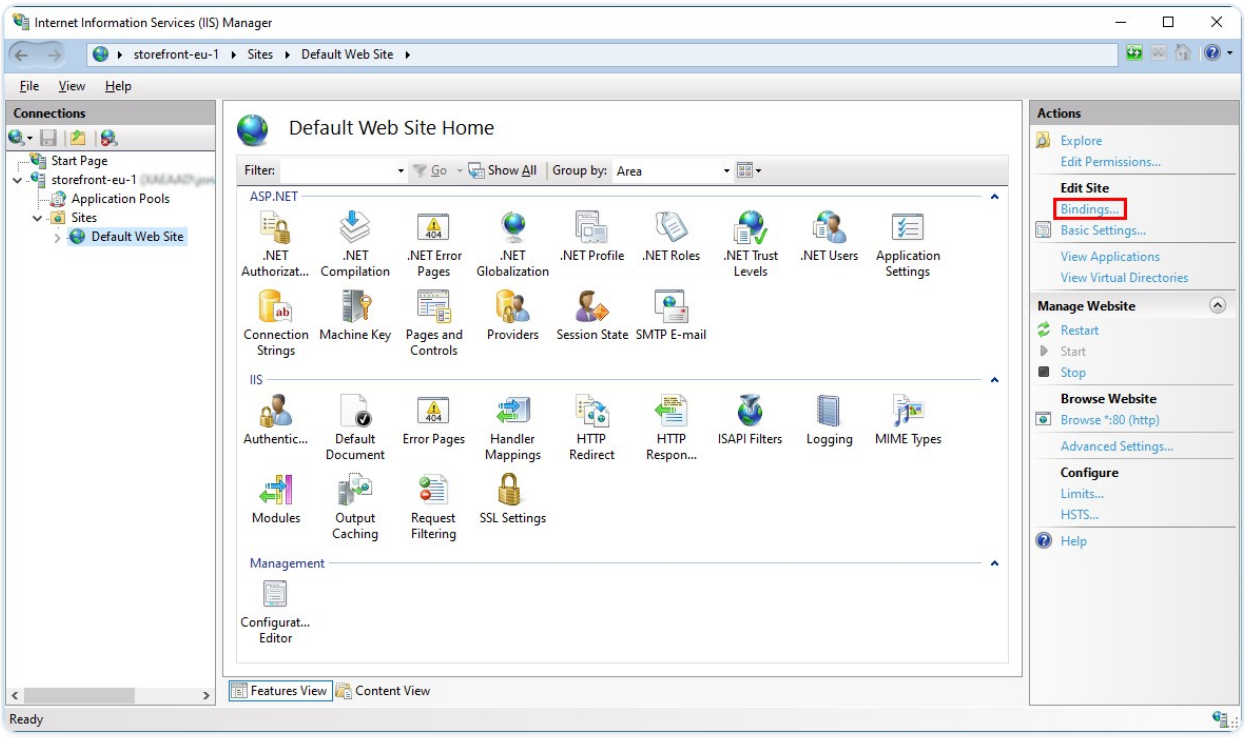
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Configure IIS for HTTPS

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

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



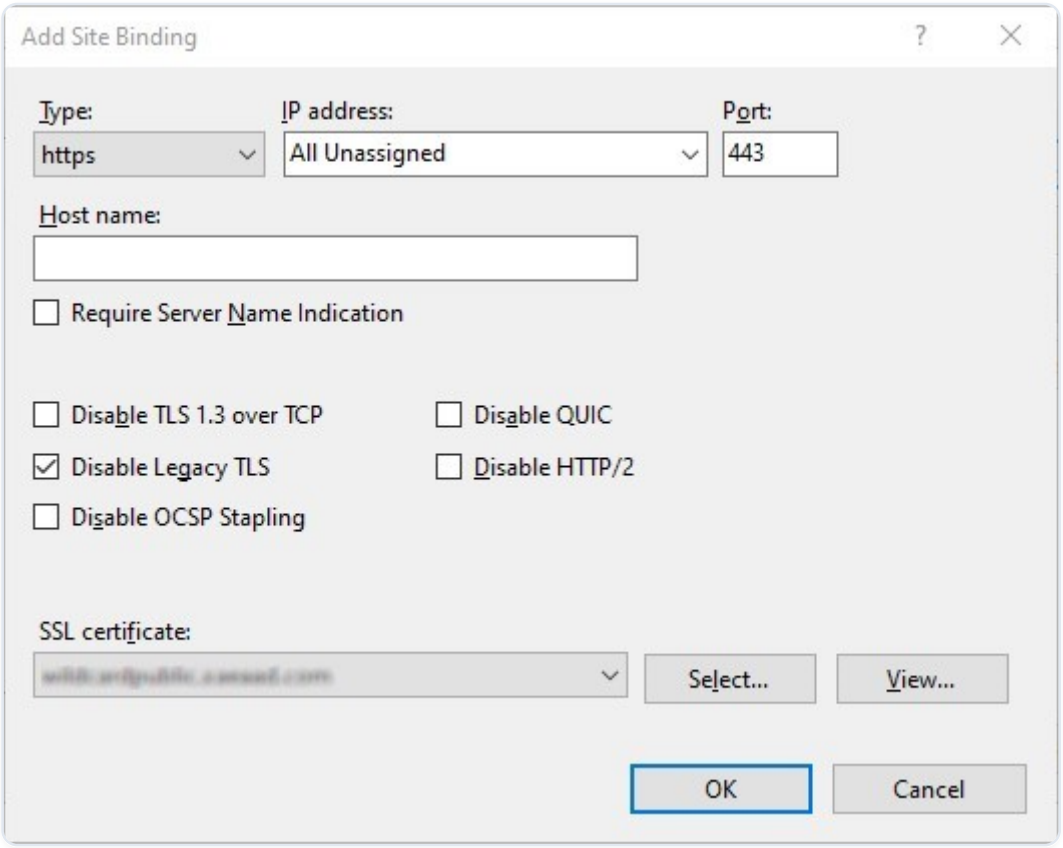
3. In the bindings window click **Add...**
4. In the **Type** drop down select **https**

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

5. On Windows Server 2022 or above, click **Disable Legacy TLS** to disable TLS older than 1.2.

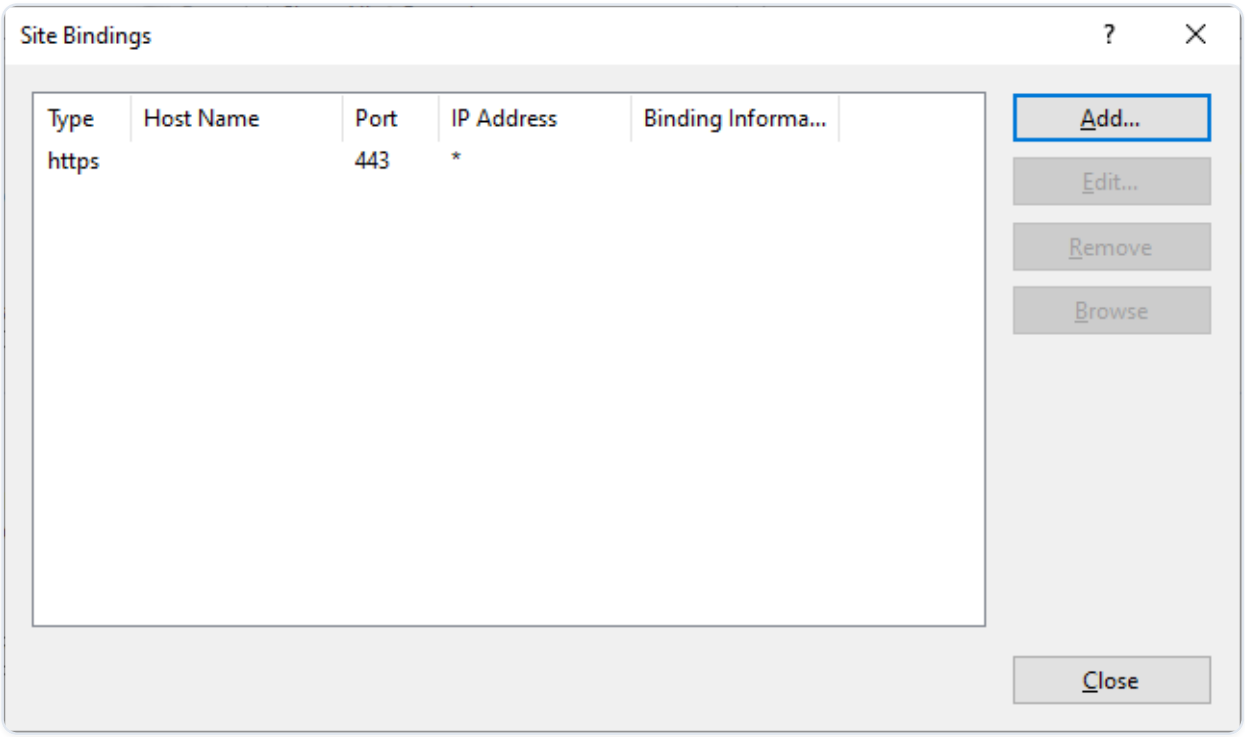
   On older Windows Server versions, you can disable legacy TLS versions using Windows registry settings, see Windows Server Documentation.

6. Select the certificate previously imported. Press OK



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

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

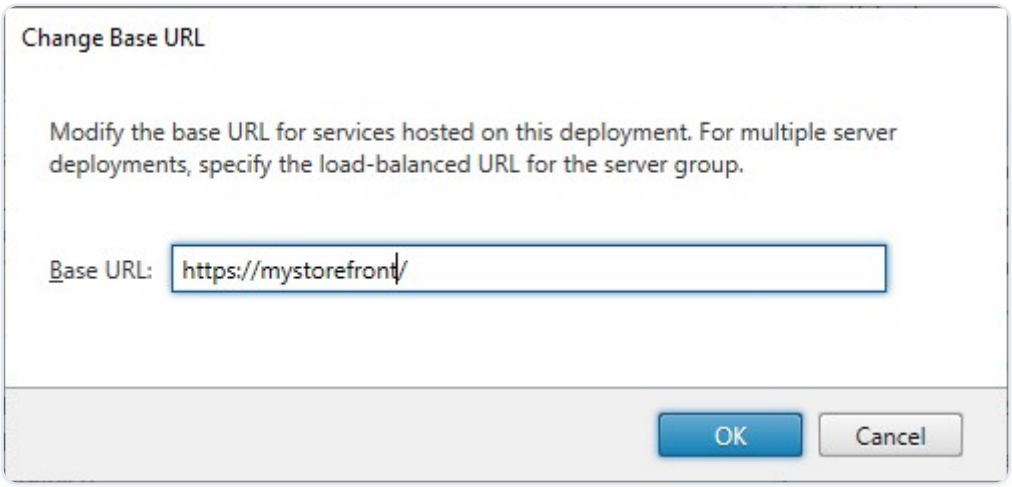


Change StoreFront server base URL from HTTP to HTTPS

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

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

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



© 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.

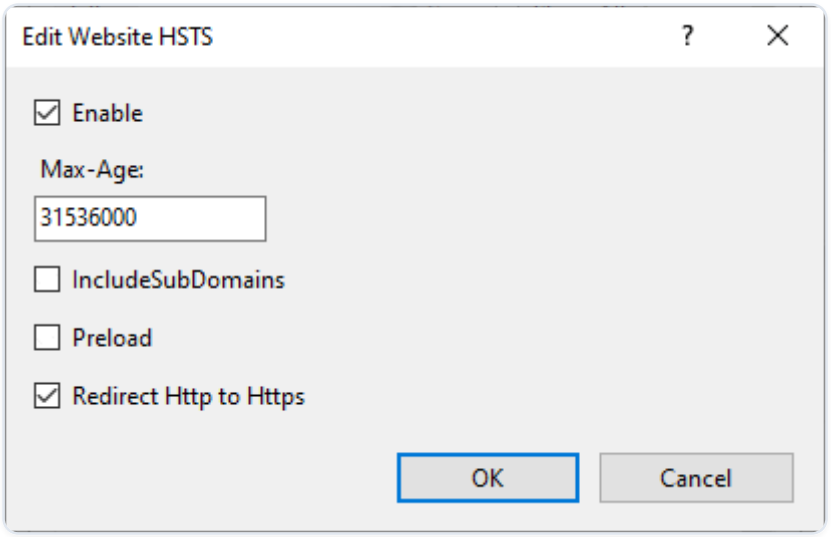
There are a number of options for enabling HSTS. You should choose only one option to avoid setting the same header multiple times.

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 Receiver for Web Sites**.
2. Select the website and click **Configure...**
3. Go to the **Advanced Settings** tab
4. Select **Enable strict transport security**.
5. Update **Strict transport security policy duration** to the required value.
6. Click **OK**.

Option 3 - NetScaler® load balancer

If you are using a NetScaler load balancer in front of your StoreFront servers then you can configure HSTS on the virtual server. For more information, see NetScaler documentation.

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.

Secure your StoreFront deployment

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

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

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 2022, you can configure IIS to disable TLS 1.0 and 1.1 for client connections, see Securing StoreFront with HTTPS. On all Windows server versions, you can disable TLS 1.0 and 1.1 using Group Policy or Windows registry settings, see Microsoft documentation.

Older versions of Citrix Receiver cannot connect using TLS 1.2, see CTX232266 for more details.

Communication with Delivery Controllers

Citrix recommends using the HTTPS protocol to secure data passing between StoreFront and your Citrix Virtual Apps and Desktops delivery controllers. For more information, see Enable HTTPS on Delivery Controllers. To configure StoreFront to use HTTPS, see Add resource feeds 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.

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

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 resource feeds for Citrix Desktops as a Service and Add Citrix Gateway appliance. In case the certificates are compromised, you can use Certificate Revocation List (CRL) checking. StoreFront uses TLS 1.2 or higher to communicate with Cloud Connectors.

It is recommended that you configure DaaS and StoreFront to ensure that only trusted StoreFront servers can communicate with the Cloud Connectors. For more information, see Manage security keys.

Communication with Federated Authentication Service

For information on communication between StoreFront and Federated Authentication Service (FAS) servers, see Federated Authentication Service - Security and network configuration.

Remote access

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

Microsoft Internet Information Services (IIS) hardening

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

Filename extensions

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

StoreFront requires the following file name extensions:

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

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

- .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

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

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

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.

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.

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

Handler Mappings

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

- ExtensionlessUrlHandler-Integrated-4.0
- PageHandlerFactory-Integrated-4.0
- StaticFile

See IIS Handlers Documentation.

ISAPI filters

StoreFront does not require any ISAPI filters. You can remove all ISAPI filters. However, ASP.NET requires the ISAPI Windows feature. See IIS ISAPI Filters documentation.

.NET Authorization Rules

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

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

Retail mode

You can enable Retail mode, see IIS documentation.

Application Pools

StoreFront creates the following application pools:

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

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

Under the Recycling settings, you can set the application pool idle time-out and Virtual Memory Limit. Note that when the "Citrix Receiver for Web" application pool recycles it causes users logged in through a web browser to be logged out, therefore it is set by default to recycle at 02:00 each

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

day to minimize disruption. If you change any of the recycling settings this may result in users being logged off at other times of the day.

Default IIS landing page

You can delete files `iisstart.htm`, `welcome.png` from `c:\inetpub\wwwroot`.

Required settings

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

Services

StoreFront installation creates the following Windows services:

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

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

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

User rights assignment

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

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

- Microsoft IIS is enabled as part of StoreFront installation. Microsoft IIS grants the logon right **Log on as a batch job**, and the privilege **Impersonate a client after authentication** to the built-in group IIS_IUSRS. This is normal Microsoft IIS installation behavior. Do not change these user rights. Refer to Microsoft documentation for details.
- When you install StoreFront, it creates Application Pools which IIS grants user rights **Log on as a service**, **Adjust memory quotas for a process**, **Generate security audits**, and **Replace a process level token**.
- To create or change a deployment, the admin must have rights **Restore files and directories**.
- For a server to join a server group, the Administrators group must have rights **Restore files and directories**, **Access this computer from the network** and **Manage auditing and security log**.
- For users to log on with a username and password authentication (directly or via a gateway), they must have rights to **Allow log on locally**, unless you have configured StoreFront to validate passwords via the delivery controller.

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

Configure group memberships

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

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

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

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

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

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

StoreFront installation also creates the following local security groups:

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

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

NTLM

If you have favorites enabled using the local ESENT database then StoreFront uses NTLM when synchronizing favorites between servers in a server group. If you disable NTLM then favorites will fail to synchronize. This might be resolved using StoreFront 2402 CU3 or higher. As an alternative you can use a SQL Server database.

StoreFront uses NTLM when synchronizing credentials between servers in a server group. If NTLM is disabled then users might to need to re-authenticate if the load balancer changes which server the user is connected to. This might be resolved using StoreFront CU3 or higher. This can be mitagated against by using sticky load balancing. Note that for web browser access, sticky load balancing is always required.

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.

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

You can configure the server to only use NTLMv2 and reject NTLMv1, see Microsoft documentation. In Windows Server 2025 and higher, NTLMv1 has been removed so NTLMv2 is always used.

Certificates in StoreFront

Server certificates

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

For more information see Communication between end users and StoreFront and Ica file signing.

Token management certificates

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

Citrix Delivery Services certificates

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

Code signing certificates

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

Although StoreFront does not install a code signing certificate in the Trusted Publishers store, Windows can automatically add the code signing certificate there. This happens when the PowerShell script is executed with the **Always run** option. (If you select the **Never run** option, the

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

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 Workspace app deployment.

ICA file signing

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

App protection

You can use App Protection to prevent screen capture and screen loggers. For hybrid launches, App Protection is disabled by default. To enable it see App Protection.

User change password

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

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

prevents users from changing their passwords, even if they have expired. For more information, see Enable users to change their passwords.

Customizations

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

Security Headers

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

HEADER NAME	VALUE	DESCRIPTION
`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, from CU3, the HTML page includes a `meta` tag containing a `content-security-policy` that 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`

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

HEADER NAME	VALUE	DESCRIPTION
`X-XSS-Protection`	`1; mode=block`	Used by some browsers to mitigate against XSS (cross-site-scripting) attacks

`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 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.

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

Additional security information

NOTE:

This information may change at any time, without notice.

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

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

Email-based account discovery

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

During the initial configuration process, Citrix Workspace app prompts users to enter either an email address or a store URL. If the user enters an email address, Citrix Workspace app looks up the email domain in a number of locations to determine the StoreFront server. It then lists all visible stores for the user to choose from.

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

Global App Config Service

To configure email discovery using the Global App Config Service, see Setup email based discovery.

DNS SRV records records

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

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

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

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

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

DNS discoverReceiver record

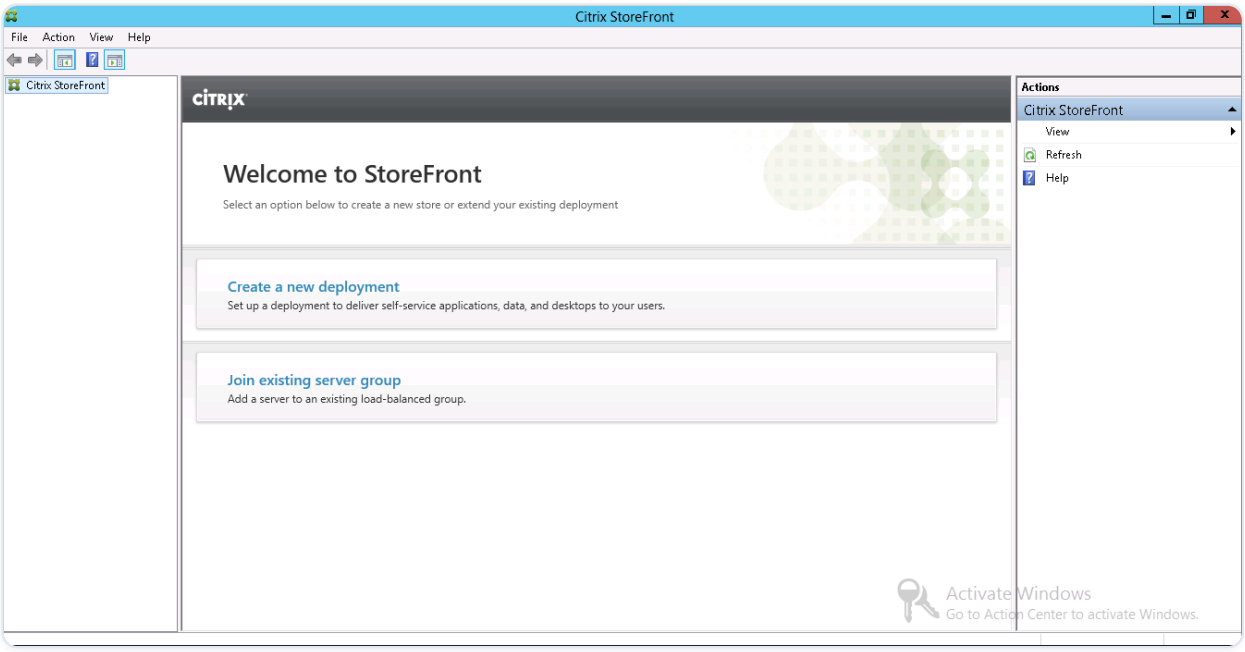
As a fallback to the other methods, you can create an DNS alias to the StoreFront server `discoverReceiver` on the email domain. For example if your email domain is `example.com`, create a DNS alias called `discoverReceiver.example.com`. If no SRV record is found in the specified domain, Citrix Workspace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

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

Create a new deployment

1. If the Citrix StoreFront management console is not already open after installation of StoreFront, on the Windows Start menu, select Citrix StoreFront.

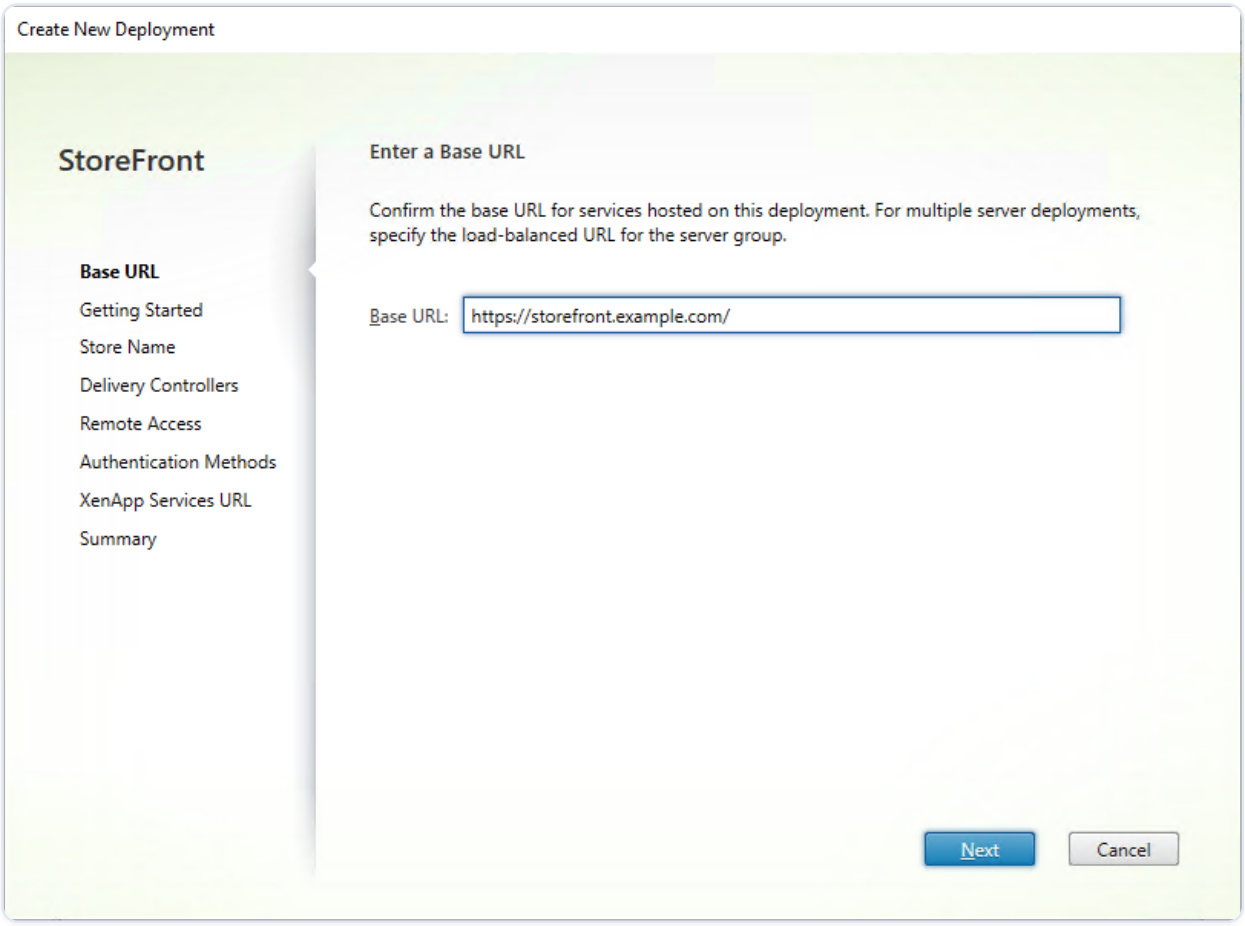
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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 the PowerShell SDK

To create a deployment using the PowerShell SDK, call cmdlet Add-STFDeployment.

Multiple Internet Information Services (IIS) websites

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

To create multiple web sites see Microsoft IIS documentation.

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

© 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 configure the sites using the StoreFront SDK and include the `SiteID` in each command.

Join an existing 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 and CU 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 on the other servers in the group.

NOTE:

For recommendation on server group size, see StoreFront Server groups.

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

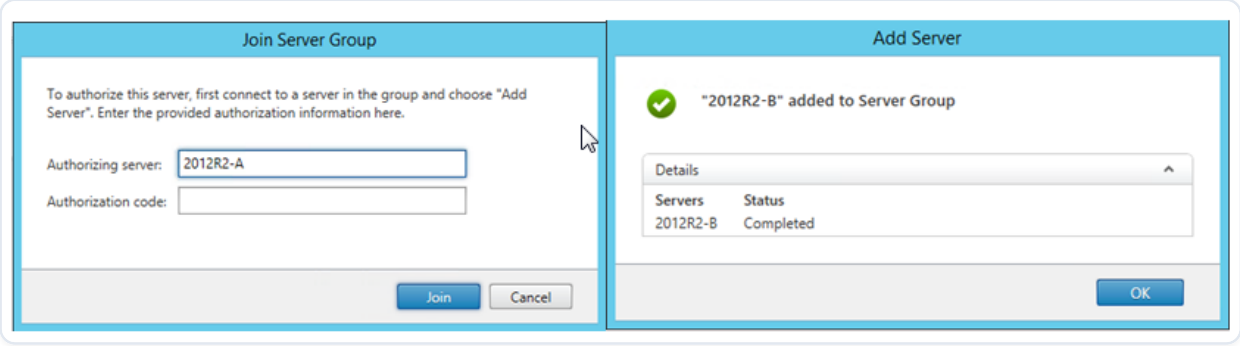
© 1997–2026 Citrix Systems, Inc. All rights reserved.

IMPORTANT:

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

1. If the Citrix StoreFront management console is not already open after installation of StoreFront, on the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. In the results pane of the Citrix StoreFront management console, click **Join existing server group**.
3. Log on to a server in the StoreFront deployment that you wish to join and open the Citrix StoreFront management console. Select the Server Group node in the left pane of the console and, in the Actions pane, click **Add Server**. Make a note of the authorization code that is displayed.
4. Return to the new server and, in the Join Server Group dialog box, specify the name of the existing server in the Authorizing server box. Enter the authorization code obtained from that server and click **Join**.

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



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

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

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 2402 from:

- StoreFront 2311
- StoreFront 2308
- StoreFront 2203 LTSR (any CU)
- StoreFront 1912 LTSR (any CU)
- StoreFront 3.12 LTSR CU9

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

WARNING:

When you upgrade from versions prior to 1912, any Desktop Appliance sites in your deployment are automatically removed. As an alternative, Citrix recommend using Citrix Workspace app Desktop Lock for all non-domain-joined use cases.

Good to know

- 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,

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

    - importing the StoreFront configuration you exported before the upgrade, see Export and import the StoreFront configuration,
    - performing the troubleshooting advice in Troubleshoot StoreFront upgrade issues.

- Any StoreFront upgrade failures which occur from the Citrix Virtual Apps and Desktops metainstaller are reported in a dialog, with a link to the relevant failure log.
- Hybrid launch through StoreFront versions between 1912 and 2203

  StoreFront versions between 1912 and 2203 supports the enabling of hybrid launch of virtual apps and desktops that are enabled with App Protection policies using a customization as follows:

  Citrix® recommends removing this customization when upgrading to StoreFront 2308 or later.

  For more information, see Hybrid launch through StoreFront versions between 1912 and 2203

Get ready to upgrade

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

- Plan your backup strategy before upgrading.
- Verify that you are upgrading from a supported version.
- Download the StoreFront installer from the Citrix website.

Upgrade a single StoreFront server

1. Back up the server by creating a VM snapshot.
2. Export the existing StoreFront configuration. If you have multiple servers in a server group then only export the server group configuration from one server. Provided you have propagated all changes between them, all servers in a server group maintain identical copies of the configuration. This backup allows you to easily build a new server group. so that you can easily restore the configuration in case of issues. Note that you will only be able to restore this backup into a server running the same version it was exported from.
3. If you have made modifications to files in `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data` or `C:\inetpub\wwwroot\Citrix\<StoreName>Auth\App_Data`, such as default.ica and usernamepassword.tfrm, back them up for each store. After the upgrade you can restore them to reinstate your modifications.

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

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.
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.

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

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

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

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.
3. If there are no exception errors in the Event Viewer, check the Admin logs in *C:\Program Files\Citrix\Receiver StoreFront\logs* for any errors containing the preceding exception error messages. Follow the corresponding advice.

For more details of logs files, see Installation Logs.

Reset a server to factory defaults

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

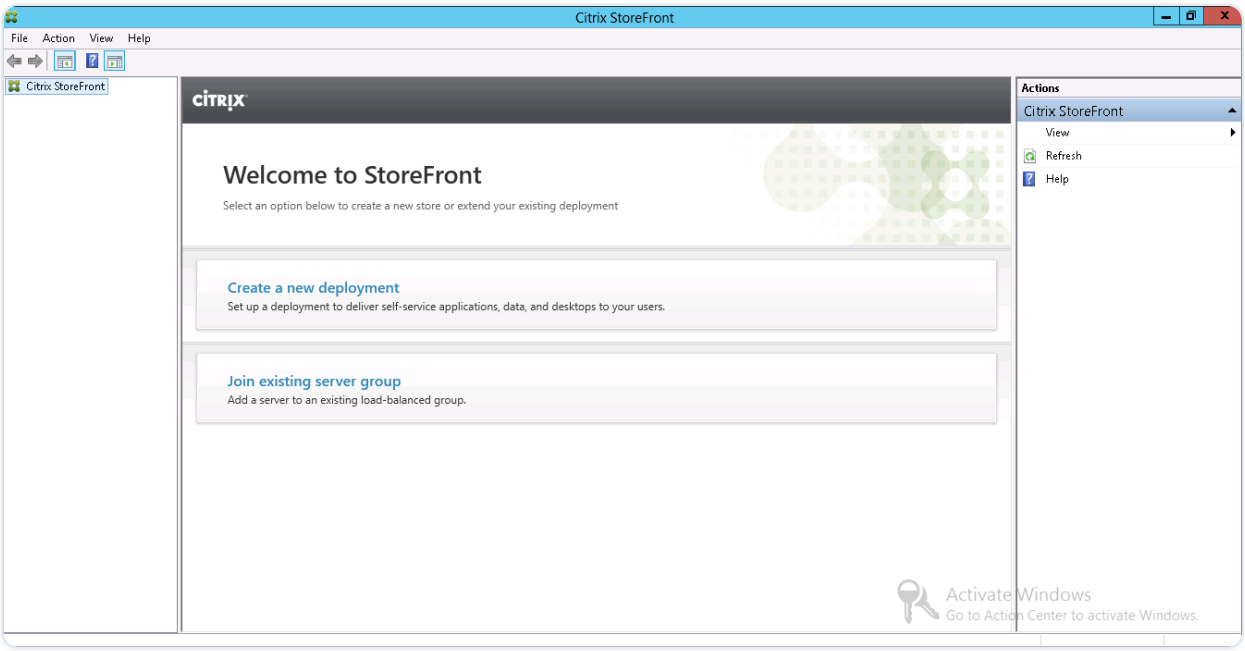
© 1997–2026 Citrix Systems, Inc. All rights reserved.

manual uninstall and reinstall can be performed, but this is more time consuming and may cause other unforeseen issues. Instead you can use PowerShell to reset configuration to defaults.

1. Ensure that the StoreFront management console is closed.
2. Run the PowerShell SDK cmdlet Clear-STFDeployment.

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

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

1. Log on to the StoreFront server using an account with local administrator permissions.
2. Close the StoreFront management console if it is open.

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

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

To manually remove StoreFront

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

1. Remove 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.

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
User name 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.

To select and configure which methods users can use to log into StoreFront through Citrix Workspace app, see Configure authentication. To select which methods users can use to log in using a web browser, see Configure Authentication for website.

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

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

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.

Authentication method customizations

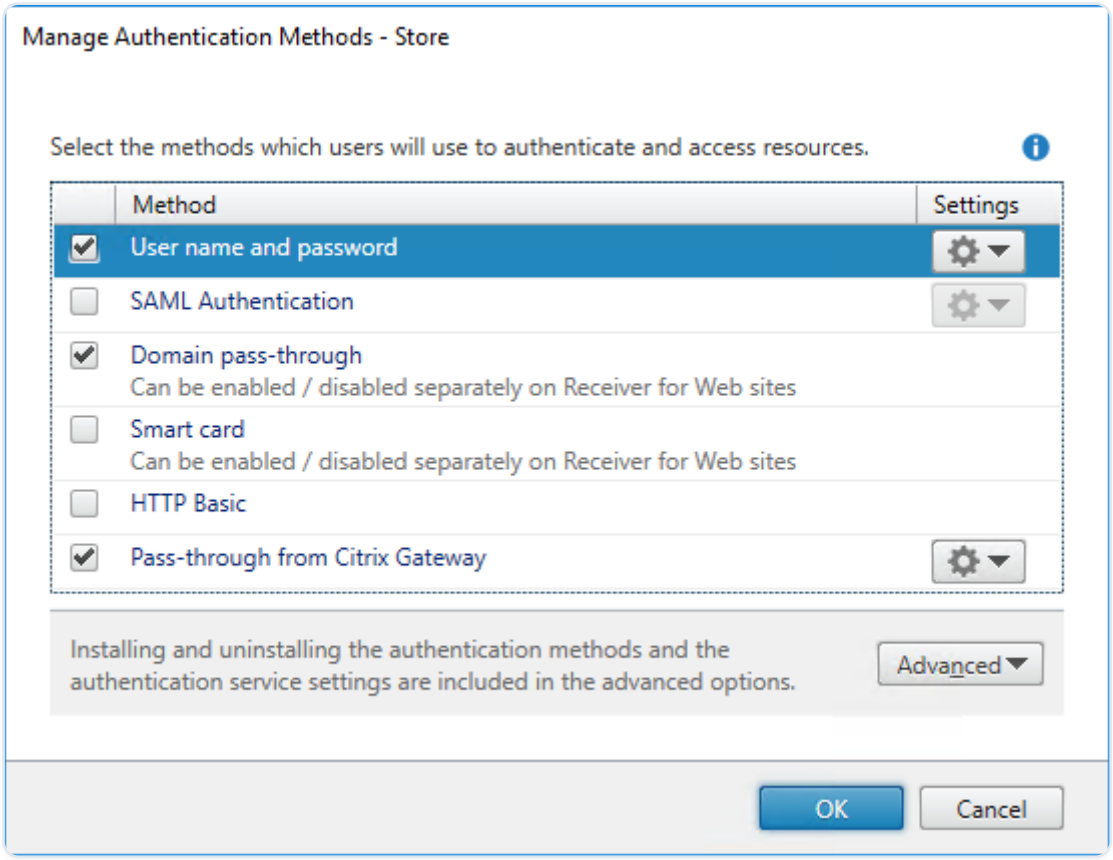
You can customize existing methods or create your own authentication methods using the Authentication SDK.

Configure authentication

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.

For available authentication methods, see Authentication.

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 SDK

To configure authentication using the PowerShell SDK:

1. Call Get-STFAuthenticationService to get the authentication service for a store or a virtual directory and to view its current configuration.
2. On the authentication service, enable or disable the required authentication protocols. To get a list of available protocols, run Get-STFAuthenticationServiceProtocol. To enable the protocols, run Enable-STFAuthenticationServiceProtocol with a list of protocols to enable. To disable the protocols, run Disable-STFAuthenticationServiceProtocol with the list of protocols to disable.

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:

- User name and password settings
- SAML authentication settings
- Pass-through from Citrix Gateway settings

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.

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

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

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**.

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.

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.

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

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

Prerequisites

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

Configure StoreFront

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

Configure Delivery Controller™ to trust StoreFront

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

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

Remote access via Citrix Gateway

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

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

Single sign-on to VDAs

You can enable single sign-on to the VDAs by passing-through users' smart card credentials. The store can be accessed through a web browser or Citrix Workspace™ app for Windows but the resource must be opened in Citrix Workspace app for Windows. On other operating systems or when accessing the resources through a browser, users must re-enter their credentials when connecting to a VDA.

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

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

separate stores for each group of users. Then, direct your users to the appropriate store for their method of authentication.

Alternatively you can configure Federated Authentication Service to single sign-on to VDAs

Important considerations

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

- To use virtual private network (VPN) tunnels with smart card authentication, users must install the Citrix Gateway plug-in and log on through a webpage, using their smart cards and PINs to authenticate at each step. Pass-through authentication to StoreFront with the Citrix Gateway plug-in isn't available for smart card users.
- Multiple smart cards and multiple readers can be used on the same user device, but if you enable pass-through with smart card authentication, users must ensure that only one smart card is inserted when accessing a desktop or application.
- When a smart card is used within an application, such as for digital signing or encryption, users might see extra prompts to insert a smart card or enter a PIN. This can occur if more than one smart card has been inserted at the same time. It can also occur due to configuration settings - such as middleware settings like PIN caching that are typically configured using group policy. Users who are prompted to insert a smart card when the smart card is already in the reader must click Cancel. If users are prompted for a PIN, they must enter their PINs again.
- If you enable pass-through with smart card authentication to Citrix Virtual Apps and Desktops for Citrix Workspace app for Windows users with domain-joined devices who do not access stores through Citrix Gateway, this setting applies to all users of the store. To enable both domain pass-through and pass-through with smart card authentication to desktops and applications, you must create separate stores for each authentication method. Your users must then connect to the appropriate store for their method of authentication.
- If you enable pass-through with smart card authentication to Citrix Virtual Apps and Desktops for Citrix Workspace app for Windows users with domain-joined devices accessing stores through Citrix Gateway, this setting applies to all users of the store. To enable pass-through authentication for some users and require others to log on to their desktops and applications, you must create separate stores for each group of users. Then, direct your users to the appropriate store for their method of authentication.
- Only one authentication method can be configured for each XenApp® Services URL and only one URL is available per store. If you need to enable other types of authentication in addition to smart card authentication, you must create separate stores, each with a XenApp Services URL,

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

for each authentication method. Then, direct your users to the appropriate store for their method of authentication.

- When StoreFront is installed, the default configuration in Microsoft Internet Information Services (IIS) only requires that client certificates are presented for HTTPS connections to the certificate authentication URL of the StoreFront authentication service. IIS does not request client certificates for any other StoreFront URLs. This configuration enables you to provide smart card users with the option to fall back to explicit authentication if they experience any issues with their smart cards. Subject to the appropriate Windows policy settings, users can also remove their smart cards without needing to reauthenticate.

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

Domain pass-through authentication

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**.

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

Configure Delivery Controller™ to trust StoreFront

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

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

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.

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.

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

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.

Pass-through from Citrix Gateway

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

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

- **Domain** Users log 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.

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

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

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

To enable multi domain authentication through Citrix Gateway to StoreFront, set SSO Name Attribute to userPrincipalName in the Citrix Gateway LDAP authentication policy for each domain. You can require users to specify a domain on the Citrix Gateway logon page so that the appropriate LDAP policy to use can be determined. When you configure the Citrix Gateway session profiles for connections to StoreFront, do not specify a single sign-on domain. You must configure trust relationships between each of the domains. Ensure that you allow users to log on to StoreFront from any domain by not restricting access to explicitly trusted domains only.

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

Enable Gateway pass-through

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

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

Configure trusted user domains

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

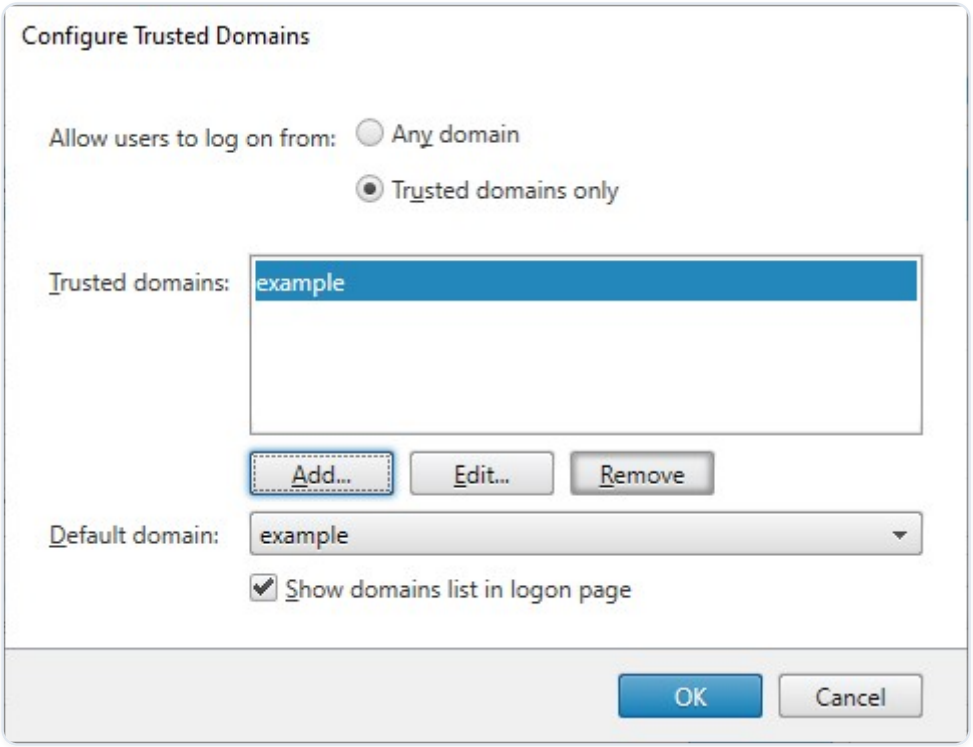
1. In the "Manage Authentication methods" window, from the **Pass-through from Citrix Gateway** > **Settings** drop-down menu, select **Configure Trusted Domains**.
2. Select **Trusted Domains only** and click **Add** to enter the name of a trusted domain. Users with accounts in that domain are able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

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

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

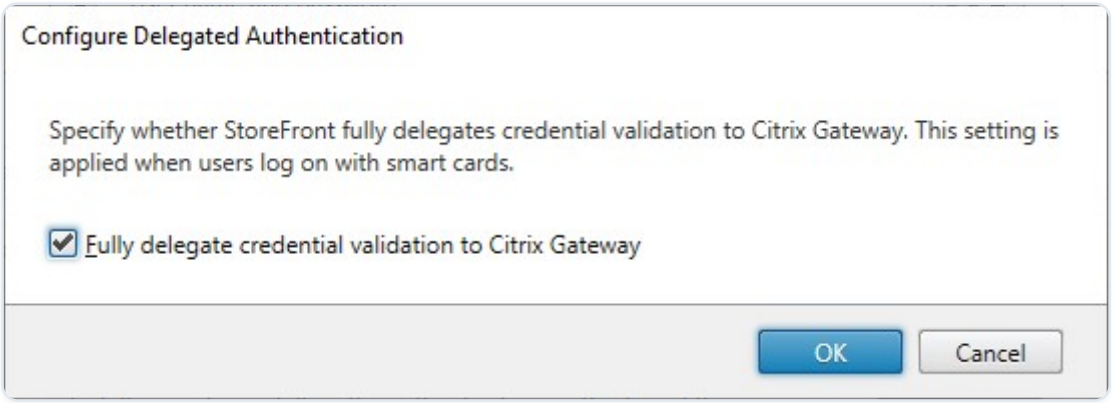


Delegated authentication

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

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

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



.

PowerShell SDK

To configure the store to delegate authentication to the Citrix Gateway using the PowerShell SDK, use cmdlet Set-STFCitrixAGBasicOptions

- To delegate authentication to the gateway set `CredentialValidationMode` to `Auto`.
- For StoreFront to validate the credentials, set `CredentialValidationMode` to `Password`.

Password validation

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

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

Allow users to change expired passwords at logon

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

1. Log into the NetScaler® administration website
2. On the side menu go to **Authentication** > **Dashboard**.
3. Click the authentication server.

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

4. Under **Other Settings** tick **Allow Password Change**.

Allow users to change passwords after logon

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

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

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



NOTE:

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

PowerShell SDK

To modify change password options using the PowerShell SDK, use cmdlet Set-STFExplicitCommonOptions.

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

Configure Delivery Controller™ to trust StoreFront

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

Single sign-on to VDAs using Federated Authentication Service

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

SAML authentication

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

NOTE

Configure StoreFront with SAML authentication for internal access. For external access configure Citrix Gateway with SAML authentication then configure StoreFront with Gateway pass-through authentication.

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

- Microsoft AD Federation Services using SAML bindings (not WS-Federation bindings). For more information, see CTX220638.
- Citrix Gateway (configured as an IdP).
- Microsoft Entra ID. For more information, see CTX237490.

The SAML assertion must 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 enables it for all

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

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
+ "/SamlForms/ServiceProvider/Metadata")

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

Write-Host "SAML Service Provider information:
```

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

```
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:

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



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

$StoreVirtualPath = "/Citrix/Store"
```

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

```
$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:

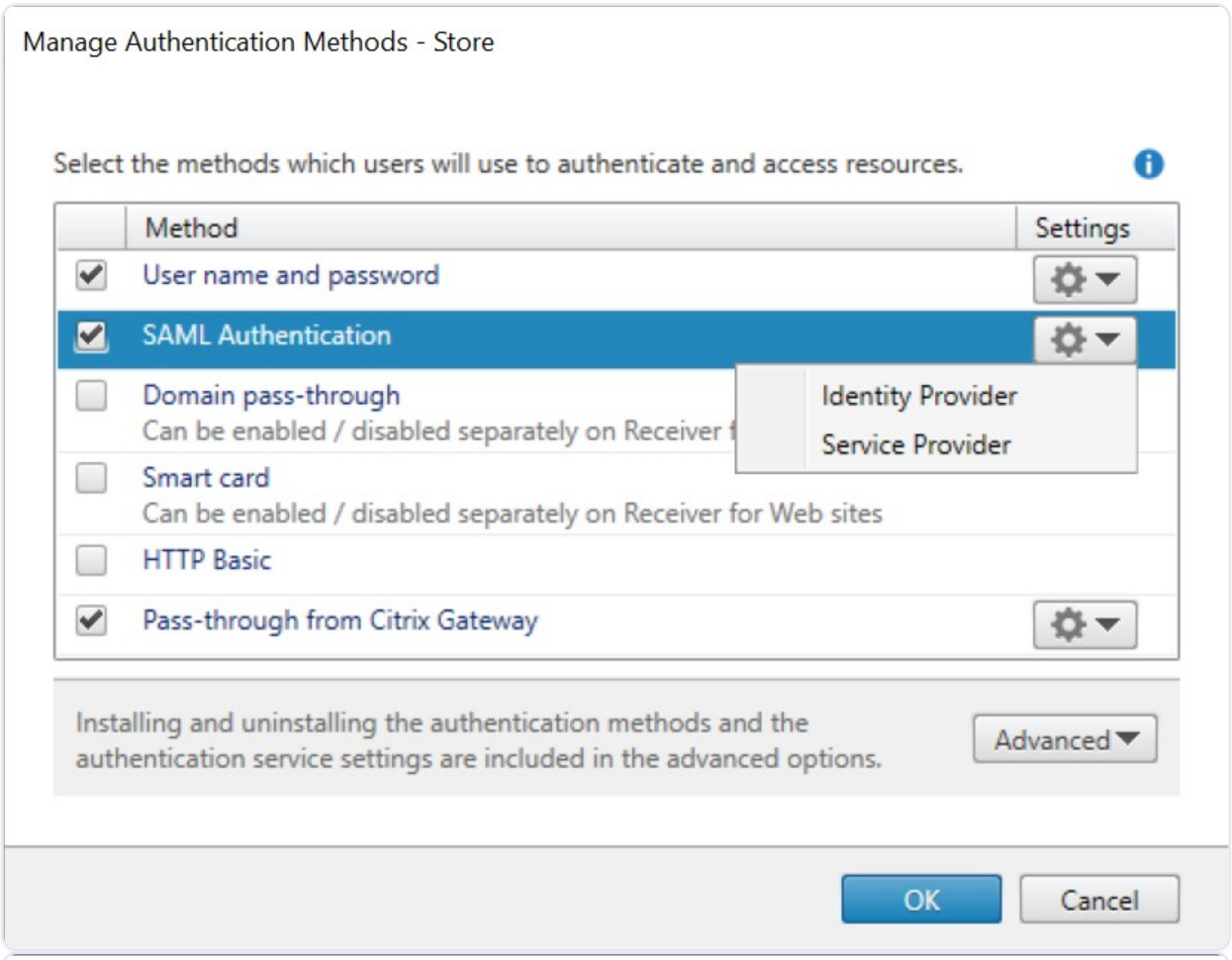
# Note: Ensure that the file is encoded as UTF-8

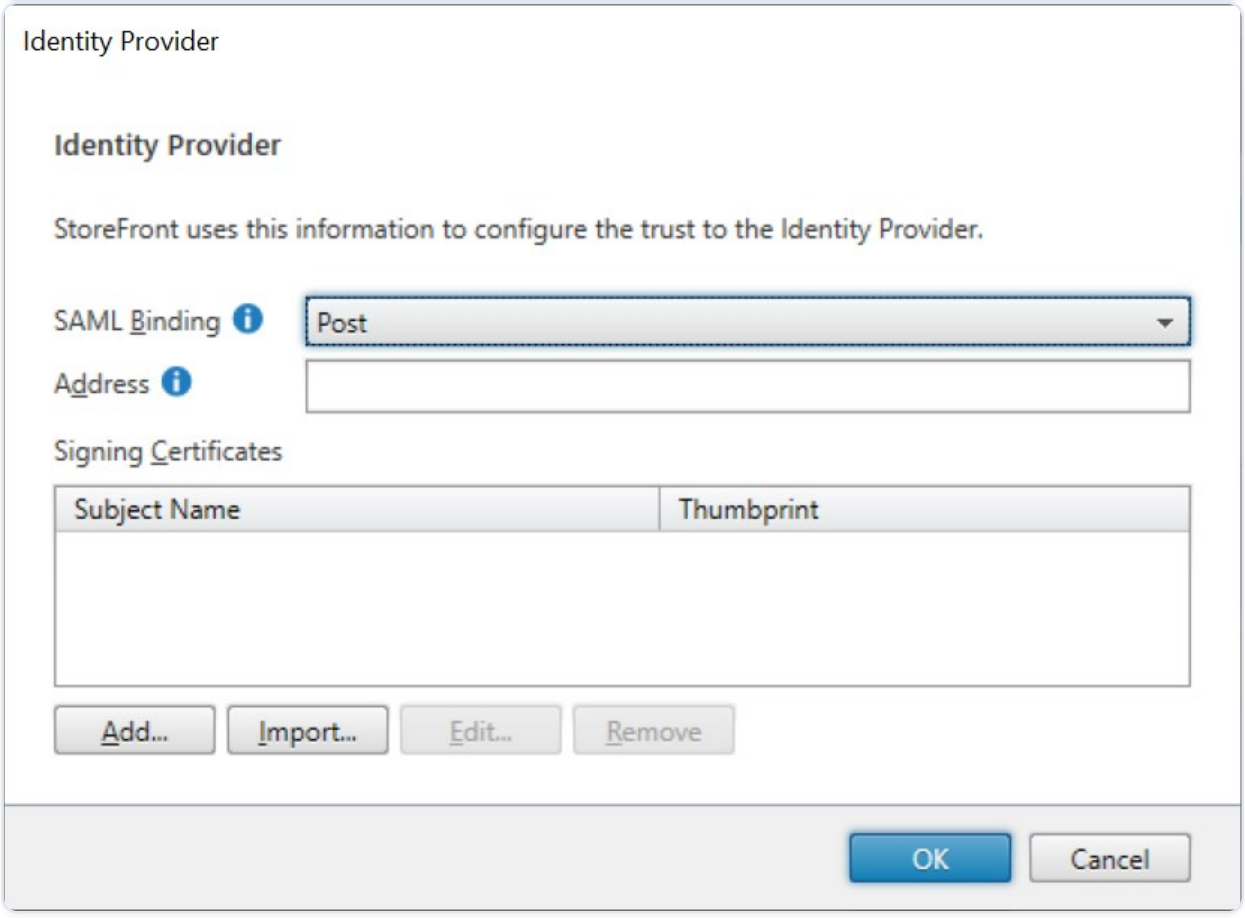
Update-STFSamlIdPFromMetadata -AuthenticationService $auth -FilePath "C:
\Users\exampleusername\Downloads\FederationMetadata.xml"
```

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.





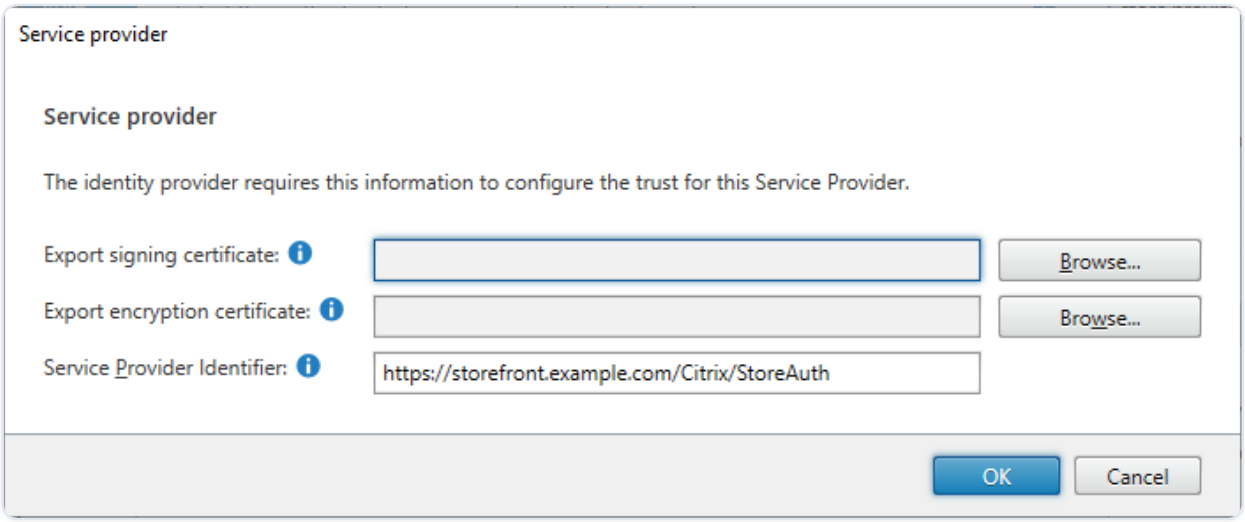
2. Choose **SAML Binding** of **Post** or **Redirect**.

© 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 SDK

Using the PowerShell SDK:

- To import a signing certificate call cmdlet Import-STFSamlSigningCertificate.
- To import an encryption certificate call cmdlet Import-STFSamlEncryptionCertificate.

Testing

To test the SAML integration:

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

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

Configure Delivery Controller™ to trust StoreFront

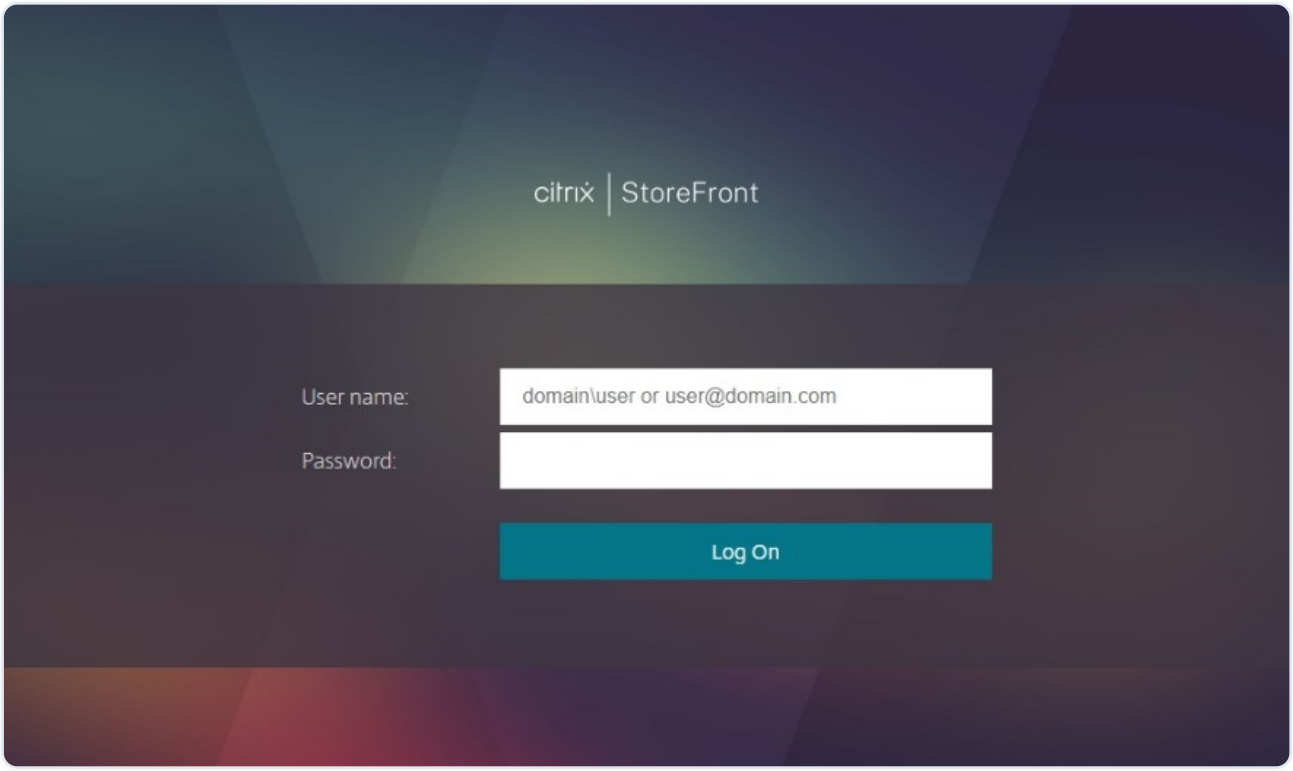
When using SAML authentication, StoreFront does not have access to the user's credentials so is unable to authenticate to Citrix Virtual Apps and Desktops. You must therefore configure the Delivery Controller to trust requests from StoreFront, see Citrix Virtual Apps and Desktops Security considerations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

Single sign-on to VDAs using Federated Authentication Service

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

User name and password authentication

With user name and password authentication, users are prompted to enter their active directory username and password.



.

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

To enable or disable user name and password authentication for a store when using Citrix Workspace app, in the Authentication Methods window tick or untick **User name and password**.

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

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 Receiver for Web Sites Authentication methods tab.

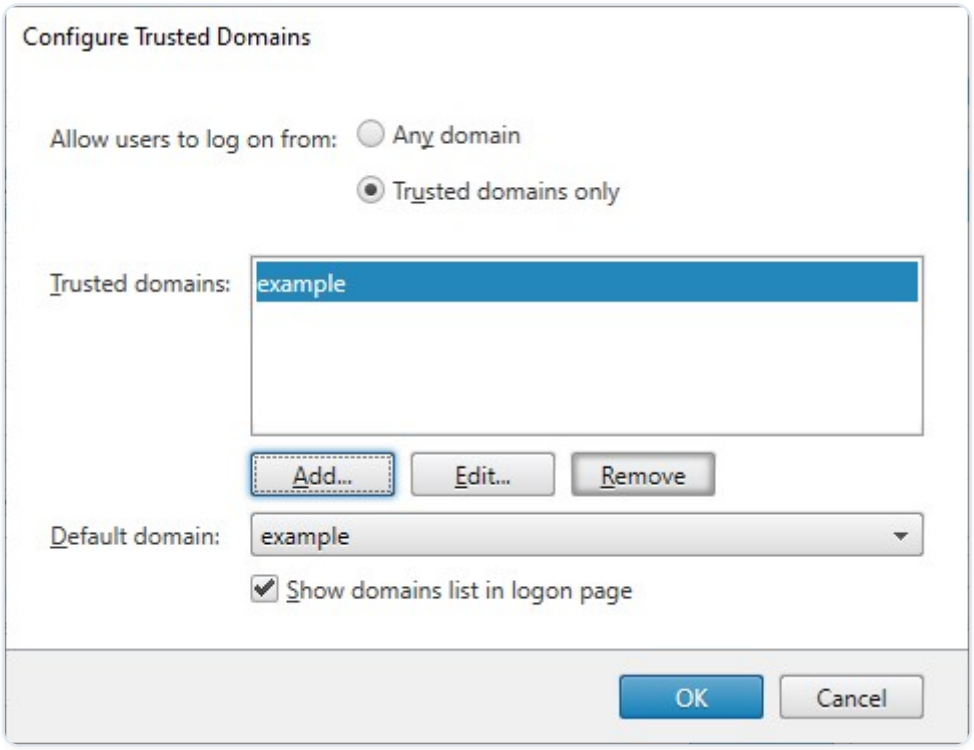
Configure trusted user domains

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

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

   The way in which you specify the domain name determines the format in which users must enter their credentials. If you want users to enter their credentials in domain user name format, add the NetBIOS name to the list. To require that users to enter their credentials in user principal name format, add the fully qualified domain name to the list. If you want to enable users to enter their credentials in both domain user name format and user principal name format, you must add both the NetBIOS name and the fully qualified domain name to the list.
4. If you configure multiple trusted domains, select from the Default domain list the domain that is selected by default when users log on.
5. If you want to list the trusted domains on the logon page, select the Show domains list in the logon page check box.

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



PowerShell

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

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

Enable users to change their passwords

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

Change password functionality is available in the following clients:

CITRIX WORKSPACE APPS	USER CAN CHANGE AN EXPIRED PASSWORD IF ENABLED ON STOREFRONT	USER IS NOTIFIED THAT PASSWORD WILL EXPIRE	USER CAN CHANGE PASSWORD BEFORE IT EXPIRES IF ENABLED ON STOREFRONT
Windows	Yes		
Mac	Yes		
Android			

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

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
iOS			
Linux	Yes		
Web	Yes	Yes	Yes

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

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

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

   NOTE:
   If you do not select this option, you must make your own arrangements to support users who can't access their desktops and applications because their passwords have expired.
3. Choose whether to allow users to change passwords **Only when they expire** or **At any time**.
4. Choose whether to remind users before their passwords expire. 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.

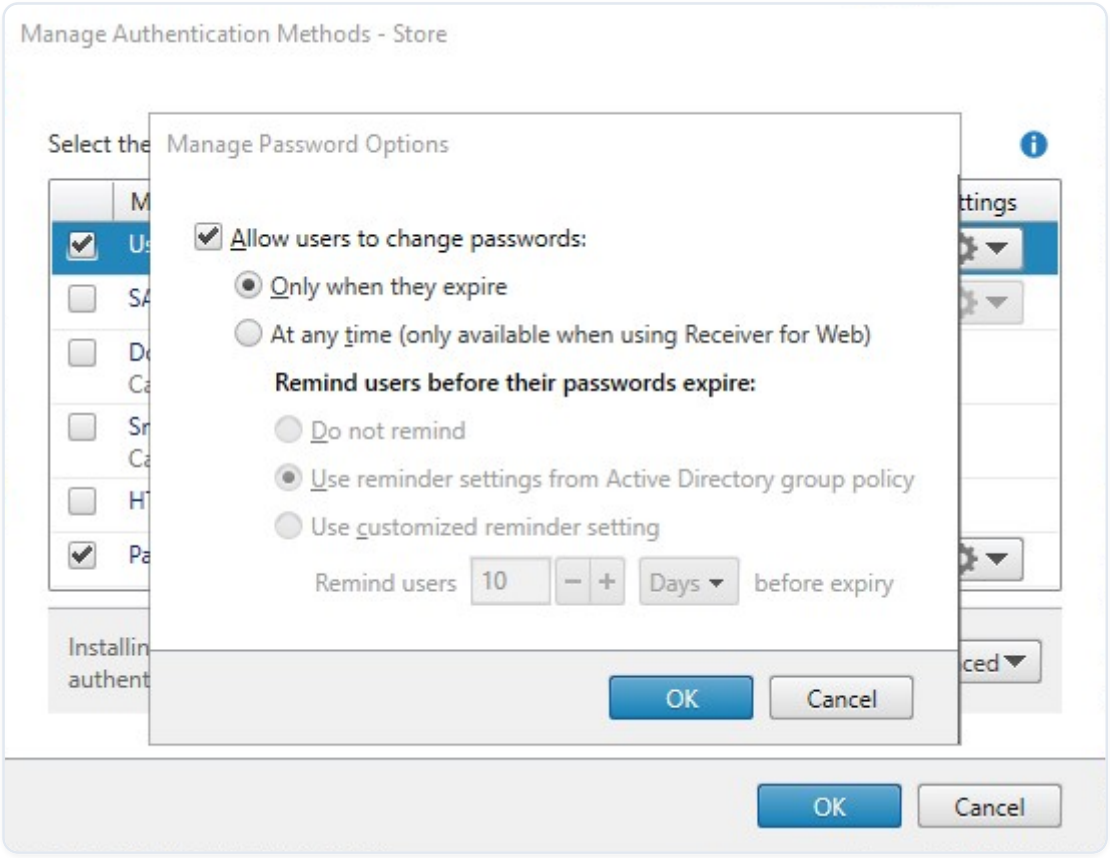
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **Use reminder settings from Active Directory group policy** - After logging in, the user interface notifies if their password is going to expire in the number days configured in group policy. The user is given the option to change their password.

  NOTE:

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

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



NOTES

Note 1:

Ensure that there's sufficient disk space on your StoreFront servers to store profiles for all your users. To check whether a user's password is about to expire, StoreFront creates a local profile for

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

that user on the server. StoreFront must be able to contact the domain controller to change users' passwords.

Note 2:

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

PowerShell

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

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

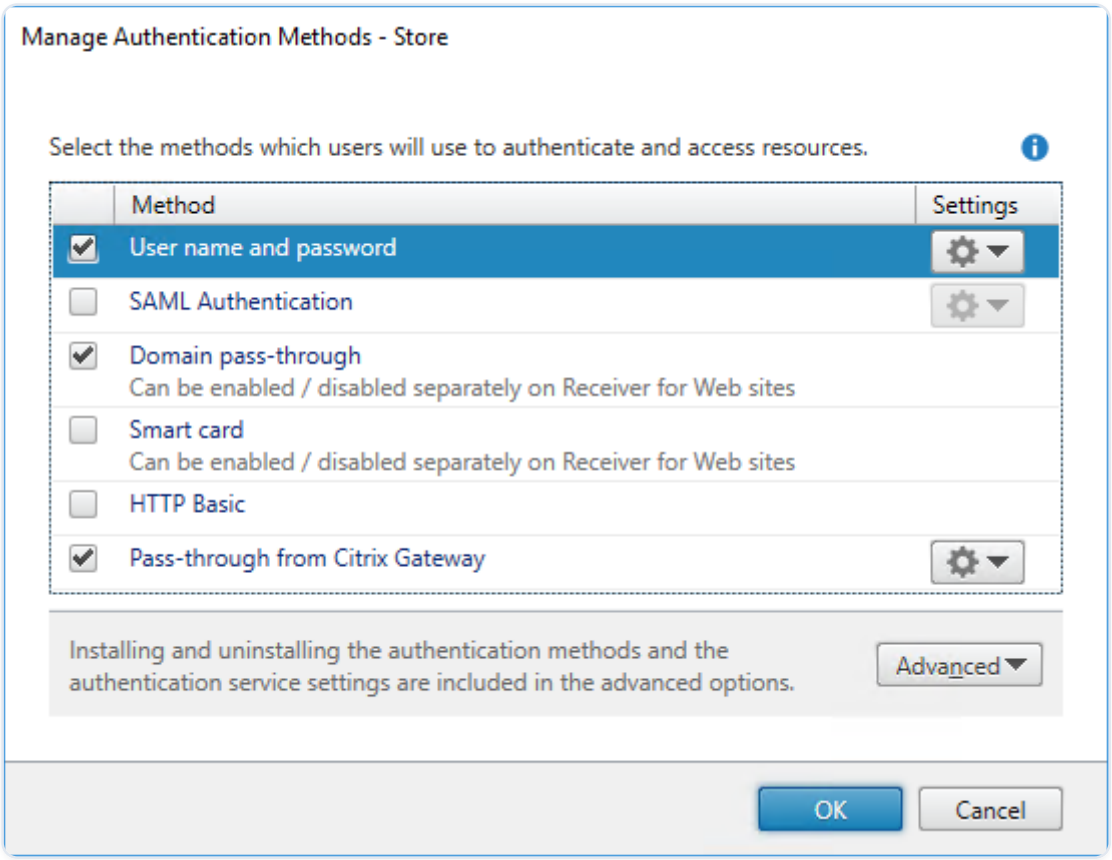
Password validation

Normally StoreFront asks Windows to validate the credentials in Active Directory. This requires that the Windows server is on the same domain as the user, or there is a trust relationship between the two domains. When it is not possible to put Active Directory trusts in place, you can configure StoreFront to use the Citrix Virtual Apps and Desktops delivery controllers to authenticate the credentials. This also affects HTTP Basic and Gateway Pass-through authentication.

To configure how StoreFront validates passwords:

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

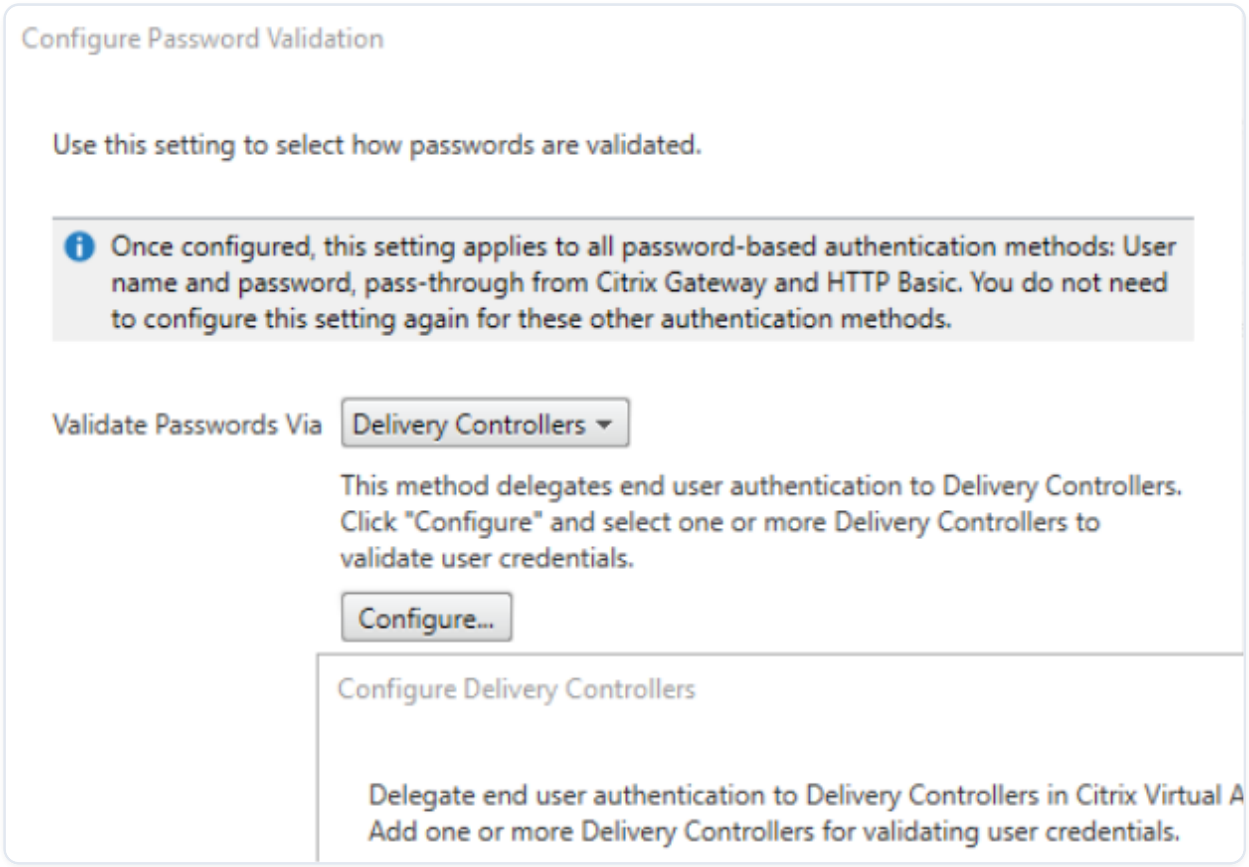
© 1997–2026 Citrix Systems, Inc. All rights reserved.



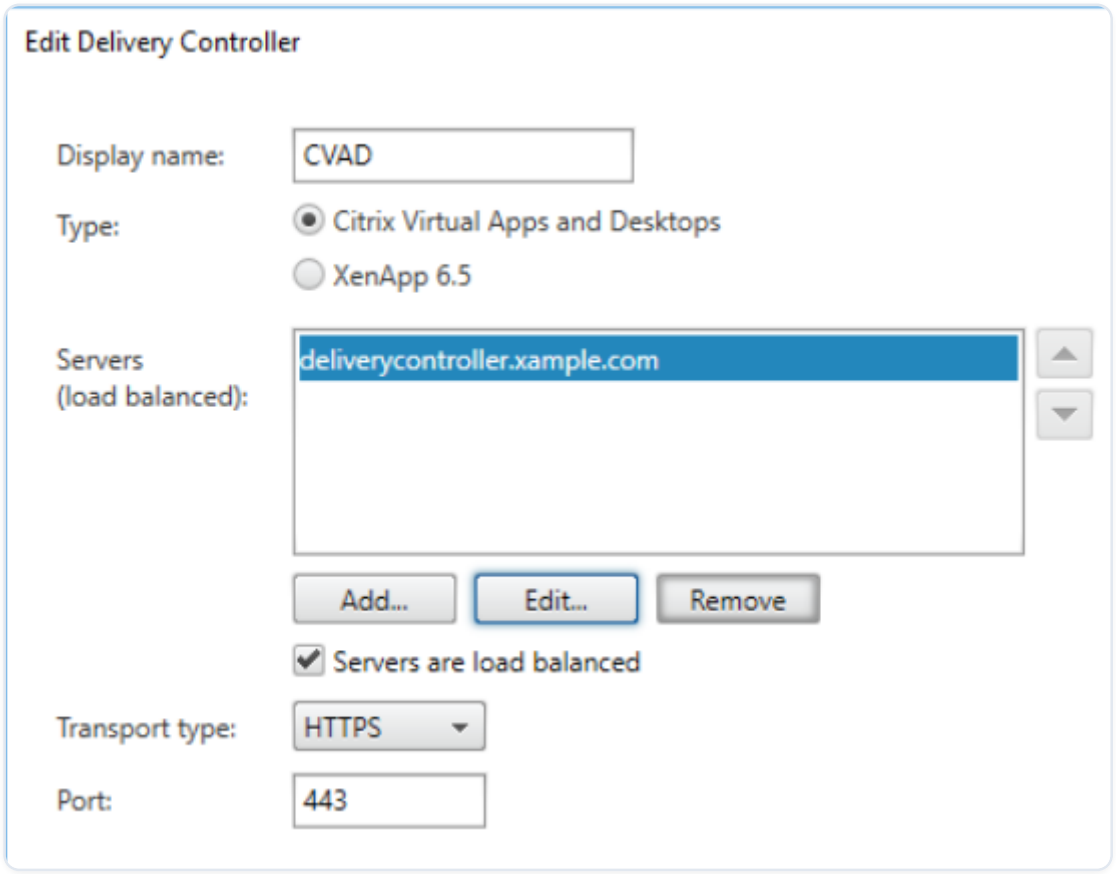
2. From the **Validate Password Via** drop down, choose:

   - **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.

Federated Authentication Service Configuration

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

Enable FAS for a Store

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

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

By default, StoreFront selects the FAS server at launch. You can change this so that StoreFront selects the FAS server at login. This has the advantage that it avoid delays that can occur at launch, particularly if a FAS server is unavailable so it has to try multiple FAS servers. However it has the disadvantage that if the FAS server becomes unavailable between login and launch then the launch either fails or falls back to username and password authentication (see FAS server unavailability). To configure the behavior, run PowerShell cmdlet Set-STFClaimsFactoryNames

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

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

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

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider
"FASLogonDataProvider"

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName
"FASClaimsFactory"
```

To disable FAS for a store:

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

$auth = Get-STFAuthenticationService -StoreService $store

Set-STFStoreLaunchOptions -StoreService $store -VdaLogonDataProvider ""

Set-STFClaimsFactoryNames -AuthenticationService $auth -ClaimsFactoryName
"standardClaimsFactory"
```

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

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

FAS server unavailability

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

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

```
$storeService = Get-STFStoreService -VirtualPath [VirtualPath]

Set-STFStoreLaunchOptions $storeService
-FederatedAuthenticationServiceFailover $True
```

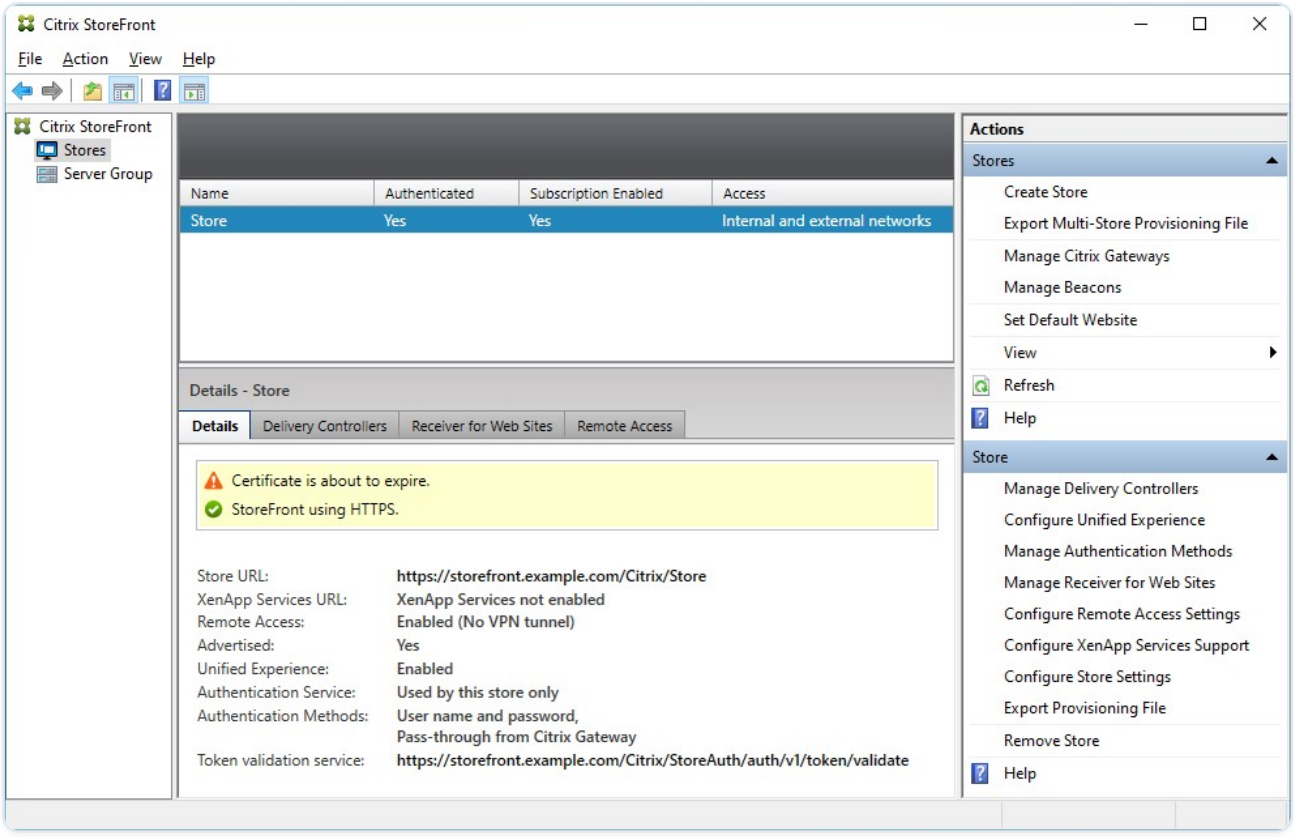
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Configure and manage stores

In Citrix StoreFront, you can create and manage stores that aggregate applications and desktops from Citrix Virtual Apps and Desktops giving users on-demand, self-service access to resources. You can create multiple stores, each with their own set of configuration and one or more websites. 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:

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

TAB	DETAIL
Details	Gives store details such as the URL and authentication methods
Delivery Controllers	Lists the resource feeds, such as CVAD sites or DaaS, that have been configured for the store
Receiver for Web Sites	Lists all websites configured for the store.
Remote Access	Details of whether remote access is enabled via a Citrix Gateway

Create a store

From the **Actions** pane **Stores** section, press **Create store**. For more details, see Create Store.

Store actions

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

TASK	DETAIL
Manage Delivery Controller	Add and remove sites.
Manage authentication methods	Choose which methods users can use to authenticate to the store
Manage Receiver for web sites	Manage the website used to access the store
Manage remote access settings	Configure access to stores through Citrix Gateway for users connecting from public networks.
Configure Store Settings	Configure Favorites, Kerberos Delegation, Optimal HDX routing, Advertise Store and Advanced Settings
Export provisioning file	Generate files containing connection details for stores, including any Citrix Gateway

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

TASK	DETAIL
	deployments and beacons configured for the store.
Remove a store	Remove an unneeded store.

Advanced configuration

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

TASK	DETAIL
Certificate Revocation List (CRL) checking	configure StoreFront to check the status of TLS certificates used by CVAD delivery controllers using a published certificate revocation list (CRL).
Configure two StoreFront stores to share a common subscription datastore	Configure two StoreFront stores to share a common subscription datastore.
Manage subscription data for a store	View, import, export and purge subscription data (favorites).
Store favorites data using Microsoft SQL Server	Use an external SQL server database for storing subscription (favourite) data.
Citrix Virtual Apps and Desktops configuration	Configure Citrix Virtual Apps and Desktops settings that affect how resources are displayed in store website
Default ica settings	Configure HDX settings by adding them to default.ica
ICA file signing	Configure ica file signing
Citrix Workspace app Configuration	Use StoreFront to configure Citrix Workspace app

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

Create store

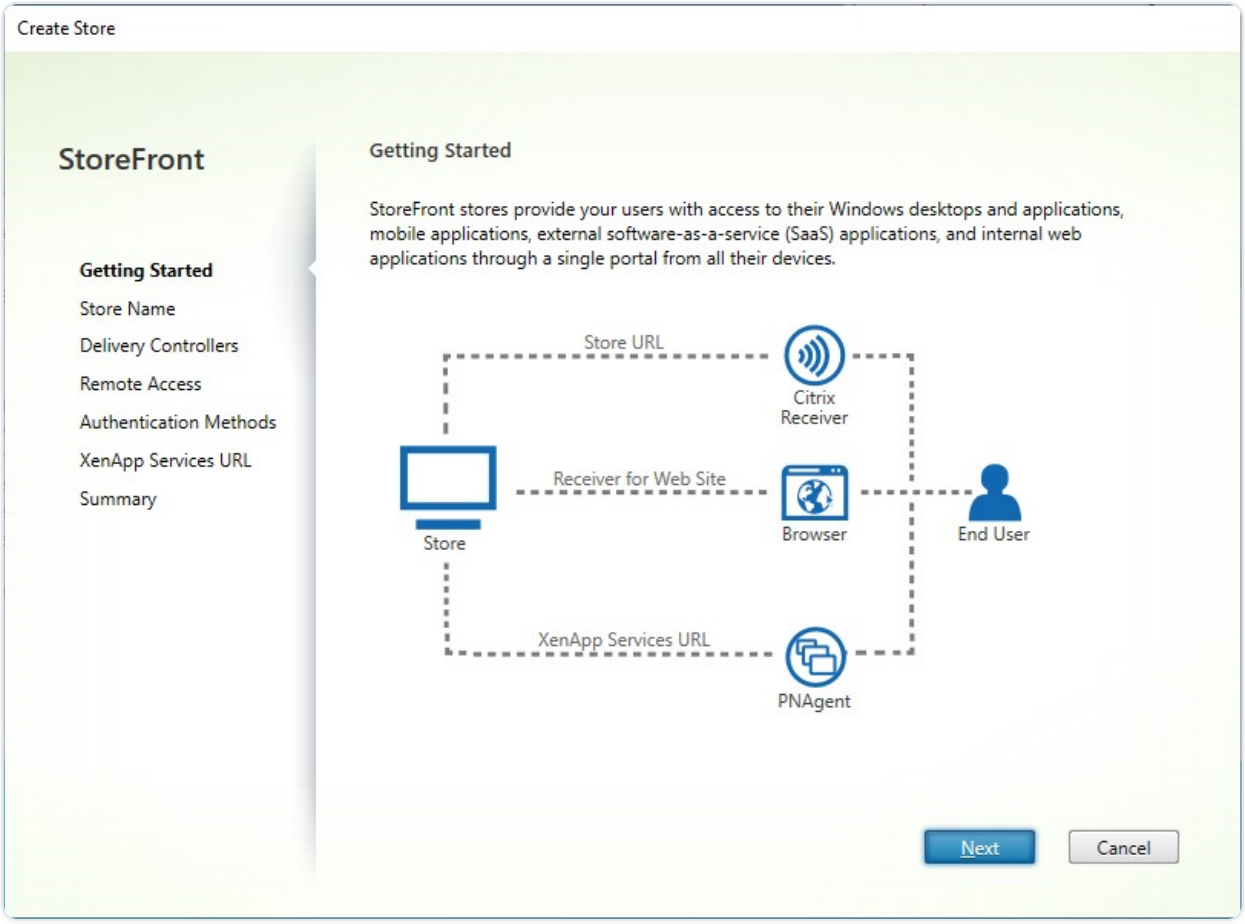
You can create as many stores as you need; for example, you can create a store for a particular group of users or to group together a specific set of resources.

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**.

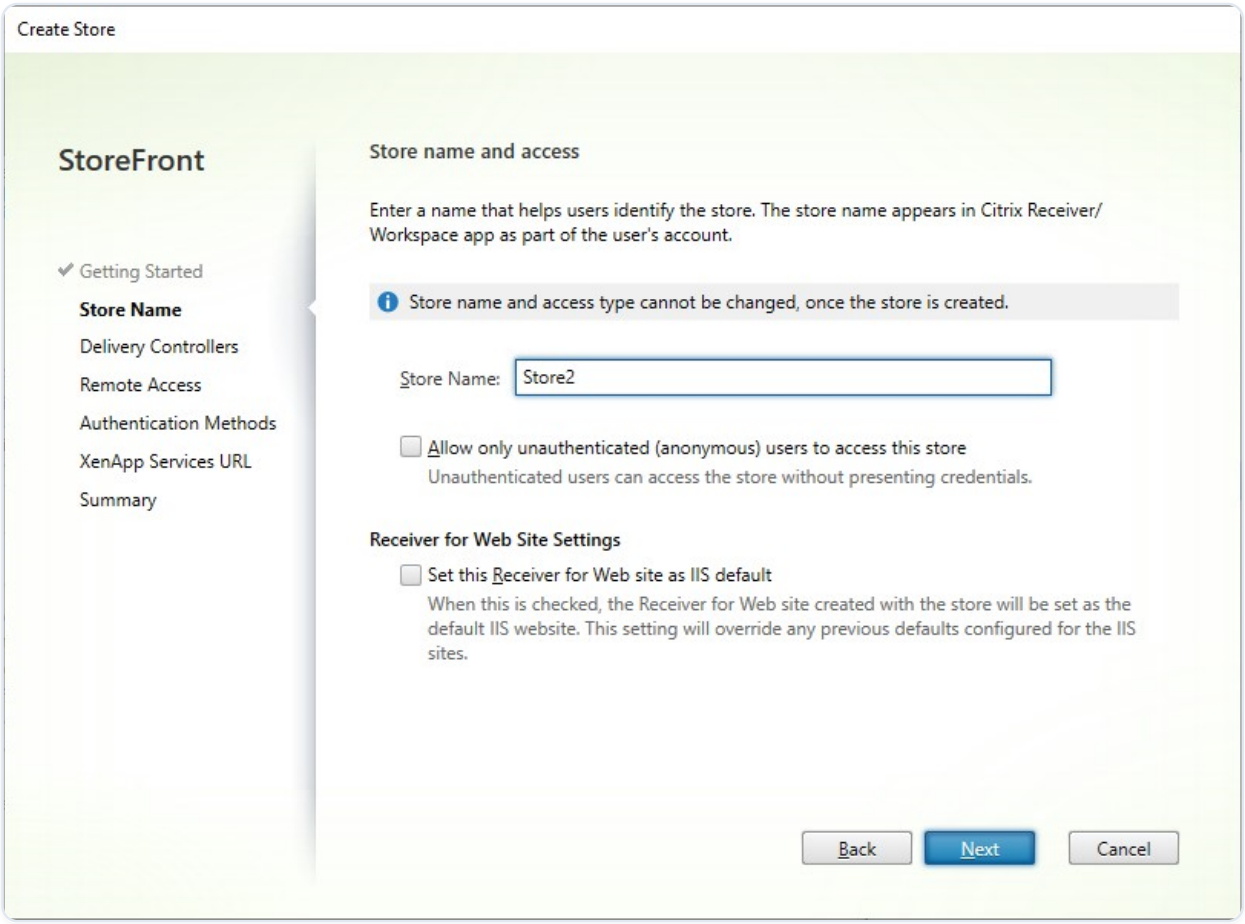


   Click **Next**

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

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

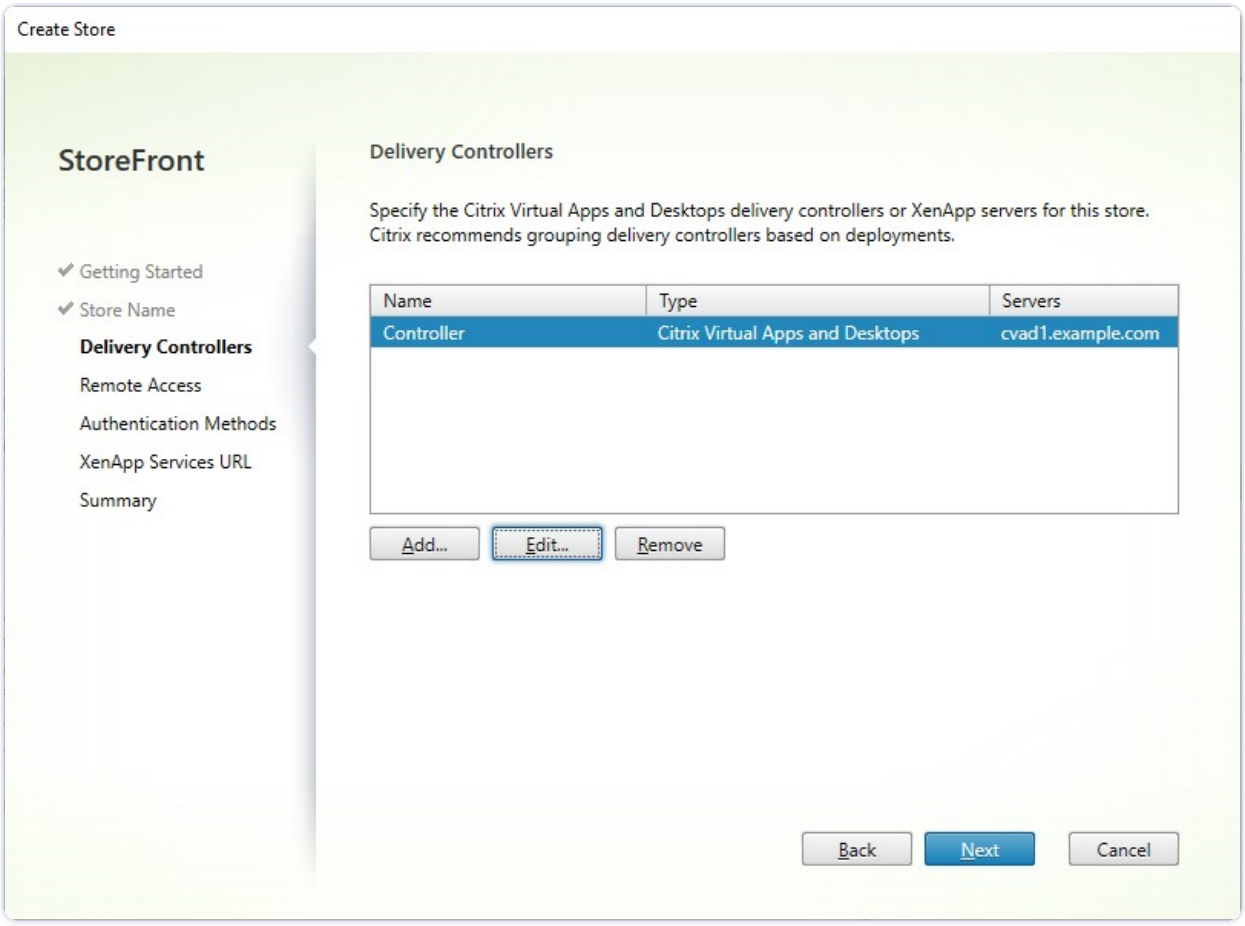
- Enter a store name
- If you wish to allow users to access the store anonymously, or unauthenticated, tick **Allow only unauthenticated users to access this store**. When you create an unauthenticated store, **Authentication Methods** and **Remote Access** pages are not available, and **Server Group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



Click **Next**

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

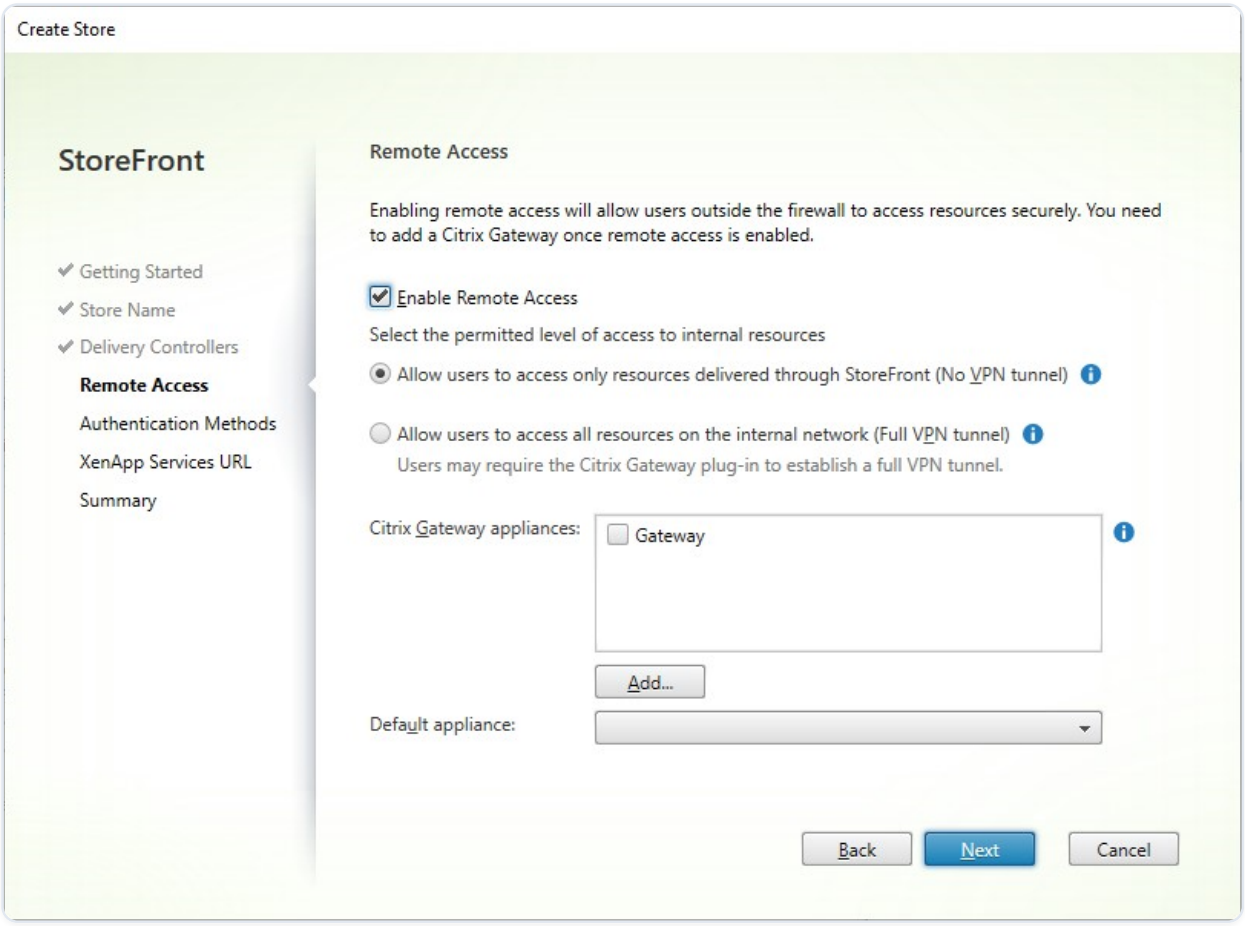
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

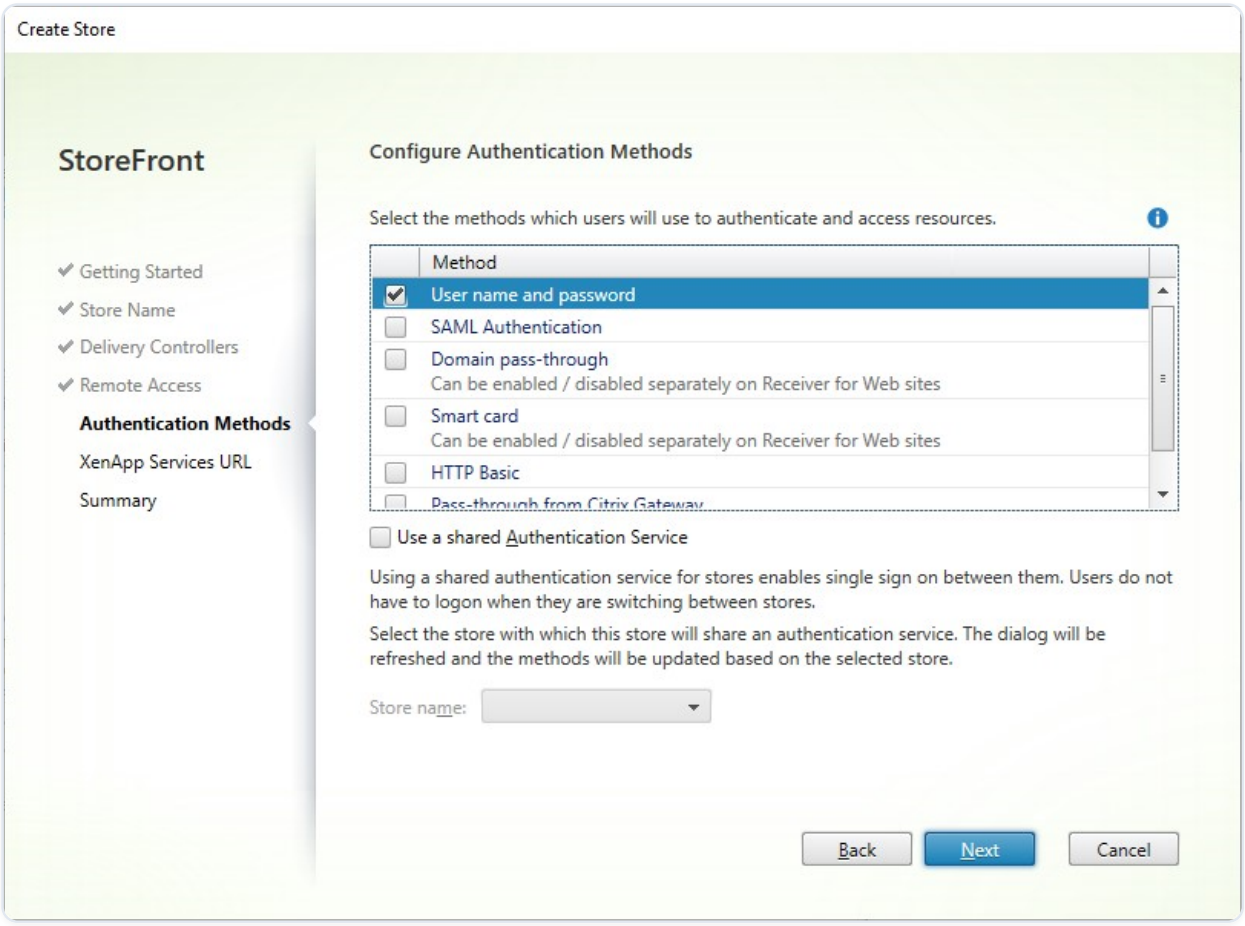


5. On the **Authentication Methods** tab, select the methods your users will use to authenticate to the store and click **Next**.

   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.

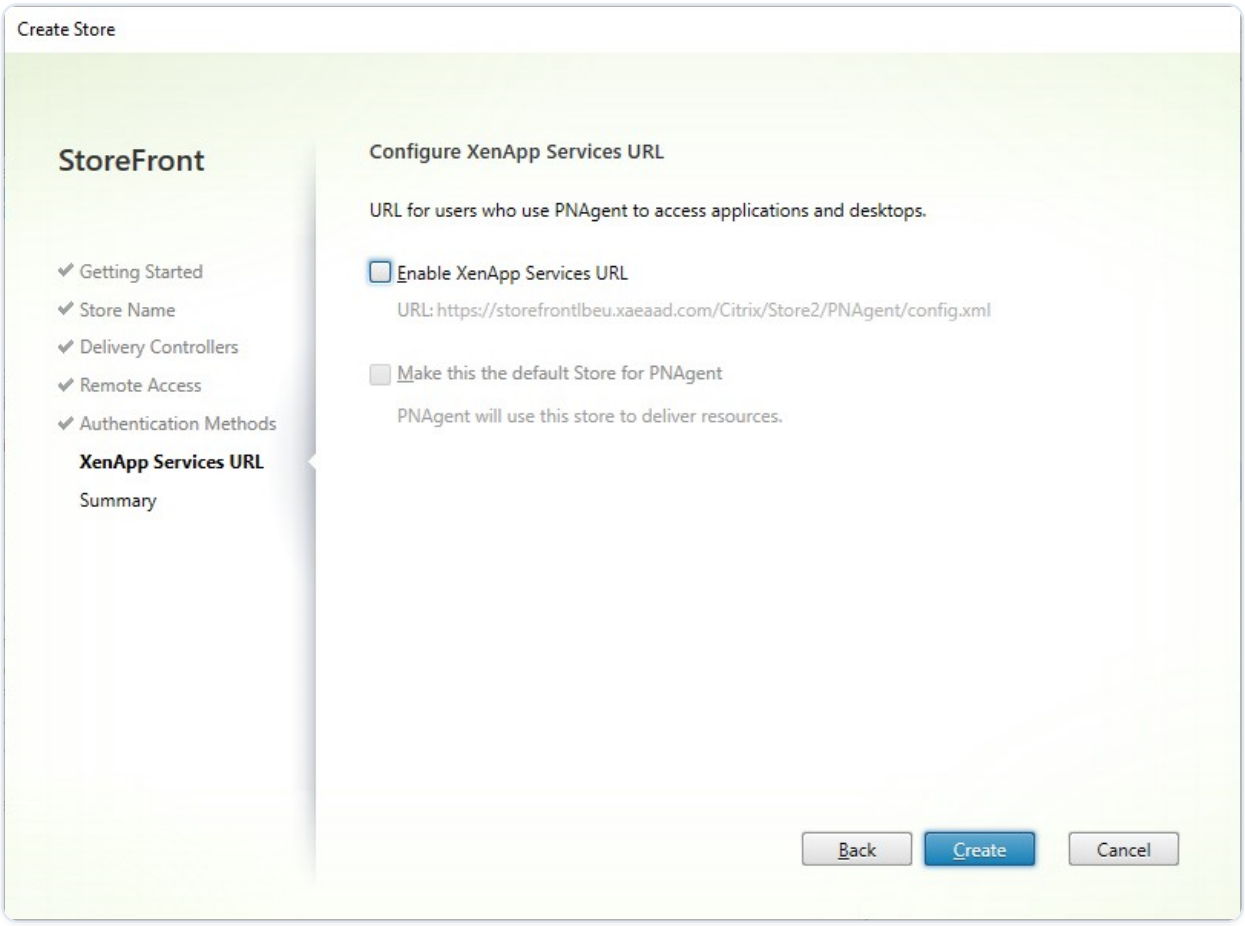
© 1997–2026 Citrix Systems, Inc. All rights reserved.



Click **Next**

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

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



Click **Create**

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

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

PowerShell SDK

To create a store using the PowerShell SDK:

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

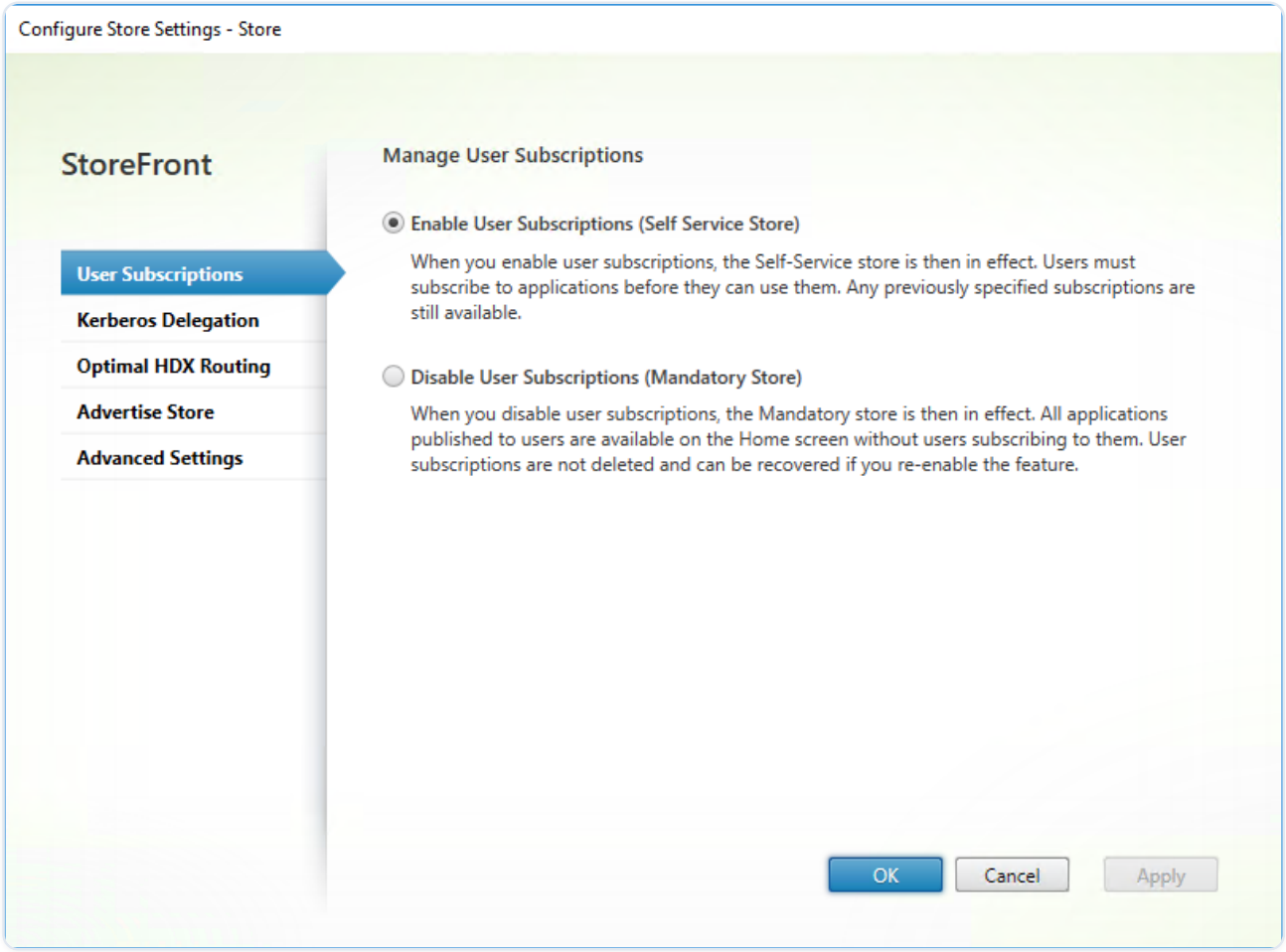
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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

Configure a Store

To modify a store:

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

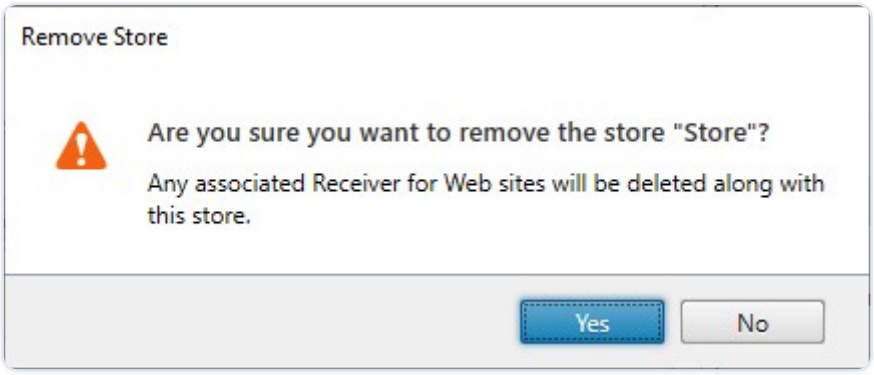


© 1997–2026 Citrix Systems, Inc. All rights reserved.

Remove a store

To remove a store:

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



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

Export store provisioning files for users

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

Important:

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

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

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

Advertise and hide stores to users

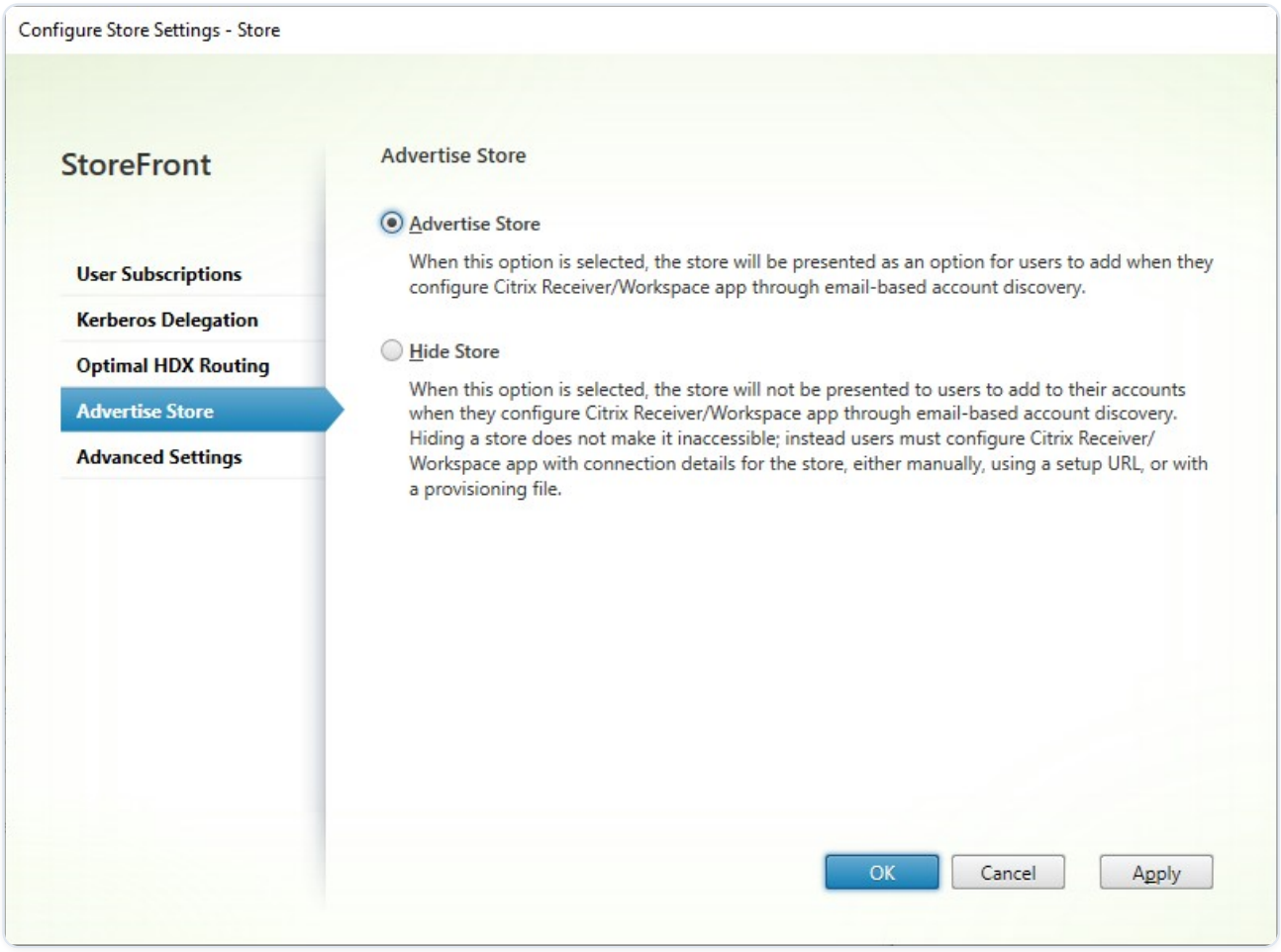
You can choose whether stores are presented to users to add to their accounts when they configure Citrix Workspace app through email-based account discovery or FQDN. By default, when you create a store it is presented as an option for users to add in Citrix Receiver when they discover the StoreFront 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.



Kerberos delegation

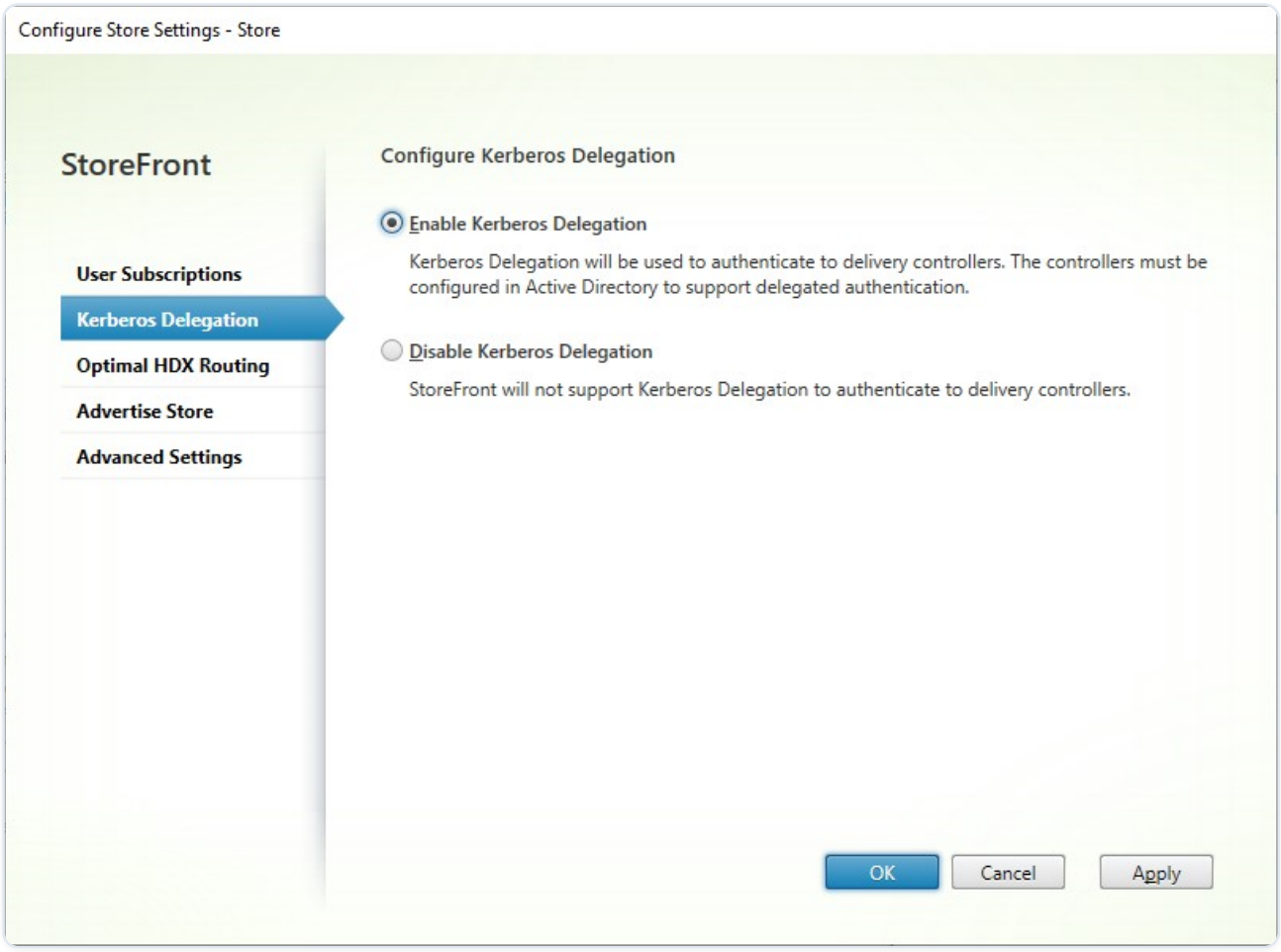
NOTE:

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.

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.

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



PowerShell SDK

To configure Kerberos delegation, use cmdlet Set-STFStoreService with parameter `-KerberosDelegation`

Manage sites and delivery controllers

Use the **Manage delivery controllers** 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 delivery controllers**.

View sites using the PowerShell SDK

With the PowerShell SDK, use the command Get-STFStoreFarm to list all sites or a specific site.

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

Add sites

Add sites for Citrix Virtual Apps and Desktops™

1. In the **Manage delivery controllers** screen, click **Add**.
2. Enter a **Display name** that helps you to identify the feed.
3. Select the **Type** as **Citrix Virtual Apps and Desktops**.
4. Under **Servers** for each DDC, click **Add** and enter the address of the DDC (or corresponding load balancer).

    - If you have placed load balancer(s) in front of the DDCs then enter the address of the load balancer(s). If you are not using a load balancer then list each DDC individually.
    - Include at least 2 DDCs for redundancy.
    - If your servers are using HTTPS (recommended), ensure that the names you specify in the servers list match exactly (including the case) the names on the certificates for those servers.

5. Citrix recommends that you select the option **Servers are load balanced**. This causes StoreFront to distribute the load between all delivery controllers or connectors by selecting a server from the list at random during each launch. If this option is not selected, then the servers list is treated as a failover list in priority order. In this case 100% of launches occur on the first active Delivery Controller or connector in the list. If that server goes offline, 100% of launches occur using the second in the list, and so on.
6. From the **Transport type** list, select the type of connections for StoreFront to use for communications with the servers.

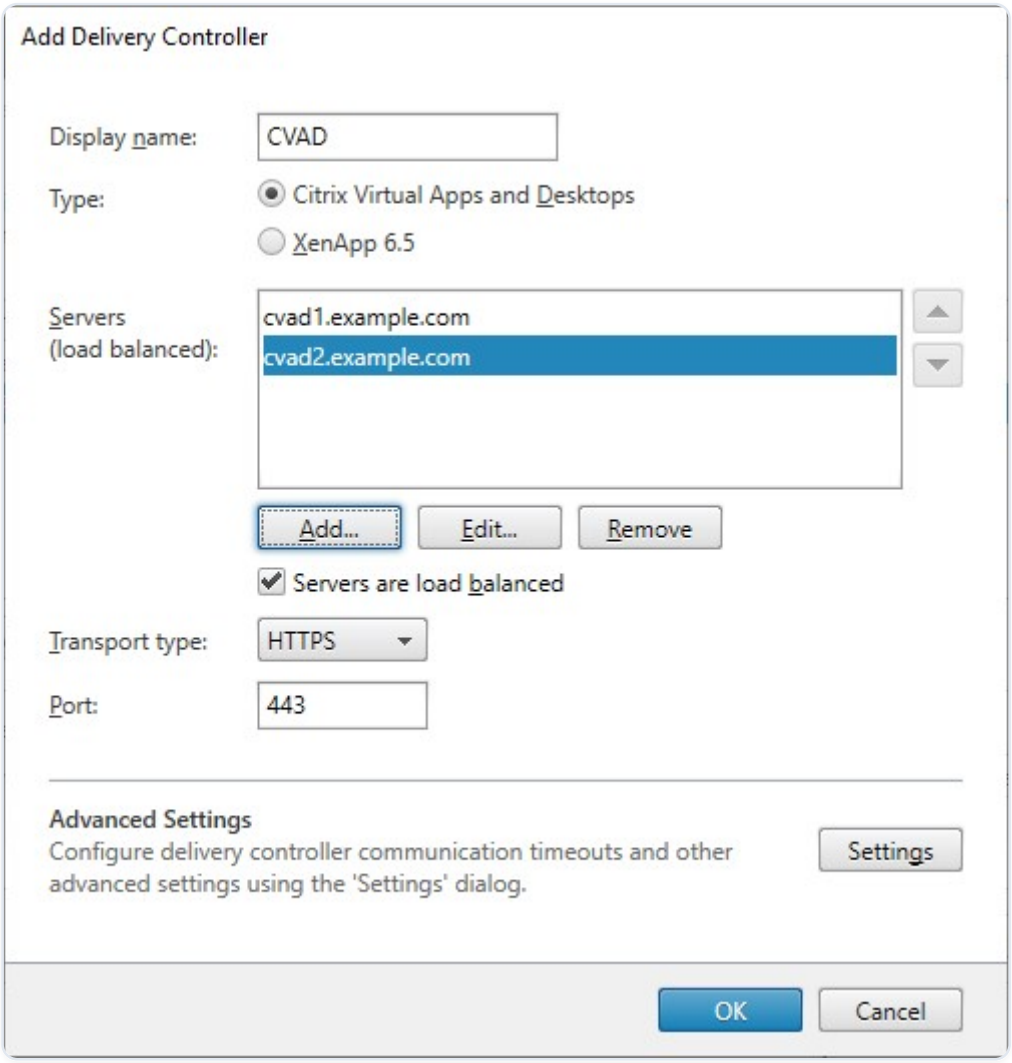
    - To send data over unencrypted connections, select **HTTP**. If you select this option, you must make your own arrangements to secure connections between StoreFront and your servers.
    - To send data over encrypted connections (recommended), select **HTTPS**. If you select this option for Citrix Virtual Apps and Desktops servers, ensure that the Citrix XML Service is set to share its port with Microsoft Internet Information Services (IIS) and that IIS is configured to support HTTPS.

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

NOTE:

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

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



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

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

```
$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 sites for Citrix Desktops as a Service

1. In the **Manage delivery controllers** screen, click **Add**.
2. Enter a **Display name** that helps you to identify the feed.
3. Select the **Type** as **Citrix Virtual Apps and Desktops**.
4. Under **Servers** 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. If you have connectors from multiple locations, Citrix recommends that you put the connectors with the lowest latency to the StoreFront server at the top of the list and clear the option **Servers are load balanced**. As the connectors are only proxying information to DaaS delivery controllers, there is limited benefit from using load balancing.
6. From the **Transport type** list, select the type of connections for StoreFront to use for communications with the servers.

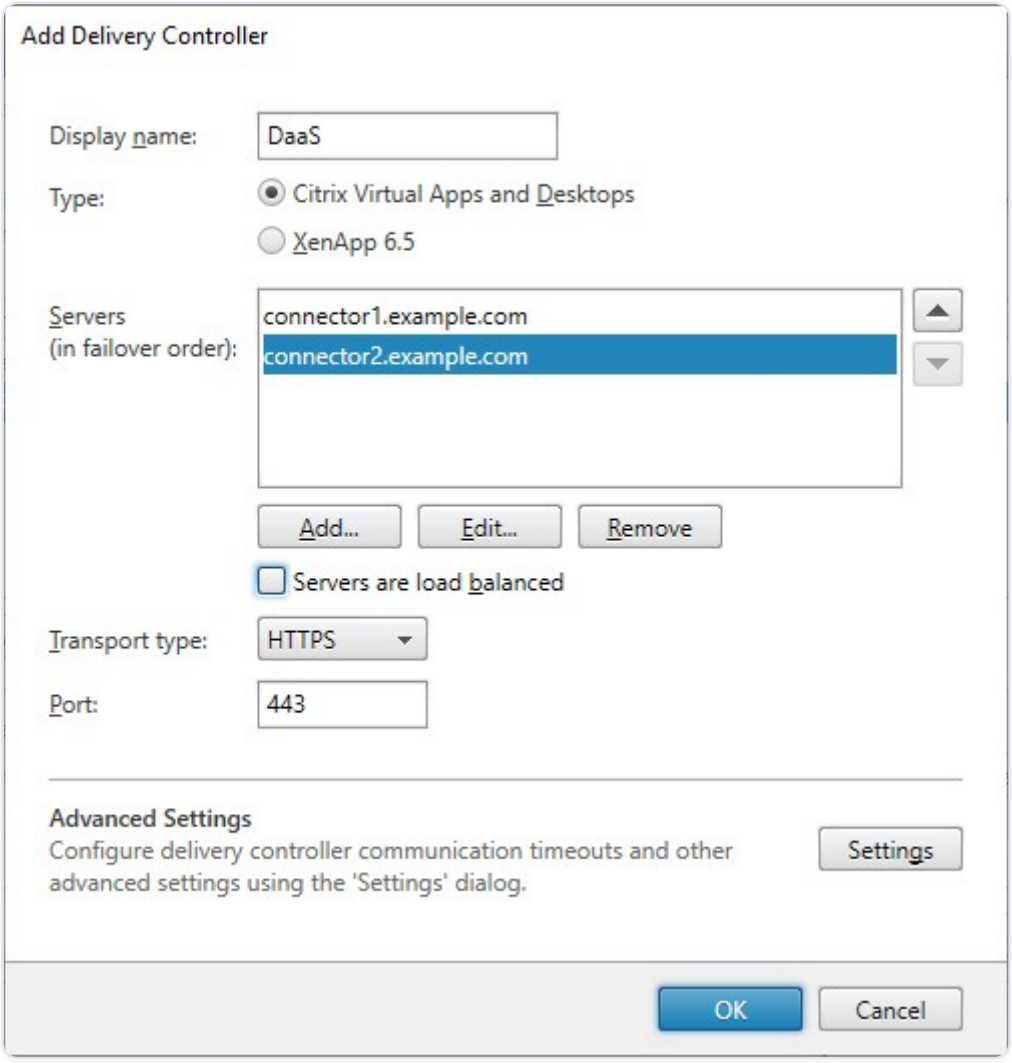
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- To send data over unencrypted connections, select **HTTP**. If you select this option, you must make your own arrangements to secure connections between StoreFront and your cloud connectors.
- To send data over encrypted connections (recommended), select **HTTPS**. If you select this option for you must ensure that the cloud connectors are configured for HTTPS.

NOTE:

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

7. Specify the port for StoreFront to use for connections to the servers. The default port is 80 for HTTP connections and 443 for HTTPS connections.
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 sites for Citrix Secure Private Access

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

1. Navigate to **Stores** > **Delivery Controllers** on StoreFront.
2. Click **Add**.
3. In the **Add Delivery Controller** window, provide a **Display name** to identify the feed.
4. Select the **Type** as **Citrix Secure Private Access**.
5. Enter the Citrix Secure Private Access server name.
6. From the **Transport type** dropdown, select the type of connection that can be used for communications with the servers.

   - **HTTP:** sends data over unencrypted connections

   NOTE:

   If you select **HTTP**, you must make your own arrangements to secure connections between StoreFront and your servers.

   - **HTTPS:** sends data over secure HTTP connections using Secure Sockets Layer (SSL) or Transport Layer Security (TLS).

7. Specify the port to be used for connections to the servers. The default port for **HTTP** is 80, and for **HTTPS** it is 443.
8. Click **OK**.

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

Create a site using the PowerShell SDK

To add a site, use the command Add-STFStoreFarm

- For Citrix Virtual Apps and Desktops or Citrix Desktops as a Service, set `FarmType` to `XenDesktop`.
- For Citrix Secure Private Access, set `FarmType` to `SPA`.

Modify a site

In the **Manage delivery controllers** 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.

Modify a site using the PowerShell SDK

To modify a site using PowerShell, use command Set-STFStoreFarm

Delete a site

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

Delete a site using the PowerShell SDK

To delete a site using PowerShell, use command Remove-STFStoreFarm

Health check and server bypass behavior

To improve performance when some of the servers providing resources become unavailable, StoreFront temporarily bypasses servers that fail to respond. While a server is being bypassed,

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

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 Delivery Controller 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 Delivery Controllers**.
4. Select a controller, click **Edit**, and then click **Settings** on the **Edit Delivery Controller** screen.
5. Under Advanced Settings click **Settings**.
6. In the Configure Advanced Settings dialog:

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

    b. On the **Bypass duration** row, click in the second column and enter a time, in minutes, for which a single server is considered offline after it fails to respond.

Map users to site

By default, users accessing a store see an aggregate of all the resources available to them from all the site 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

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

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:

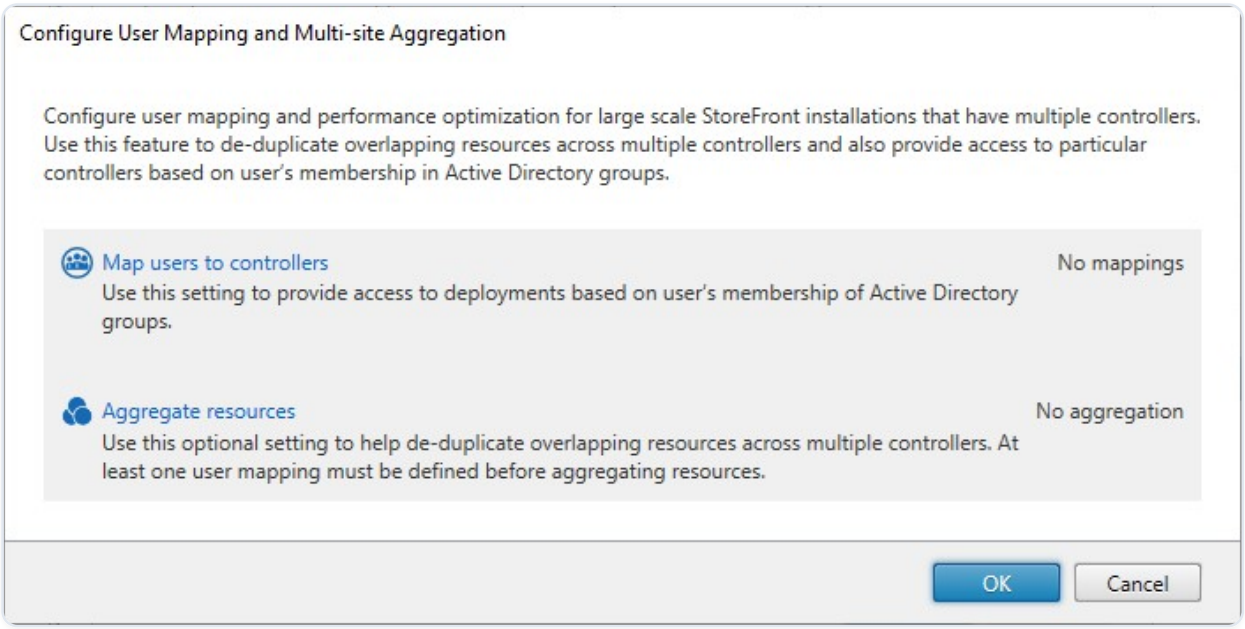
> This filters entire sites. In addition, within a site, applications may be filtered by user group within Citrix Virtual Apps and Desktops Studio configuration.

To configure specific sites for particular user groups:

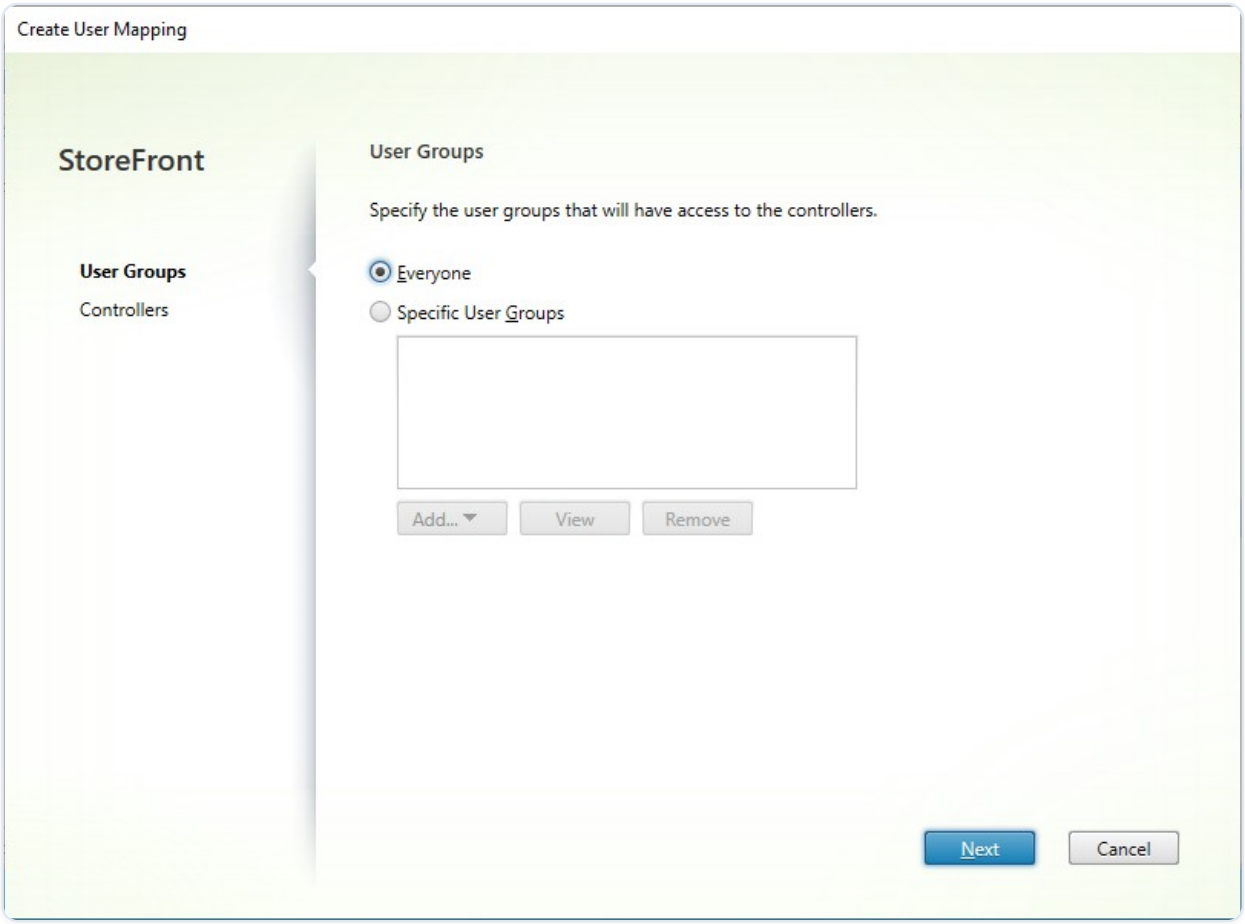
1. From the **Manage delivery controllers** screen, under **User Mapping and Multi-Site Aggregation Configuration**, click **Configure**. This option is only available if two or more sites are configured.

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

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

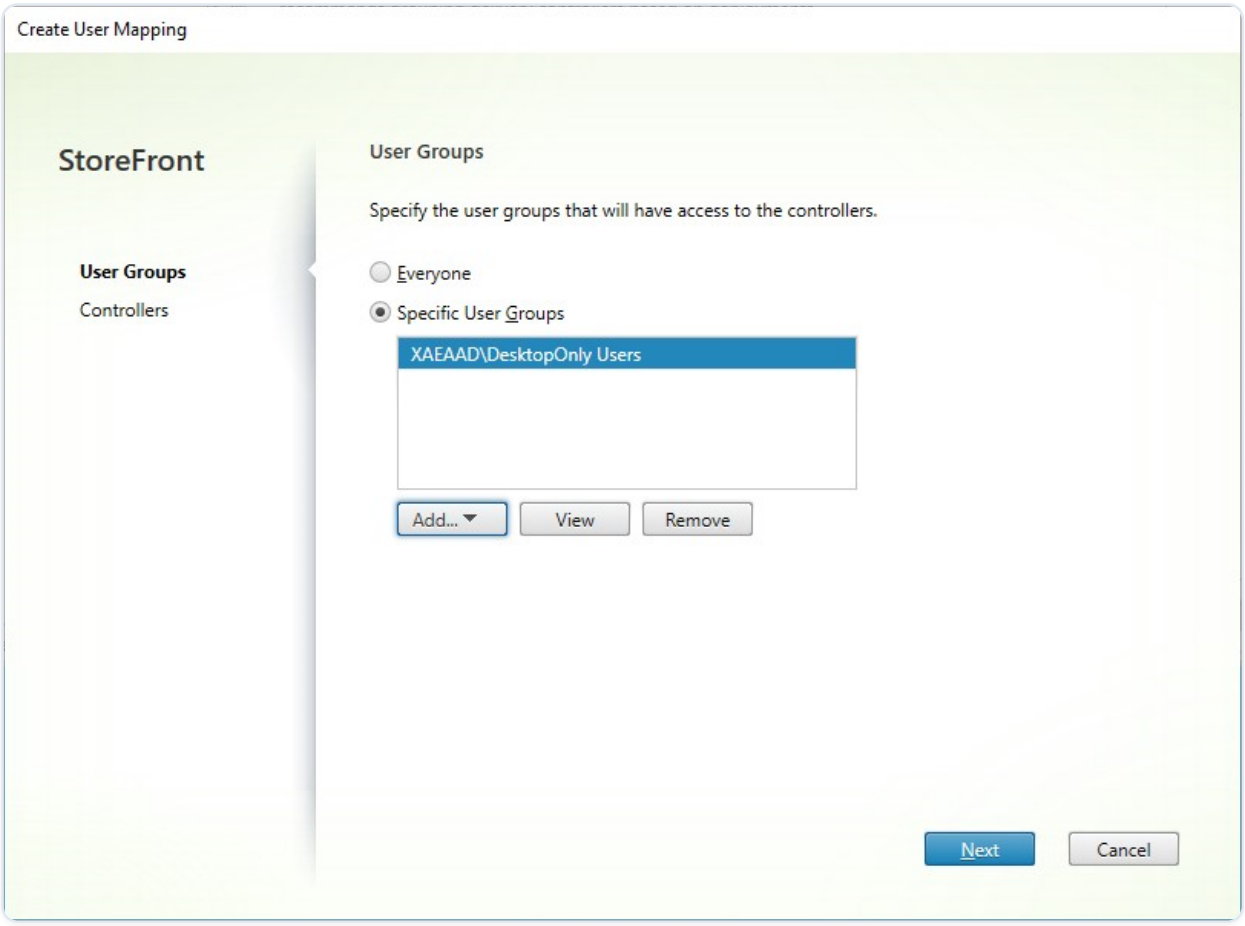


2. Click **Map users to controllers**. This opens the **Create User Mapping** screen to create your first mapping. You will be able to create further mappings later.

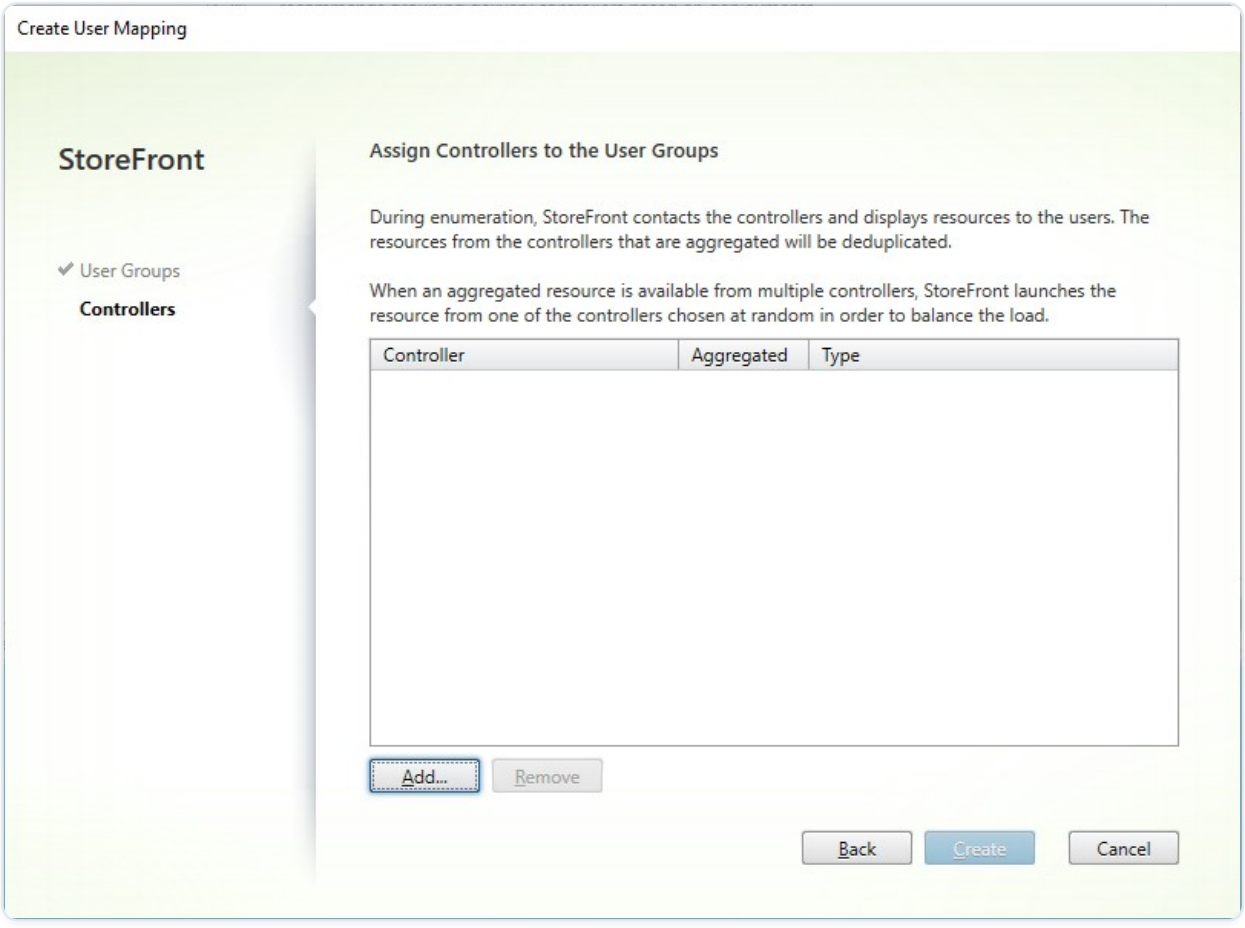


3. Either choose **Everyone** or choose **Specific User Groups** and add one or more group.

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

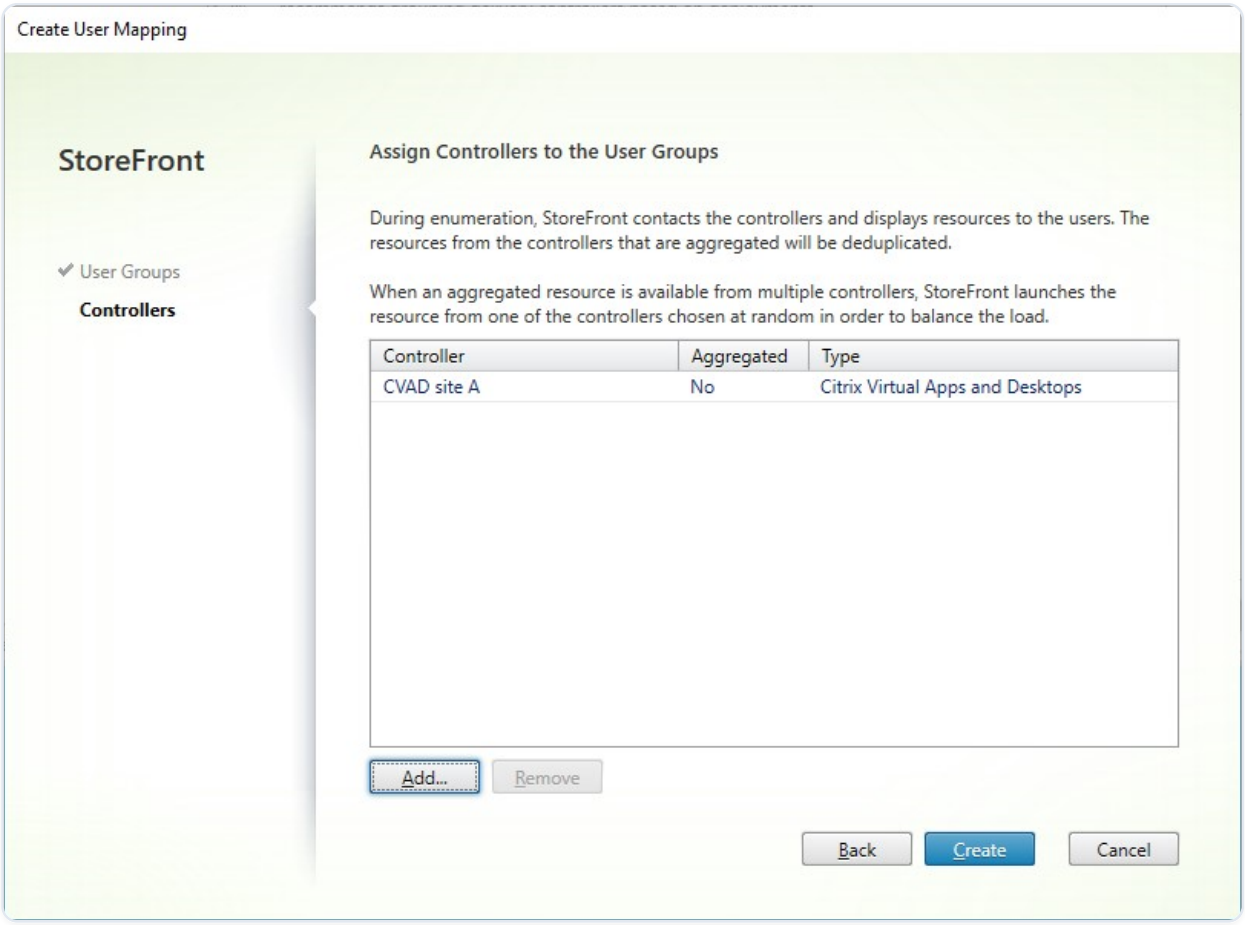


4. Click **Next**. This takes you to the **Controllers** tab.



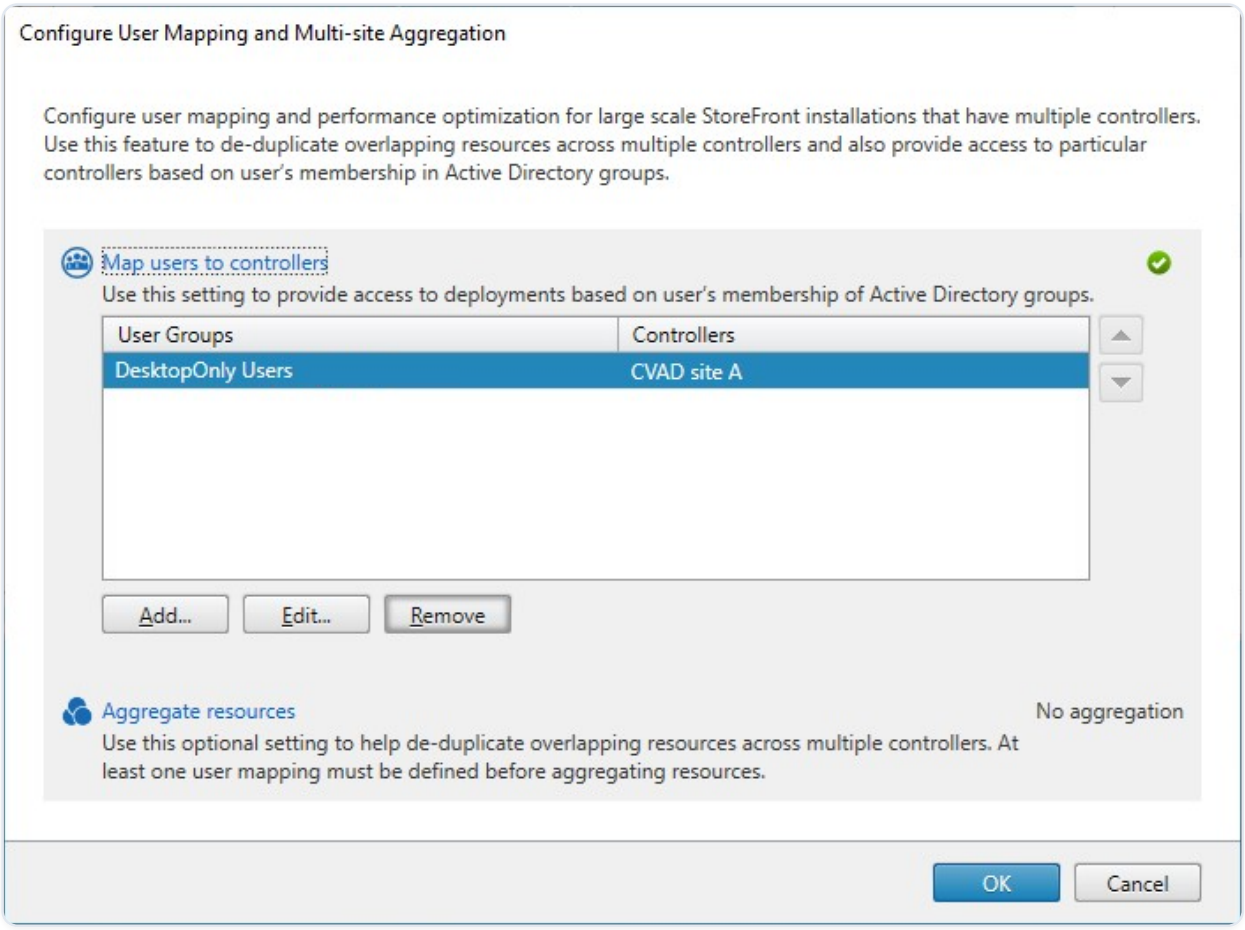
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 sites using PowerShell SDK

You can map users to sites using the PowerShell SDK

1. For each site, 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.

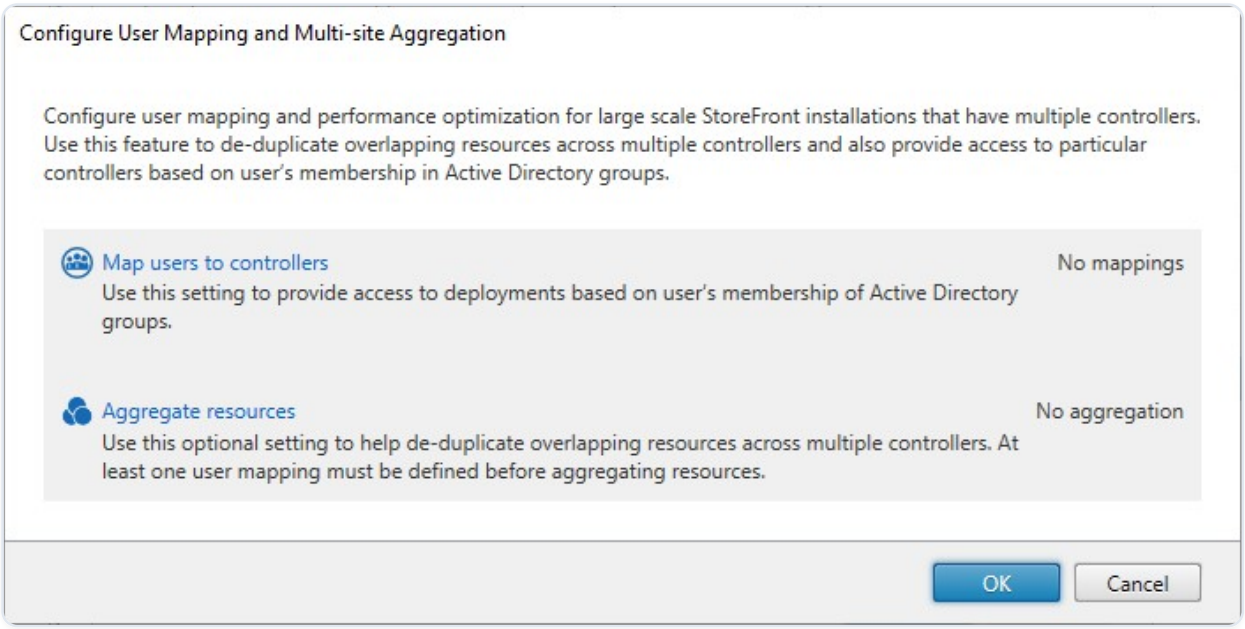
You can override the specified deployment ordering for individual Citrix Virtual Apps and Desktops resources to define preferred deployments to which users are connected when they access a particular desktop or application. This enables you to, for example, specify that users are preferentially connected 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.

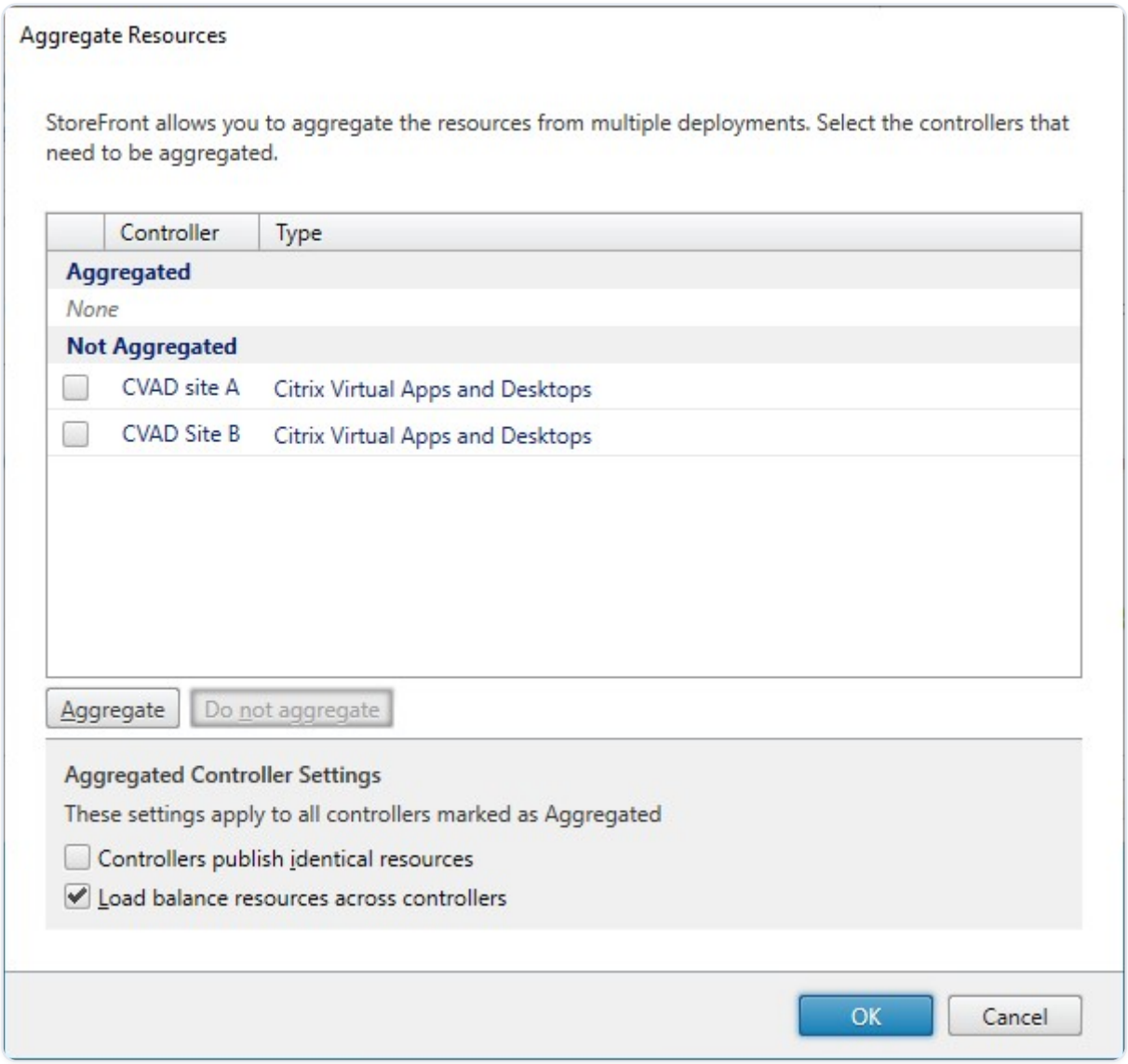
After checking the other factors, StoreFront uses the ordering specified in your configuration to determine the deployment to which the user is connected. If multiple equivalent deployments are available to the user, you can specify that users are connected either to the first available deployment or 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.

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

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

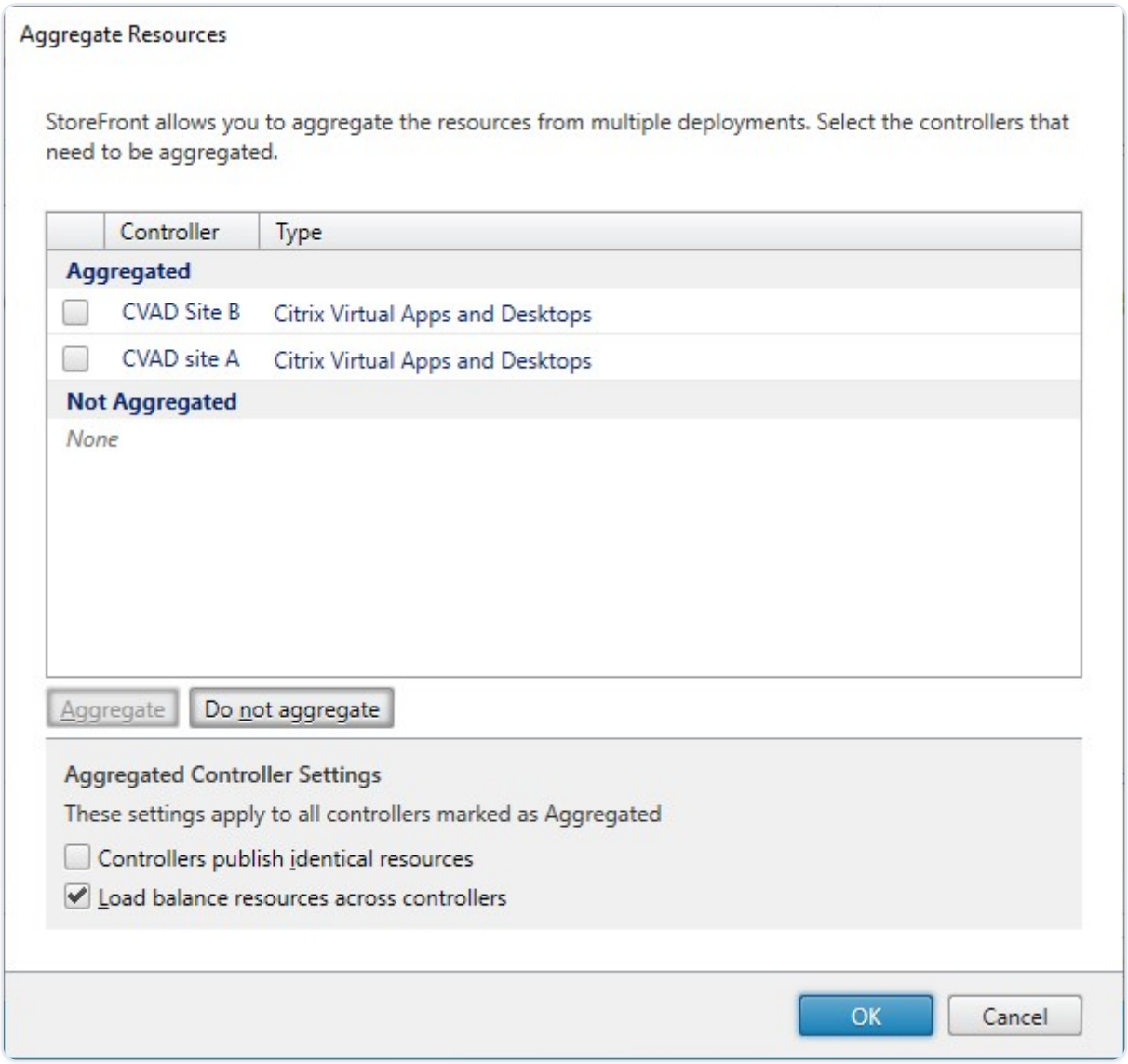


2. Click **Aggregate resources**. This shows the **Aggregate Resources** screen.



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

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

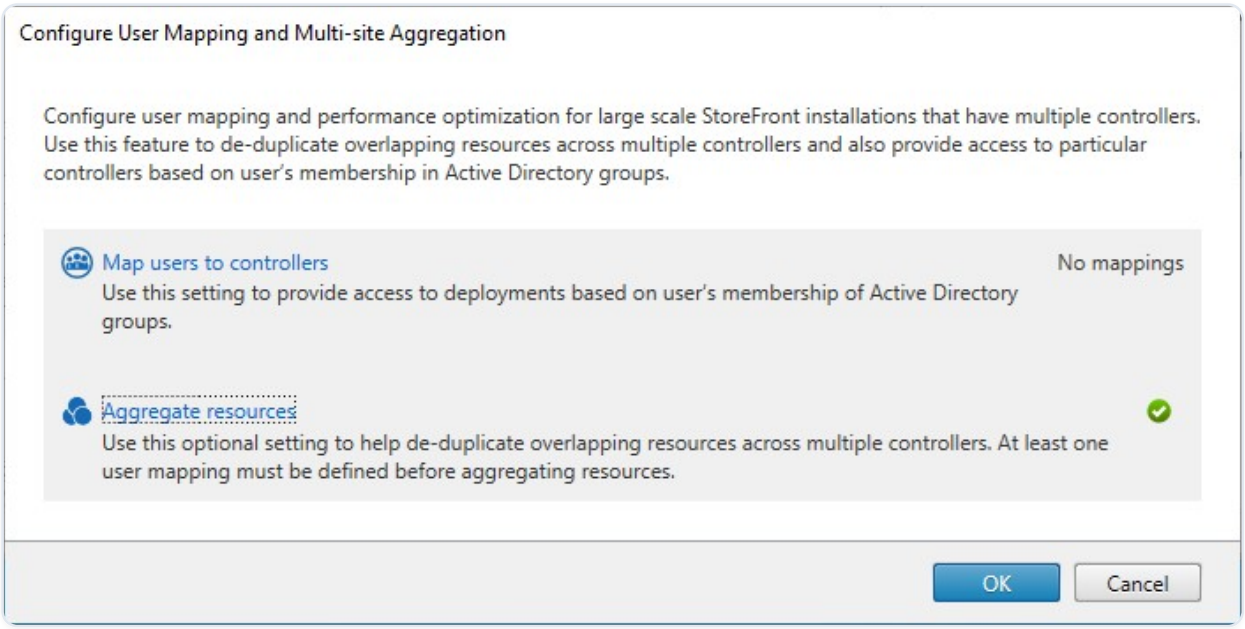


4. Select **Aggregated Controller Settings** options as required:

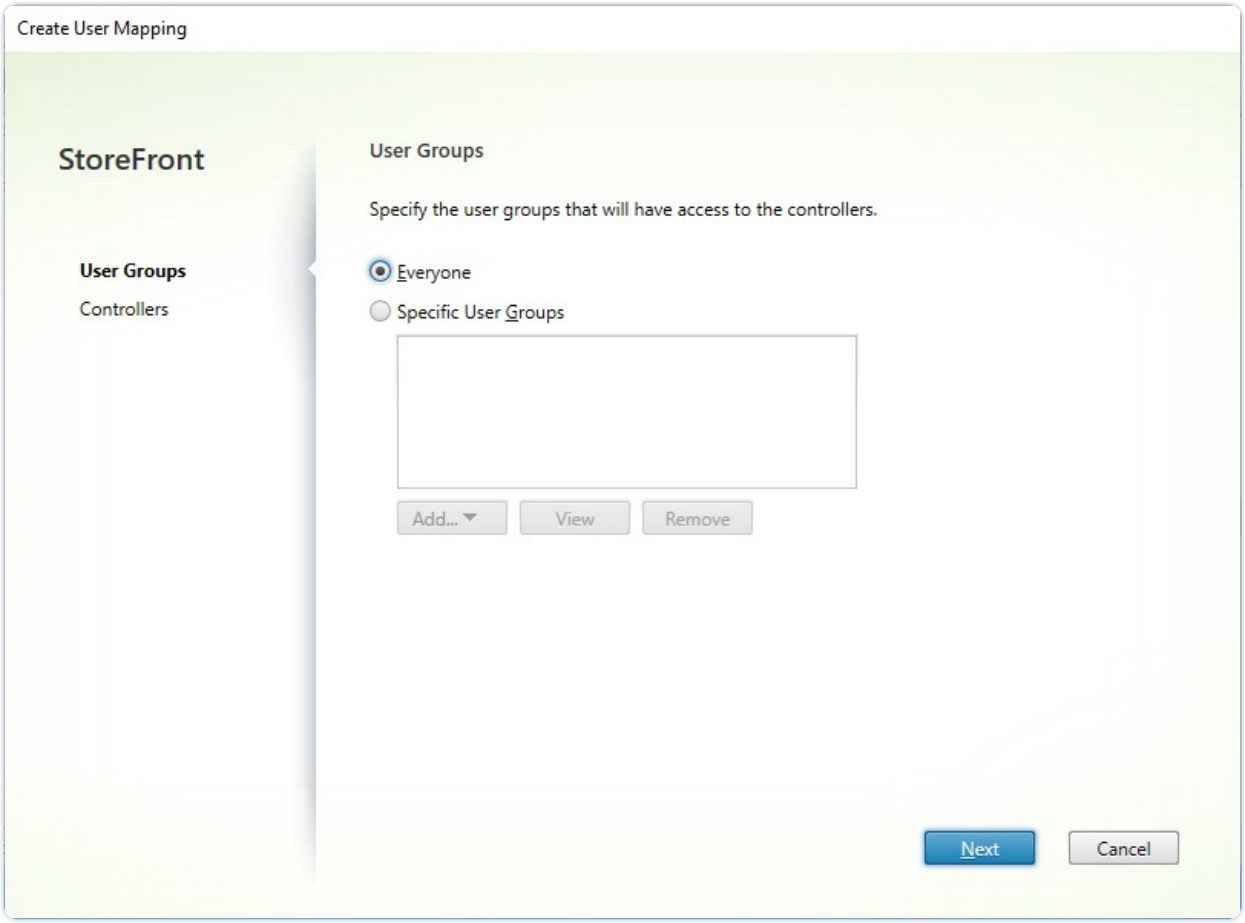
    - **Controllers publish identical resources** - When selected, StoreFront enumerates resources from only one of the controllers in the aggregated set. When not selected, StoreFront enumerates resources from all controllers in the aggregated set (to accumulate the user's entire set of available resources).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

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

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



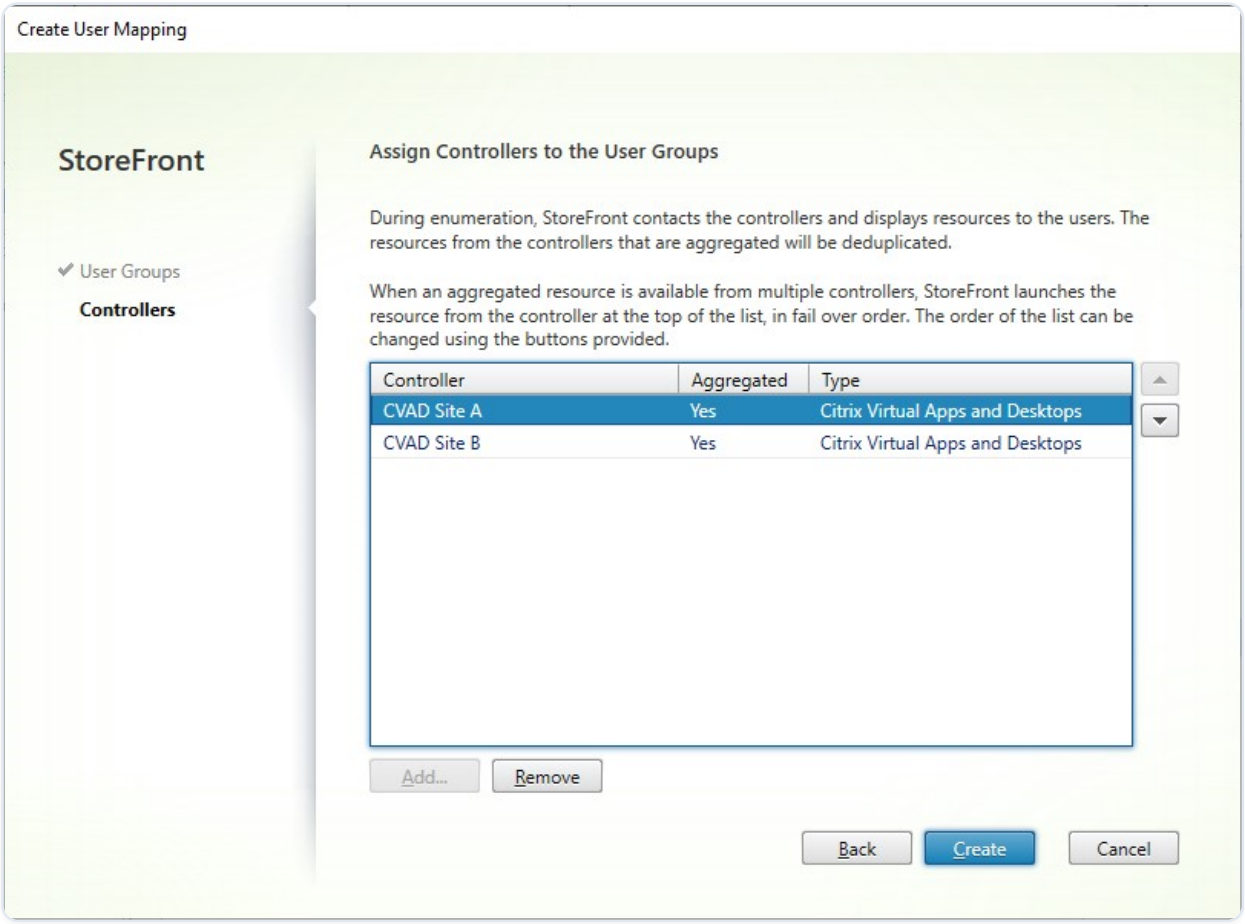
6. When resources are aggregated, by default, no users have access to the resources so you must add the user mappings. Click **Map users to controllers** This opens the **Create user mapping** screen.



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

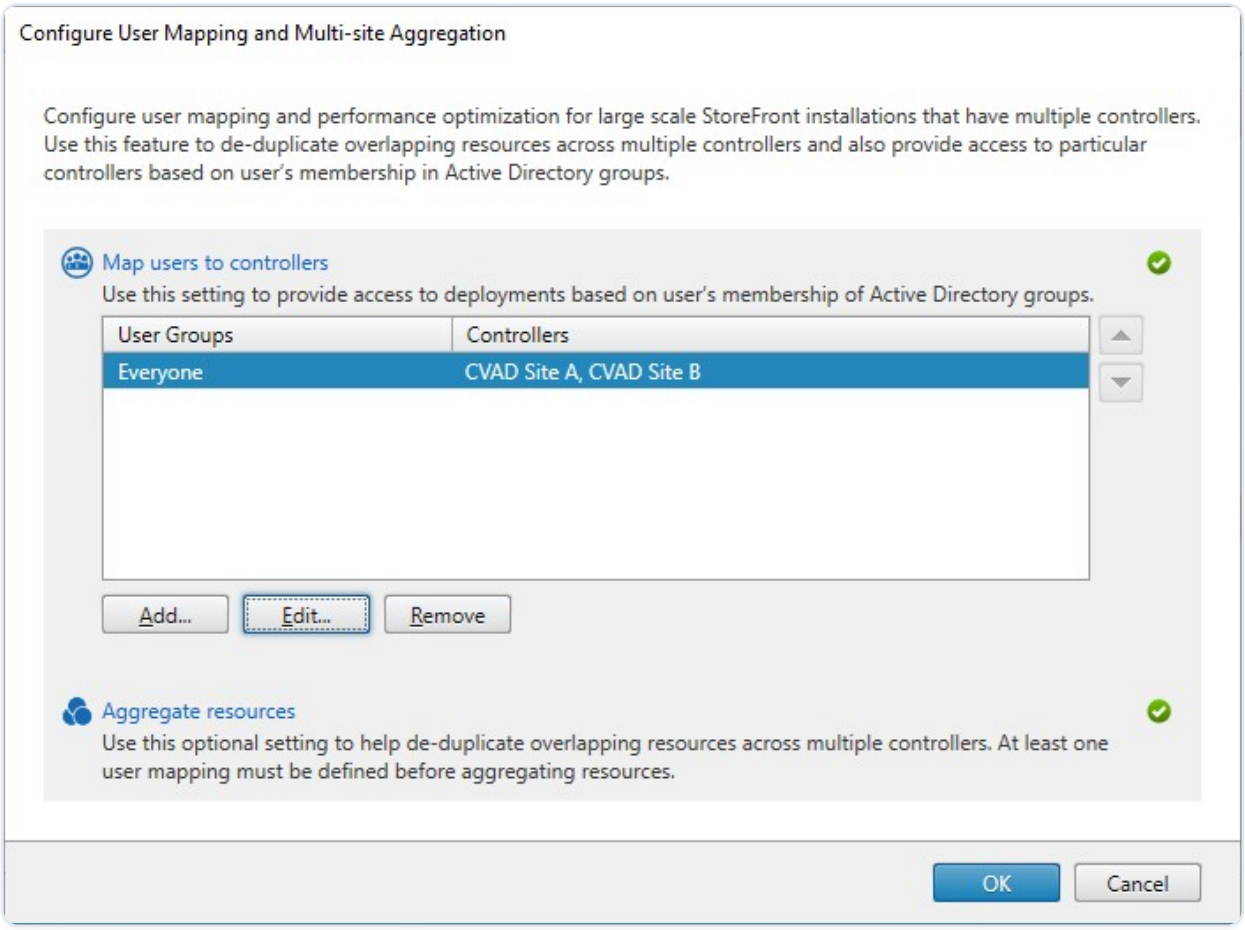
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 SDK

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

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

© 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 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.

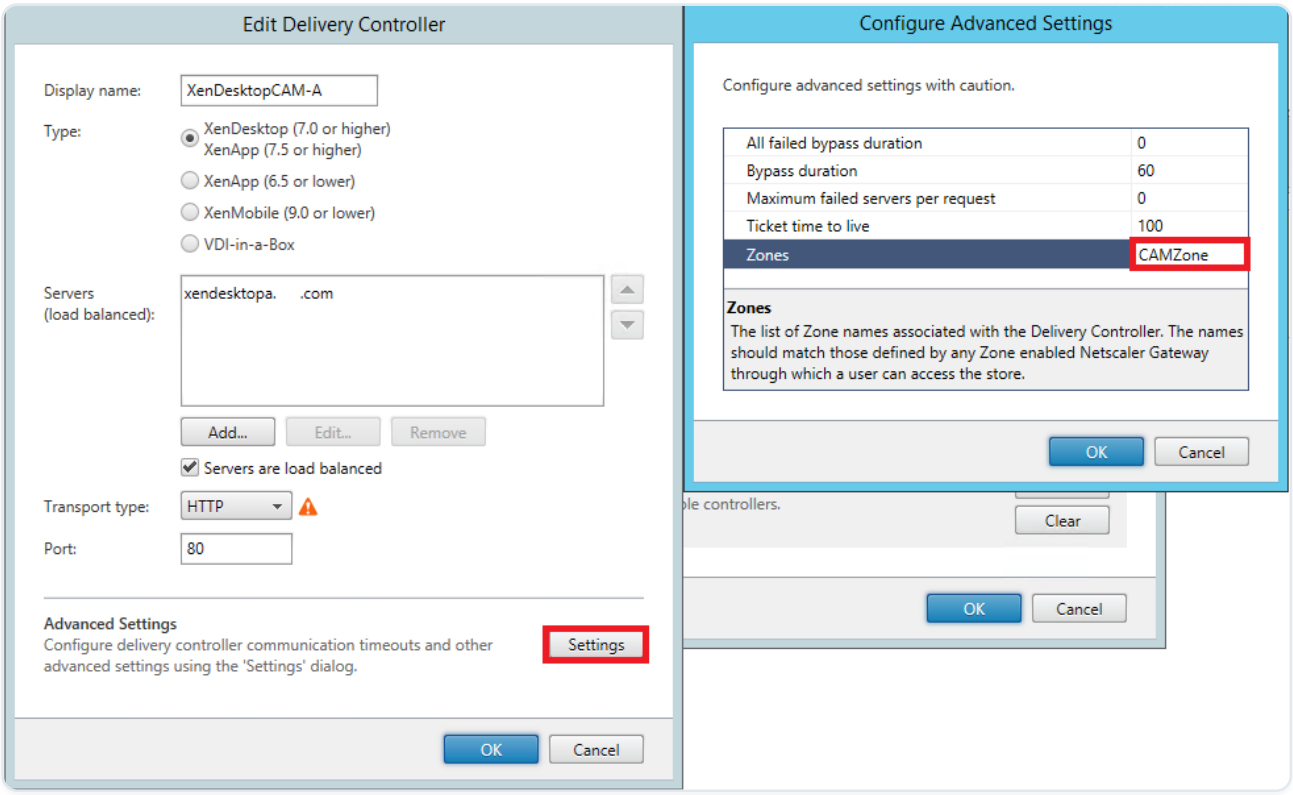
Zone preference

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 Delivery Controllers**.
4. Select a controller, click **Edit**, and then click **Settings** on the **Edit Delivery Controller** screen.
5. Under Advanced Settings click **Settings**.
6. In the Configure Advanced Settings dialog, 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.

Manage remote access to stores through Citrix Gateway

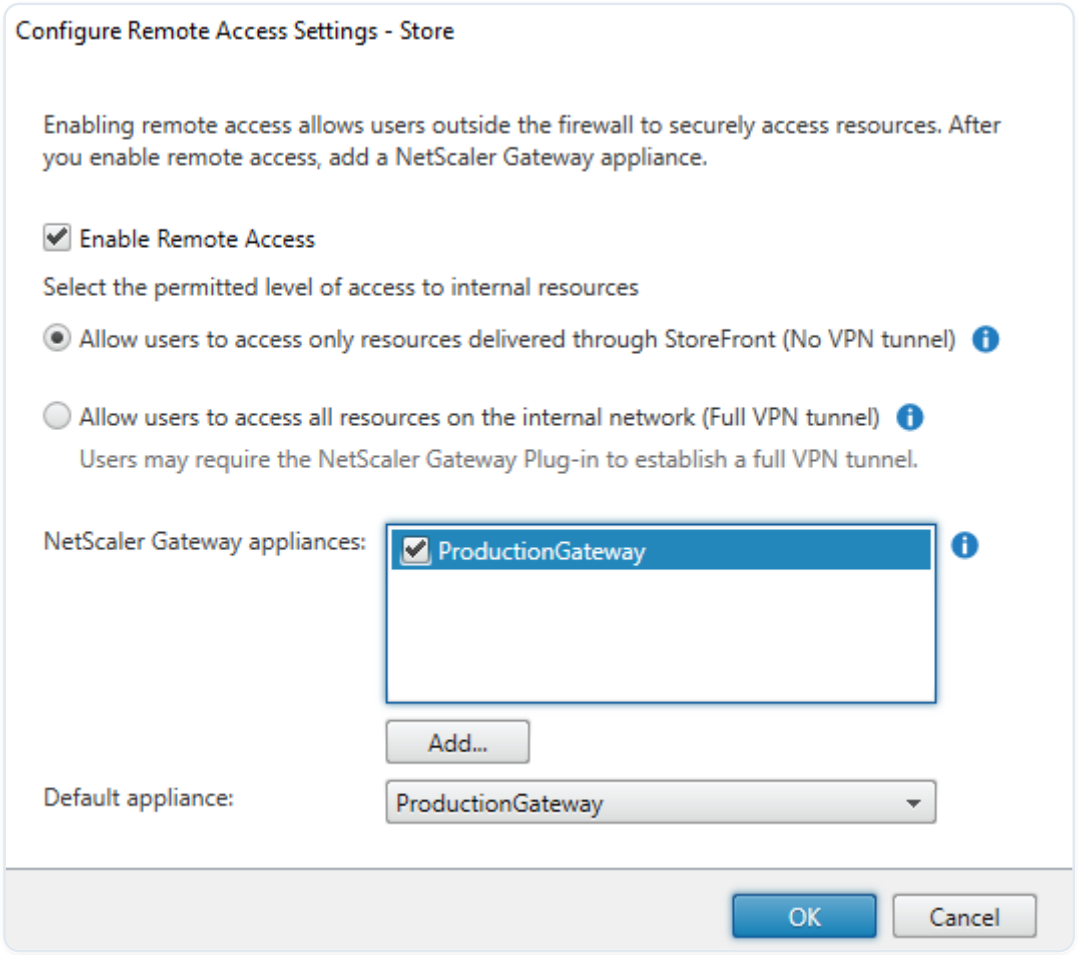
Use the Remote Access Settings task to configure access to stores through Citrix Gateway for users connecting from public networks. Remote access through a Citrix Gateway cannot be applied to unauthenticated stores.

IMPORTANT:

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

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

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



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

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

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

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

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

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

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

Certificate Revocation List (CRL) checking

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

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

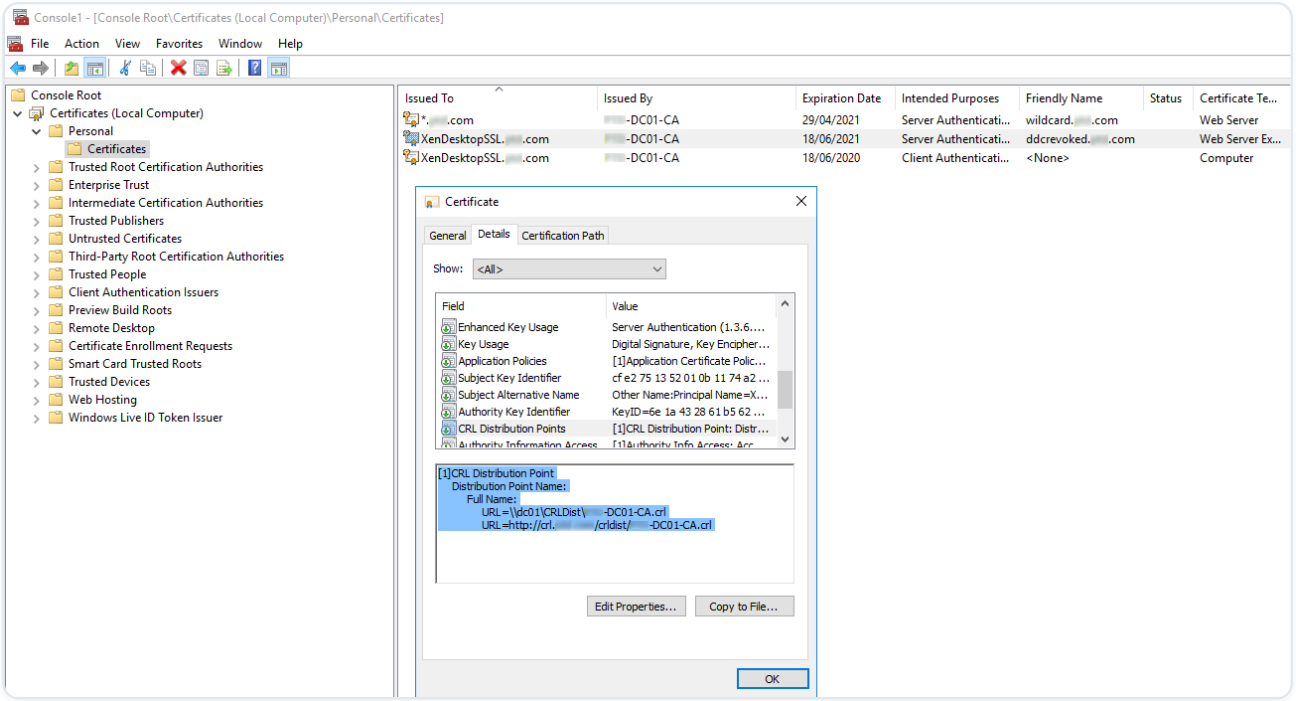
NOTE:

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

StoreFront supports certificate revocation checking using CRL Distribution Point (CDP) certificate extensions and locally installed certificate revocation lists (CRLs). StoreFront supports full CRLs only: delta CLRs are not supported.

CRL Distribution Points (CDP) extensions

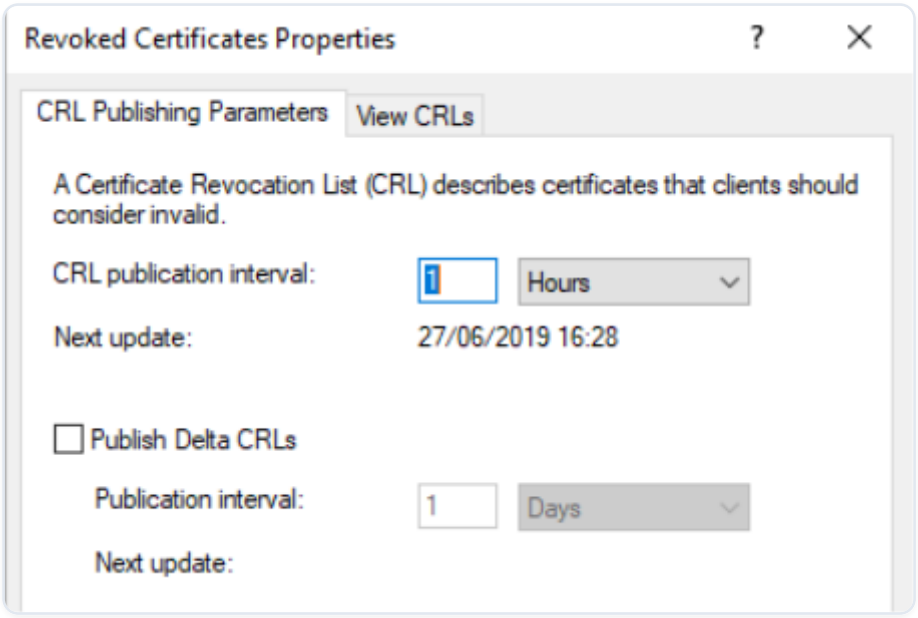
StoreFront does not enumerate resources from Citrix Virtual Apps and Desktops delivery controllers which are using revoked certificates whose serial numbers are listed in the published CRL. To detect which certificates have been revoked, StoreFront must be able to access the published CRL using one of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



CRL publishing interval

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

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



Client CRL caching

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

StoreFront's access to certificate revocation lists (CRLs)

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

Internal enterprise CAs and private certificates on delivery controllers

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

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

External public CAs and public certificates on delivery controllers

StoreFront servers and Citrix Virtual Apps and Desktops delivery controllers can use certificates issued by public CAs. StoreFront must be able to contact the public CA's webserver via the Internet, using the URL referenced in the CDP extensions. If StoreFront cannot download a copy of the CRL using a CDP URL after a public certificate has been revoked, then StoreFront cannot perform the CRL check.

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

View certificate revocation policy

To view the policy setting using the PowerShell SDK, 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 the PowerShell SDK, run cmdlet `Set-STFStoreFarmConfiguration` with parameter `-CertRevocationPolicy`.

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

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

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

SETTING	DESCRIPTION
	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 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:

```
$SiteID = 1

$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.

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

Using locally imported CRLs on the StoreFront server

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

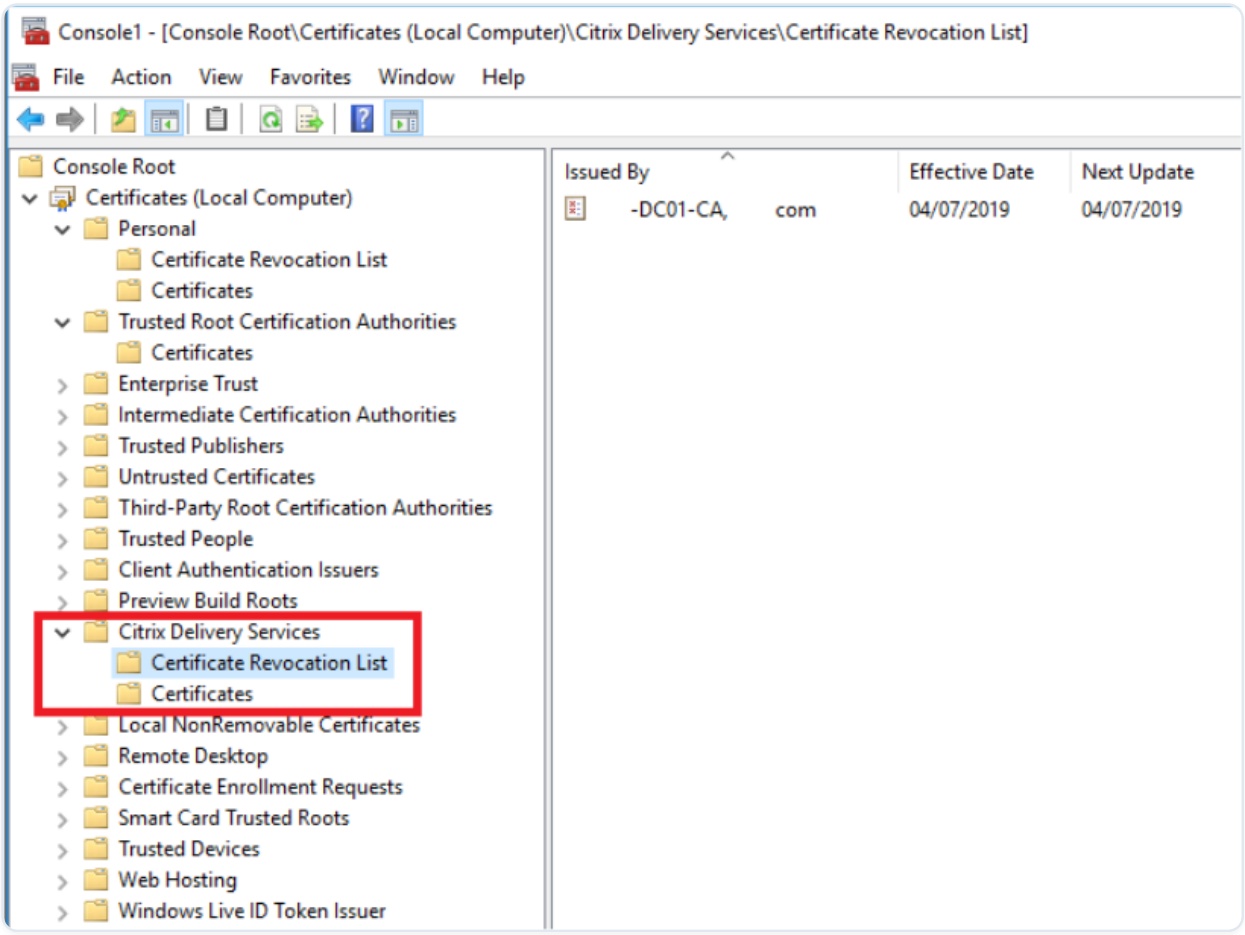
- They are difficult to manage and update in large enterprise deployments, where multiple StoreFront server groups may be involved.
- Manually updating CRLs on every StoreFront server, every time a certificate is revoked, is much less efficient than using CDP extensions and published CRLs on the entire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

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



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 a store for certificate revocation checking.
2. Configure the delivery controller to use HTTPS, following the procedure described in XML service-based authentication.

Configure an XML authentication service for certificate revocation checking

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

NOTE:

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

Make sure that the certificate revocation mode is set to the same value for both the store and the authentication service. Alternatively, if the authentication configuration is identical for all stores, multiple stores can be configured to share a single authentication service.
The authentication service PowerShell cmdlets have no equivalent of **Set-STFStoreFarmConfiguration**, so a slightly different PowerShell approach is required. Use the same Certificate revocation policy settings describe in the earlier section.

1. Open the PowerShell ISE and select **Run As Admin**.

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

```
$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.

To open the Event Viewer:

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

- 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)
```

Configure two StoreFront stores to share a common subscription datastore

The StoreFront installation process installs a Windows datastore locally on each StoreFront server to maintain its subscription data. In StoreFront server group environments, each server also maintains a copy of the subscription data used by its store. This data is propagated to other servers to maintain user subscriptions across the whole group. By default, StoreFront creates a single datastore for each store. Each subscription datastore is updated independently from each other store.

Where different configuration settings are required, it is common for administrators to configure StoreFront with two distinct stores; one for external access to resources using Citrix Gateway and another for internal access using the corporate LAN. You can configure both "external" and "internal" stores to share a common subscription datastore by making a simple change to the store web.config file.

In the default scenario involving two stores and their corresponding subscription datastores, a user must subscribe to the same resource twice. Configuring the two stores to share a common subscription database improves and simplifies the roaming experience when users access the same resource from inside or outside the corporate network. With a shared subscription datastore it does not matter whether they use the "external" or "internal" store when they initially subscribe to a new resource.

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

- Each store has a web.config file located in C:\inetpub\wwwroot\citrix\<storename>.
- Each store web.config contains a client endpoint for the Subscription Store Service.

`<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1__Citrix_<StoreName>" authenticationMode="windows" transferMode="Streamed">`

The subscription data for each Store is located in:

`C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix`

For two stores to share a subscription datastore, you need only point one store to the subscription service end point of the other store. In the case of a server group deployment, all servers have identical pairs of stores defined and identical copies of the shared datastore they both share.

Note:

> The Citrix Virtual Apps and Desktops controllers configured on each store must match exactly; otherwise, an inconsistent set of resource subscriptions on one store compared to another might occur. Sharing a datastore is supported only when the two stores reside on the same StoreFront server or server group deployment.

StoreFront subscription datastore endpoints

1. On a single StoreFront deployment, open the external store web.config file using Notepad and search for the clientEndpoint. For example:

```
<subscriptionsStoreClient enabled="true">

<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/
1__Citrix_External" authenticationMode="windows"
transferMode="Streamed">

<clientCertificate thumbprint="0" />

</clientEndpoint>

</subscriptionsStoreClient>
```

2. Change the external to match the internal store endpoint:

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

```
<subscriptionsStoreClient enabled="true">

<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/
1__Citrix_Internal" authenticationMode="windows"
transferMode="Streamed">

<clientCertificate thumbprint="0" />

</clientEndpoint>

</subscriptionsStoreClient>
```

3. If using StoreFront server group then propagate any changes made to the web.config file of the primary node to all other nodes.

Both stores are now set to share the internal store subscription datastore.

Manage favorites for a store

You can manage subscription data (favorites) for a store using PowerShell cmdlets.

NOTE:

Use either the StoreFront management console or PowerShell to manage StoreFront. Do not use both methods at the same time. Always close the StoreFront management console before using PowerShell to change your StoreFront configuration. Citrix also recommends that you take a backup of your existing subscription data before making changes so that rollback to a previous state is possible.

Purge subscription data

A folder and datastore containing subscription data exists for each store in your deployment.

1. Stop the Citrix Subscriptions Store service on the StoreFront server. If the Citrix Subscriptions Store service is running, it is not possible to delete subscription data for any of your stores.
2. Locate the subscription store folder on the StoreFront server: `C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__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.

In StoreFront 3.5 or later, you can use the following PowerShell script to purge subscription data for a store. Run this PowerShell function as an administrator with rights to stop or start services and delete files. This PowerShell function achieves the same result as the manual steps described above.

To run the cmdlets successfully, the Citrix Subscriptions Store service must be running on the server.

```
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 following PowerShell cmdlet.

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/citrix/
&lt;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>"
```

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

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

For more information on Restore-STFStoreSubscriptions, see `<https://developer-docs.citrix.com/en-us/storefront-powershell-sdk/2402/Restore-STFStoreSubscriptions/>`

Restoring Data on a Single StoreFront Server

In a single server deployment, there is no need to shut down the Subscriptions Store service. There is also no need to purge the existing subscription data before restoring the subscription data.

Restoring Data on a StoreFront Server Group

To restore subscription data to a server group, the following steps are required.

Example Server Group Deployment containing three StoreFront servers.

- StoreFrontA
- StoreFrontB
- StoreFrontC

1. Back up of the existing subscription data from any of the three servers.
2. Stop the Subscriptions Store service on servers StoreFrontB and C. This action prevents the servers from sending or receiving subscription data during the update of StoreFrontA.
3. Purge the subscription data from servers StoreFrontB and C. This prevents mismatch of the 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.

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

7. Export the data from StoreFrontB and C to confirm that the synchronization has completed, or view the Store Subscription counters.

Import subscription data

Use **Import-STFStoreSubscriptions** when there is no subscription data for the Store. This cmdlet also allows subscription data to be transferred from one Store to another or if subscription data is imported to newly provisioned StoreFront servers.

```
$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/2402/Import-STFStoreSubscriptions/>`

Subscription data file details

The subscription data file is a text file containing one line per user subscription. Each line is a tab-separated sequence of values:

`<user-identifier> <resource-id> <subscription-id> <subscription-status> <property-name> <property-value> <property-name> <property-value> ...`

where:

- `<user-identifier>` - Required. A sequence of characters identifying the user. This identifier is the user's Windows Security Identifier.
- `<resource-id>` - Required. A sequence of characters identifying the subscribed resource.
- `<subscription-id>` - Required. A sequence of characters uniquely identifying the subscription. This value is not used (although, a value must be present in the data file).
- `<subscription-status>` - Required. The status of the subscription: subscribed or unsubscribed.
- `<property-name>` and `<property-value>` - Optional. A sequence of zero or more pairs of property name/value pairs. These represent properties associated with the subscription by a StoreFront client (typically a Citrix Workspace app). A property with multiple values that is

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

represented by multiple name/value pairs that have the same name (for example, "… MyProp A MyProp B …" represents the property MyProp with values A, B).

Example

S-0-0-00-0000000000-0000000000-0000000000-0000 XenApp.Excel 21EC2020-3AEA-4069-A2DD-08002B30309D Subscribed dazzle:position 1

Size of subscription data on the StoreFront server disk

NO OF RECORDS	SIZE MB
0	6.02
1,000	7.02
10,000	40.00
100,000	219.00
200,000	358.00
500,000	784.00
800,000	1213.02
1,000,000	1597.15
1,300,000	1919.15
1,500,000	2205.15
2,000,000	2915.15

Size of import and export .txt files

NO OF RECORDS	SIZE MB
0	0.00
1,000	0.13
10,000	1.30

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

NO OF RECORDS	SIZE MB
100,000	12.80
200,000	25.60
500,000	64.10
800,000	102.00
1,000,000	128.00
1,300,000	166.00
1,500,000	192.00
1,700,000	218.00
2,000,000	256.00

Store Subscription Counters

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

View the Subscription Counters using PowerShell

```
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"
```

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

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

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 T-SQL update statements allow you to manage, modify, or delete subscription records. If you use SQL, you do not need to export, modify and re import the entire ESENT subscription data whenever minor changes to the subscription data are performed.

To migrate existing subscription data from ESENT to Microsoft SQL server, the flat ESENT data exported from StoreFront needs to be transformed into an SQL friendly format for bulk import. For new deployments without any new subscription data, this step is not required. The data transformation step is only needed once. This article describes the supported configuration which can be used in all StoreFront versions from version 3.5, which introduced the -STF PowerShell SDK referenced in the article.

NOTE:

Failures to connect to the SQL server instance used by StoreFront to store the subscription data due to network outages do not render the StoreFront deployment unusable. Outages only result in a temporarily degraded user experience; users cannot add, remove, or view favorite resources until the connection to SQL server is restored. Resources can still be enumerated and launched during the outage. The expected behavior is the same as if the Citrix Subscription Store service were to stop while using ESENT.

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

Tip:

Resources configured with KEYWORDS:Auto or KEYWORDS:Mandatory behave the same way when using both ESENT or SQL. New SQL subscription records are created automatically when a user first logs on if either KEYWORD is included in the user's resources.

Advantages of ESENT and SQL server

ESENT	SQL
Default and requires no addition configuration to use StoreFront "out of the box".	Much more manageable and subscription data can be manipulated or updated easily using T-SQL queries. Allows records per user to be deleted or updated Allows easy means to count records per application, delivery controller or user. Allows easy means to remove unnecessary user data for users who have left the company/organization. Allows easy means to update delivery controller references such as when the admin switches to using aggregation or new delivery controllers are provisioned.
Simpler to configure replication between different server groups using subscription syncing and pull schedules. See 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.	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

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

ESENT	SQL
Potentially thousands of records may need to be changed using find and replace techniques, which is labor intensive and potentially error prone.	instance can also be shared with StoreFront to reduce costs.
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

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

use SQL. This is not recommended due to increased management complexity and the scope for misconfiguration.

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

Scenario 1: Single StoreFront Server or Server Group using ESENT (default)

By default, all versions of StoreFront since version 2.0 use a flat ESENT database to store and replicate subscription data between members of a server group. Each member of the server group maintains an identical copy of the subscription database, which is synced with all other members of the server group. This scenario requires no additional steps to configure. This scenario is suitable for most customers who do not expect frequent changes to Delivery Controller names or do not need to perform frequent management tasks on their subscription data like removing or updating old user subscriptions.

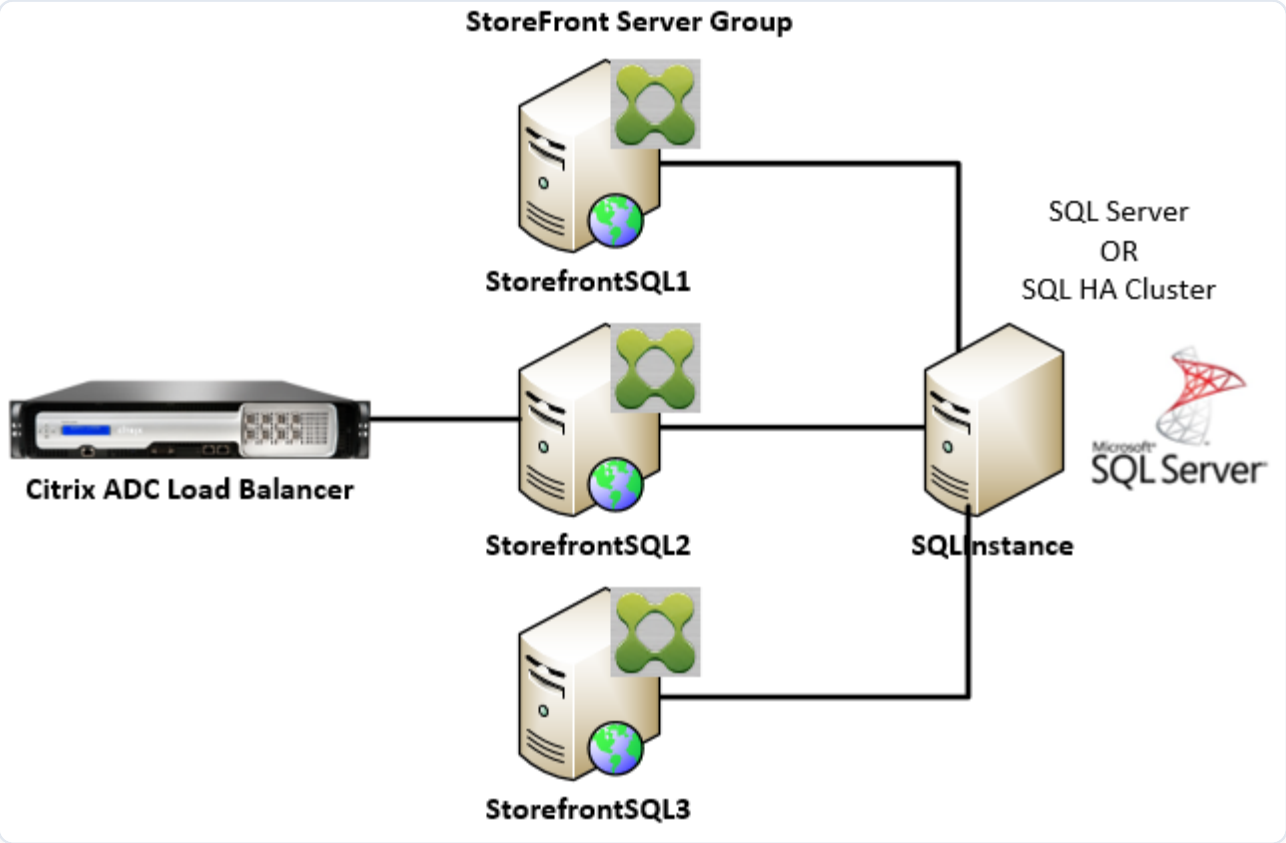
Scenario 2: Single StoreFront Server and a local Microsoft SQL server instance installed

StoreFront uses a locally installed SQL server instance and both components reside on the same server. This scenario is suitable for a simple single StoreFront deployment where customers might need to make frequent changes to Delivery Controller names, or they need to perform frequent management tasks on their subscription data like removing or updating old user subscriptions, but they do not require a high availability StoreFront deployment. Citrix do not recommend this scenario for server groups because it creates a single point of failure on the server group member that hosts the Microsoft SQL database instance. This scenario is not suitable for large enterprise deployments.

Scenario 3: StoreFront server group and a dedicated Microsoft SQL server instance configured for high availability (recommended)

All StoreFront server group members connect to the same dedicated Microsoft SQL server instance or SQL failover cluster. This is the most suitable model for large enterprise deployments where Citrix administrators want to make frequent changes to delivery controller names or want to perform frequent management tasks on their subscription data like removing or updating old user subscriptions and require high availability.

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



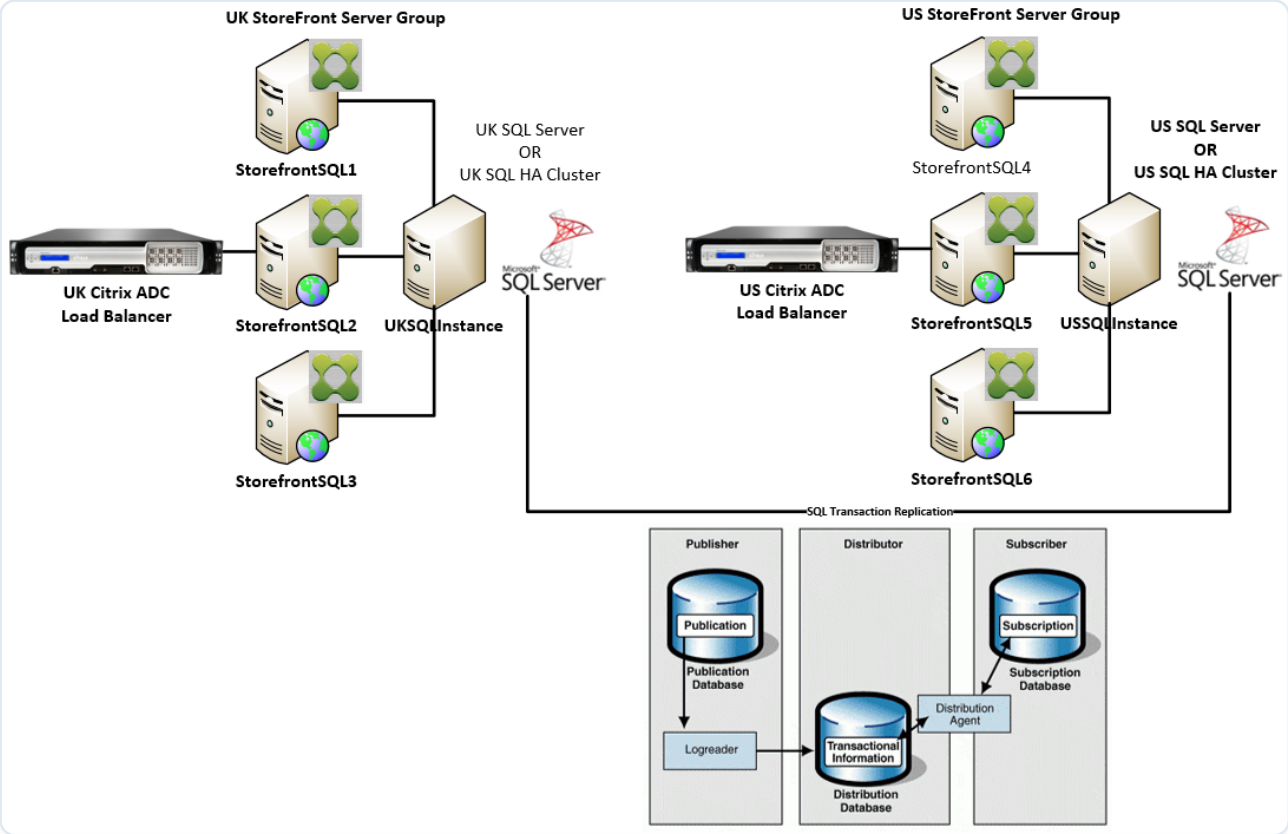
Scenario 4: Multiple StoreFront server groups and a dedicated Microsoft SQL server instance in each data center per server group

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"

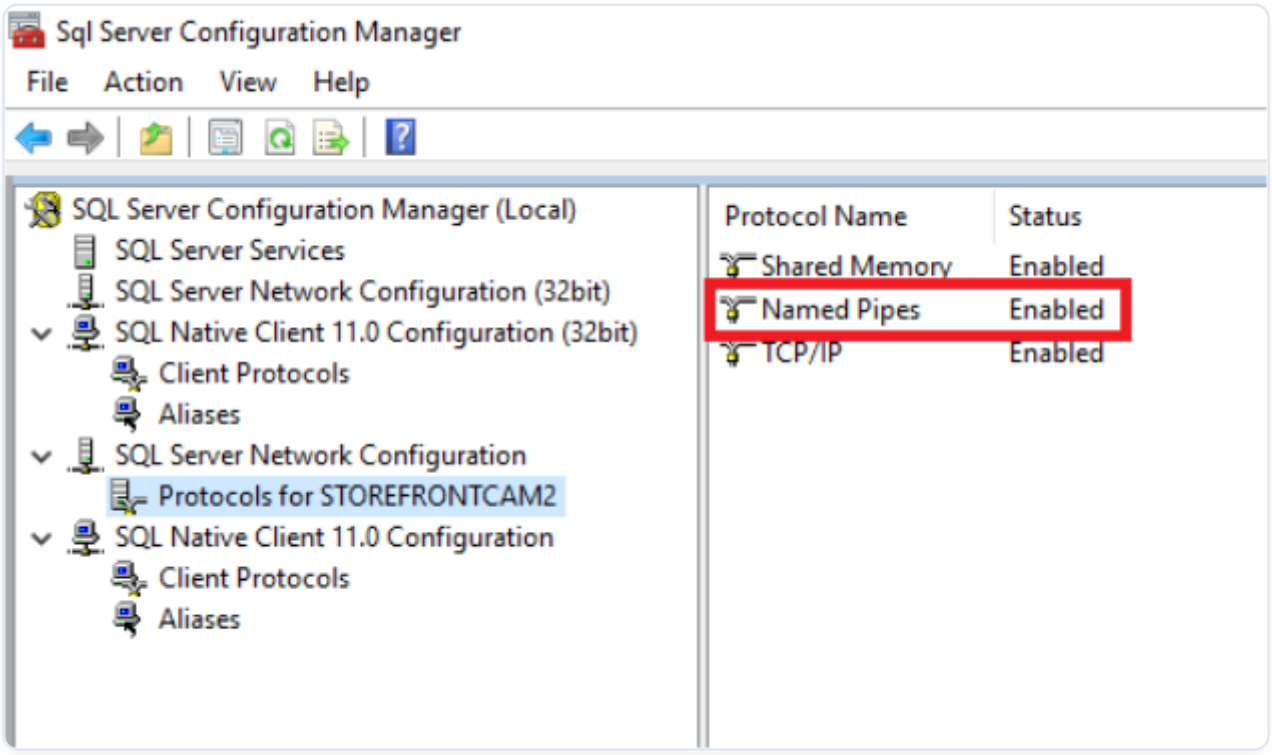
$Group.Add($Account.Path)



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.

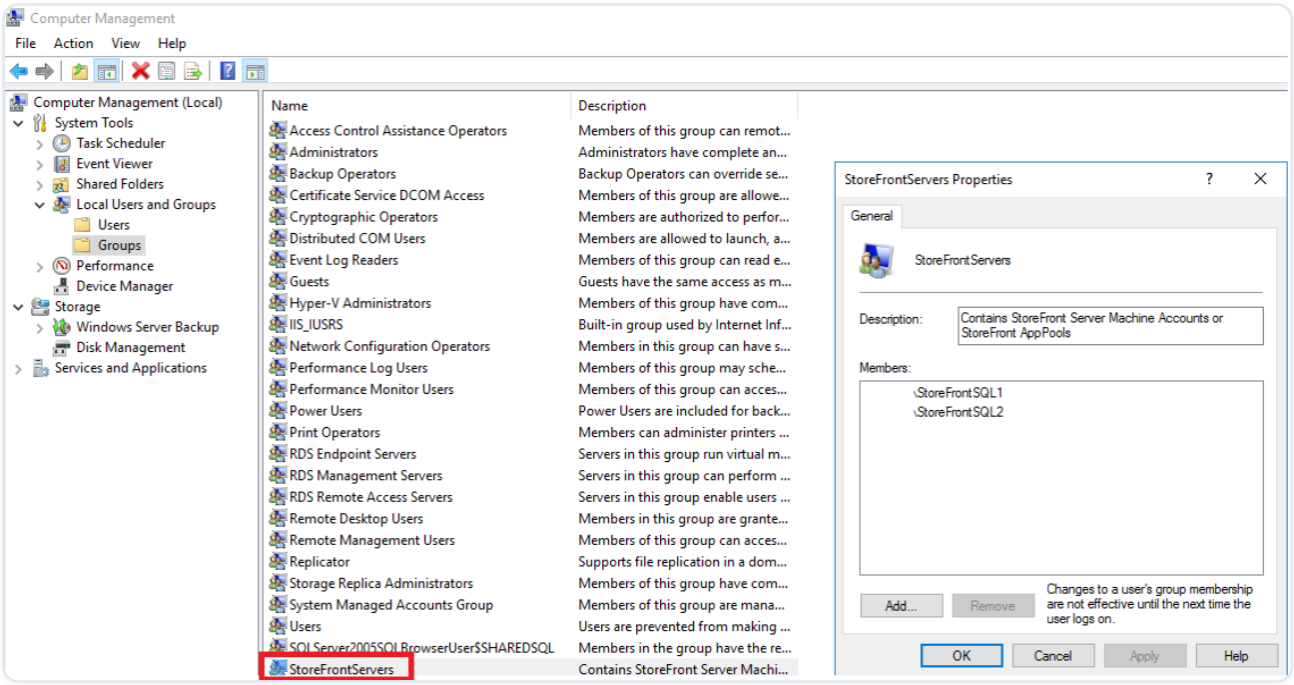
TIP:

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.

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



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.

```
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"
```

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

```
# 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"

    $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)

{
```

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

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

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

    $Group.Add($Computer.Path)

}

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

}

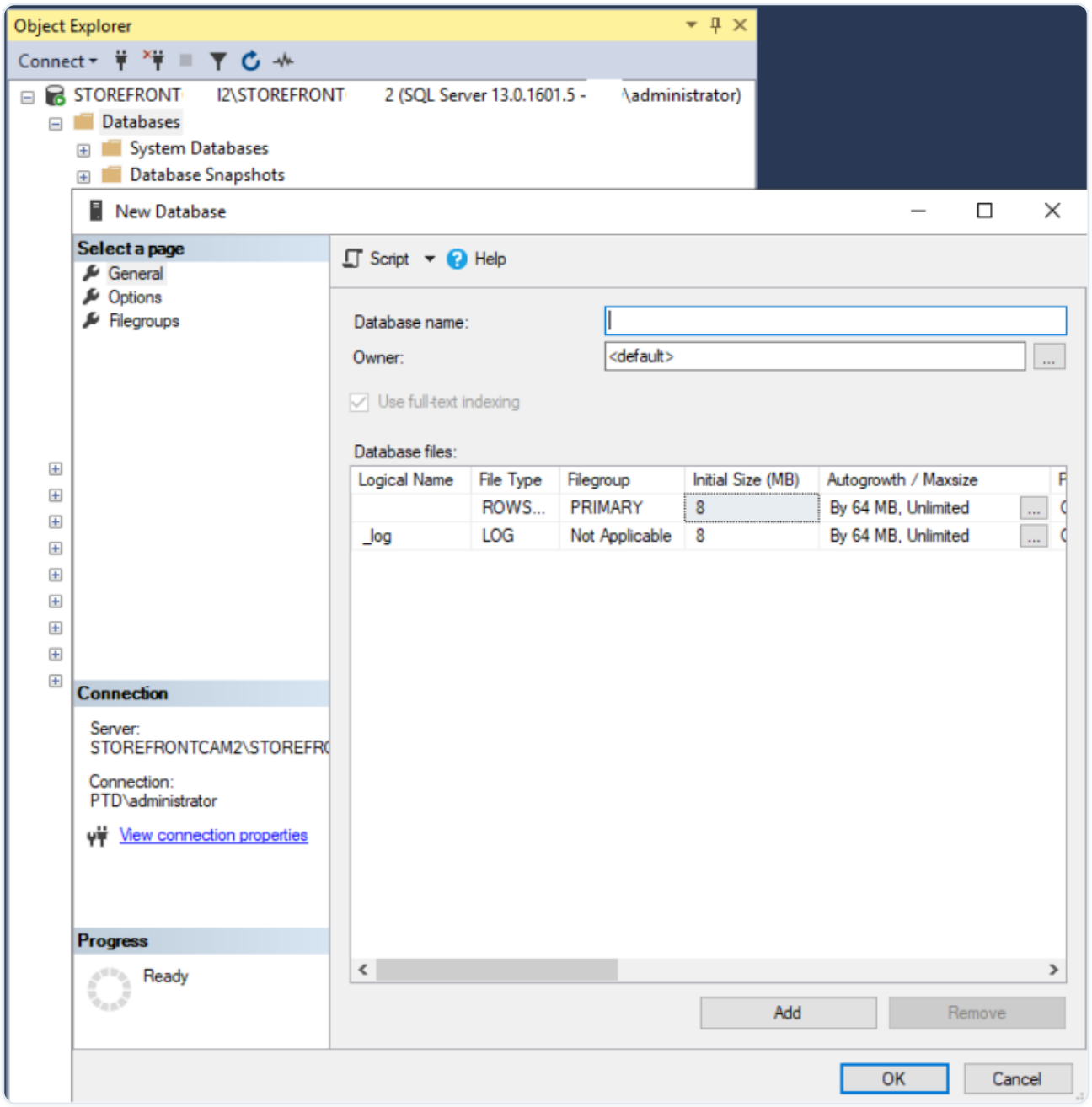
Add-RemoteSTFMachineAccounts -Domain "example" -StoreFrontServers
@("StoreFrontSQL1","StoreFrontSQL2")
```

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**.

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



Type a **Database name** to match your store, or choose a different name such as *STFSubscriptions*.

Before running the script, for each store in your StoreFront deployment, modify the references in the example script to match your StoreFront and SQL deployments. For example, modify:

- Name each database you create to match the store name in StoreFront in `USE [STFSubscriptions]`.
- Set the path to the database .mdf and .ldf files to where you want to store the database.

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

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

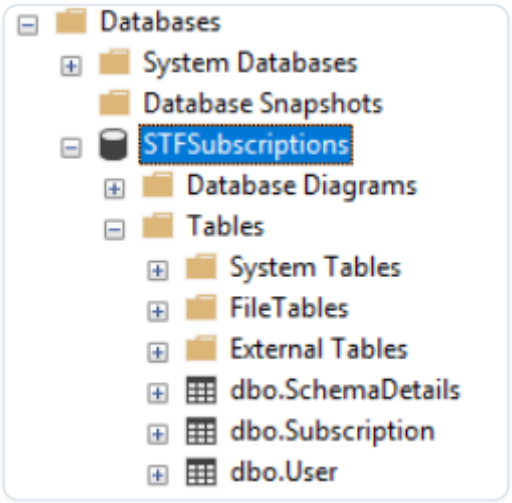
```
C:\Program Files\Microsoft SQL
Server\MSSQL13.SQL2016\MSSQL\DATA\STFSubscriptions.ldf
```

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

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

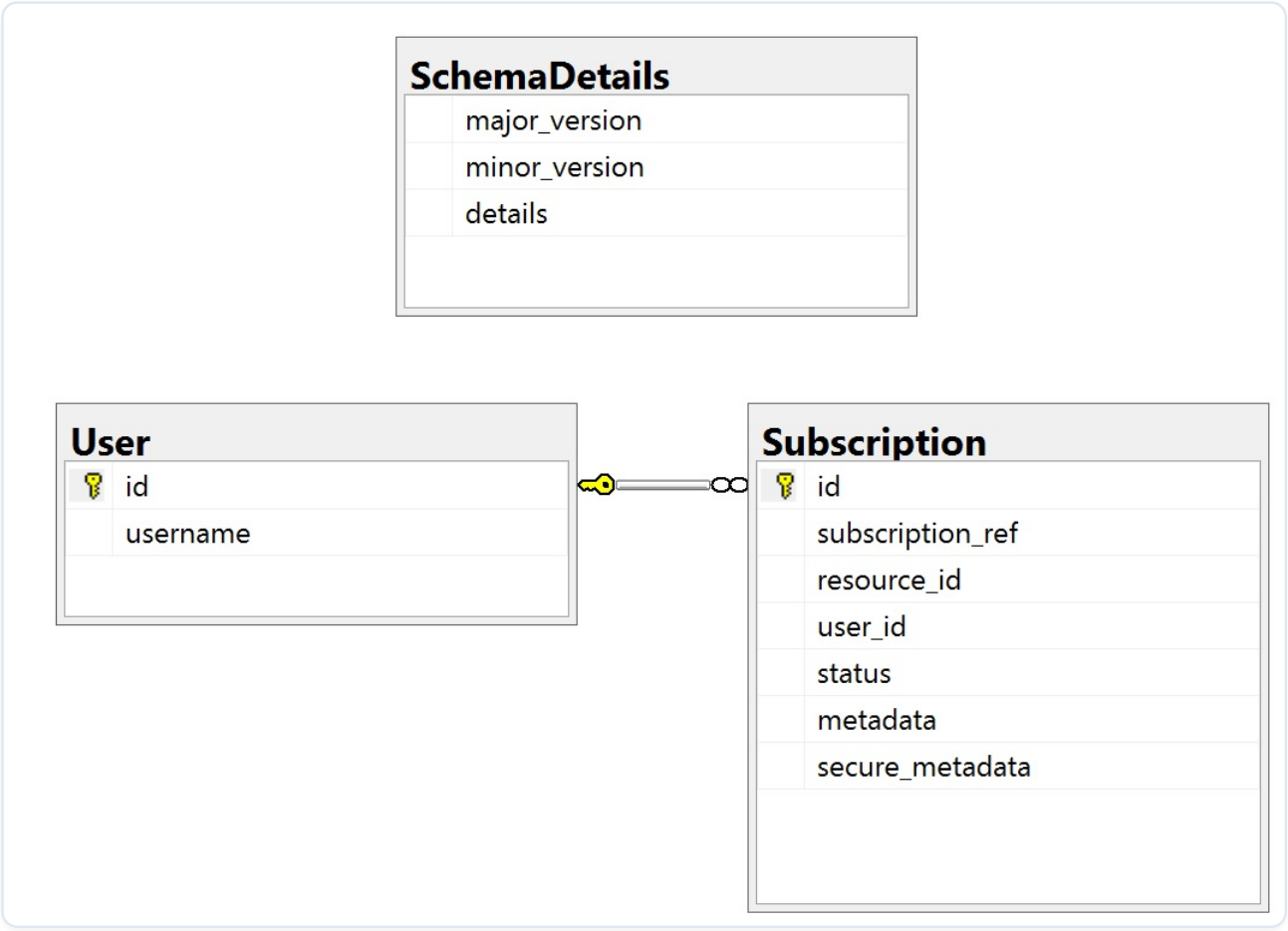
ALTER LOGIN [SQL2016\StoreFrontServers]
```

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.

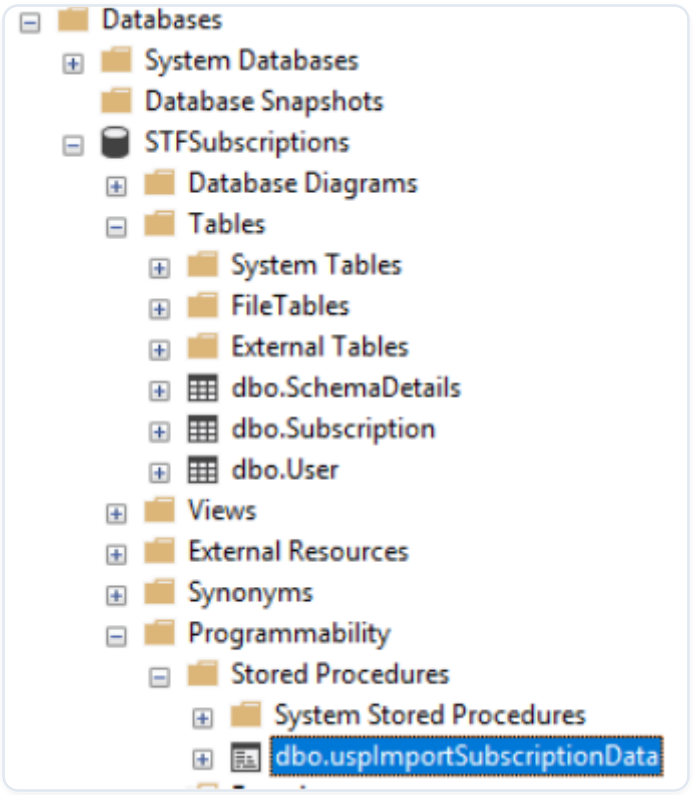
Before executing *Create-ImportSubscriptionDataSP.sql*, change `USE [STFSubscriptions]` to match the database under which you want to create the Stored Procedure.

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.

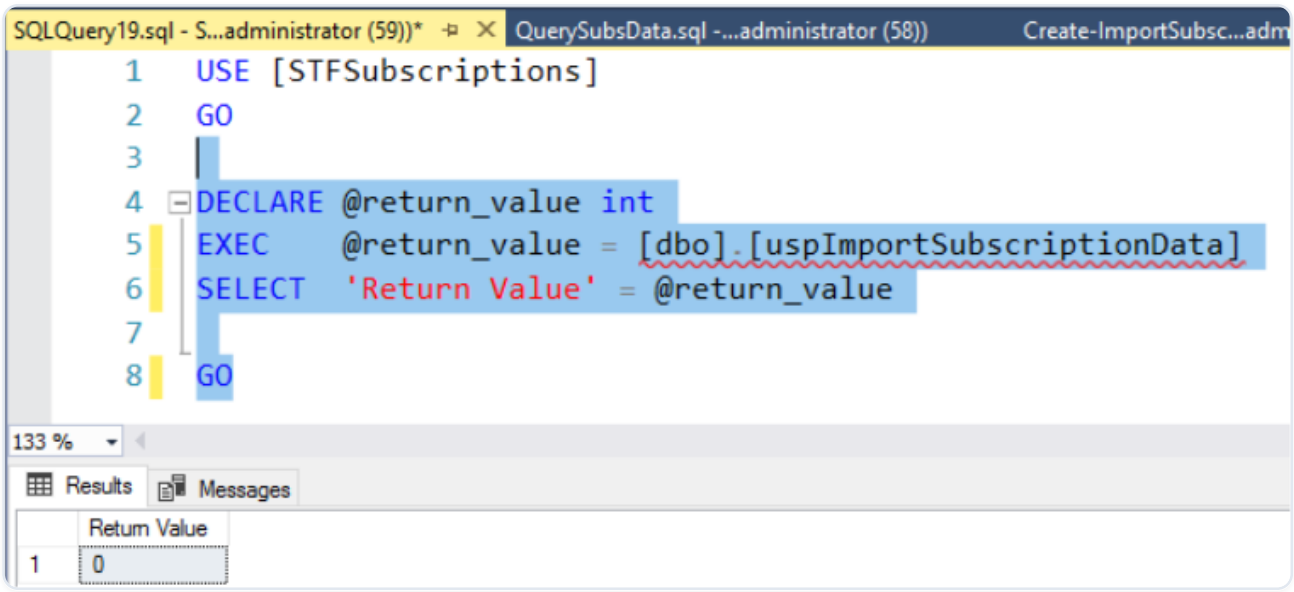
After successful creation of the Stored Procedure the following message is shown in the SQL console, and the ImportSubscriptionDataSP Stored Procedure is added to the database:

© 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 Delivery Controller names are case sensitive and must exactly match the case and name used within StoreFront.

```
-- Update the delivery controller used in all subscriptions.

Use [STFSubscriptions]

UPDATE [Subscription]

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

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

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

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

Use [STFSubscriptions]

UPDATE [Subscription]

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

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

```
-- Delete all subscription records for a particular Delivery Controller

Use [STFSubscriptions]

DELETE FROM [Subscription]

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

```
-- 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'
```

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

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

Use [STFSubscriptions]

DELETE FROM [Subscription]

FROM [Subscription]

WHERE [resource_id] = 'DeliveryController.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.

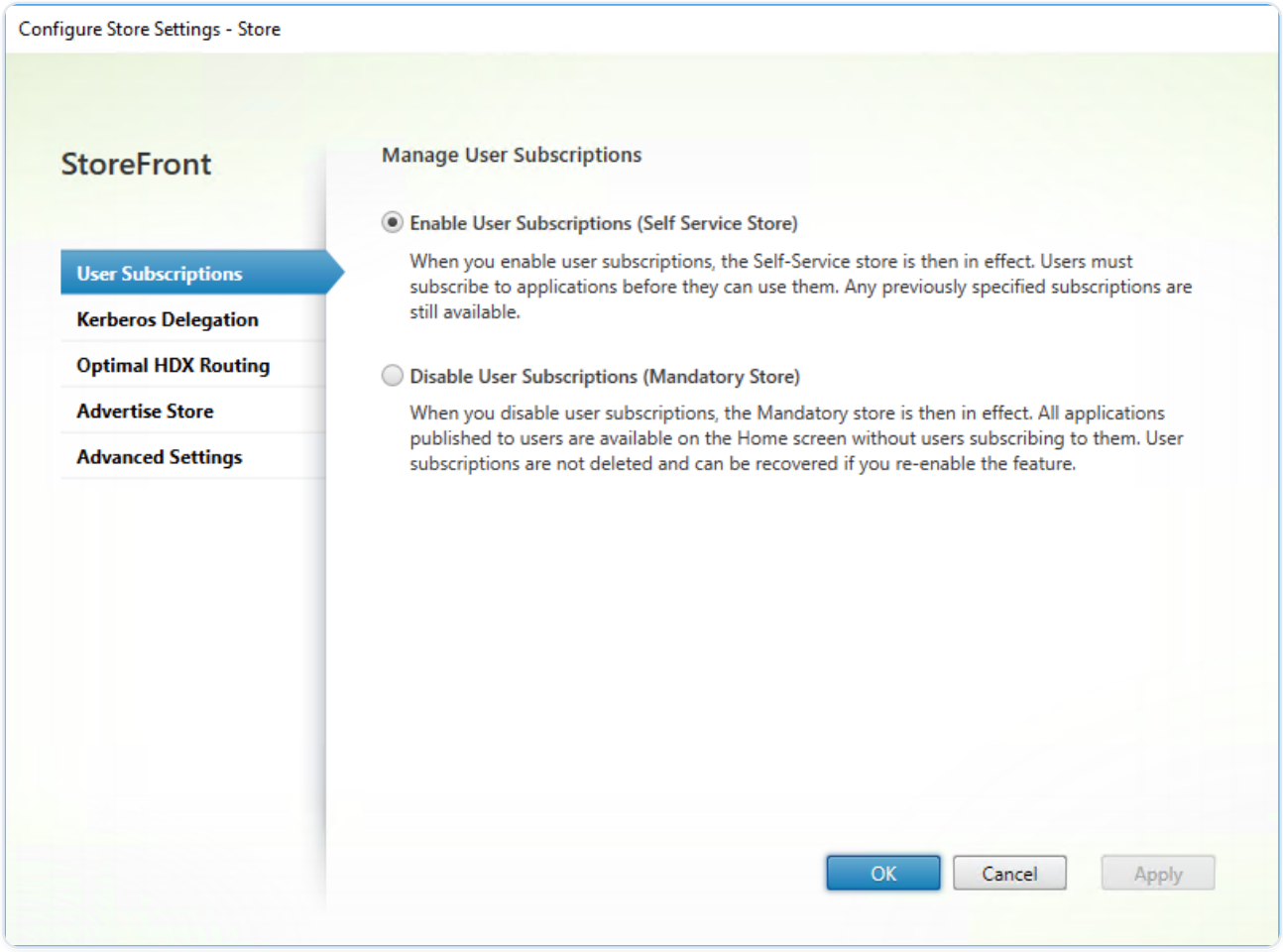
Enable or disable favorites

Use the User Subscriptions screen to do select one of the following options:

- Allow users to create and remove favorites (Self Service Store). Users can favorite an app by clicking the star on the app tile. Users can click the star again un-favorite an app. Favorite apps are displayed on the **Home** tab.
- Disable favorites (Mandatory Store). Users cannot favorite or un-favorite apps. The home tab is not displayed.

Disabling subscriptions does not delete the Store subscription data. Re-enabling subscriptions for the store will allow the user to see their favourites whenever they next log on.

1. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the **Actions** pane, click **Configure Store Settings**
2. Click on the **User Subscriptions** tab to toggle the user favorites feature off or on.
3. Choose **Enable user subscriptions (Self Service Store)** to enable favorites.
4. Choose **Disable user subscriptions (Mandatory Store)** to disable favorites.



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

Alternatively, you can use the PowerShell cmdlet Get-STFStoreService to configure user subscriptions for a store, for example:

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

Set-STFStoreService -StoreService $StoreObject -LockedDown $True -Confirm:
$False
```

Citrix Virtual Apps and Desktops™ configuration

When delivering applications with Citrix Virtual Apps and Desktops or Citrix Desktops as a Service, consider the following options to enhance the experience for users when they access their applications through your stores. For more information about delivering applications, see Applications.

- In the **Application name (for user)** field enter the application name as you wish it to appear within your store website.
- In the **Description and keywords** field enter the description that is displayed on the store website when you expand the app details, alongside any keywords.
- Choose the **Application icon** to help users visually identify an application on the StoreFront website.
- In the **Application category** field, optionally enter a category. Include `\` in the category name to create a folder hierarchy. You could, for example, group applications according to type or, alternatively, create folders for different user roles in your organization. In the store website **Apps** tab, **Category** view displays a list of categories and the apps in each category.

Keywords

You can add keywords to an app or desktop by appending the string `KEYWORDS:[keywordname]` to the application description. Multiple keywords must be separated by spaces only; for example, `KEYWORDS:Accounts Featured`. Keywords can used in a number of ways:

- Filter applications - see Advanced store settings.
- Create Featured app groups.
- Some keywords have special meanings.

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

KEYWORD NAME	DESCRIPTION
Mandatory	Adds an application to the Home tab. Unlike favourites, users cannot remove mandatory applications from the Home tab. Has no effect if favourites are disabled for the store.
Auto	When users log on to the store, the application or desktop is automatically favourited and added to their Home tab. Users can unfavourite such applications. Has no effect if favourites are disabled for the store.
TreatAsApp	Apply to desktops to force StoreFront to treat it as an app. The desktop is displayed on the **Apps** tab rather than the **Desktops** tab. In addition, the desktop is not automatically started when the user logs on to the store website and is not accessed with the Desktop Viewer, even if the site is configured to do this for other desktops.
prefer="*application*"	Where *application* identifies a locally installed application. Applies only on Citrix Workspace app on Windows. This indicates that the locally installed version of an application should be used in preference to the equivalent delivered instance if both are available. For more information, see Configuring Local App Access applications.
Primary and **Secondary**	When using Multi-Site Aggregation, the one with the keyword **primary** specified always preferred over the one with the keyword **secondary**.

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:

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

- 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`

Advanced store settings

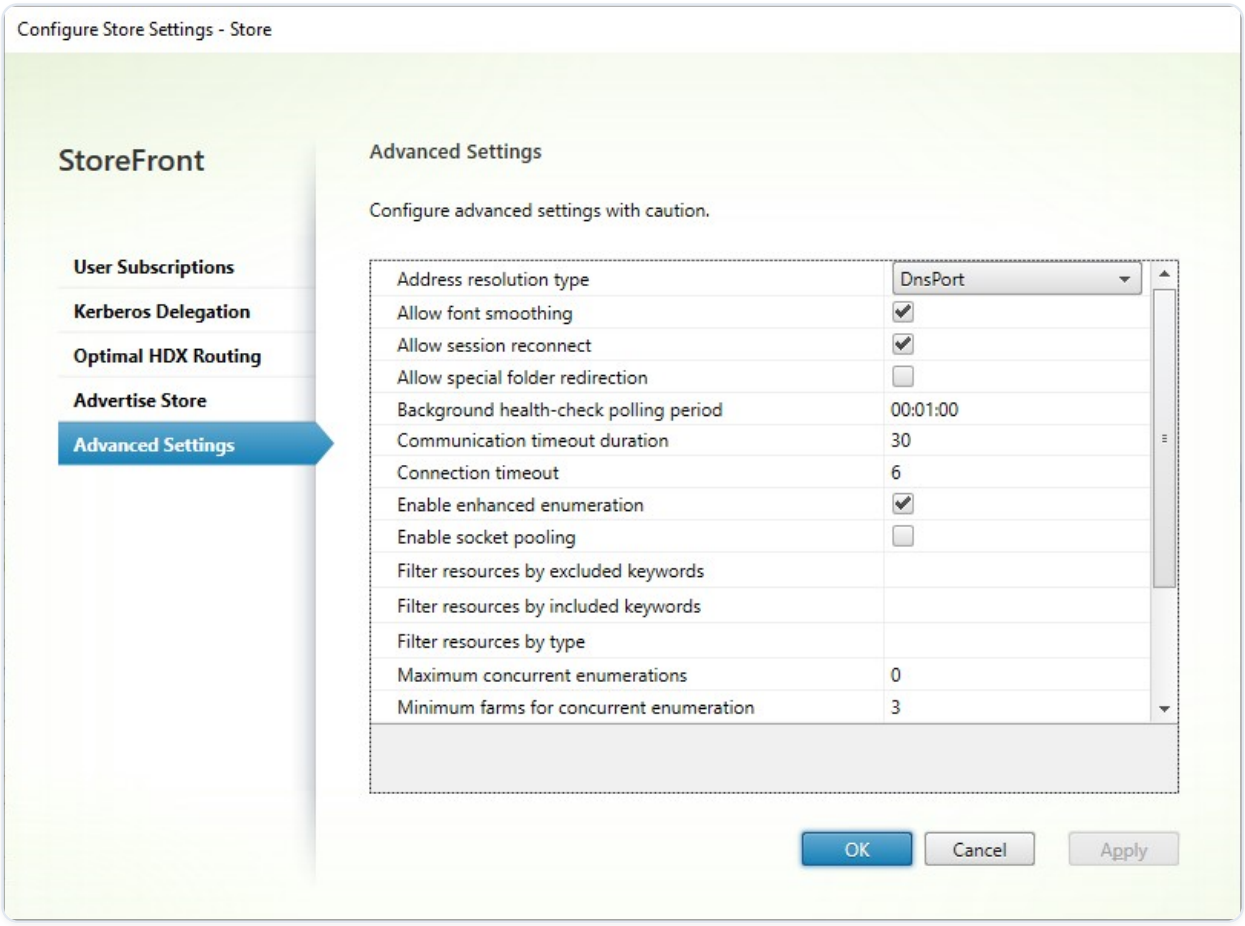
You can configure most advanced store properties by using the Advanced Settings page in the Configure Store Settings. Some settings can only be modified using PowerShell.

IMPORTANT:

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

1. Select the Stores node in the left pane of the Citrix StoreFront management console, select a store in the center pane, and in the Action pane, select **Configure Store Settings**.
2. On the **Configure Store Settings** page, select **Advanced Settings** and make the required changes.

© 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 resource feed to include all cloud connectors in all resource locations and enable the advanced health check feature.

Advanced health check is enabled by default for new stores and is also turned on for existing stores on upgrade to 2402. To enable or disable advanced health check, use the PowerShell

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

cmdlet Set-STFStoreFarmConfiguration with parameter `AdvancedHealthCheck`. Disabling advanced health check is not recommended as it would reduce resiliency.

Background health check polling period

StoreFront runs periodic health checks on each Citrix Virtual Apps and Desktops delivery controller, Cloud Connector and Secure Private Access server to reduce the impact of intermittent server availability. The default is every minute (00:01:00). From the **Advanced Settings** window, specify a time for the **Background health-check Polling period**, and click **OK** to control the frequency of the health check. To disable the health check, set the polling period to 00:00:00, this is not recommended. Setting the polling period to a low value is not recommended when the Advanced health check is enabled as it may have an impact on performance.

Communication time-out duration

By default, requests from StoreFront to a server providing resources for a store time out after 30 seconds. The server is considered unavailable after 1 unsuccessful communication attempt. From the **Advanced Settings** window, make your changes to the default time, and click **OK** to change these settings.

Connection timeout

You can specify the number of seconds to wait when establishing an initial connection with a Delivery Controller. The default is 6.

From the **Advanced Settings** window, specify the seconds to wait when establishing the initial connection, and click **OK**

Enable enhanced enumeration

This option controls whether StoreFront queries Delivery Controllers concurrently or sequentially when enumerating apps and desktops across multiple Citrix Virtual Apps and Desktops Sites. Concurrent enumeration provides faster responses to user queries when aggregating resources across multiple Sites. When this option is selected (the default), StoreFront sends out enumeration requests to all Delivery Controllers at the same time and aggregates responses when they have all responded. You can use the options **Maximum concurrent enumerations** and **Minimum farms for concurrent enumeration** to tune this behavior.

From the **Advanced Settings** window, select (or clear) the **Enable enhanced enumeration** option, and click **OK**.

© 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'

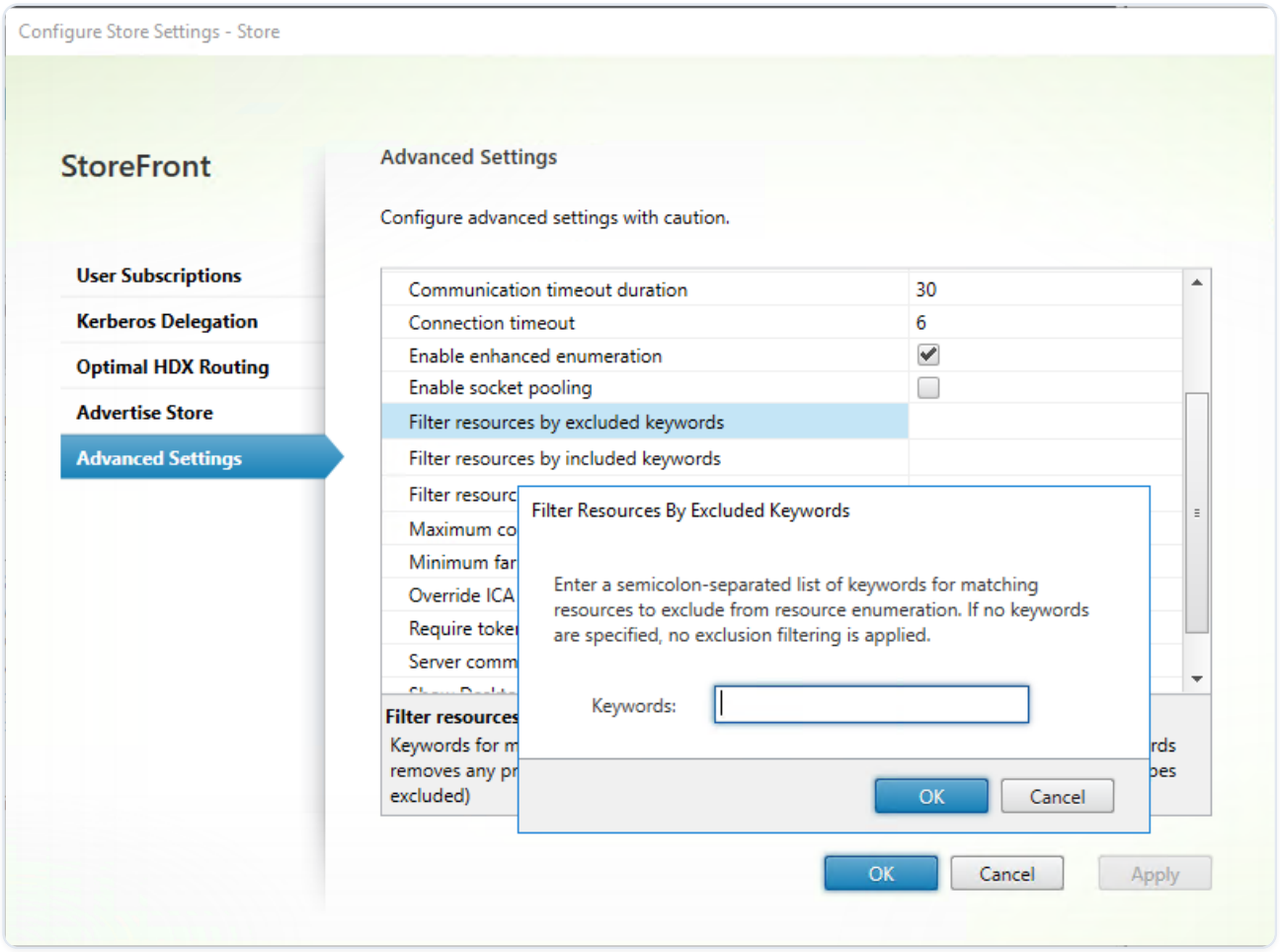
Set-STFStoreFarmConfiguration $storeService -EnableFileTypeAssociation
$false
```

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**.

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.

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

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 resource feeds (delivery controllers) 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 farms

1 x UK Gateway -> 1 x UK StoreFront

- UK Apps and Desktops local
- US Apps and Desktops used only for UK failover

1 x US Gateway -> 1 x US StoreFront

- US Apps and Desktops local
- UK Apps and Desktops used only for US failover

A UK gateway provides remote access to UK hosted resources such as apps and desktops using a UK StoreFront.

The UK StoreFront has both a UK-based and US-based Citrix Gateway defined and UK and US controllers in its Delivery Controller list. UK users access remote resources through their geographically colocated gateway, StoreFront, and farms. If their UK resources become unavailable, they can connect to US resources as a temporary failover alternative.

Without optimal gateway routing all ICA launches would pass through the UK gateway that made the launch request regardless of where the resources are geographically located. By default, gateways used to make launch requests are identified dynamically by StoreFront when the request

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

is made. Optimal gateway routing overrides this and forces US connections through the gateway closest to the US farms that provides apps and desktops.

NOTE:

You can map only one optimal gateway per site for each StoreFront store.

Example scenario using zones

1 x CAMZone -> 2 x UK StoreFronts

- Cambridge, UK: Apps and Desktops
- Fort Lauderdale, Eastern US: Apps and Desktops
- Bangalore, India: Apps and Desktops

1 x FTLZone -> 2 x US StoreFronts

- Fort Lauderdale, Eastern US: Apps and Desktops
- Cambridge, UK: Apps and Desktops
- Bangalore, India: Apps and Desktops

1 x BGLZone -> 2 x IN StoreFronts

- Bangalore, India: Apps and Desktops
- Cambridge, UK: Apps and Desktops
- Fort Lauderdale, Eastern US: Apps and Desktops

Figure 1. Suboptimal gateway routing

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

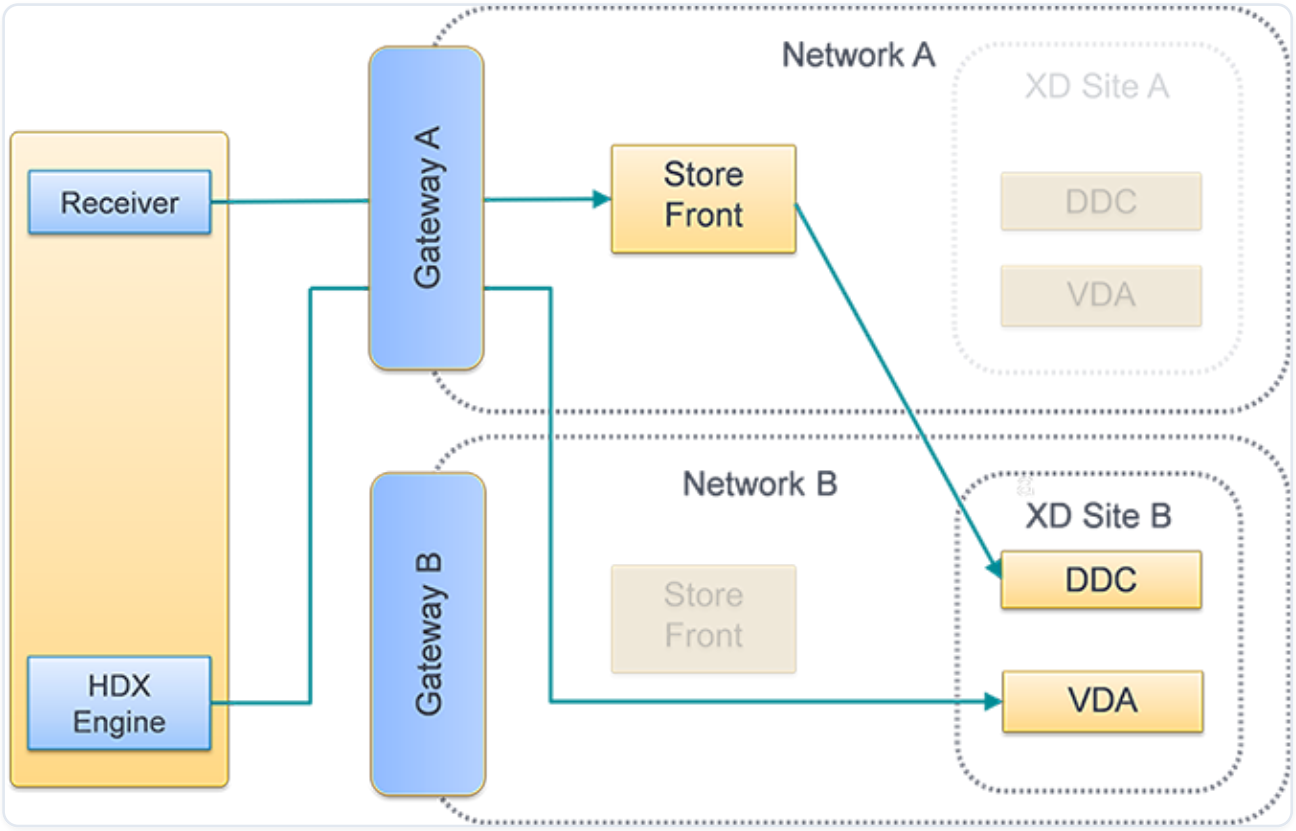
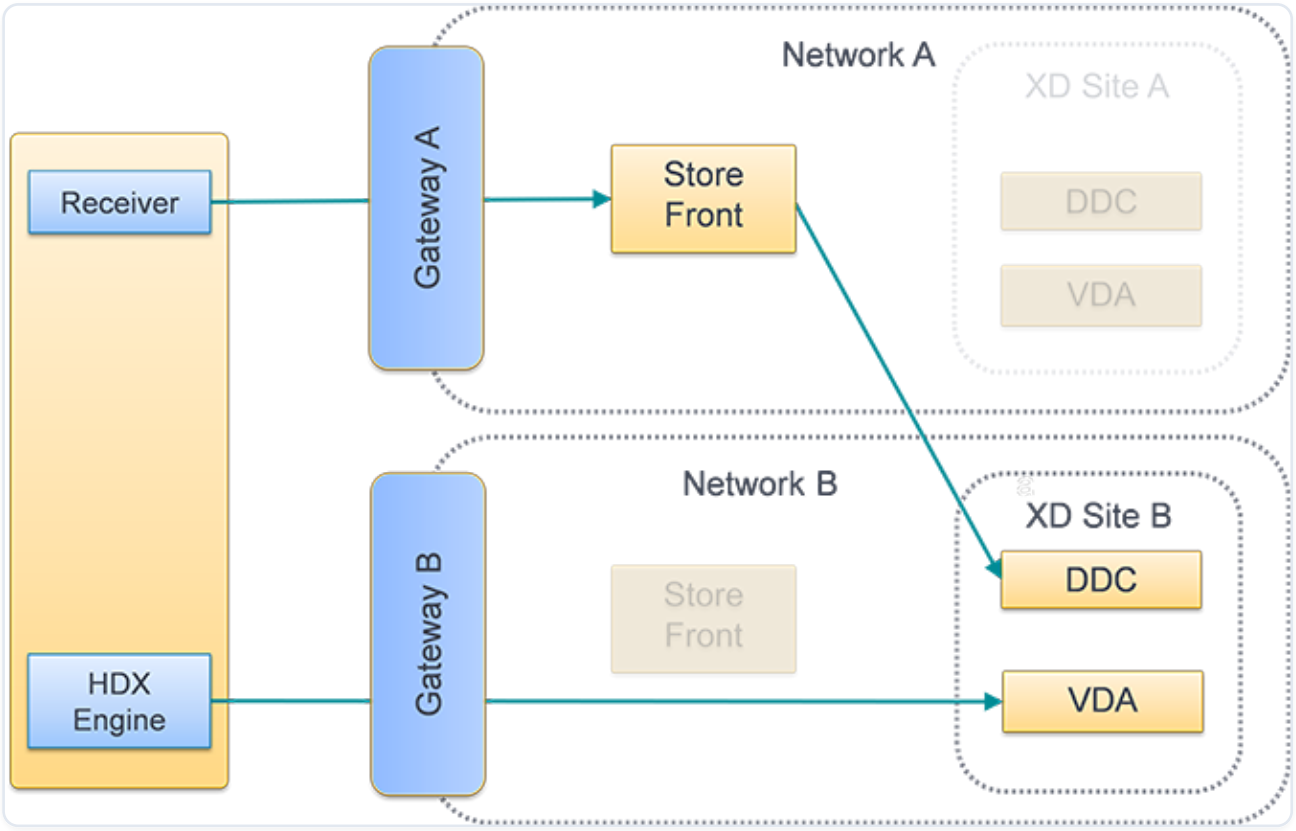


Figure 2. Optimal gateway routing



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

Configure Optimal HDX routing

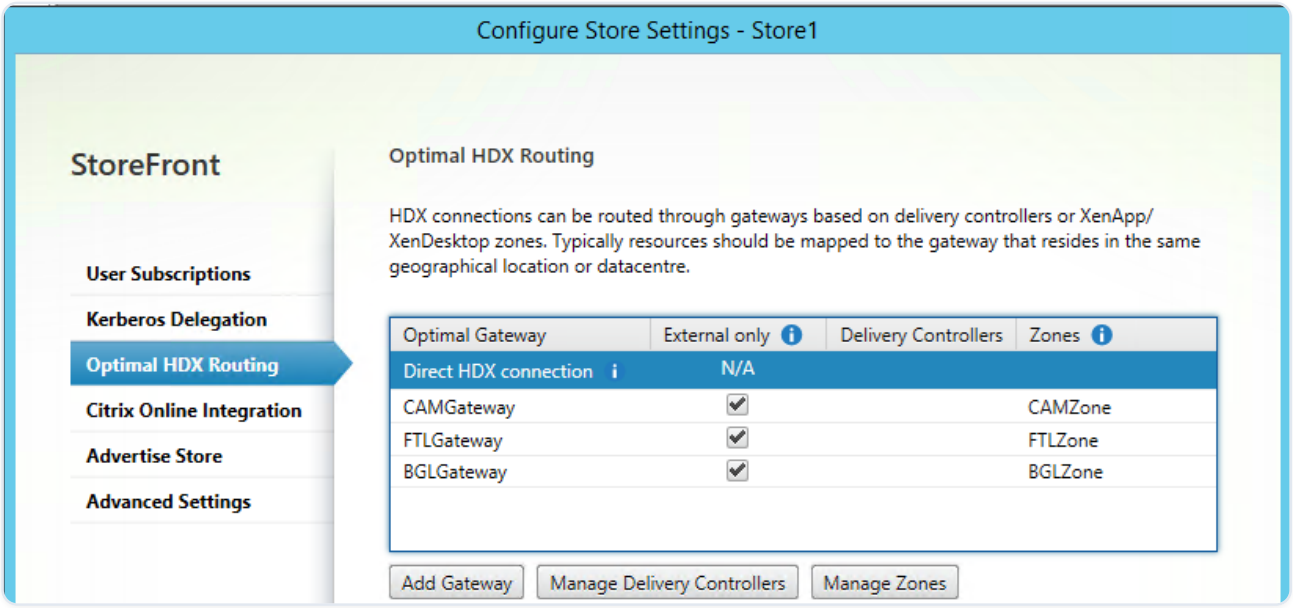
1. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the **Actions** pane, click **Configure Store Settings**.
2. Select the **Optimal HDX Routing** tab.
3. Select a gateway.

    a. To use the gateway when accessing resources from specific delivery controllers, click **Manage Delivery Controllers** and tick one or more delivery controllers

    b. To use the gateway when accessing resources from a group of delivery controllers in a Zone, click **Manage Zones** and enter one or more zone.

    c. By default once you add a delivery controller or zone, **External Only** is ticked, meaning StoreFront only uses the gateway to launch StoreFront for users connected to StoreFront via a gateway. If you wish to also use the gateway to launch resources for users who have connected directly to StoreFront without going via a gateway, untick **External Only**.

4. If you wish to always connect directly to certain resources without using a gateway, even for users accessing StoreFront remotely via a gateway, select **Direct HDX connection** and choose some delivery controllers or zones.



.

Use PowerShell to configure optimal Citrix Gateway routing for a store

- To configure optimal gateway routing for a store use Register-STFStoreOptimalLaunchGateway.

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

- To remove optimal gateway routing for a store use Unregister-STFStoreOptimalLaunchGateway.
- To view optimal routing for a store use Get-STFStoreRegisteredOptimalLaunchGateway.

Subscription synchronization

StoreFront automatically synchronizes subscriptions between servers in a StoreFront server group. If you have multiple server groups (typically in different geographic location) then you can configure periodic pull synchronization of users' subscriptions from stores in different StoreFront deployments. This must be done using PowerShell.

NOTE:

The StoreFront and PowerShell consoles cannot be open at the same time. Always close the StoreFront management console before using the PowerShell console to administer your StoreFront configuration. Likewise, close all instances of PowerShell before opening the StoreFront console.

When establishing your subscription synchronization, note that the configured Delivery Controllers must be named identically between the synchronized Stores including the case. Failing to duplicate the Delivery Controller™ names exactly may lead to users having different subscriptions across the synchronized Stores. If you synchronizing subscriptions from aggregated resources, the name of the aggregation groups used by both Stores must also match. Delivery Controller names and Aggregation Group names are case sensitive; for example, *CVAD_US* is different to *Cvad_Us*.

1. Use an account with local administrator permissions to start the Windows PowerShell ISE.
2. To configure synchronization, use the Publish-STFServerGroupConfiguration command. You can either specify a start time and recurring interval or a list of times. For example to start synchronizing at 08:00 then every 30 minutes:

   ```
   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.

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

3. To specify the remote StoreFront deployment containing the store to be synchronized, type the following command. You must configure this for each data center where a StoreFront server group resides so it can pull subscription data from other remote datacenters. See the following US and UK datacenter examples:

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

     ```
     $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"

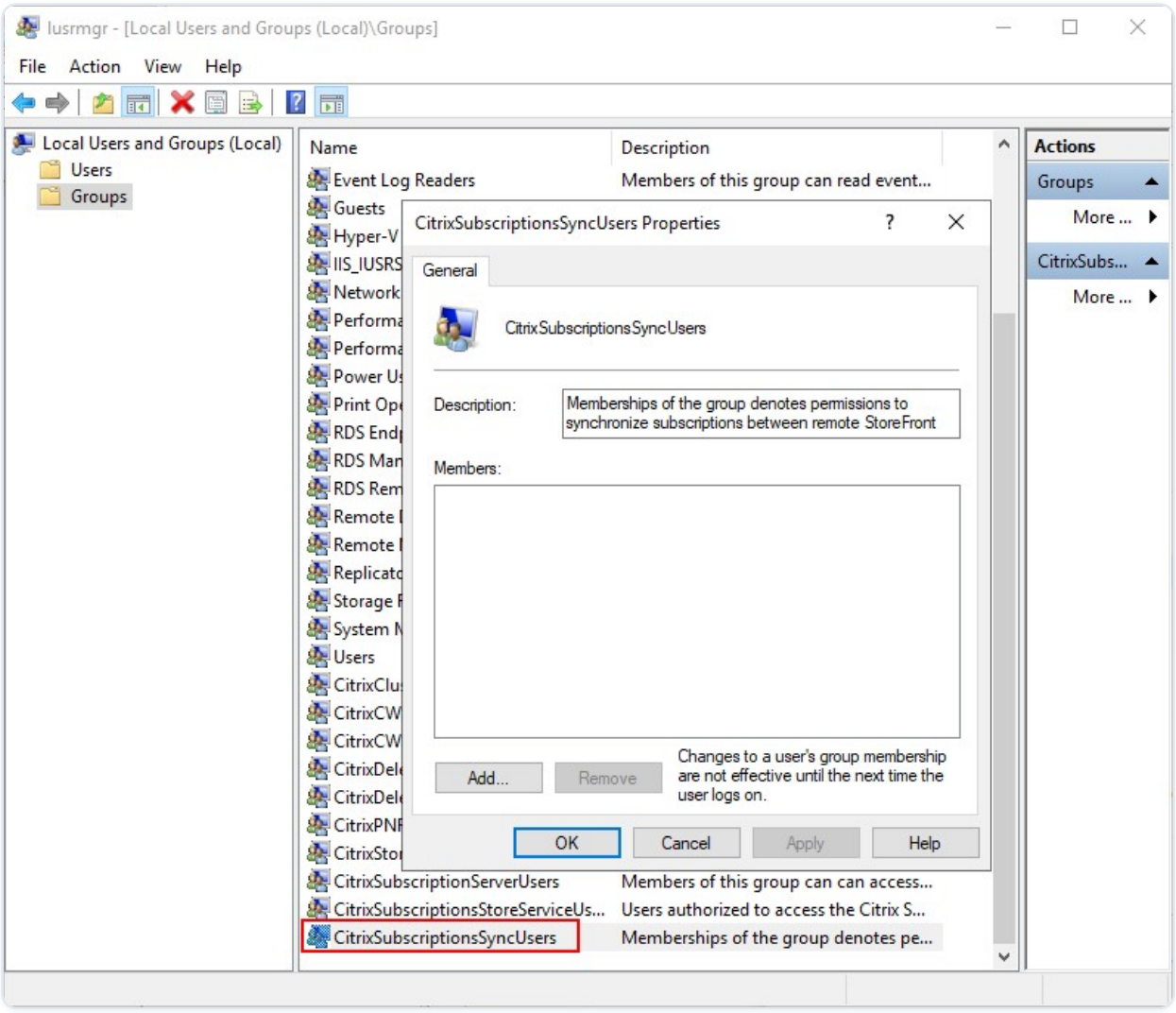
     Add-STFSubscriptionSynchronizationSource -FriendlyName
     "SyncFromUSStore" -StoreService $StoreObject
     -RemoteStoreFrontAddress "USloadbalancedStoreFront.example.com"
     ```

   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
```

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.

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

- On the StoreFront server, add settings to the store's default.ica file.

You can find default.ica on the StoreFront server in the `\inetpub\wwwroot\Citrix\[StoreName]\App_Data` directory.

For a list of available settings see ICA Settings Reference. Some settings apply globally. You can also add sections that apply to specific apps by adding a section whose name exactly matches the application name as configured in Studio.

Example: Launch Notepad in windowed mode

To configure an application to launch in Windowed mode, in default.ica, add a section for the application with the settings:

- TWIMode - set to Off to enable windowed mode.
- DesiredHRES - optionally the horizontal number of pixels.
- DesiredVRES - optionally the vertical number of pixels.

For example:

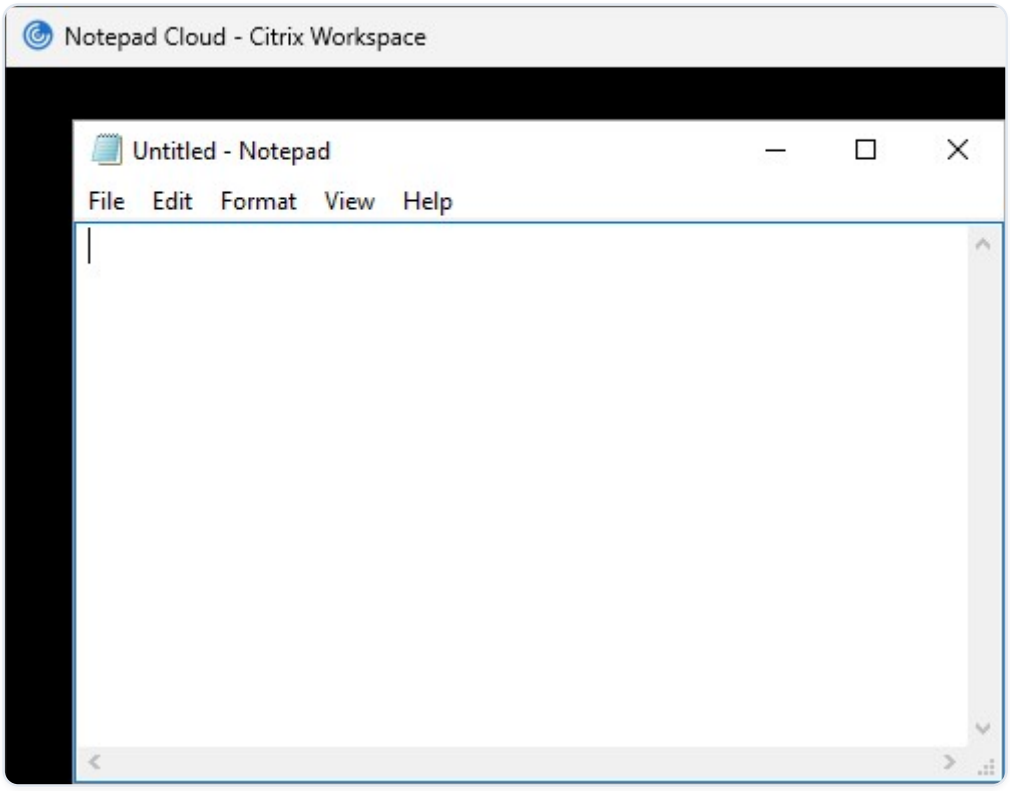
```
[Notepad]

TWIMode=Off

DesiredHRES=1024

DesiredVRES=768
```

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



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 existing SSL certificate, such as a server certificate, or create a new root certification authority certificate and distribute it to users' devices.

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

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.
5. If using a version of StoreFront 2402 prior to CU2 then in addition run:

   ```
   $certificate = Get-DSCertificate "[certificatethumbprint]"

   . "C:\Program Files\Citrix\Receiver
   StoreFront\Scripts\ImportModules.ps1"

   Add-DSCertificateKeyReadAccess -certificate $certificates[0]
   -accountName “IIS APPPOOL\Citrix Delivery Services Resources”
   ```

© 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.

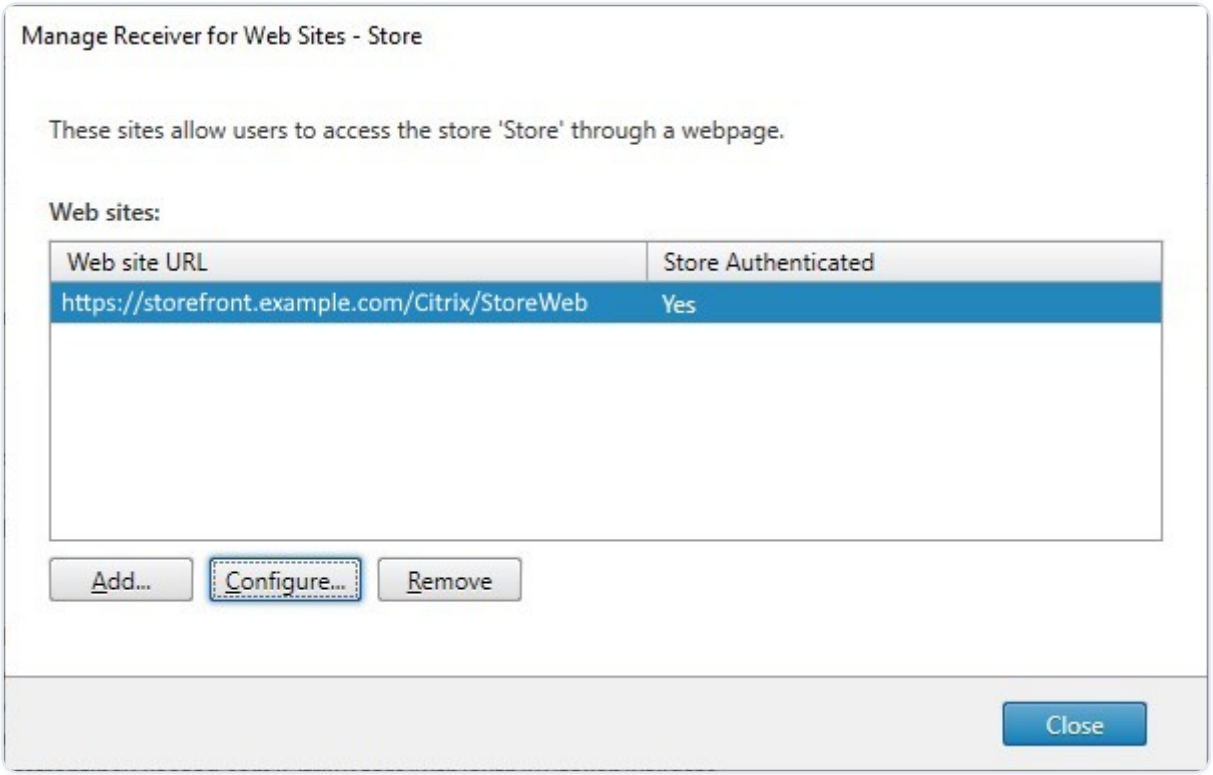
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Manage a website

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.

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, click **Manage Receiver for Web**.



From the **Manager Receiver for Web Sites** screen, you can perform the following tasks:

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

TASK	DETAIL
Create a website	Create websites, which enable users to access stores through a web page or Workspace app.
Configure a website	Modify settings for your website.
Remove a website	Remove a Citrix Receiver for Web site.
Configure Workspace app website	Choose which website to use from within the Citrix Workspace app.

PowerShell

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

Create a website

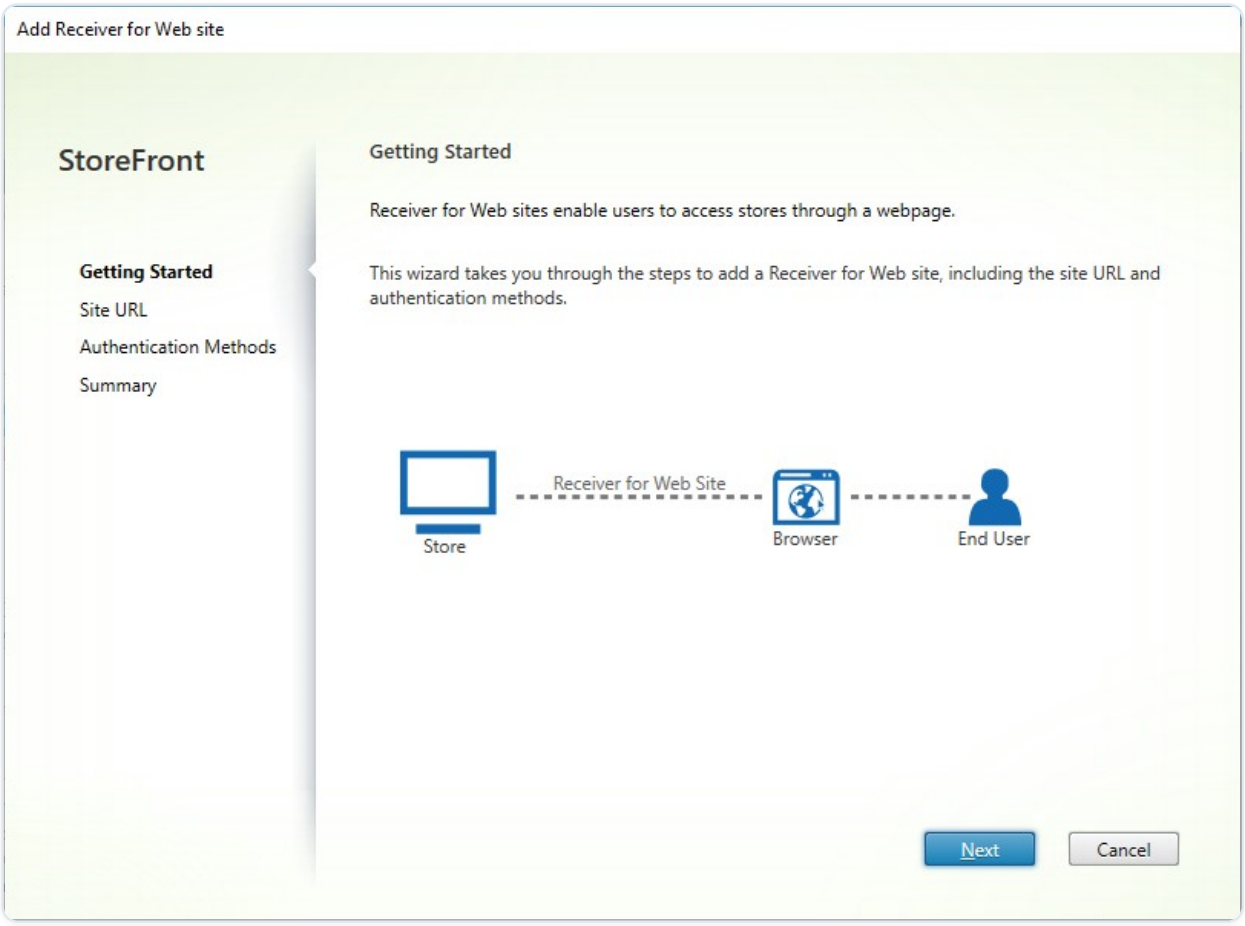
When you create a store, a website is created for it automatically. You can add additional websites to existing stores. This allows you to provide different URLs with different configurations to your users. However multiple websites can only be accessed through a web browser as Citrix Workspace Apps are configured to use one specific website for a store, see Configure Workspace app website.

Important:

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

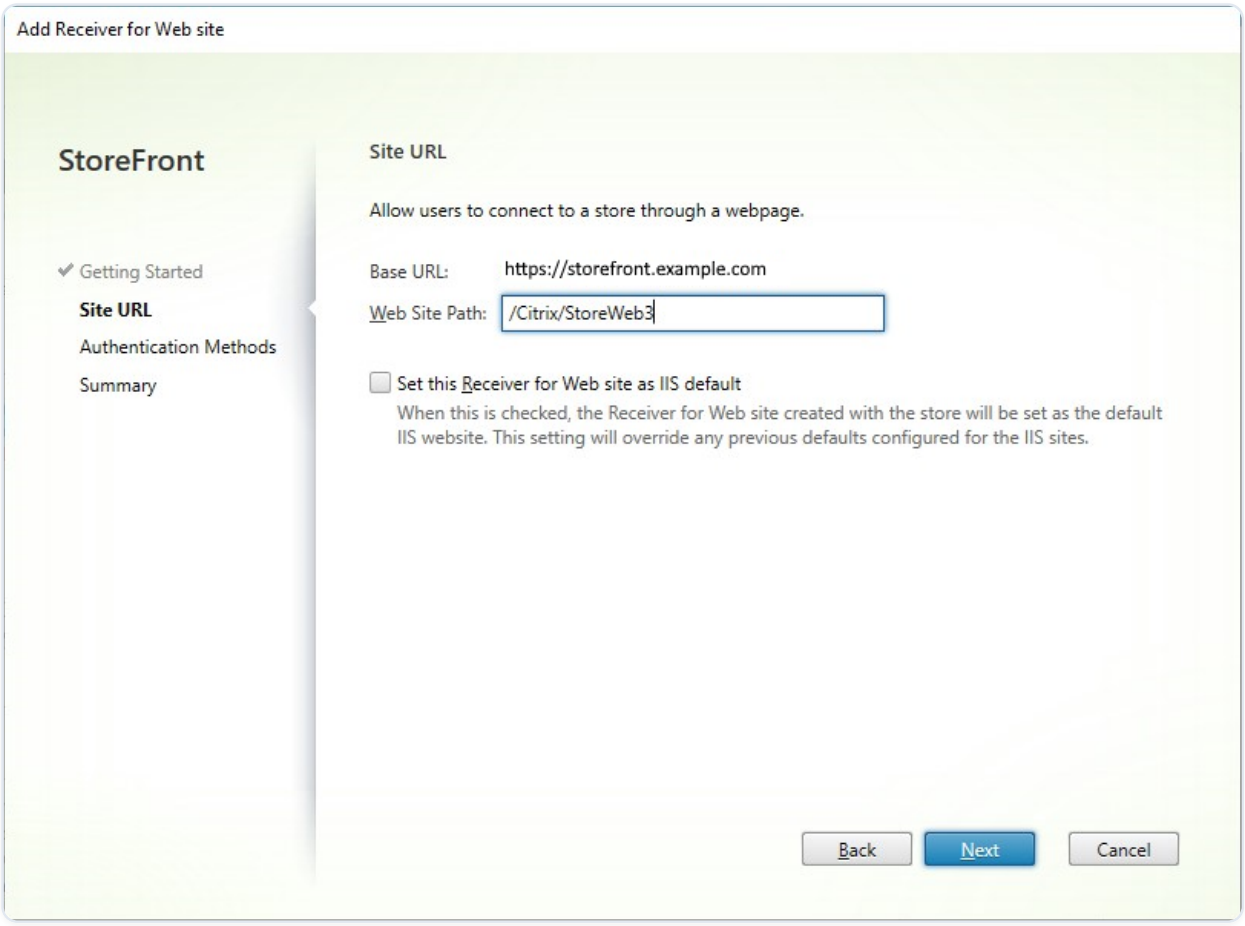
1. From the management console, select the store for which you want to create the website, and in the Actions pane, click **Manage Receiver for Web Sites**.
2. Click **Add** then click **Next**.

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



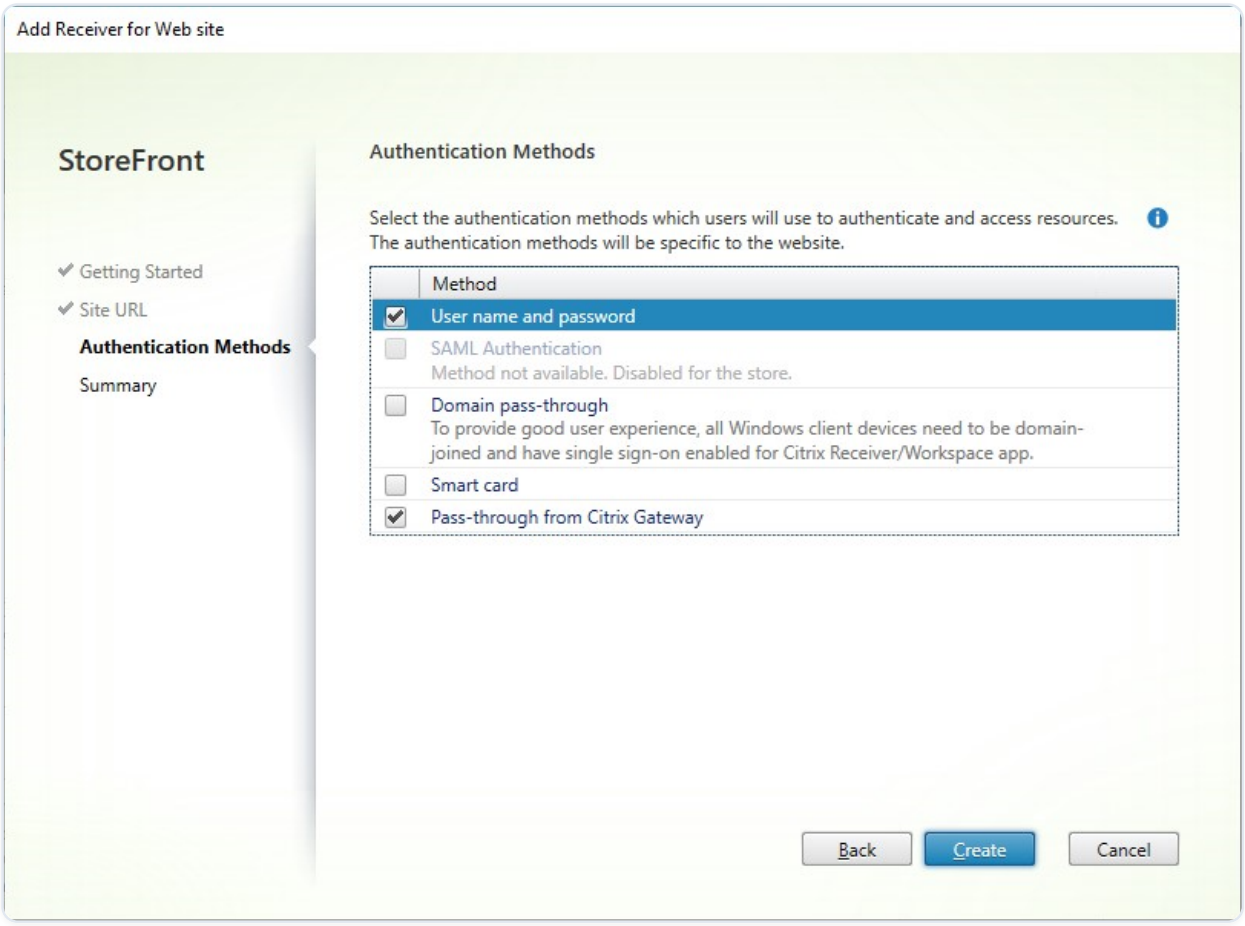
3. Type the desired **Web Site Path**, choose if you want to this to be the default website for the base URL and click **Next**.

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



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.

Create a website using the PowerShell SDK

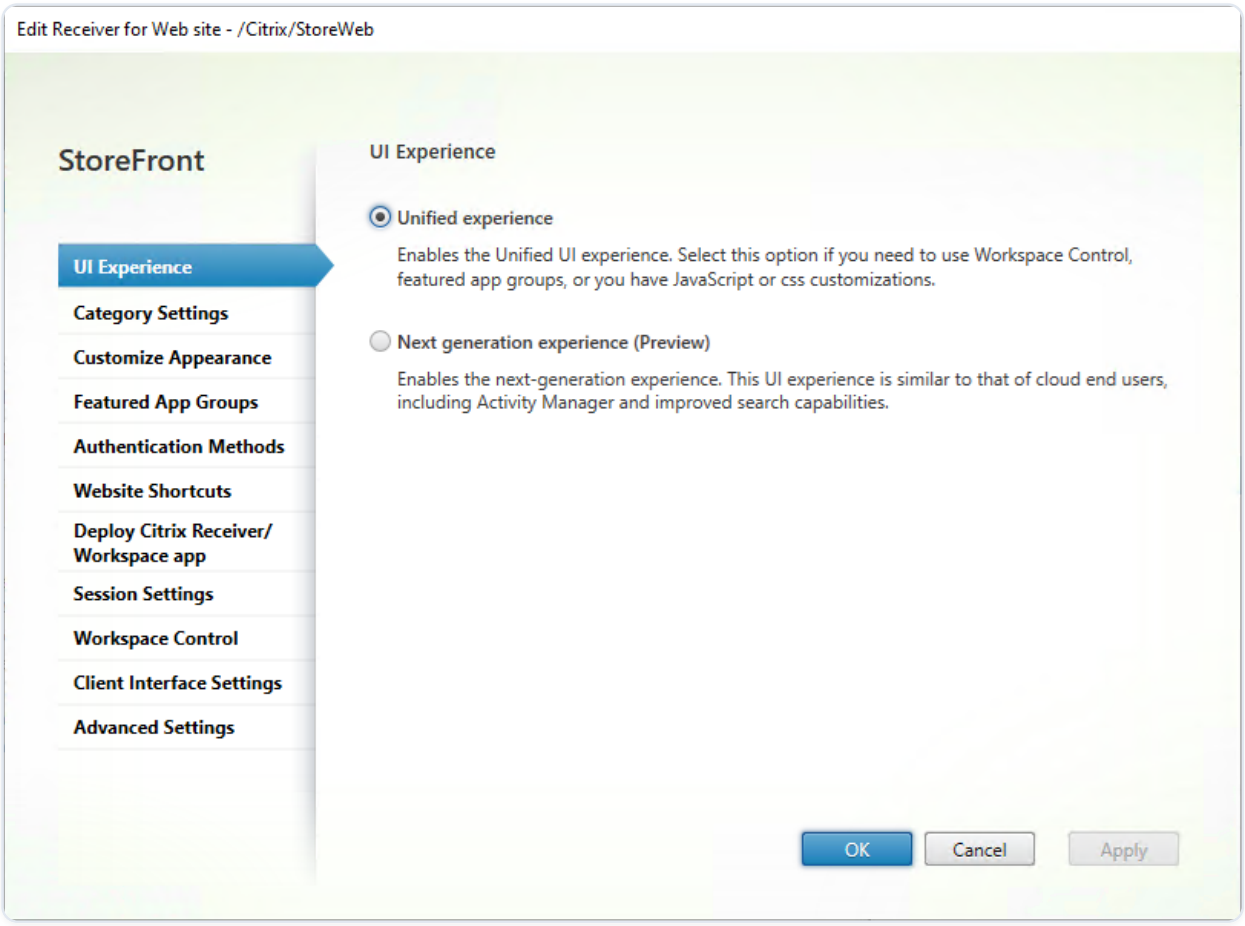
To create a website with the PowerShell SDK, call the Add-STFWebReceiverService cmdlet.

Configure website

To configure a website:

1. Select the **Stores** node in the left pane and in the **Actions** pane, click **Manage Receiver for Web**
2. Select a web site and press **Configure...**

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



3. Modify the settings on the appropriate tabs.

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

4. Once you have finished your changes, click **OK**.
5. To configure App Protection you must use PowerShell. Ensure you close StoreFront management console before running PowerShell commands.

© 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.

UI Experience

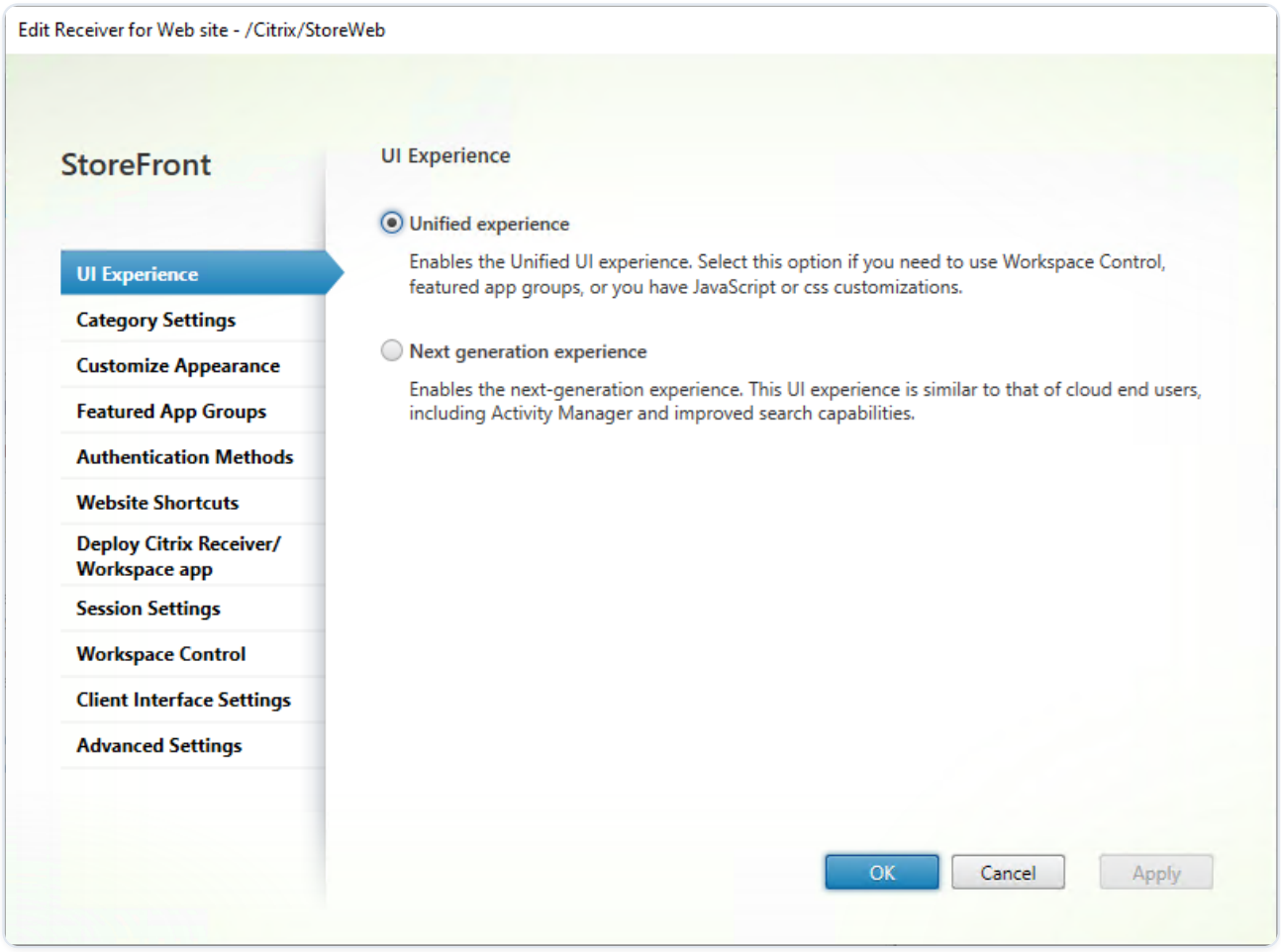
IMPORTANT:

When using versions of StoreFront 2402 earlier than CU2, the modern experience is available as a tech preview and should not be used in production. From CU2 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** (previously labelled **Unified experience**) - For more information, see User experience.
- **Modern experience** (previously labelled **Next generation experience**) - For more information, see Modern user experience.

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



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

PowerShell

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

For example:

```
(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`.

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

For example to use the modern experience:

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

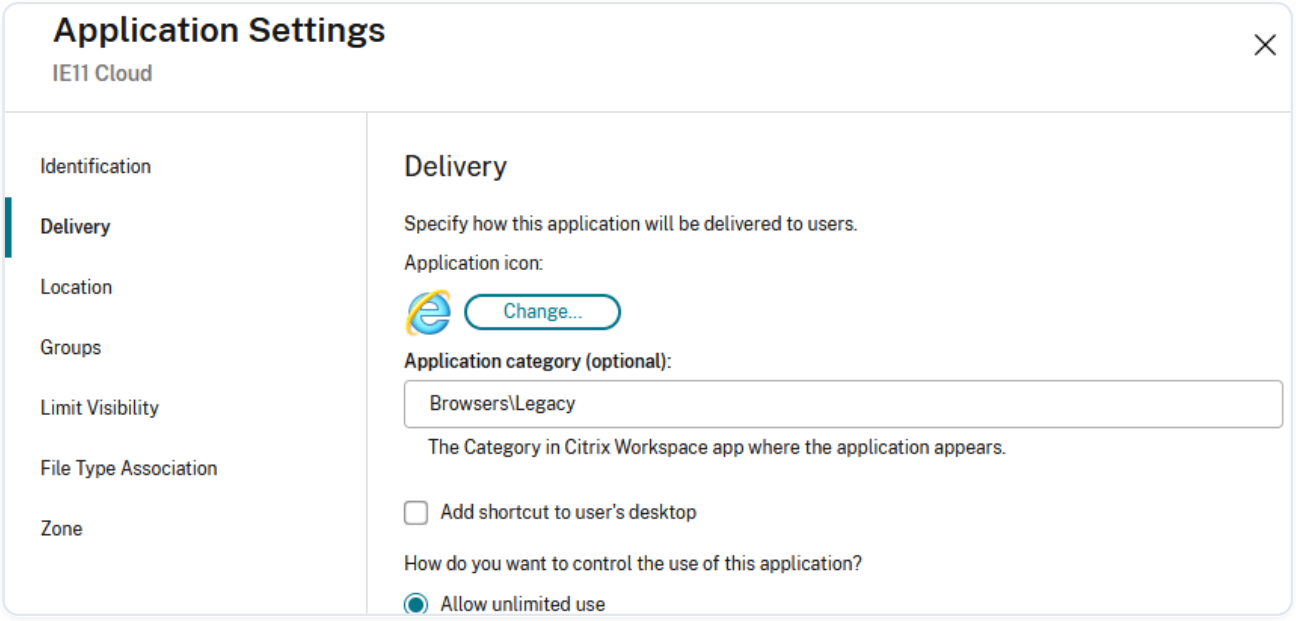
Set-STFWebReceiverService -WebReceiverService $rfw -WebUIExperience
Workspace
```

Category Settings

NOTE:

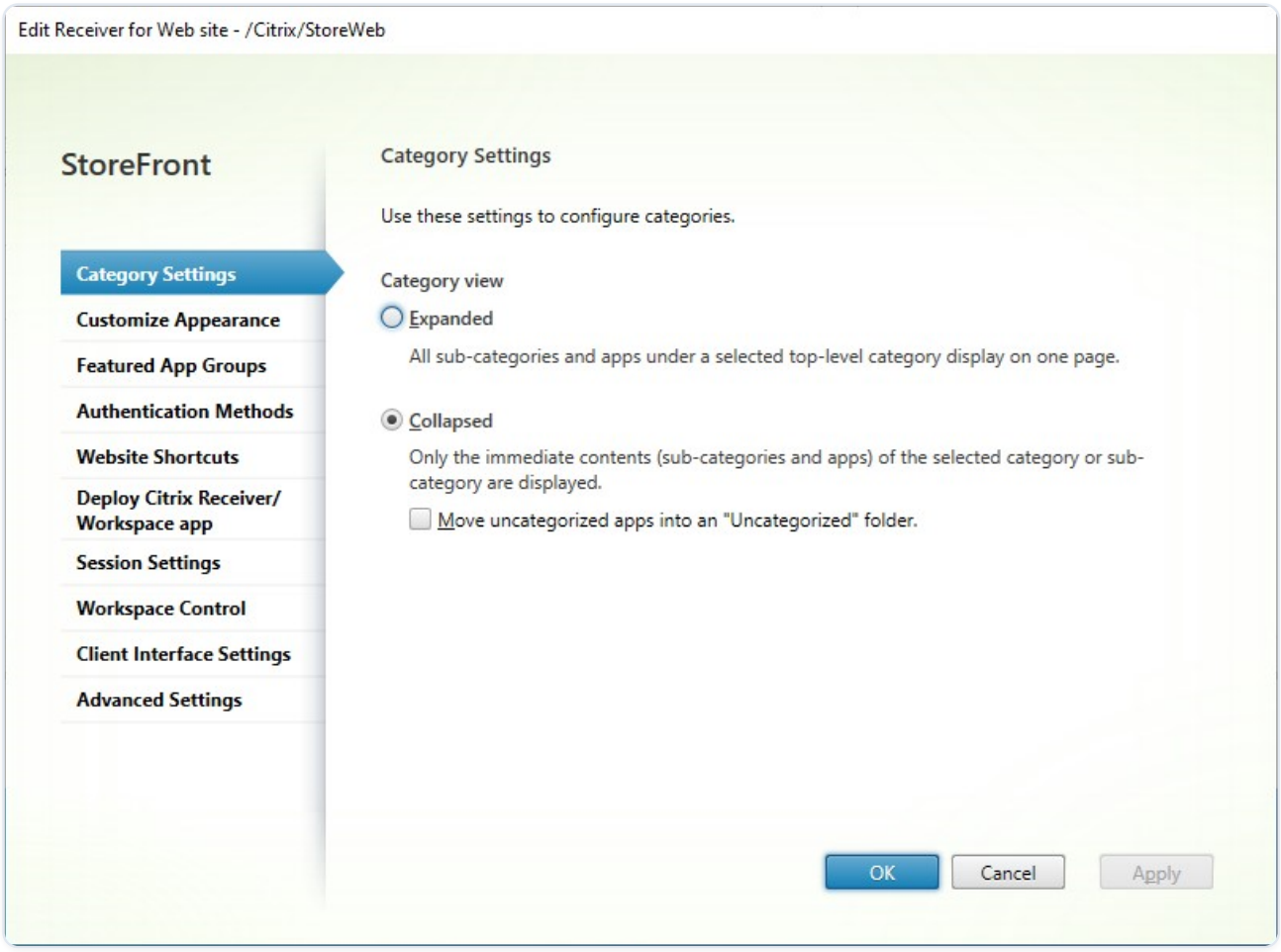
This functionality is only available using the classic experience.

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 Receiver for web site and select the **Category Settings** tab.

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

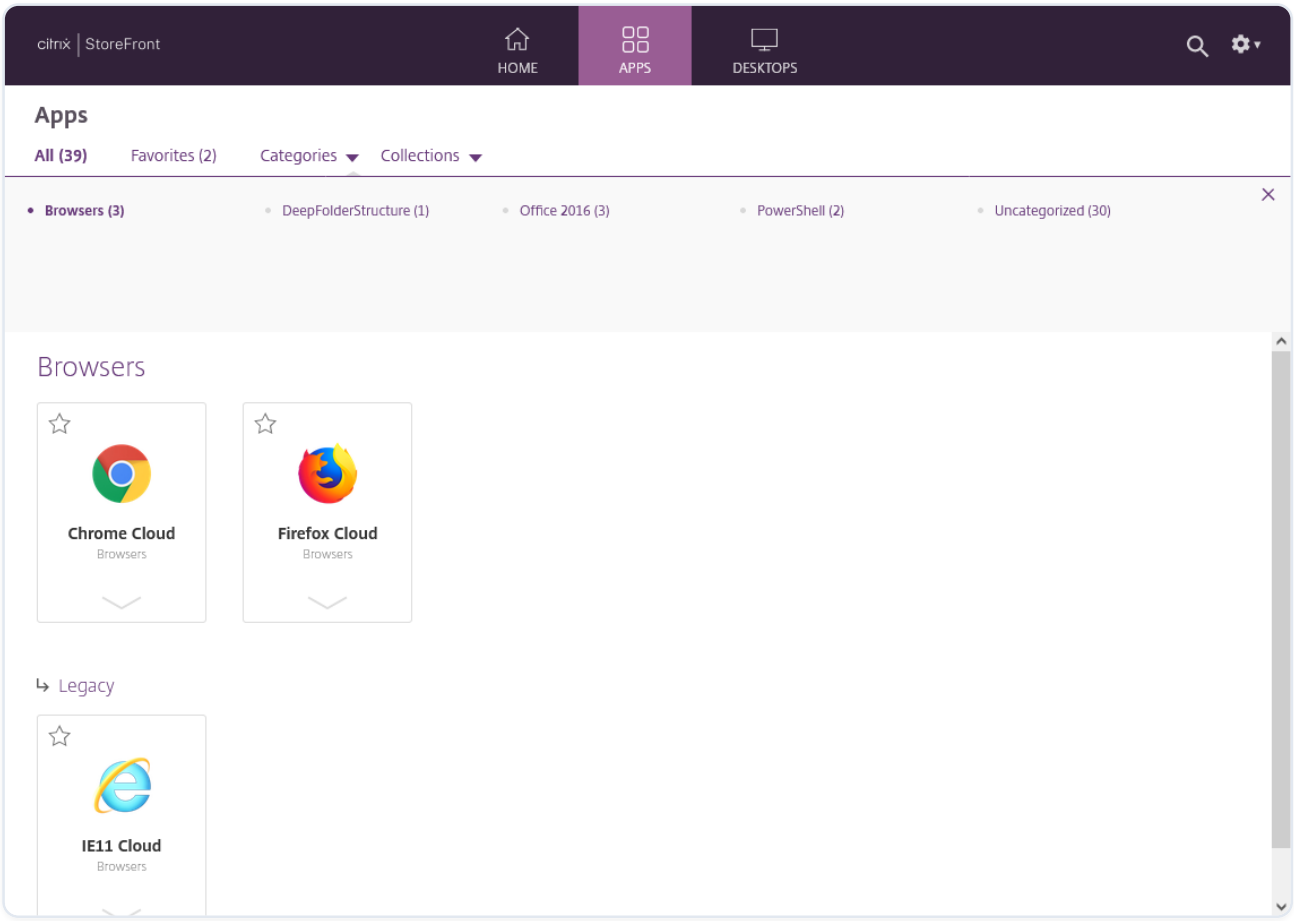


Category view

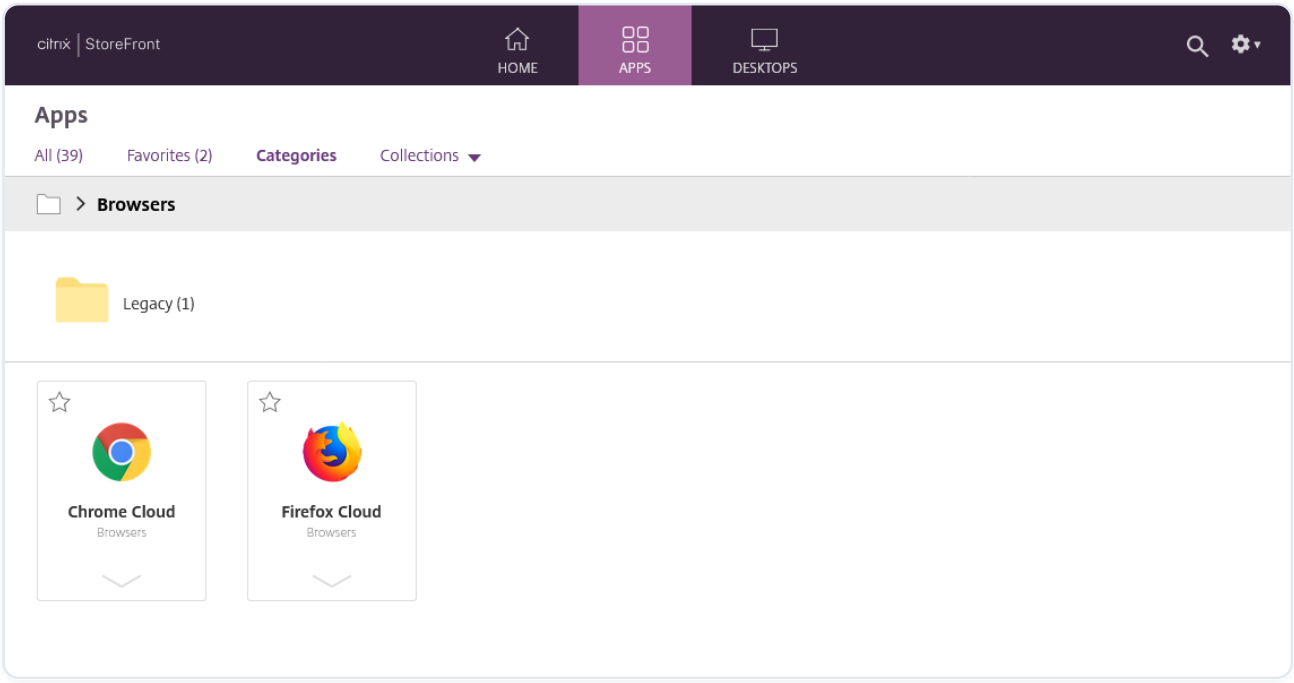
In the expanded view, StoreFront displays a list of top level categories. When the user clicks a top level category, StoreFront displays all apps in all subcategories on one page.

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.



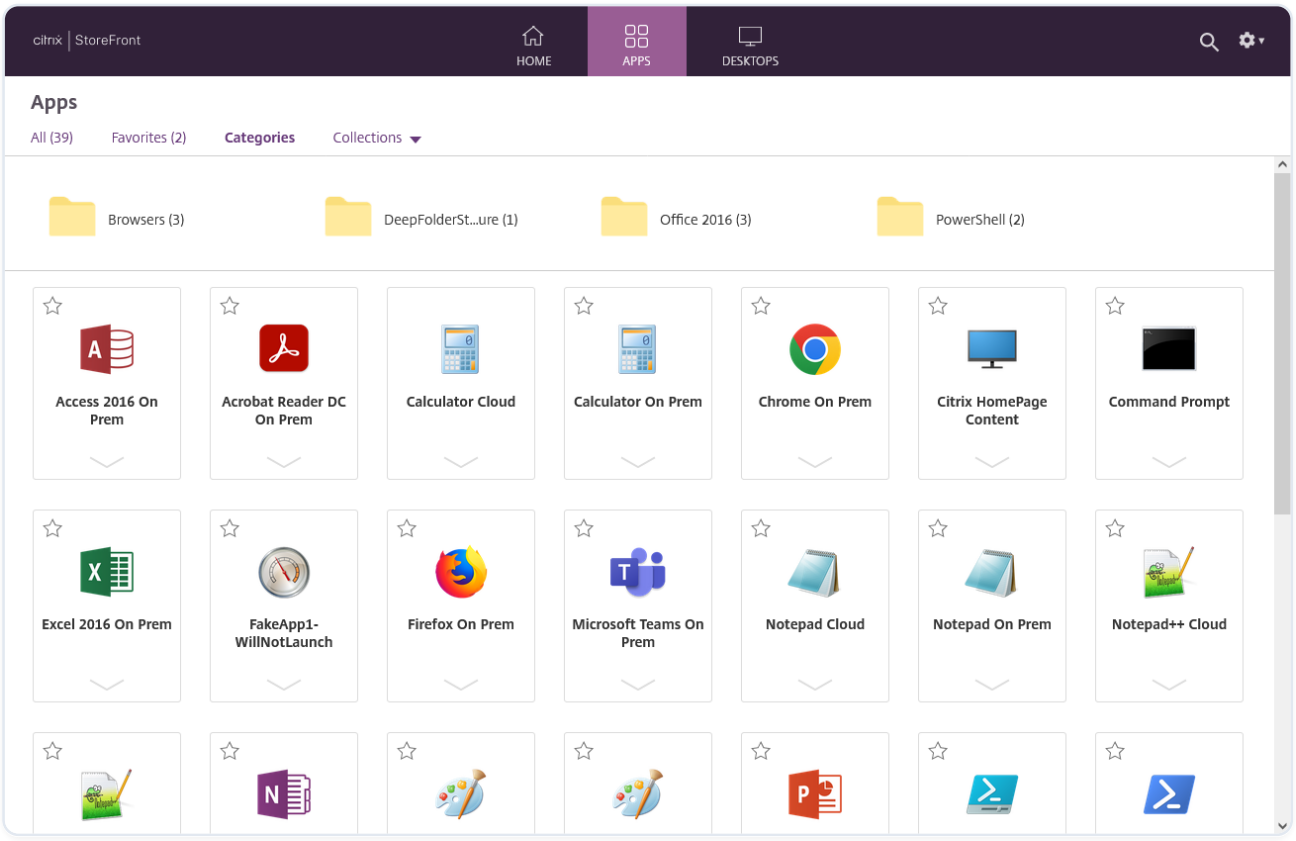
In the collapsed view, StoreFront initially displays a list of top level categories, and optionally all uncategorized apps. When the user clicks a category, StoreFront displays only the immediate contents (subcategories and apps) of the selected category. The user can click each subcategory to expand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



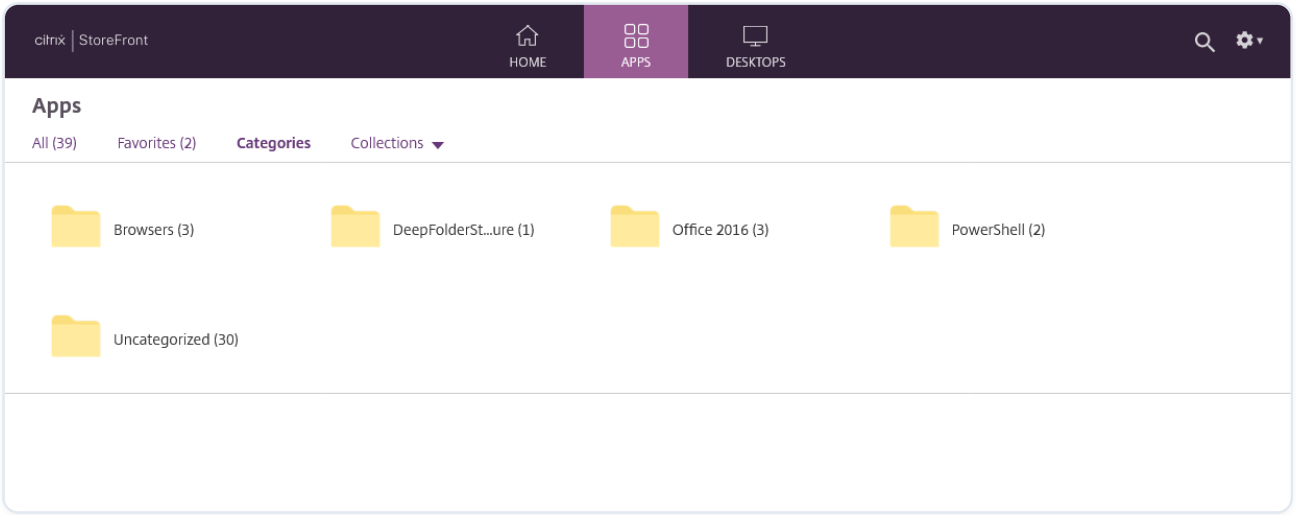
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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 using PowerShell SDK

To use the PowerShell SDK to enable or disable category view call cmdlet Set-STFWebReceiverUserInterface with parameter `EnableAppsFolderView`.

To use the PowerShell SDK to change the category view call cmdlet Set-STFWebReceiverUserInterface with parameter `CategoryViewCollapsed`.

Customize appearance

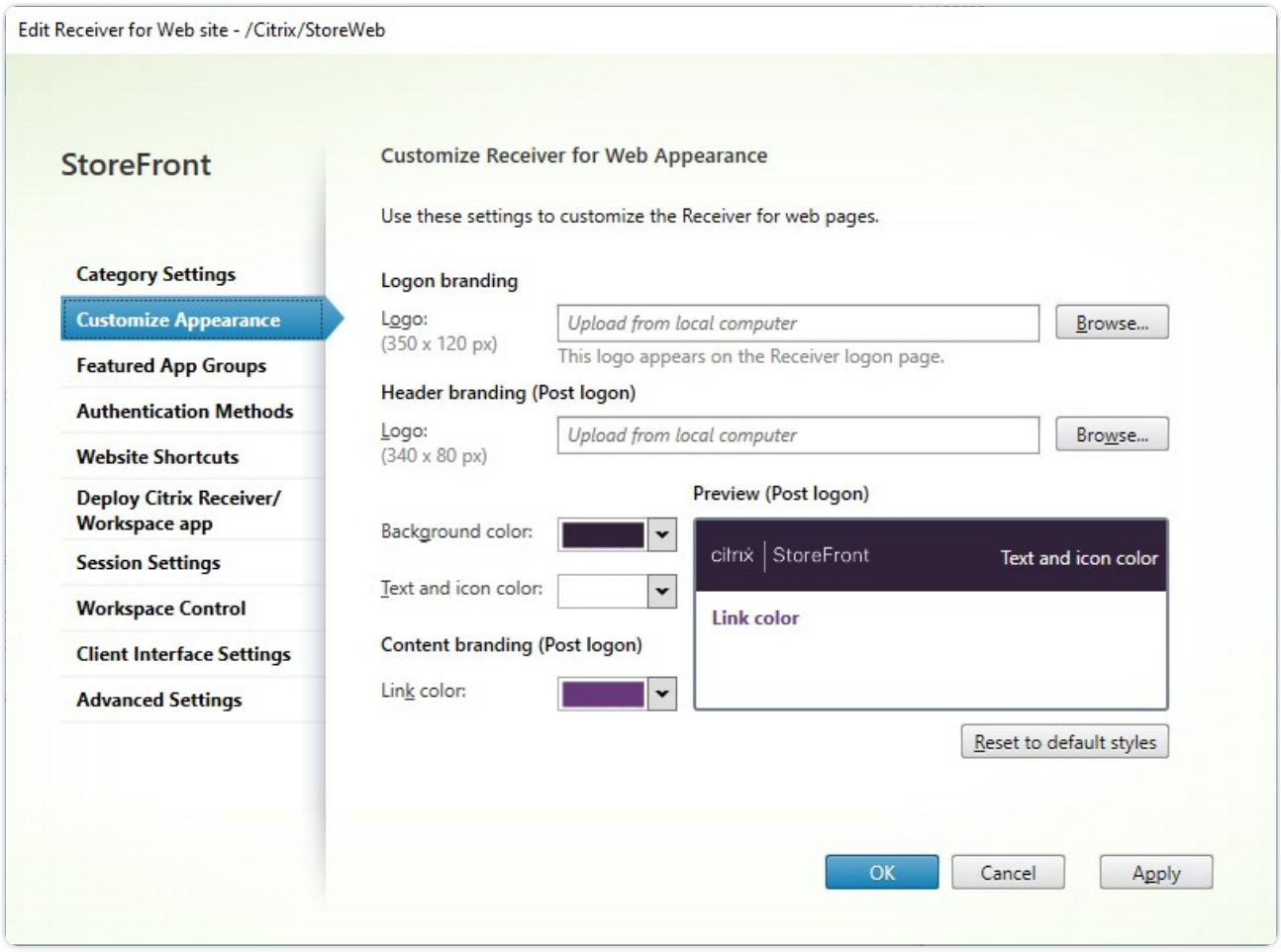
You can modify the logo and colors used within your store website.

Edit logo and colors

To customize the appearance, go to Edit Receiver for web site and select the **Customize Appearance** tab. You can modify the following:

- **Logon branding logo** - The logo displayed on the logon screen. It is not displayed when logging 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 text and icon color in the navigation section at the top of the page.
- **Link color** - The color used to highlight the currently selected item.

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



Edit logo and colors using PowerShell SDK

Using the PowerShell SDK, call cmdlet Set-STFWebReceiverSiteStyle.

Reset appearance to default

Press **Reset to default style** to return the logos and colors to the default.

Reset appearance to default using PowerShell SDK

Using the PowerShell SDK, call cmdlet Clear-STFWebReceiverSiteStyle.

Customization using Javascript and CSS

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

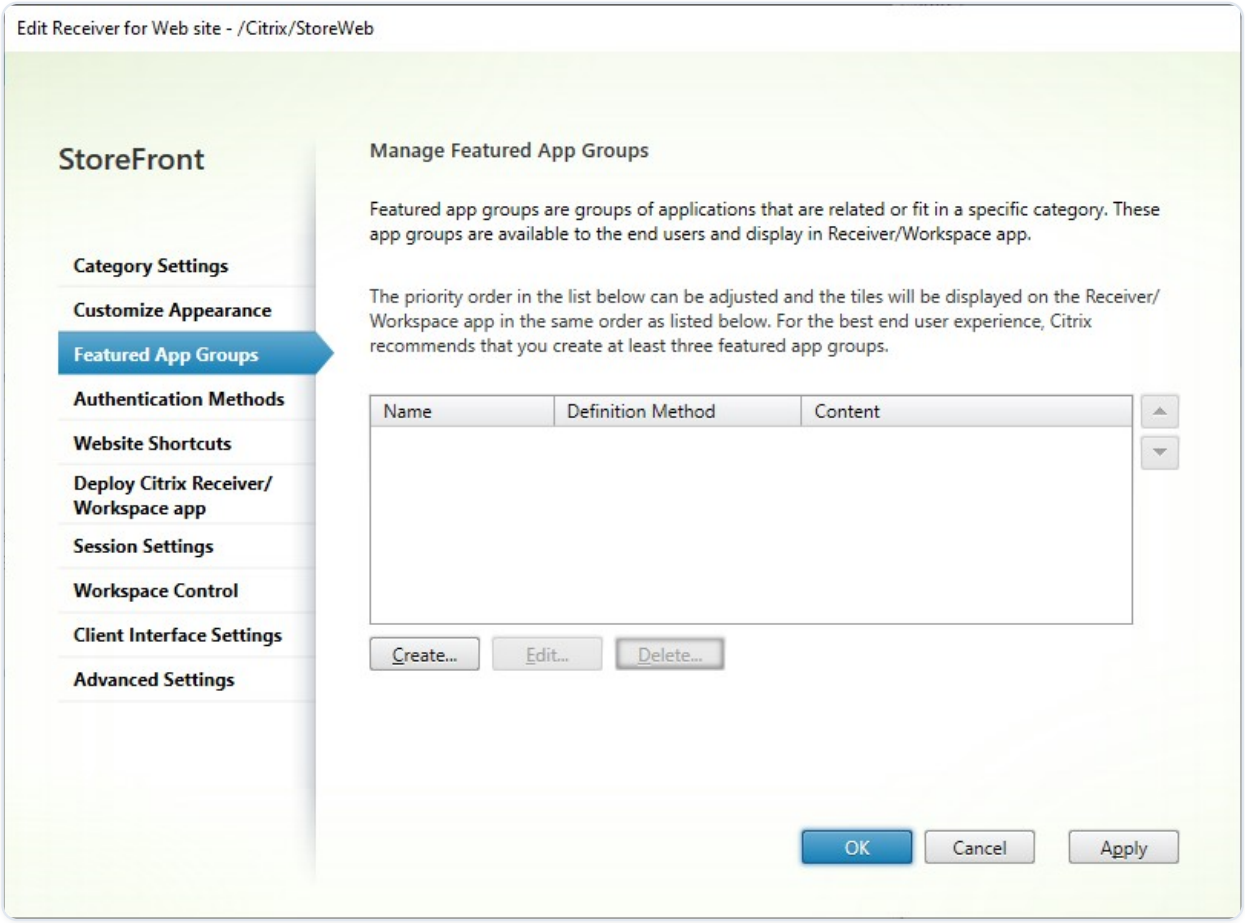
NOTE:

This functionality is only available using the classic 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 Receiver for web site screen, select the **Featured App Groups** tab.

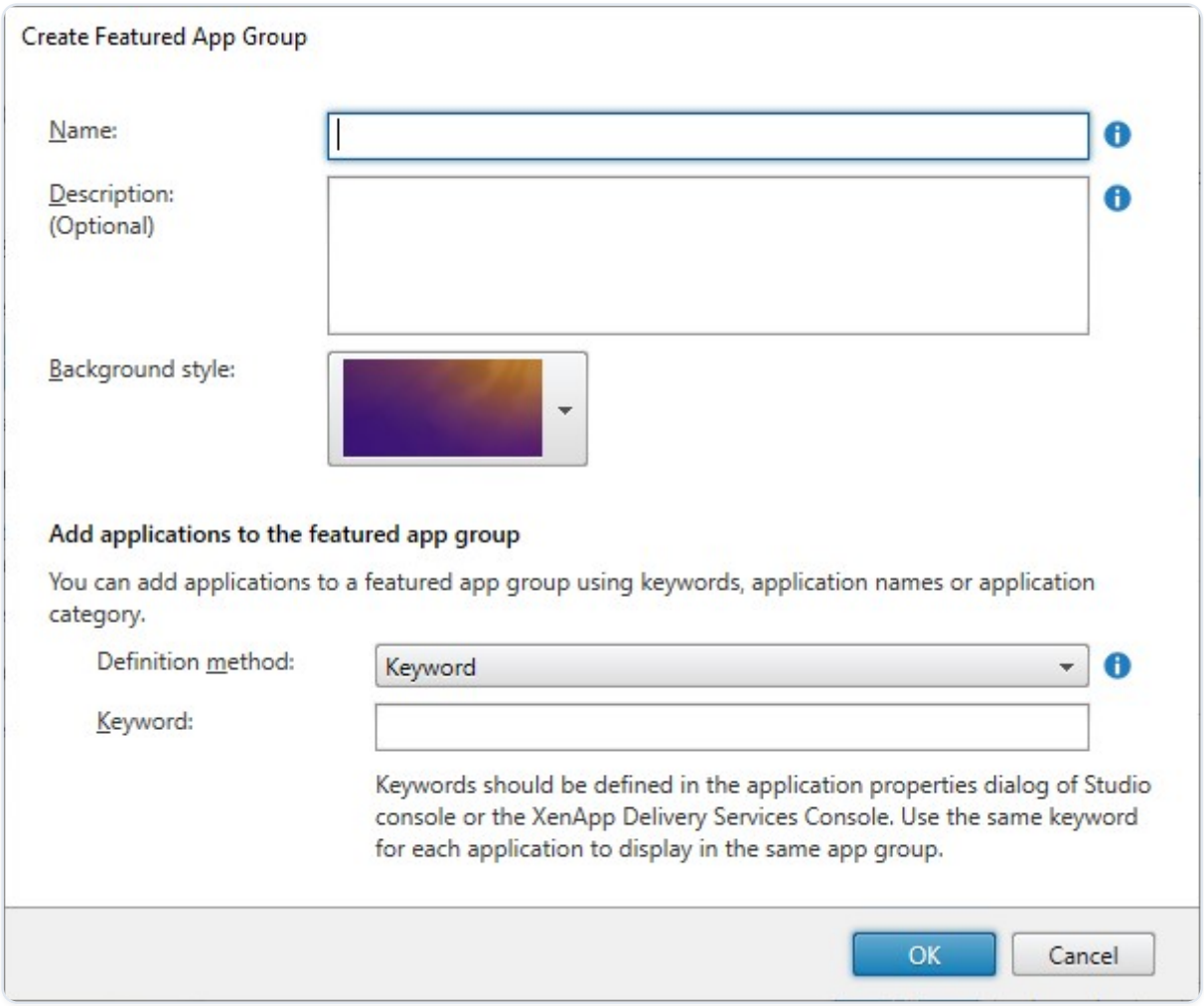


2. Click **Create** to define a new featured app group.
3. Specify a featured app group name, description (optional), background, and the method by which you define the featured app groups. You can choose keywords, application names, or application category.

© 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.



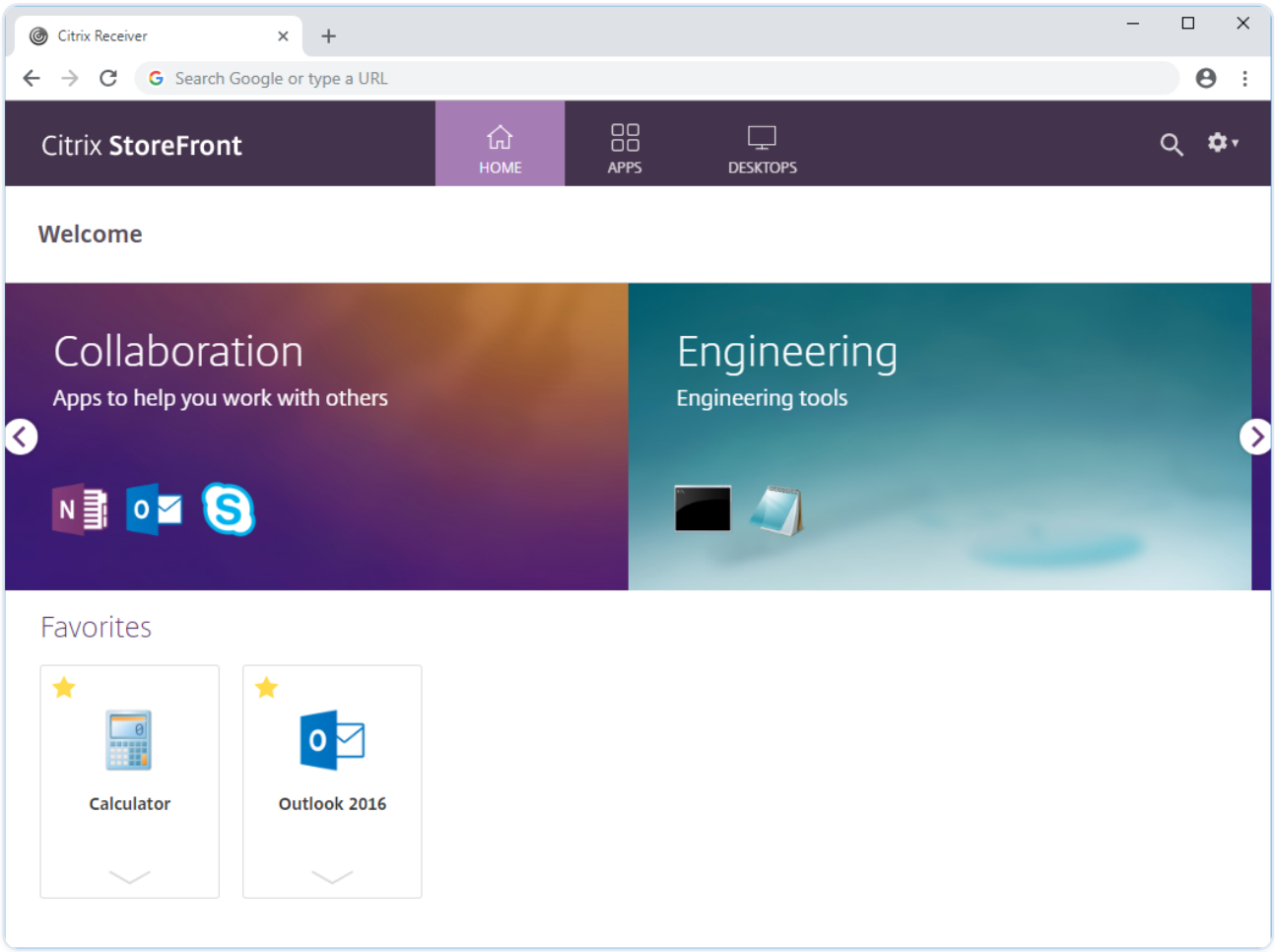
4. Click **OK**

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 the PowerShell SDK

To add a feature app group with the PowerShell SDK, use the cmdlet New-STFWebReceiverFeaturedAppGroup.

Edit featured app group

In the Edit Receiver for web site screen, select the **Featured App Groups** tab. Select the group that you want to edit and click **Edit...**

Edit featured app group using the PowerShell SDK

To modify a feature app group with the PowerShell SDK, use the cmdlet Set-STFWebReceiverFeaturedAppGroup.

Delete featured app group

In the Edit Receiver for web site screen, select the **Featured App Groups** tab. Select the group that you want to edit and click **Delete...**

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

Delete featured app group using the PowerShell SDK

Using the PowerShell SDK to delete a feature app group use the cmdlet Remove-STFWebReceiverFeaturedAppGroup and to delete all featured app groups use the cmdlet Clear-STFWebReceiverFeaturedAppGroup.

Authentication methods

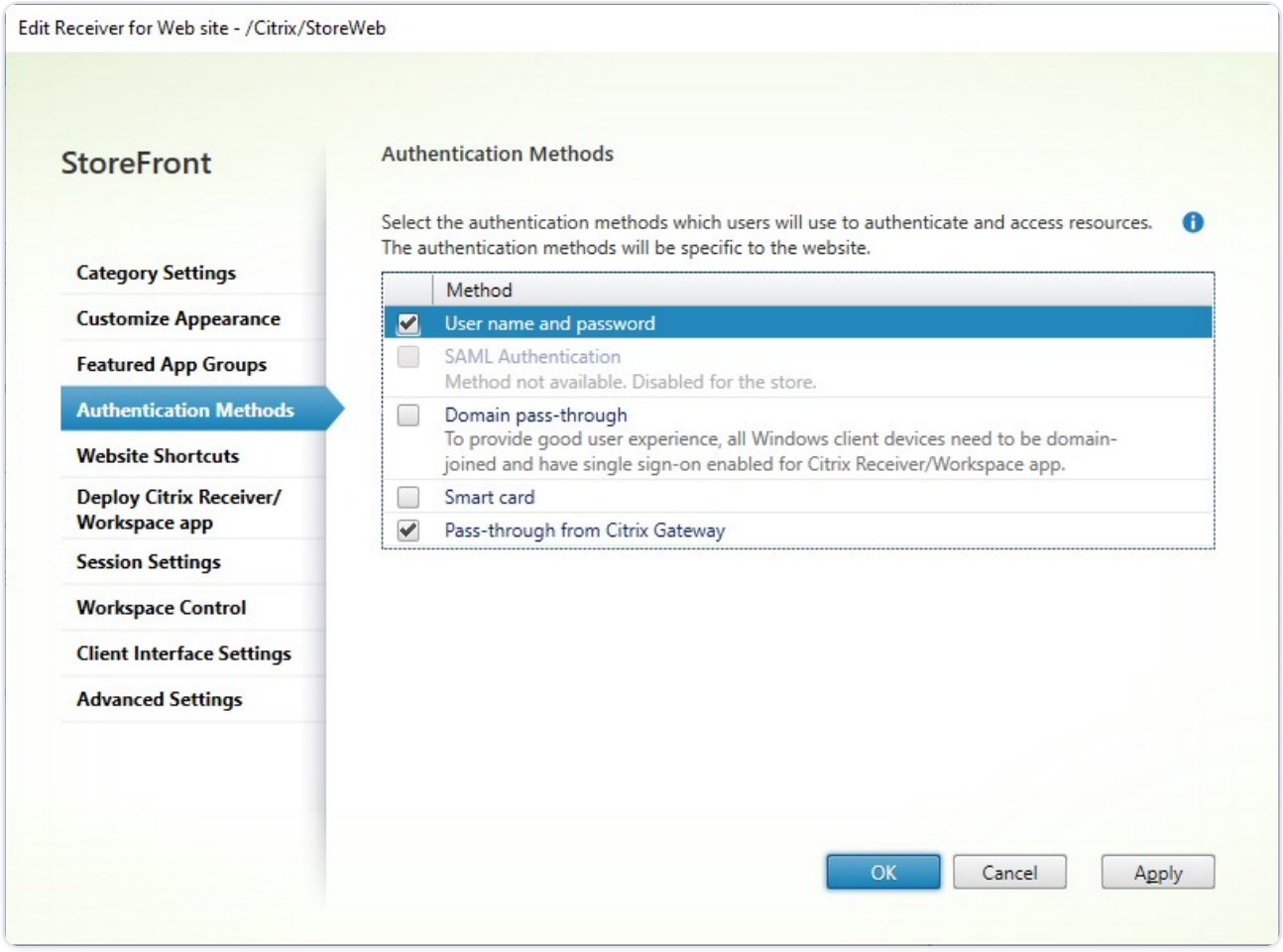
To configure the authentication methods available for a store, see Configure Authentication. You can override some of these settings for a particular website. These overrides only apply when users open the store in a web browser. Locally installed Citrix Workspace app uses the settings from the store 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 Receiver for web site and select the **Authentication Methods** tab.

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



- Select the **Username and password** check box to enable explicit authentication. See User name and password authentication. This option is only available if it's enabled for the store.
- Select the **SAML Authentication** check box to enable integration with a SAML Identity Provider. See SAML authentication. This option is only available if it's been enabled for the store.
- Select **Domain pass-through** to enable pass-through of Active Directory domain credentials from users' devices. See Domain pass-through authentication. This option is only available if it has been enabled for the store.
- Select **Smart card** to enable smart card authentication. See Smart card authentication.
- Select **Pass-through from Citrix Gateway** to enable pass-through authentication from Citrix Gateway. Enable this if users connect to StoreFront through a Citrix Gateway with authentication enabled. See Pass-through from Citrix Gateway.

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

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

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 SDK

To configure the available authentication methods using the PowerShell SDK, use the cmdlet Set-STFWebReceiverAuthenticationMethods.

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.

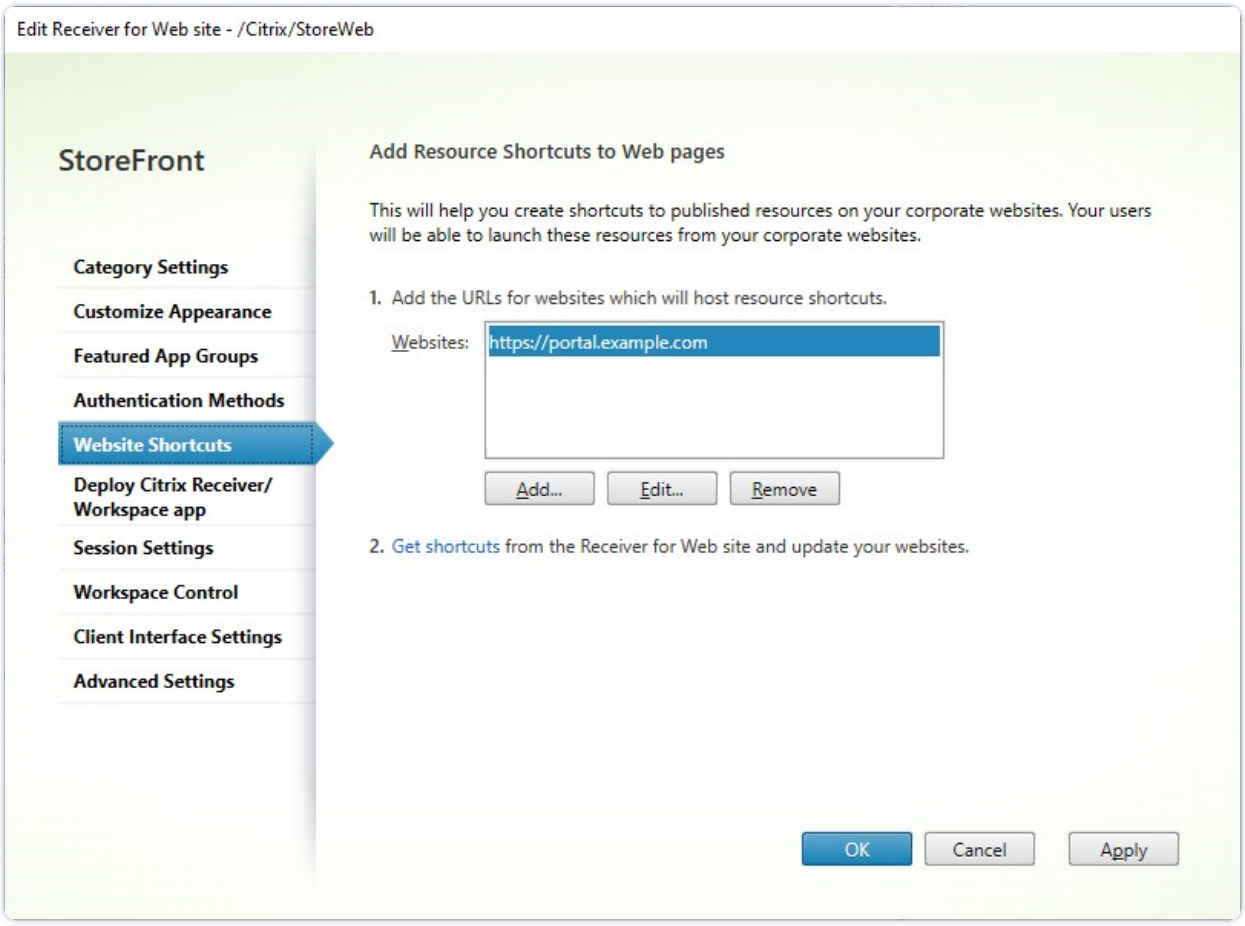
By default, StoreFront warns users if they attempt to launch resource shortcuts from untrusted websites, but users can still choose to launch the resource. To stop these warnings from appearing, on Advanced settings, clear prompt for untrusted shortcuts.

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

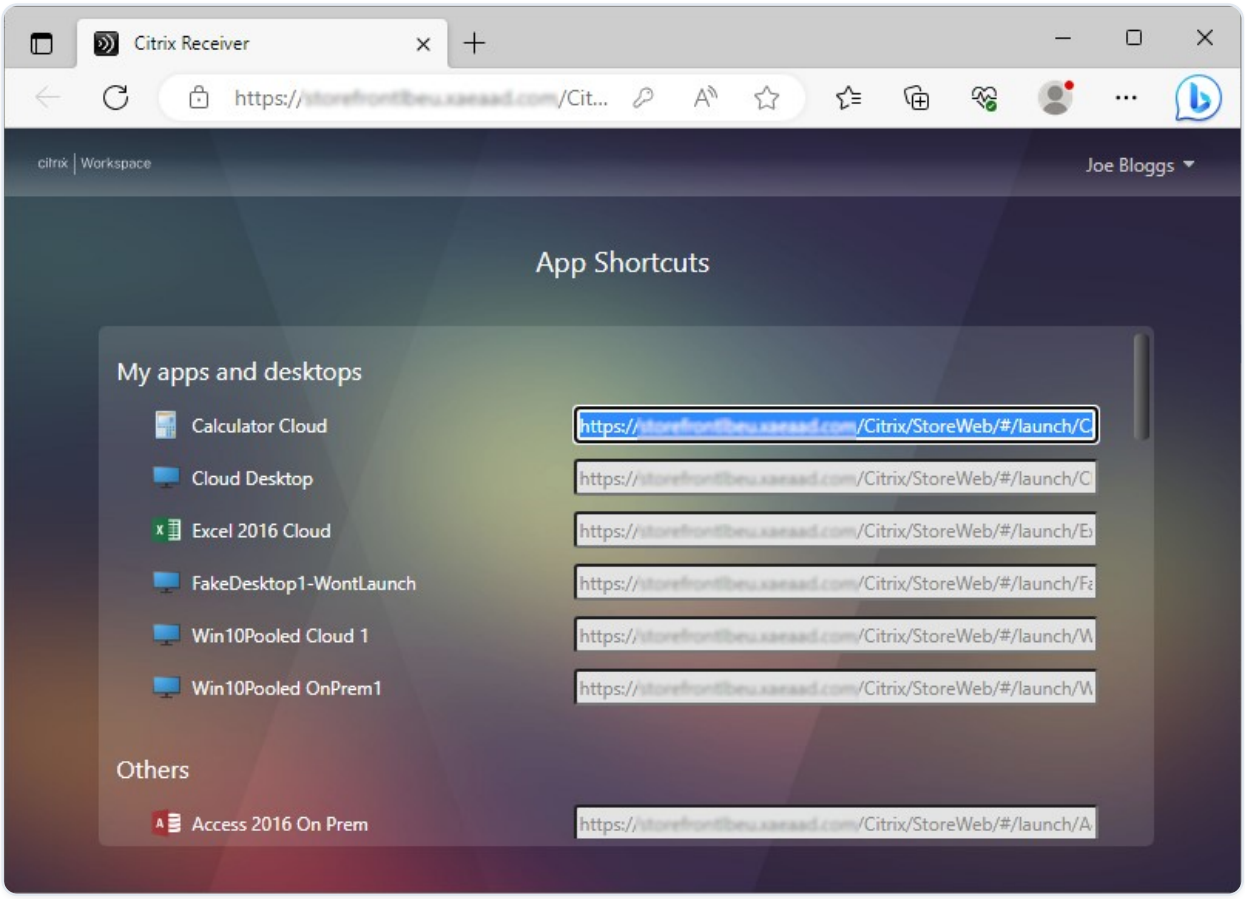
1. On the Edit Receiver for web site screen, select the **Website Shortcuts** tab.

© 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 SDK

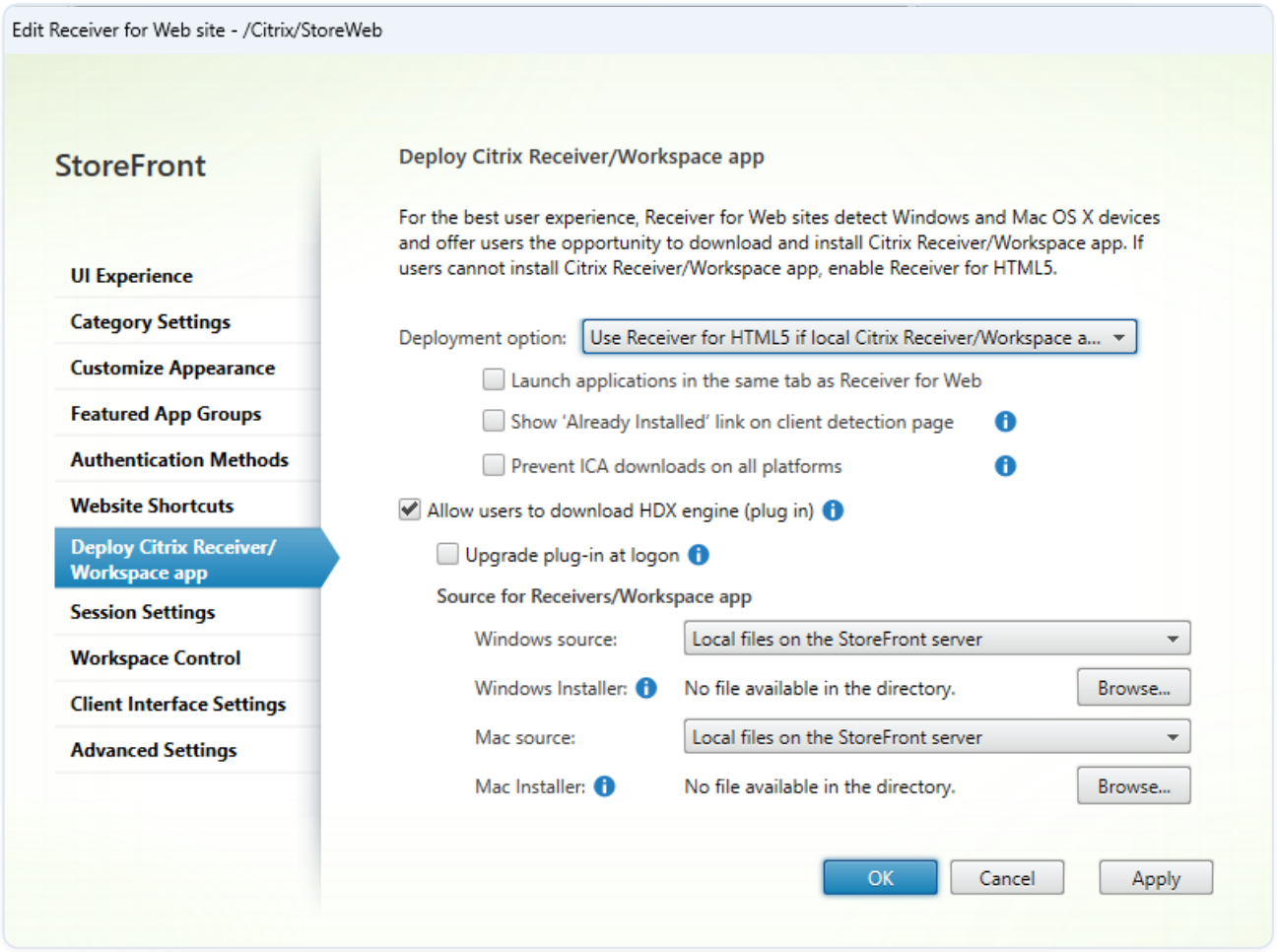
You can add trusted URLs using the Set-STFWebReceiverApplicationShortcuts PowerShell cmdlet.

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 Receiver for web site and select the **Deploy Citrix Receiver/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 is available via a plug-in when using either the classic experience or a Citrix Gateway. It is not available when using the modern experience without 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
- {{cwa-ios}} 24.9.0 or later

Configure on StoreFront using classic experience

You can install a plug-in on the StoreFront server to require the use of Citrix Workspace app.

1. Download the plug-in from Citrix Downloads.
2. Extract the zip file and citrix-ui-plugin.tar.gz to any directory on the StoreFront server. It contains PowerShell files, Javascript files, and config files.
3. Open the plugin.config file in a text editor. Configure as follows:

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

   If you want to disable the native app mandate feature keep the key-value pair as follows:
   `<param name="requireNativeAppUse" value="false" />`
4. Open PowerShell as an administrator.
5. Navigate to the extracted folder.
6. Run `./CitrixPluginInstaller.ps1 -VirtualPath /Citrix/<store web name>`.
7. Repeat for each server in the StoreFront server group.
8. Validate that it has installed correctly by opening a web browser and navigating to the store website.

Configure using a Citrix Gateway

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

Deployment option

- Select **Always use Receiver for HTML5** if you want the user to always to access resources through a web browser without prompting the user to download and install Citrix Workspace app locally. With this option selected, Workspace for HTML5 users always access resources directly through their browsers.
- Select **Use Receiver for HTML5 if local Receiver is unavailable** if you want the store web site to prompt the user to download and install Citrix Workspace app locally, but fall back to accessing resources through a browser if Citrix Workspace app cannot be installed. Users

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

without Citrix Workspace app are prompted to download and install it every time they log on to the site.

- Select **Install locally** if you want the site always to access resources through a locally installed Citrix Workspace app. Users are prompted to download and install the appropriate Citrix Workspace app for their platform. Users can continue to access the store through a web browser but when the launch a resource it opens in the locally installed Workspace app.

Launch applications in the same tab

If you have chosen **Always use Receiver for HTML5** or **Use Receiver for HTML5 if local Receiver is unavailable**, by default, resources launched in the browser open a new browser tab. If you want your resources to open in the same tab, replacing Workspace app for HTML5, select **Launch applications in the same tab as Receiver for Web**. This setting only applies to the classic experience.

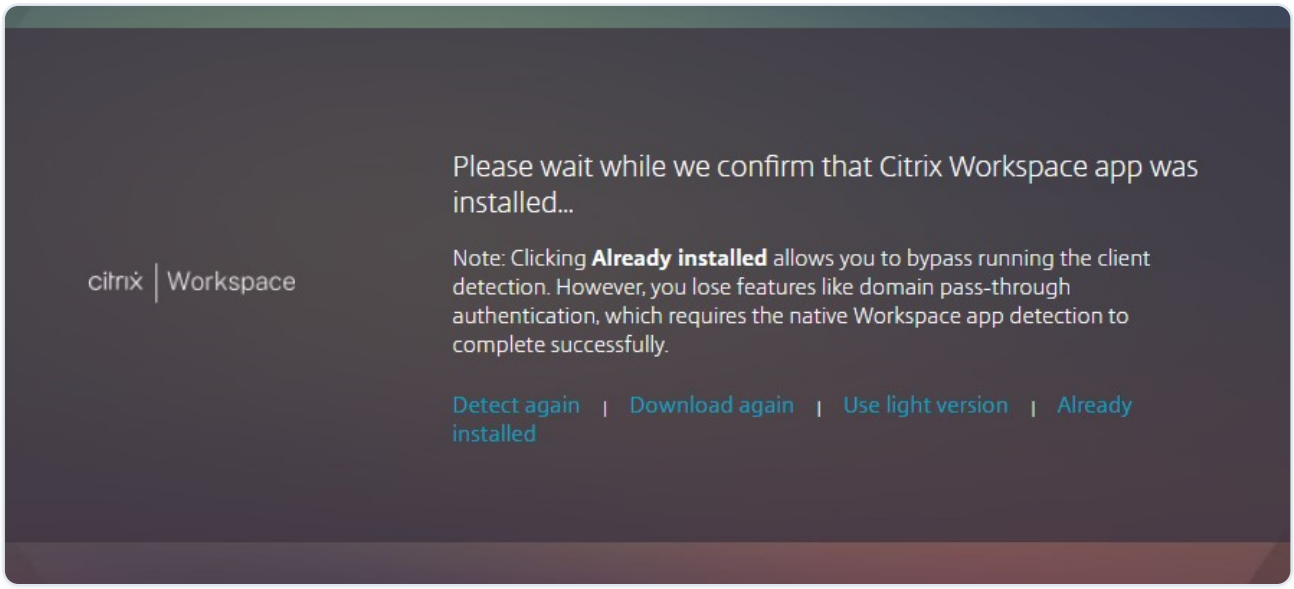
Show the 'Already installed' link on the client detection page

NOTE:

This setting is applicable only for Windows, MacOS, and Linux devices. If a user has installed Workspace web extensions, then the client detection and launch is handled by the web extensions. In such cases, this setting is not applicable.

When end users open a store in their browser for the first time on Windows, macOS, or Linux, the website attempts to detect the locally installed app using the Citrix Workspace launcher. Subsequently, when a user launches a resource, the Citrix Workspace launcher communicates with the locally installed Citrix Workspace app. If users click the **Already installed** option, the client detection process is skipped. As a result, when the user launches a resource, an `.ica` file is downloaded that users can open with their locally installed Citrix Workspace app. This does not support features such as domain pass-through and app protection.

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



This downloaded `.ica` file may pose a security risk. Citrix recommends that you clear the **Show 'Already installed' link on the client detection page** checkbox to hide the **Already installed** option.

IMPORTANT:

Hiding the **Already installed** option has no impact on users who have previously selected **Already installed**. These users continue to download ICA files, unless this is blocked. To reset Citrix Workspace app detection for those users, add the following script to `custom/script.js` in the website directory:

```
CTXS.Extensions.preInitialize = function() {

   if(CTXS.getCookie("CtxsClientDetectionDone")=="true" &&
CTXS.getCookie("CtxsUserPreferredClient")=="Native" &&
CTXS.getCookie("CtxsClientVersion")==null)

   {

       CTXS.removeCookie("CtxsClientDetectionDone");

       CTXS.removeCookie("CtxsUserPreferredClient");

   }

   callback();
```

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

```
};
```

Prevent Ica downloads on all platforms

This provides an additional level of protection by completely blocking `.ica` downloads across all platforms. As Citrix Workspace launcher is not available on iOS, Android or Chrome, users must either select **Use Light version** if available, or they must add their store to their locally installed Citrix Workspace app.

IMPORTANT:

This option should not be used in conjunction with the **Show Already installed** option on the client detection page.

Allow users to download Citrix Workspace app

If you select **Allow users to download HDX™ engine (plug in)**, the first time a user logs on to a device on Windows or Mac, they are given the option to download the app.

This is not available if you have chosen **Deployment option** of **Always use Receiver for HTML5**.

Upgrade Workspace app on logon

If you select **Upgrade plug-in at logon**, Workspace app for HTML5 offers users a choice to upgrade the Citrix Workspace app locally installed client when they log on. Users may choose to skip the upgrade and will not be prompted to upgrade again unless their browser cookies are cleared. To enable this feature, ensure the Citrix Workspace app files are available on the StoreFront server.

Download source

When end users click the download button you can choose whether they are redirected to the Citrix website or to download files directly from the server. You can choose **Citrix website**, **Local files on the StoreFront server** or **Files on remote server (through URL)**.

PowerShell SDK

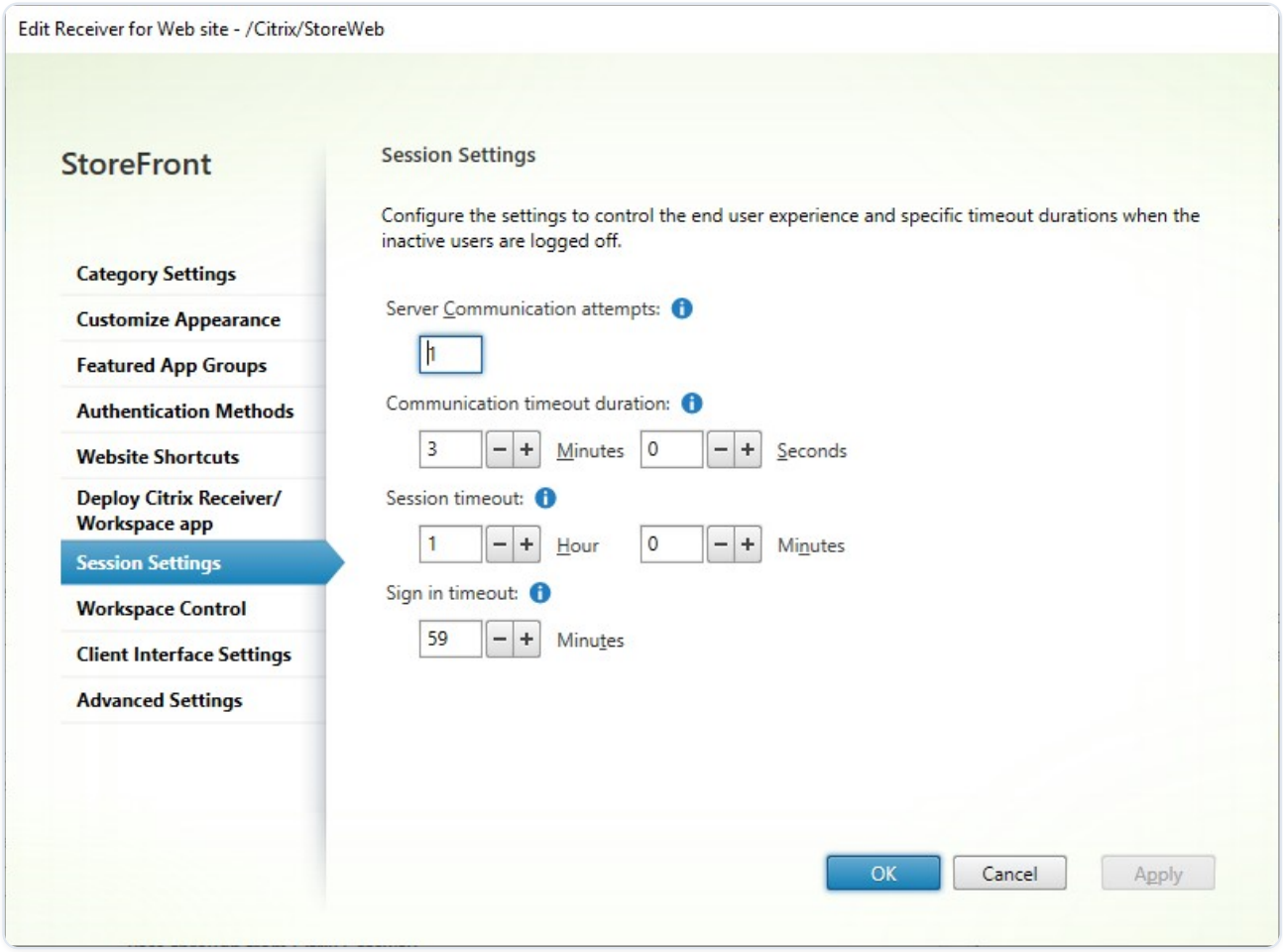
To configure these settings using the PowerShell SDK, use cmdlet Set-STFWebReceiverPluginAssistant.

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

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

Configure session settings

To modify session settings, go to the Edit Receiver for web site screen, select the **Session Settings** tab.



Server communication attempts

The number of attempts for calls between the web proxy and store services, internal to StoreFront. Normally there is no need to modify this setting.

Communication timeout duration

The amount of time allowed for calls between the web proxy and store services, internal to StoreFront. Normally there is no need to modify this setting.

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

Session inactivity timeout

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

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

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

PowerShell

```
$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
```

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

```
$rfweb

$rfauth.TokenLifeTime.ToString()
```

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

```
$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 the same value as the StoreFront **Session timeout**. The StoreFront timeout notifies the gateway to log out slightly before 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.

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

Maximum token lifetime of Authentication Service

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

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

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

To view the maximum token lifetime run the following PowerShell:

```
$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
```

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

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`.

Workspace control

NOTE:

This functionality is only available using the classic experience.

As users move between devices, workspace control ensures that the applications they are using follow them. Users can keep working with the same application instances across multiple devices rather than having to restart all their applications each time they log on to a new device. This enables, for example, clinicians in hospitals to save time as they move from workstation to workstation accessing patient data.

When users log on, they are automatically reconnected to any applications that they left running. For example, consider a user logging on to a store, and starting some applications. If the user then logs on to the same store using the same access method but on a different device, the running applications are automatically transferred to the new device. All the applications that the user starts from a particular store are automatically disconnected, but not shut down, when the user logs off from that store. In the case of accessing a store through a web browser, the same browser must be used to log on, start the applications, and log off.

Configure Workspace Control in a web browser

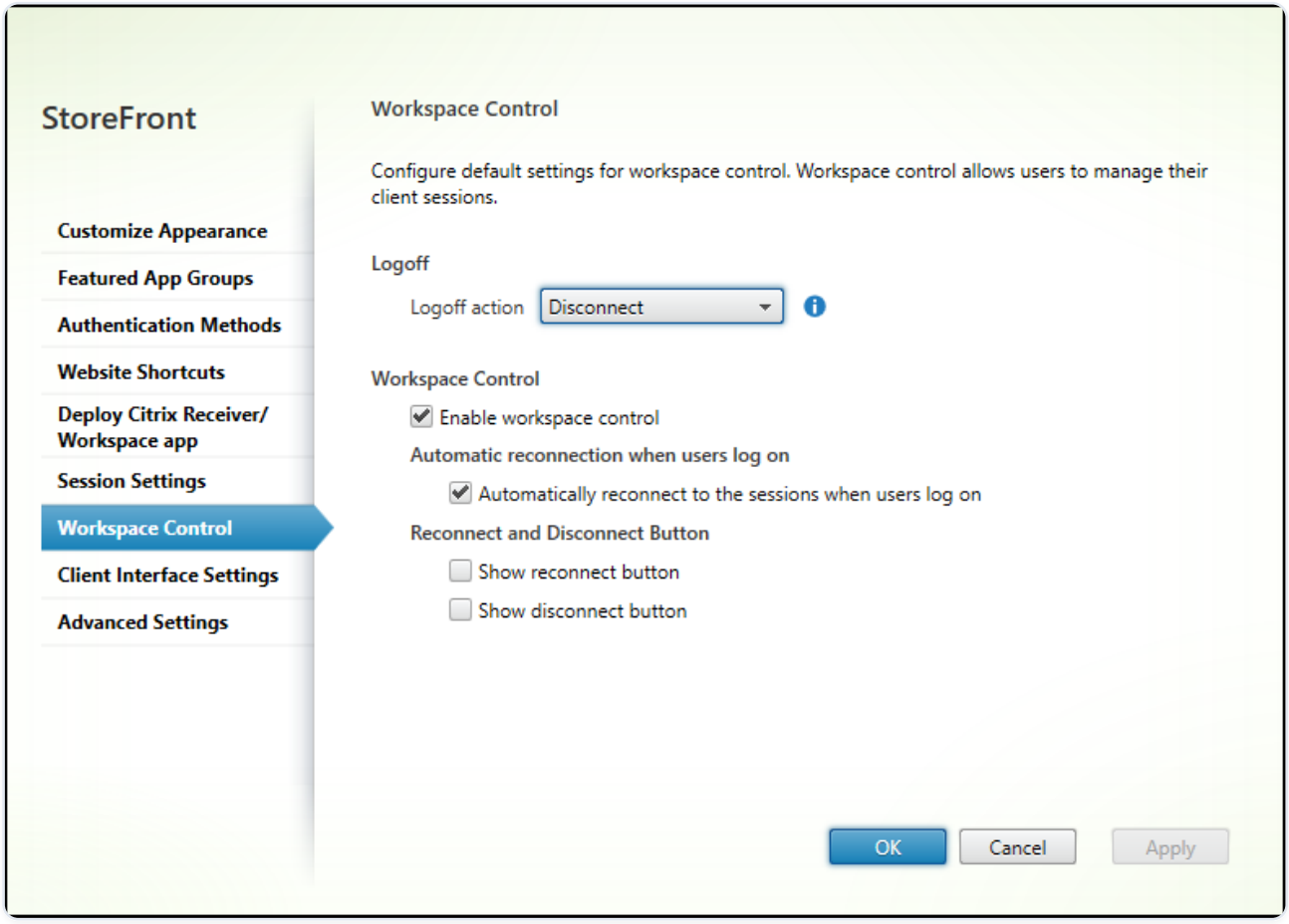
The workspace control settings within StoreFront management console only apply when accessing the store through a web browser. This is subject to the following requirements and restrictions:

- Workspace control is not available when the web browser is running within a hosted desktops or application.
- For users accessing websites from Windows devices, workspace control is only enabled if the site can detect that Citrix Workspace app for Windows is installed on users' devices or if 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.

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

- If there is only one desktop available for a user on a website that is configured to start single desktops automatically when the user logs on, that user's applications are not reconnected, regardless of the workspace control configuration.
- Users must disconnect from their applications using the same browser that was originally used to start them. Resources started using a different browser, or started locally from the desktop or Start menu using Citrix Workspace™ app, cannot be disconnected or shut down from the web client.
- Workspace control is not available when resources open within the same browser tab. To configure this, see Citrix Workspace app deployment.

To modify workspace control settings when a store is accessed through a web browser, select **Workspace Control** on the Edit Receiver for web site screen.

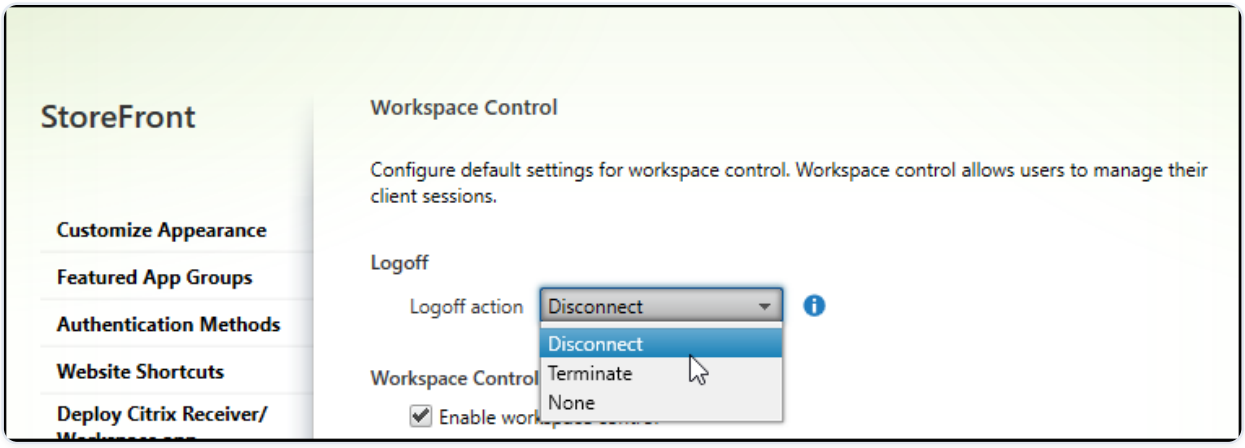


Configure settings for workspace control as follows:

- Specify the **Logoff action**. The log off actions are as follows:
  - **Disconnect**: When you log off from the site, the app and desktop sessions are automatically disconnected from the client device.

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

- **Terminate**: When you log off the site, app and desktop sessions are automatically terminated on the server.
- **None**: When you log off from the site, app and desktop sessions remain running.



- Select the **Enable workspace control** check box.
- Select the **Automatically reconnect to the sessions when users logon** check box under **Automatic reconnections when users logon**.

Configure Workspace Control using PowerShell SDK

You can configure workspace control using the PowerShell cmdlet Set-STFWebReceiverUserInterface.

Configure Workspace Control on Workspace app for Windows

To configure Workspace Control on Workspace for Windows, see Manage workspace control reconnect.

Configure Workspace Control on Workspace app for Mac

To configure Workspace control Workspace app for Mac, see Configure workspace control settings.

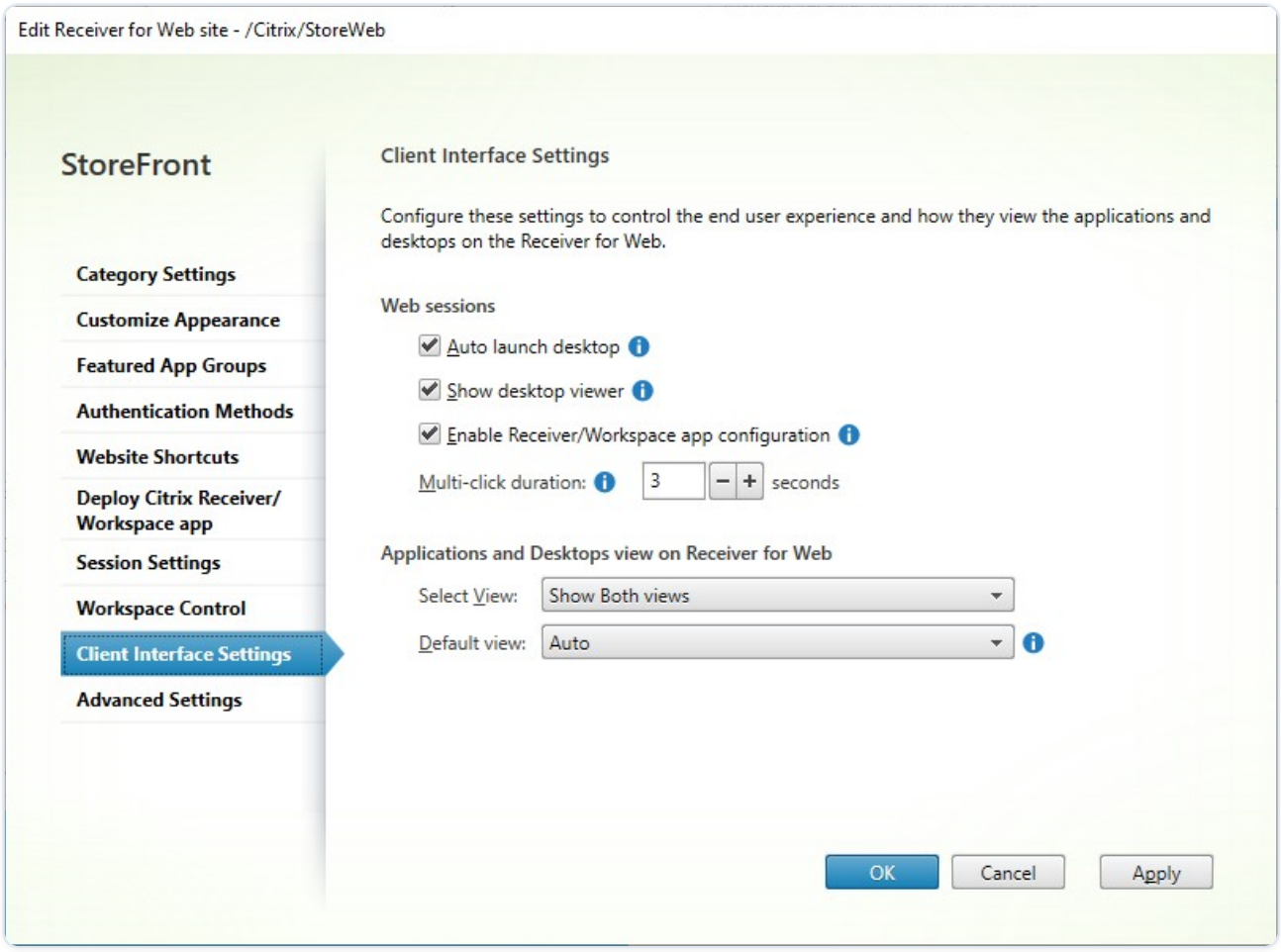
Disable Workspace Control across all apps

To disable session reconnect in StoreFront across Workspace apps, regardless of how they are configured, go to the **Advanced Settings** tab and uncheck **Allow session reconnect**.

Client Interface Settings

To modify client interface settings from the Edit Receiver for web site screen, select the **Client Interface Settings** tab.

© 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 the PowerShell SDK to change auto launch desktop setting call 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.

Show Desktop Viewer

The Desktop Viewer is the toolbar that provides easy access to HDX™ preferences. Use this setting to choose whether this is displayed. The desktop viewer provides the best user experience and is enabled by default.

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

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

To use PowerShell to change this option call cmdlet Set-STFWebReceiverResourcesService with parameter `ShowDesktopViewer`.

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 the PowerShell SDK to change the multi-click duration call 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.

Enable Receiver/Workspace app configuration

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 the PowerShell SDK to change this option call cmdlet Set-STFWebReceiverUserInterface with parameter `ReceiverConfigurationEnabled`.

Application and desktops view

NOTE:

These settings are only available when using the classic experience.

When both desktops and applications are available, Citrix Workspace app displays separate desktop and application views by default. Favorites are displayed on the **Home** view. Users see the **Home** view first when they log on to the site.

From the **Select View** drop-down list, select whether to display apps or desktops, or both.

From the **Default** view drop-down list, select which view is displayed when the user logs in.

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

OPTION	DESCRIPTION
Auto	Display the Home view
Apps	Display the apps view
Desktops	Display the desktops view

To use the PowerShell SDK to change these options call cmdlet Set-STFWebReceiverUserInterface with parameters `ShowAppsView`, `ShowDesktopsView` and `DefaultView`.

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:

```
$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:

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

```
$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
```

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.

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 can be configured to display protected resources when it detects the following minimum versions for the Citrix Workspace app:

APP	VERSION
Citrix Workspace app for Windows	1912

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

APP	VERSION
Citrix Workspace app for Mac	2001
Citrix Workspace app for Linux	2108

The store website never displays protected resources when using earlier versions of Citrix Workspace app, or on iOS, Android, ChromeOS, or when launching apps in the browser.

StoreFront determines the Citrix Workspace app version using Citrix web extensions or Citrix Workspace launcher. If neither are available, or the user has skipped Citrix Workspace app detection, then the website does not display protected resources.

WARNING

It is not guaranteed that the store website always correctly identifies the version of Citrix Workspace app so it may be possible to launch apps using a client that does not support App Protection. Therefore before you enable App Protection for hybrid launches, Citrix recommends configuring App Protection Posture Check which blocks launching virtual apps and desktops from Citrix Workspace app versions that do not support App Protection.

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
   ```

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

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

4. If the user has chosen to open resources in their web browser, either through admin configuration or because the user chose **Use light version**, 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 **Already installed** 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 **Already installed** 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
```

Remove 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 Receiver for Web Sites** in the **Actions** pane.
2. Select a site and click **Remove**. When you remove a site, users can no longer use that webpage to access the store.

Configure Workspace app website

When you create a new store using StoreFront, a website is automatically created and associated with the store. When a store has multiple websites, select which website is displayed when users access the store using Citrix Workspace app.

1. Select the **Stores** node in the left pane of the Citrix StoreFront management console.
2. Select a store in the center pane, and click **Configure Unified Experience** in the **Actions** pane. If you don't have a Citrix Receiver™ for Web website created, a message displays including a link to the Add Receiver for Web site wizard.

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

3. Select the website which you wish Citrix Workspace app clients display when users access this store.
4. Click **OK**.

Advanced settings

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

Enable Fiddler tracing

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

Enable Folder view

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

Enable loopback communication

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

VALUE	DESCRIPTION
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.

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

VALUE	DESCRIPTION
On using HTTP	As **On** but changes the protocol from HTTP to HTTPS. Select this option when using load balancer that terminate HTTPS, connecting to StoreFront over HTTP. To change the port, see Loopback port when using HTTP

Enable Protocol Handler

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.

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

Enable strict transport security

When enabled, adds the `Strict-Transport-Security` header to tell browsers to only connect to the website over HTTPS.

ICA® file cache expiry

The number of seconds for which an ICA file is cached in memory. Defaults to 90s.

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.

Loopback port when using HTTP

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

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.

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

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.

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.

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

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 automatically synchronizes favorites data between the servers.

To manage a multiple-server deployment, use only one server at a time to make changes to the configuration of the server group. Ensure that the Citrix StoreFront management console is not running on any of the other servers in the deployment. Once you have completed your changes, propagate local changes to the other servers in the server group to ensure a consistent configuration across the deployment.

View server group

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

Add a server to a server group

Use the Add Server task to obtain an authorization code to enable you to join a newly installed StoreFront server to your existing deployment. For more information about adding new servers to existing StoreFront deployments, see Join an existing server group. See the *Scalability* section of Plan your Storefront deployment to assess how many servers you need in your group.

Remove servers from a server group

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.

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

Before a removed StoreFront server can be added again, to the same or to a different server group, you must reset it to a factory default state. See Reset a server to factory defaults

Propagate local changes to a server group

Use the Propagate Changes task to update the configuration of all the other servers in a multiple-server StoreFront deployment to match the configuration of the current server. Propagation of configuration information is initiated manually so that you retain control over when and if the servers in the group are updated with configuration changes. While running this task, you cannot make any further changes until all the servers in the group have been updated.

IMPORTANT:

Any changes made on other servers in the group are discarded during propagation. If you update the configuration of a server, propagate the changes to the other servers in the group to avoid losing those changes if you later propagate changes from different server in the deployment.

The information propagated between servers in the group includes the following:

- Contents of all web.config files, which contain the StoreFront configuration.
- Contents of `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients`, such as `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\Windows\CitrixWorkspaceAppWeb.exe` and `C:\Program Files\Citrix\Receiver StoreFront\Receiver Clients\MAC\CitrixWorkspaceAppWeb.dmg`.
- Contents of `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\contrib`.
- Contents of `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\custom folder`, such as copied images and customisation.js files.
- Contents of the Citrix Delivery Services certificate store, except any manually imported Certificate Revocation Lists (CRLs). (For details on distributing local CRLs, see Certificate Revocation List (CRL) checking.

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

NOTE:

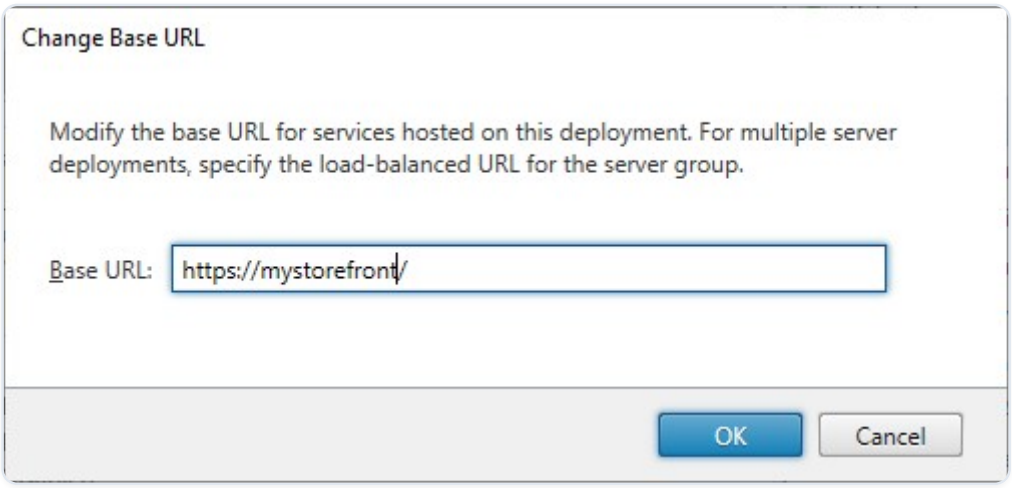
Subscription data is synchronized with the other servers independently of the Propagate Changes mechanism. It happens automatically without the Propagate Changes task being initiated.

Change the base URL for a deployment

The base URL is used as the root of the URLs for the stores and other StoreFront services hosted on a deployment. For multiple-server deployments, specify the load-balanced URL.

To change the base URL:

1. In the Citrix StoreFront management console left pane, select the **Server Group** node.
2. In the actions pane click **Change Base URL...**
3. Enter the new URL
4. Press **OK**.



© 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.

Configure Citrix Gateways

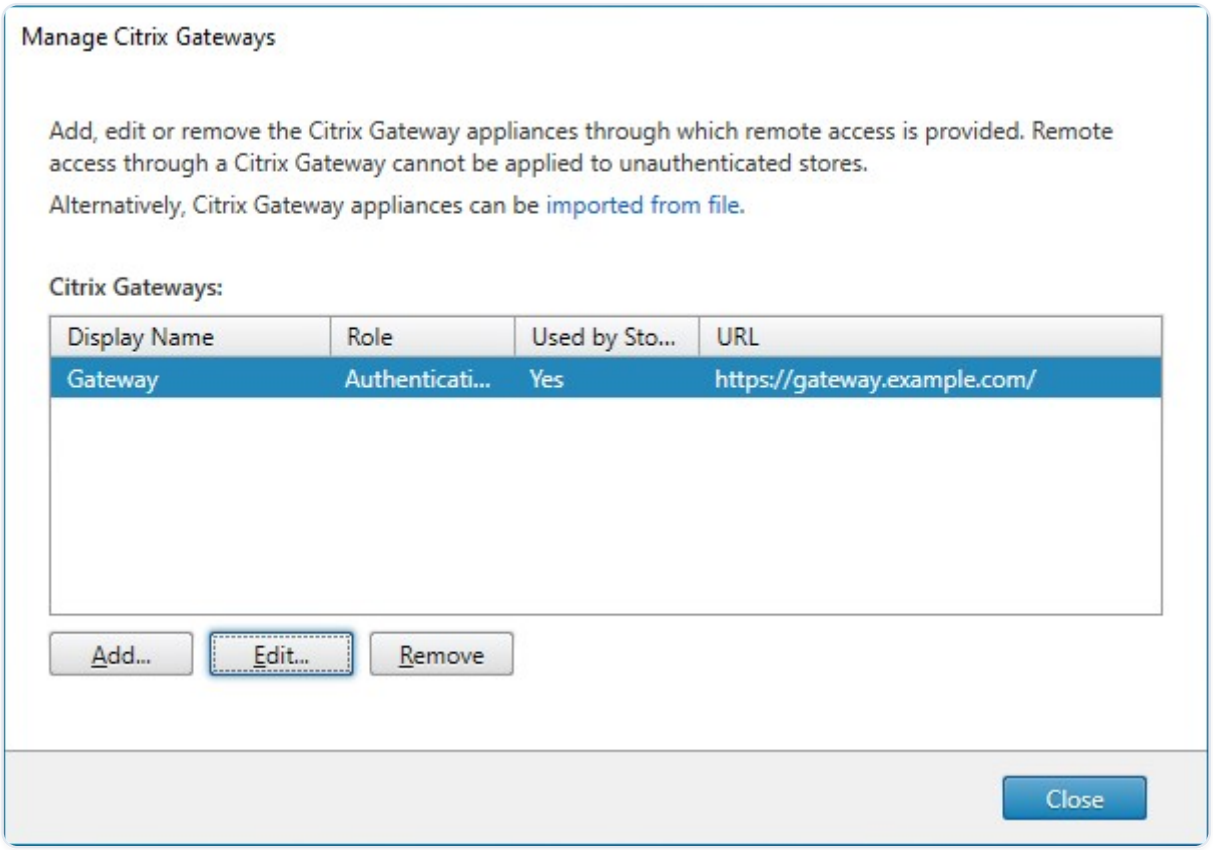
Use Citrix Gateways to provide authentication and remote access to StoreFront and your Virtual Delivery Agents (VDAs). Citrix Gateways run on a hardware or software NetScaler ADCs.

For more information about configuring your Gateway, see Integrate NetScaler Gateway with StoreFront.

You must configure your gateway within StoreFront before StoreFront allows access through that gateway.

View Gateways

To view the gateways configured within StoreFront, select the Stores node in the left pane of the Citrix StoreFront management console and pane, click **Manage Citrix Gateways**. This displays the **Manage Citrix Gateways** window.



PowerShell

To get a list of gateways and their configuration call Get-STFRoamingGateway.

Add Citrix Gateway

1. In the **Manage Citrix Gateways** window click **Add**.

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

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.

   - Enter the URL of the gateway.

     The fully qualified domain name (FQDN) for your StoreFront deployment must be unique and different from the Citrix Gateway virtual server FQDN. Using the same FQDN for StoreFront and the Citrix Gateway virtual server is not supported. The gateway adds the URL to the `X-Citrix-Via` HTTP header. StoreFront uses this header to determine which gateway is in use.

     Using the GUI it is only possible to add a single gateway URL. If a gateway can be access by multiple URLs then you need to add the same gateway twice with identical configuration apart from the URL. To simply configuration, you can configure a secondary URL used to access the gateway. This option is not available using the GUI so you must configure this using PowerShell. You should close the management console before running any PowerShell commands. For example if you have multiple gateways behind a global server load balancer, typically it is useful to add both the GSLB URL and a URL that can be used to access each specific regional gateway, for example for testing or troubleshooting purposes. Once you have created the gateway you can add an additional URL using `Set-STFRoamingGateway`, using the `-GSLBurl` parameter for the secondary URL. Although the parameter is called `GSLBurl` this can be used for any situation where you wish to add a second URL. For example:

     ```
     Set-STFRoamingGateway -Name "Europe Gateway" -GSLBurl
     "eugateway.example.com" -GatewayUrl "gslb.example.com"
     ```

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

Note:

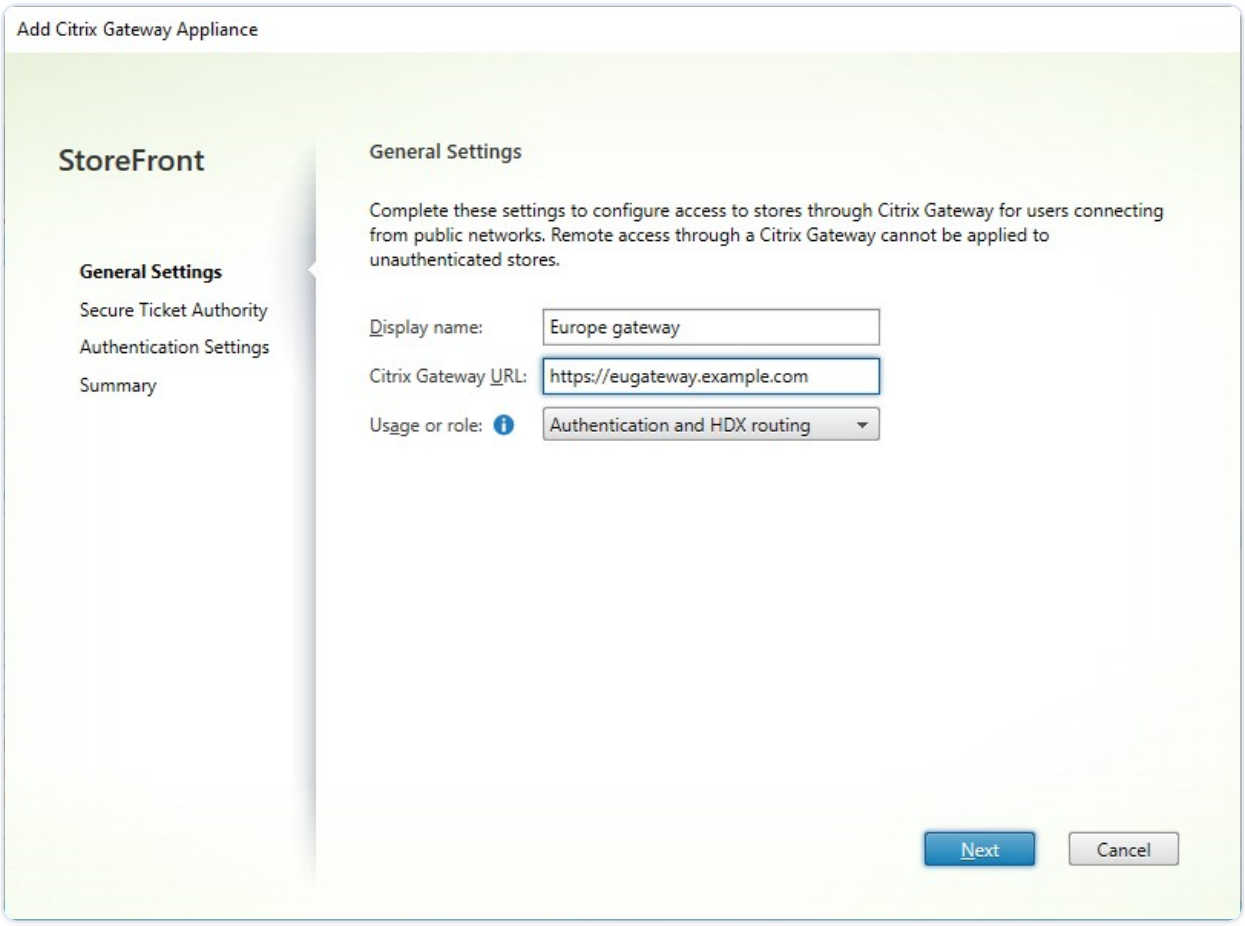
> Counterintuitively in this example, the `GSLBurl` parameter contains the regional URL while the `GatewayUrl` parameter contains the GSLB URL. For most purposes the URLs are treated identically and if the store is only accessed through a web browser they can be configured either way around. However when accessing StoreFront through Citrix Workspace app, it reads the `GatewayUrl` from StoreFront and subsequently uses it for remote access and it is preferable for it to be configured to always connect to the GSLB URL.

If you need more than two URLs then you will need to configure this as a separate gateway.

- Select the Usage or Role:

USAGE OR ROLE	DESCRIPTION
Authentication and HDX routing	Use the gateway for both providing remote access to StoreFront and to access the VDAs.
Authentication only	Select this if the gateway is used only for remote access to StoreFront. This option prevents 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.

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



3. Fill out the settings on the **Secure Ticketing Authority** tab.

   The secure ticketing authority issues session tickets in response to connection requests. These session tickets form the basis of authentication and authorization for Citrix Workspace app detection and access to VDAs.

   - Enter one or more Secure Ticket Authority server URL.
     - If you are using Citrix Virtual Apps and Desktops™ then you can use the delivery controllers as STA servers.
     - If you are using Citrix Desktop as a Service then you can use your cloud connectors as STA servers. These either proxy requests to the Citrix Cloud™ Ticketing Authority, or when in LHC mode generate their own tickets. In the future this will change so that they always generate their own tickets for improved resiliency.
     - It is recommended that you use at least 2 STA servers for redundancy. When using Cloud Connectors, 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.
     - 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

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

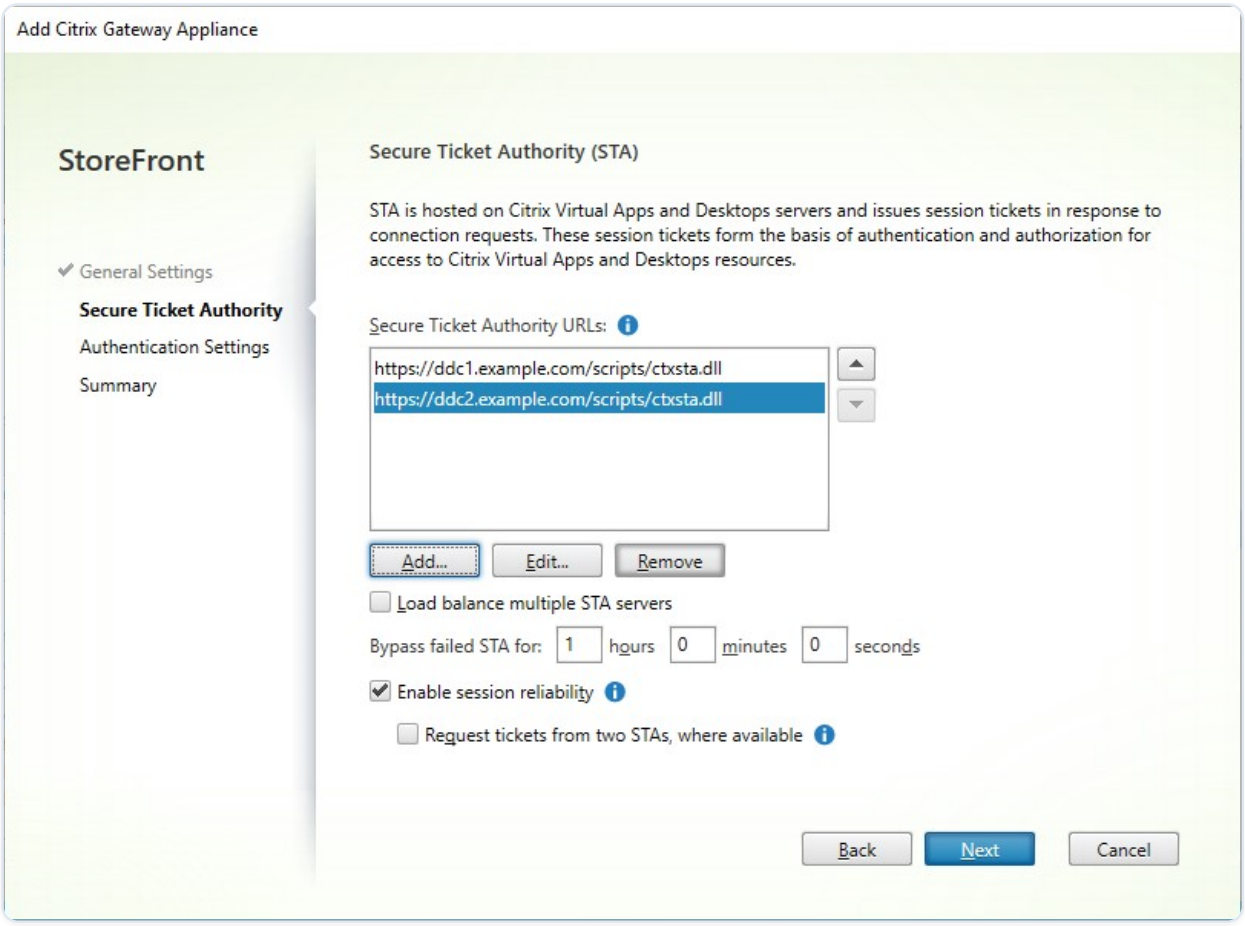
can cause launches to fail. Today when using Cloud Connectors as STAs this may not be apparent in normal use as any connector can be used to redeem tickets from the Citrix Cloud Ticking Authority. However Local Host Cache mode the connector generates its own tickets and in the future this will become the default behavior.

    - The Delivery Controller or Cloud Connector may be configured so that StoreFront must include a security key. It is not possible to add security keys using the GUI; see the later step for adding them using PowerShell.

- Select **Load balance multiple STA servers** to distribute requests between the STA servers. If cleared then StoreFront will try the servers in the order in which they are listed.
- If StoreFront cannot reach an STA server then it avoids using that server for a period of time. By default this is 1 hour but you can customize this value.
- If you want Citrix Virtual Apps and Desktops to keep disconnected sessions open while Citrix Workspace app attempts to reconnect automatically, select **Enable session reliability**.
- If you configured multiple STAs, optionally select **Request tickets from two STAs, where available**.

  When **Request tickets from two STAs, where available** is selected, StoreFront obtains session tickets from two different STAs so that user sessions are not interrupted if one STA becomes unavailable during the course of the session. If, for any reason, StoreFront is unable to contact two STAs, it falls back to using a single STA.

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



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.

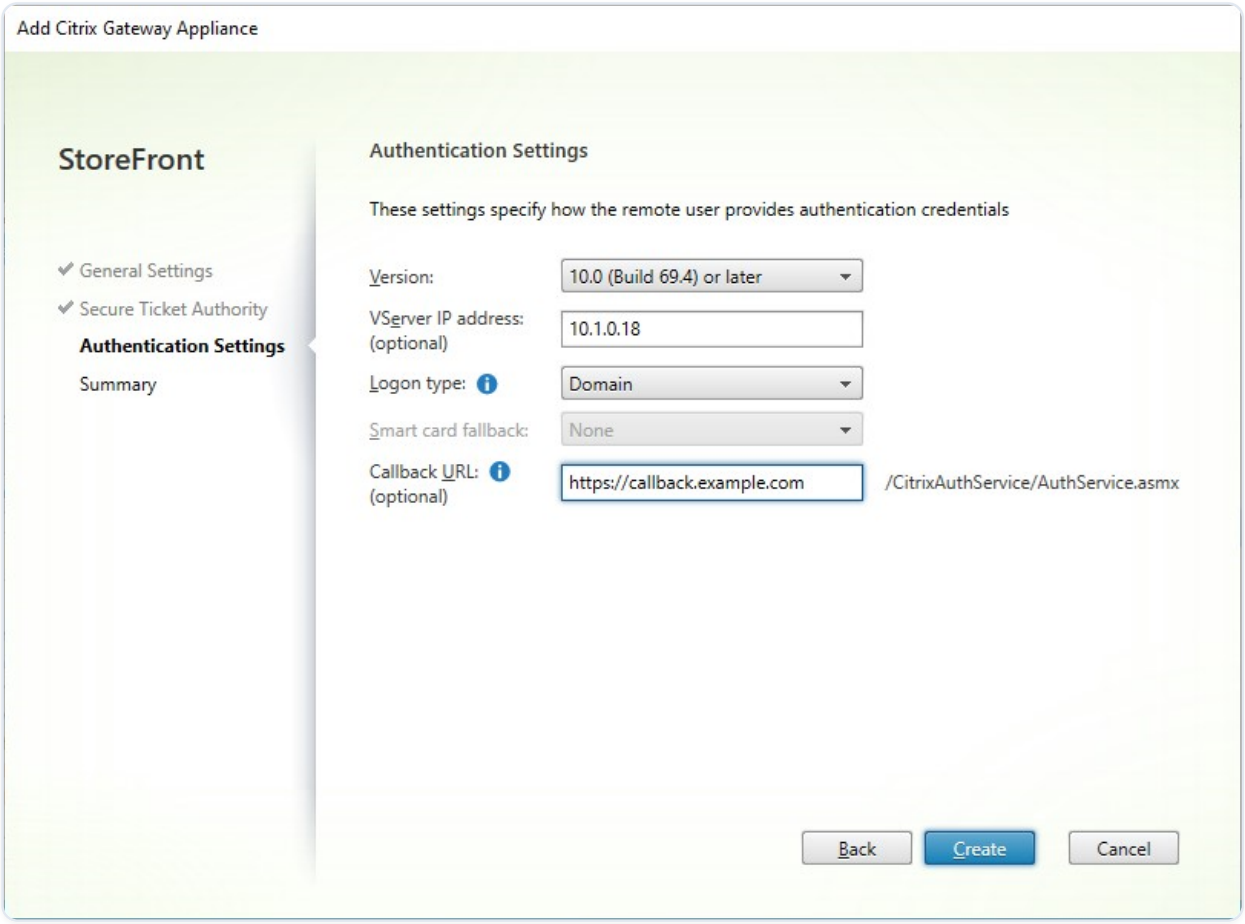
    - For LDAP authentication, select **Domain**.
    - For Native OTP authentication, select **Security token**.
    - For LDAP plus OTP authentication, select **Domain and security token**.
    - For OTP via text message, select **SMS authentication**.

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

- For certificate authentication, select **Smart card**.
- For SAML authentication, 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.

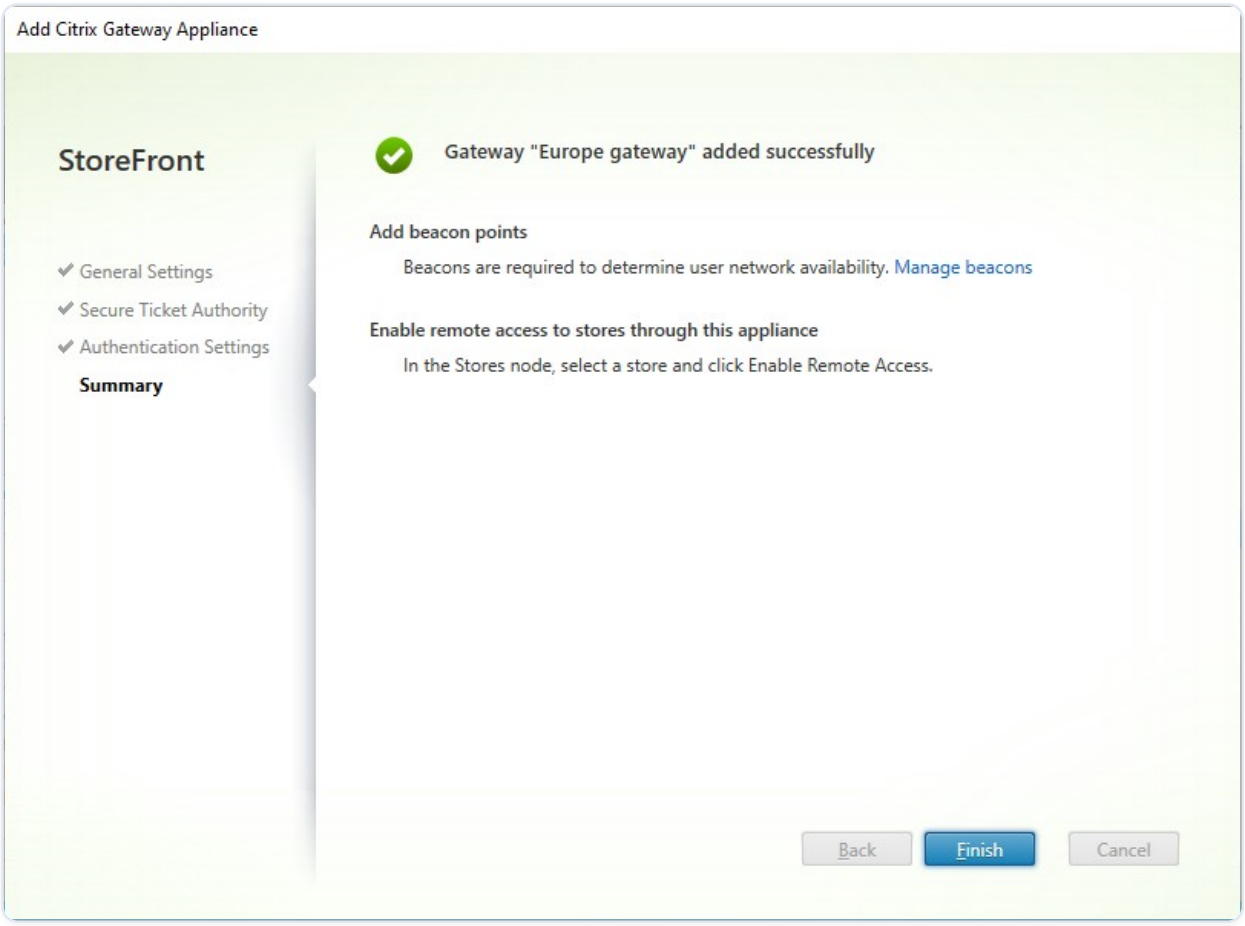
- Optionally, enter the internally accessible URL of the gateway in the Callback URL box. This allows StoreFront to contact the Citrix Gateway authentication service to verify that requests received from Citrix Gateway originate from that appliance. It is required for smart access and for password-less 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.



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

5. Click **Create** to apply the configuration.

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



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.
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.

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

PowerShell SDK

To add a gateway using the PowerShell SDK call cmdlet New-STFRoamingGateway.

Edit Citrix Gateway

1. In the **Manage Citrix Gateways** window, click on the gateway you wish to change and press **Edit**.

   For a description of the parameters, see Add Citrix Gateway

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

PowerShell SDK

To modify gateway configuration using the PowerShell SDK call cmdlet Set-STFRoamingGateway.

Remove Citrix Gateway

1. In the **Manage Citrix Gateways** window, click on the gateway you wish to change and press **Remove**.
2. In the confirmation window press **Yes**.

PowerShell SDK

To remove the gateway using the PowerShell SDK call Remove-STFRoamingGateway.

Import a Citrix Gateway

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 Citrix Receiver for Web sites before generating the ZIP file for export.
- StoreFront must be able to resolve the callback URL in DNS to the gateway VPN vServer IP address for authentication using the imported gateway to succeed.

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

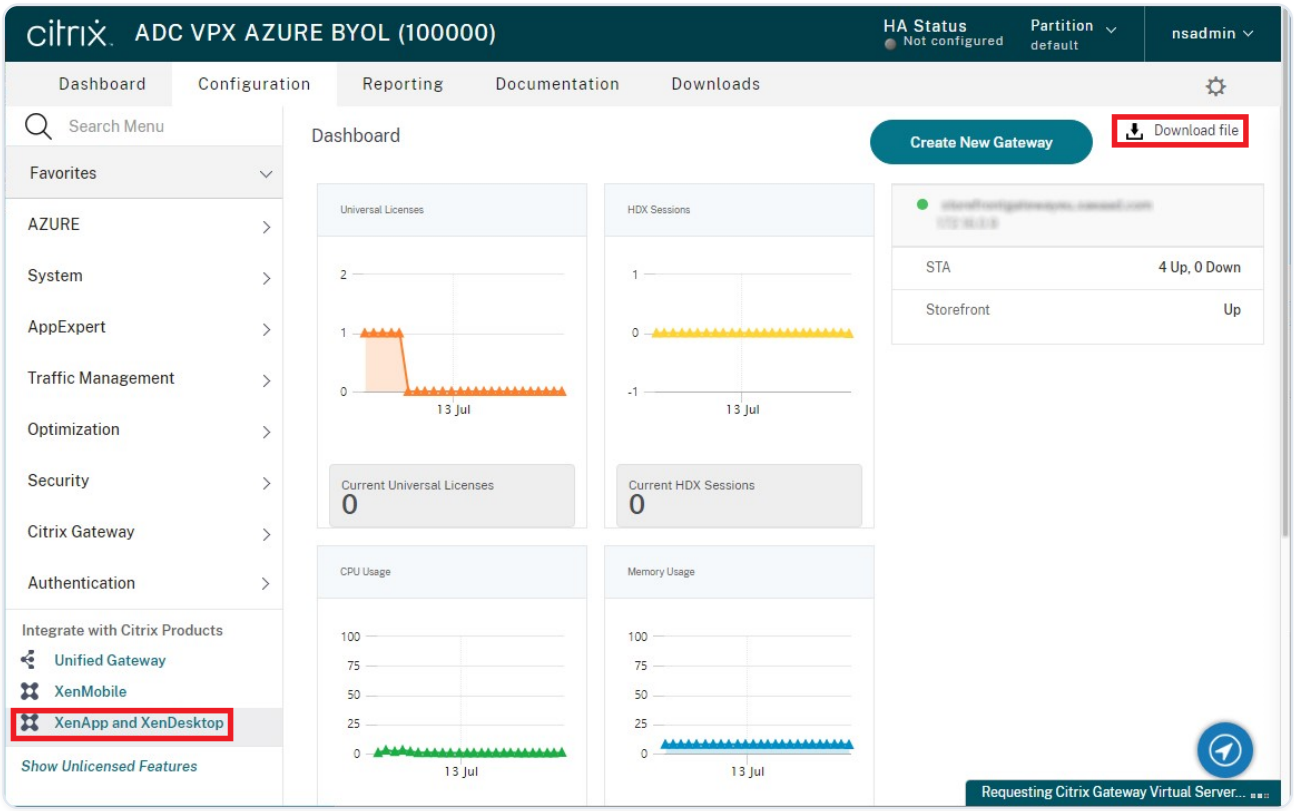
  or

  The callback URL and port combination may be different from the gateway URL and port combination if you use different external and internal DNS namespaces in your environment. If your gateway is located in a DMZ and uses an `<example.com>` URL and StoreFront is on your private corporate network and uses an `<example.local>` URL you may use an `<example.local>` callback URL to point back to the gateway vServer in the DMZ.

Export configuration from Citrix Gateway

1. Log onto the Citrix Gateway.
2. Go to the Configuration tab
3. Under "Integrate with Citrix Products", click XenApp and XenDesktop®
4. On the top right click "Download file".

© 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

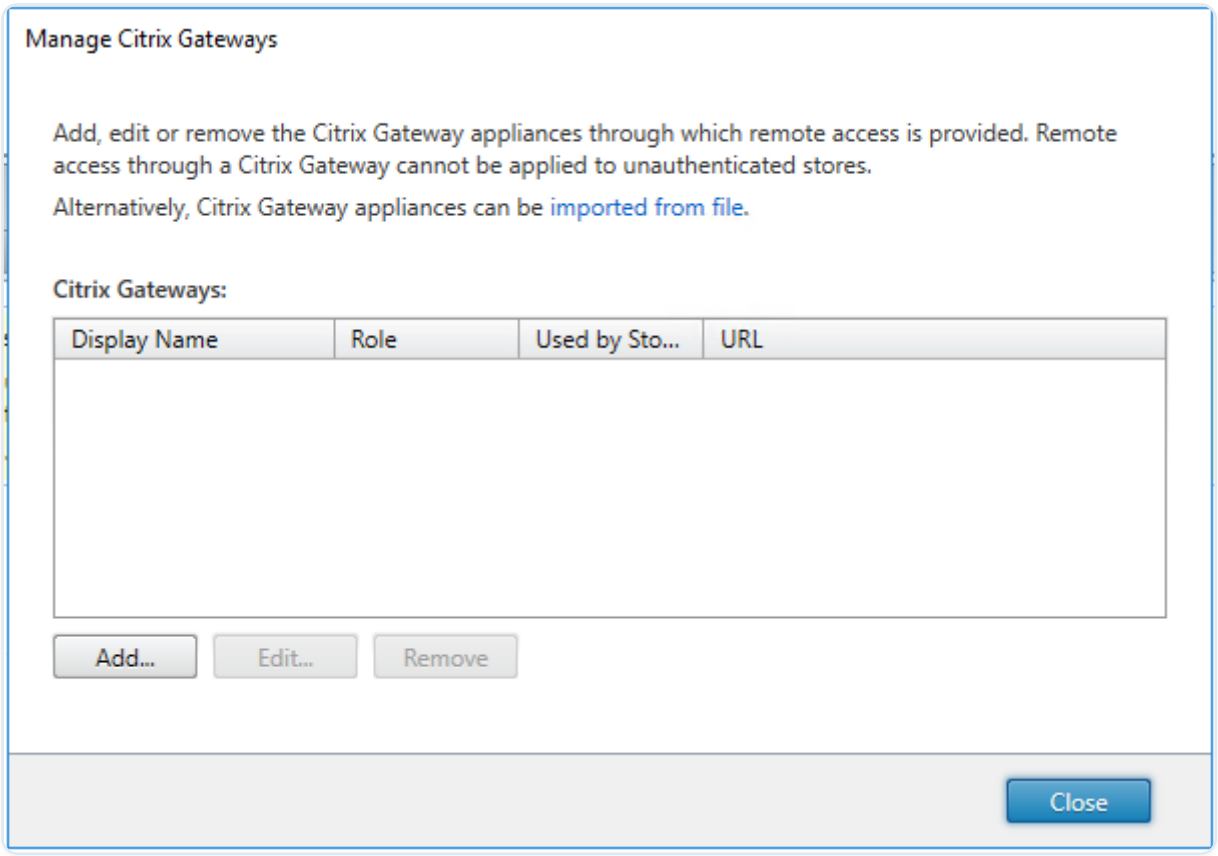
You can import one or more Citrix Gateway virtual server configurations using the same import file. If you have multiple gateway virtual servers from different Citrix Gateway, you must use multiple import files.

Important:

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

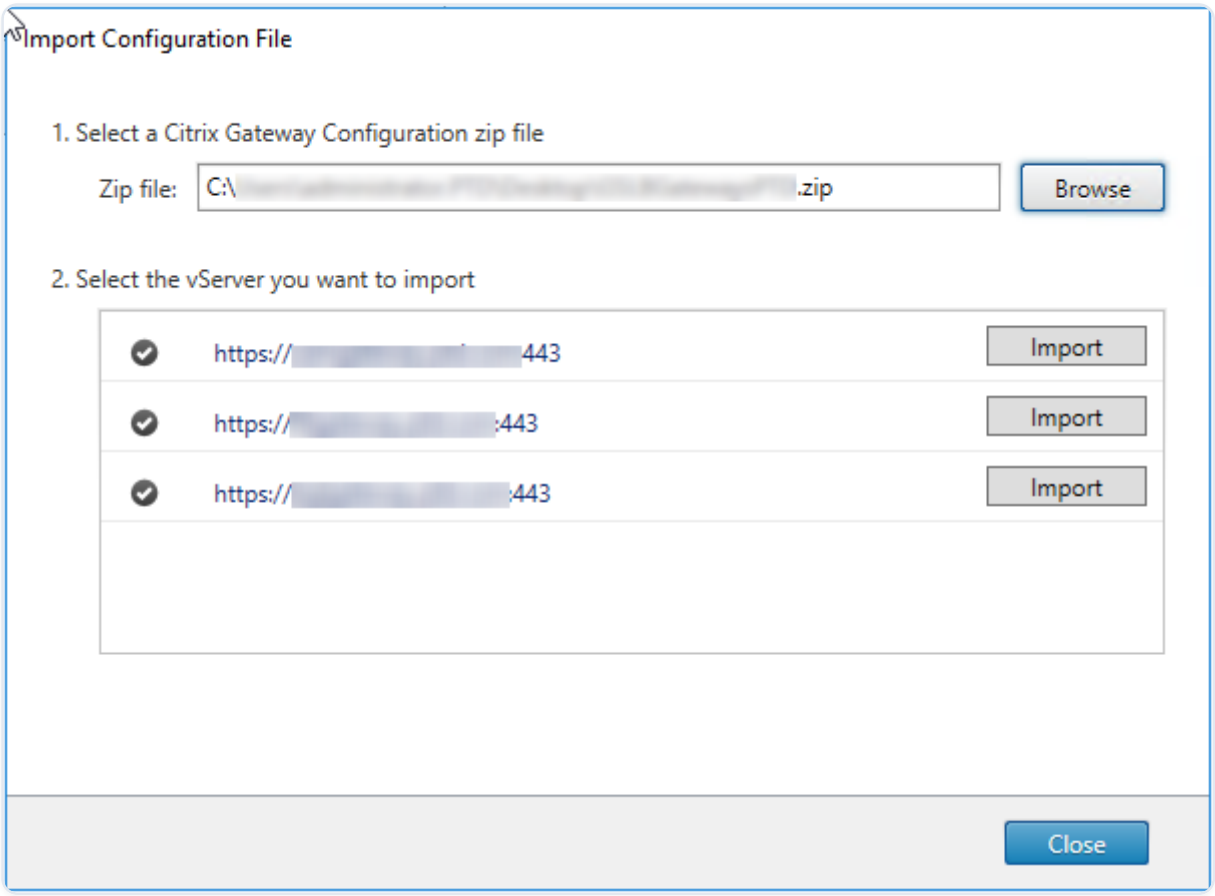
1. Select **Stores** in the left pane of the Citrix StoreFront management console, and in the **Actions** pane, click **Manage Citrix Gateways**.
2. On the Manage Citrix Gateways screen, click the **imported from file** link.

© 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.

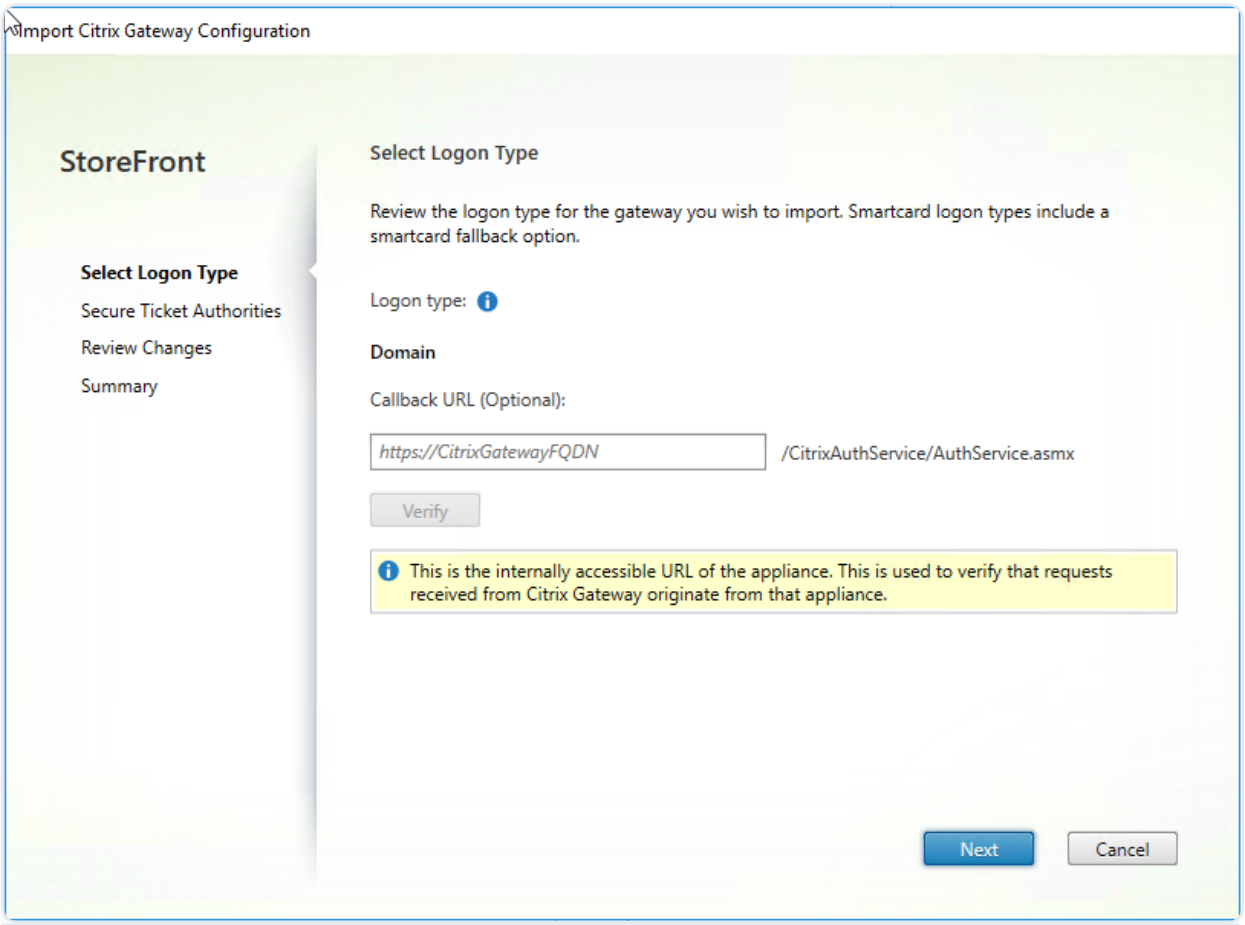
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.



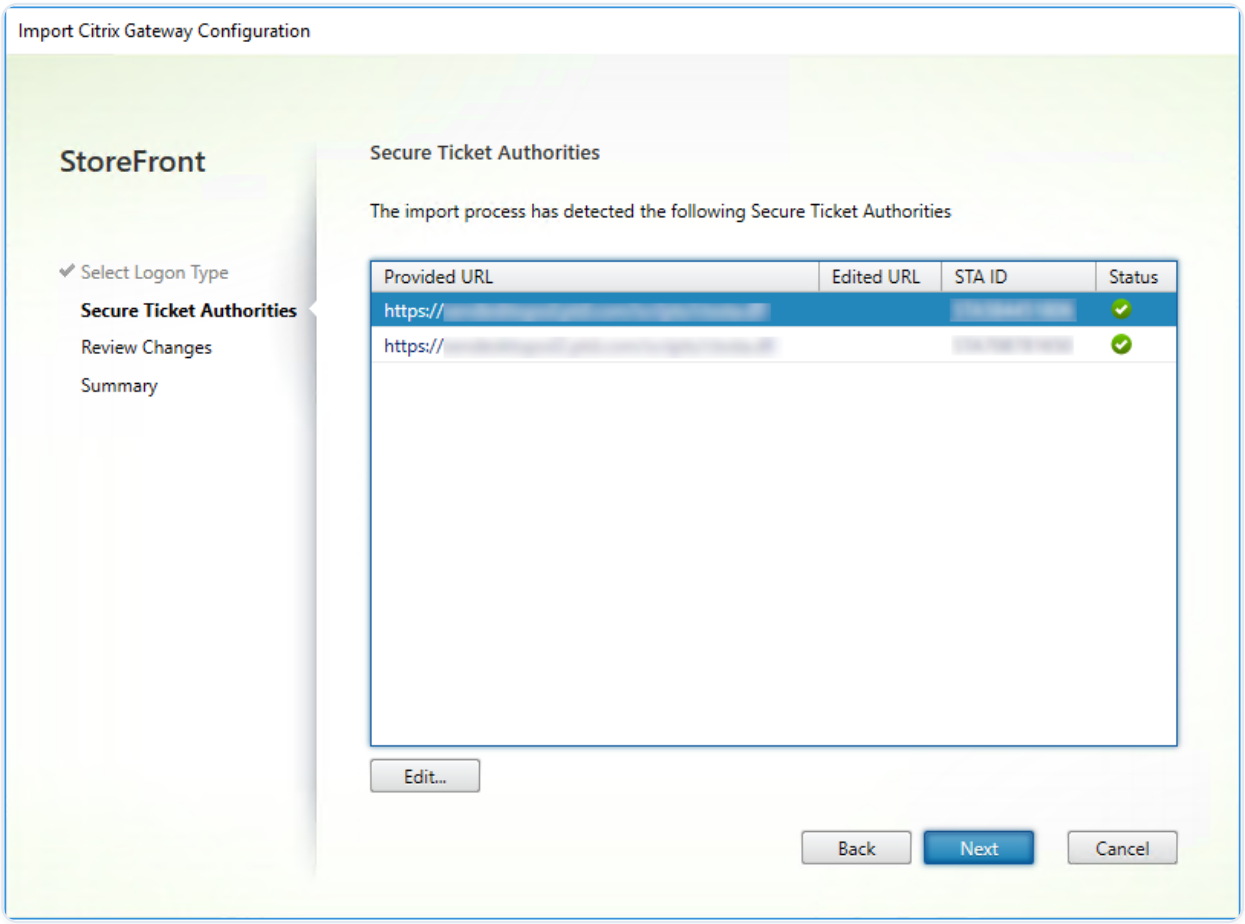
LOGON TYPE IN CONSOLE	LOGONTYPE IN JSON FILE	CALLBACK URL REQUIRED
Domain	Domain	No
Domain and security token	DomainAndRSA	No
Security token	RSA	Yes
Smart card - no fallback	SmartCard	Yes
Smart card - domain	SmartCardDomain	Yes
Smart card - domain and security token	SmartCardDomainAndRSA	Yes
Smart card - 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.

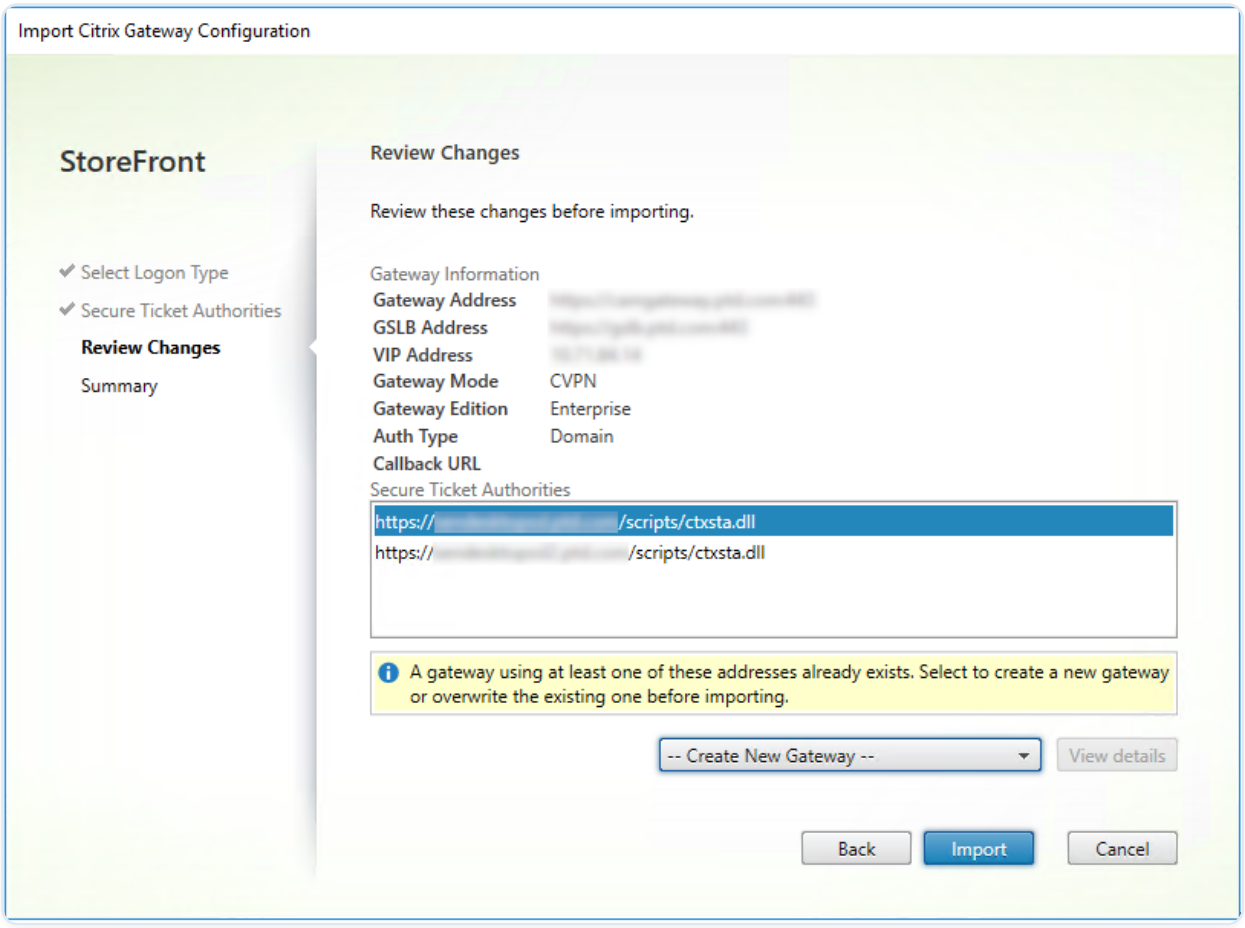
To use Smart Access or password-less authentication, a Callback URL is required.

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:

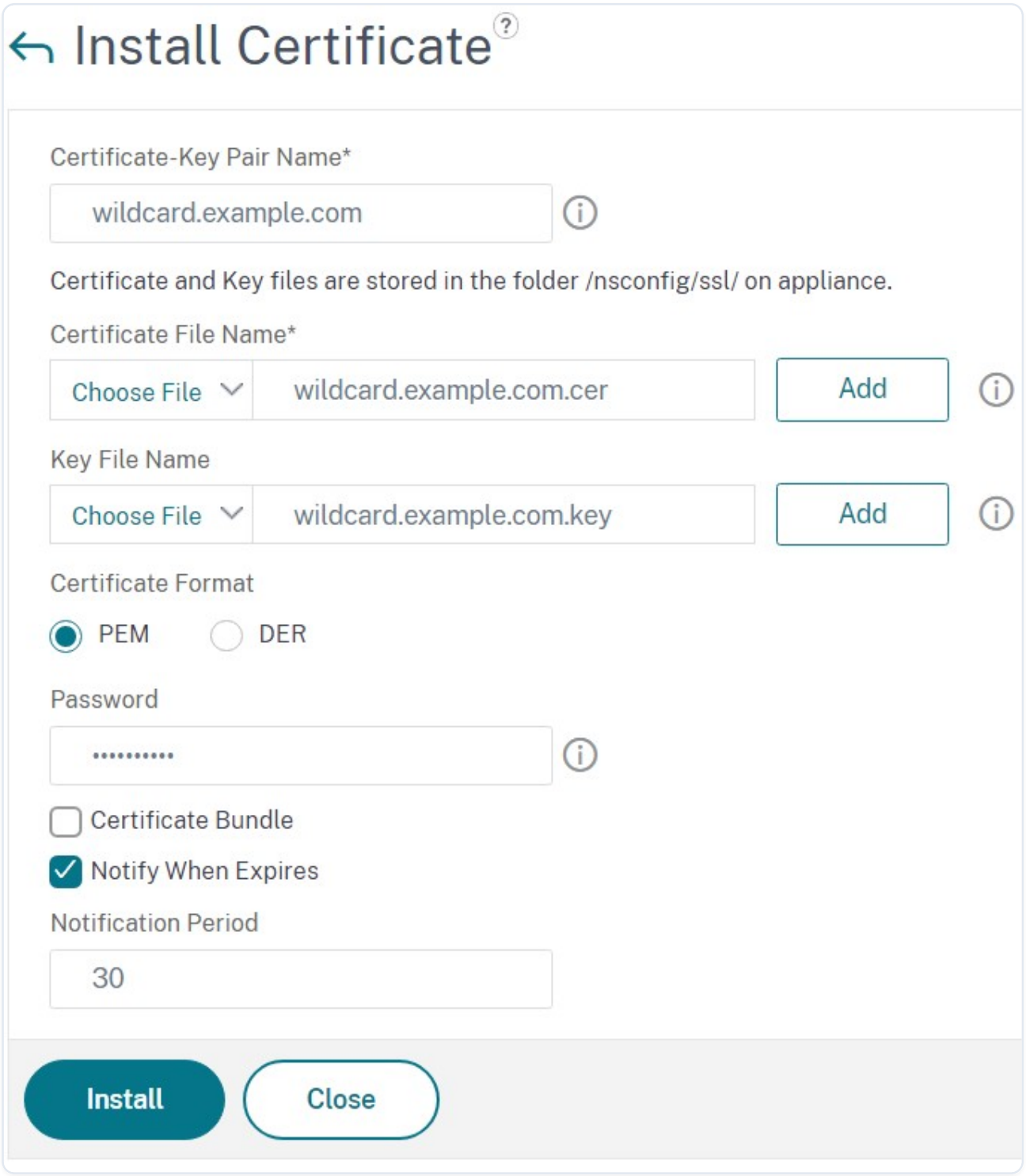
1. Log on to the NetScaler ADC appliance management GUI.
2. Select **Traffic Management** > **SSL** > **Certificates** > **CA Certificates**.
3. Click **Install**.
4. On the **Install CA Certificate** page:
    a. Enter a **Certificate-Key Pair Name**.
    b. Under **Certificate File Name**, click **Choose 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.



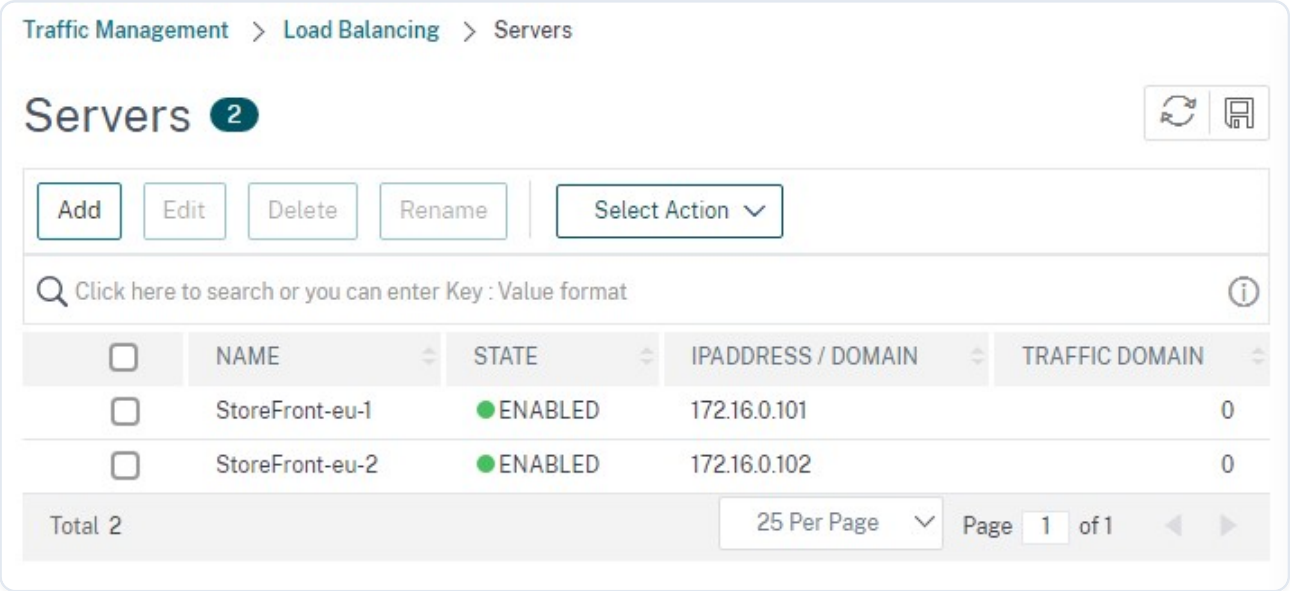
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.



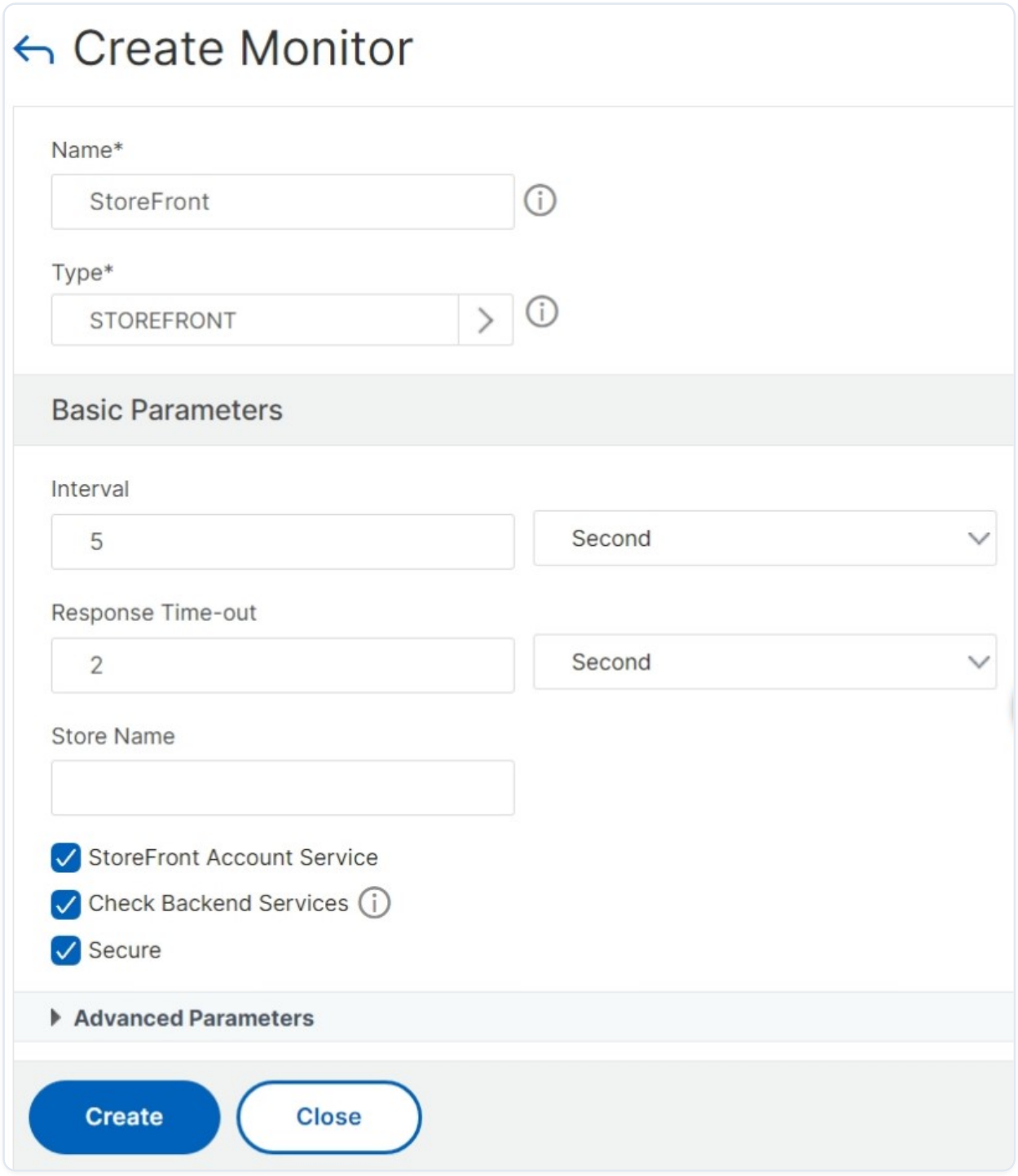
Define a StoreFront monitor to check the status of all StoreFront nodes in the server group

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

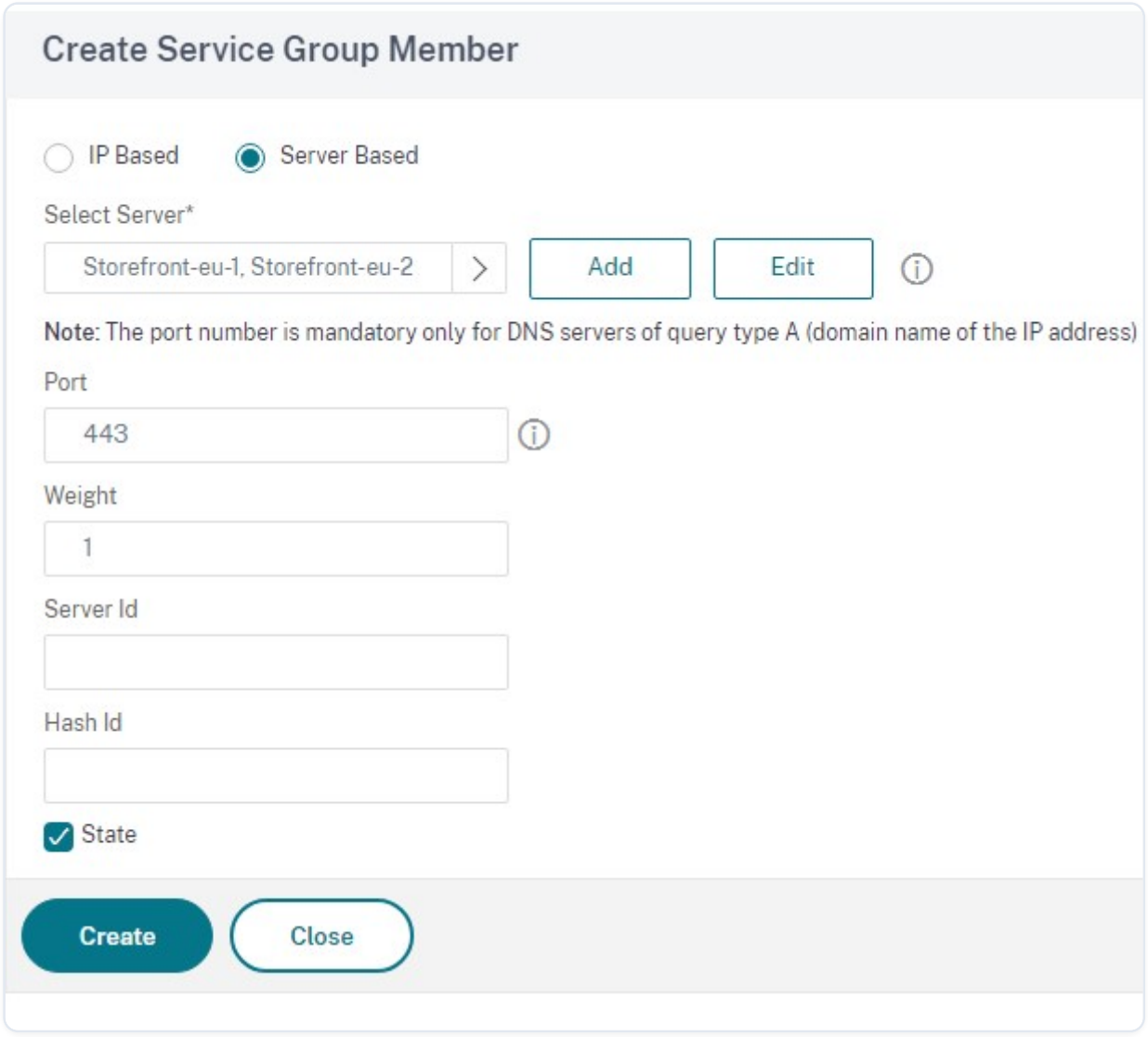
1. Navigate to **Traffic Management > Load Balancing > Service Groups**. Press **Add**. To connect to the StoreFront servers over HTTPS, select a protocol of SSL. Leave other settings as default. Press **OK**.
2. Within your Service Group, under **Service Group Members**, click **No Service Group Member**.

   a. Click **Service Based**.

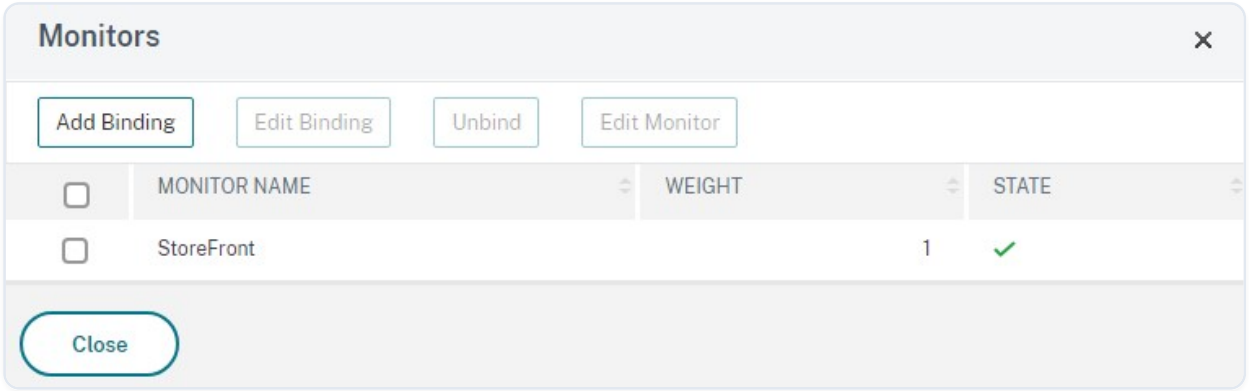
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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.

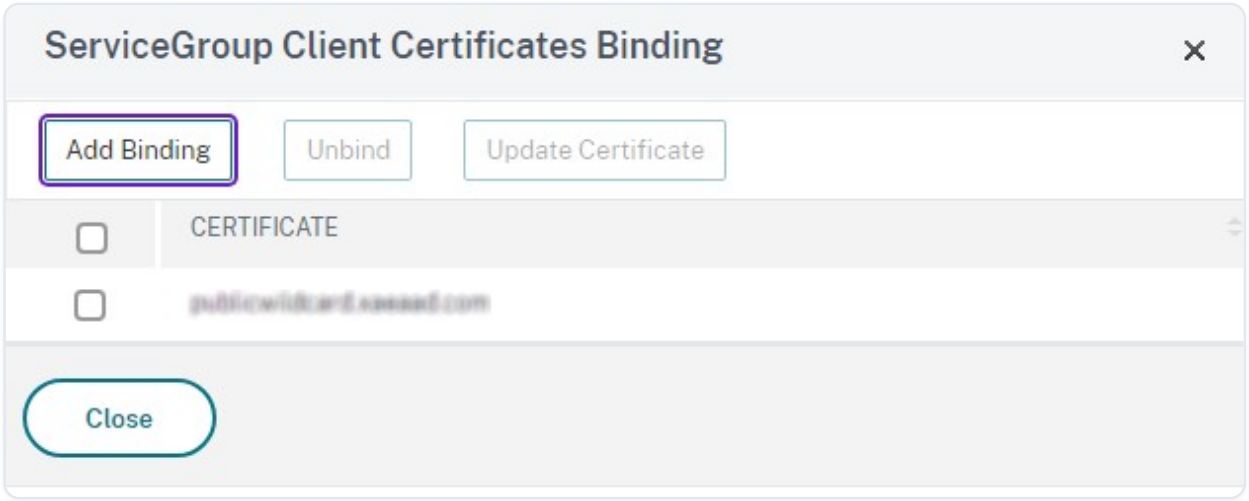


4. Add the **Certificates** section.

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.

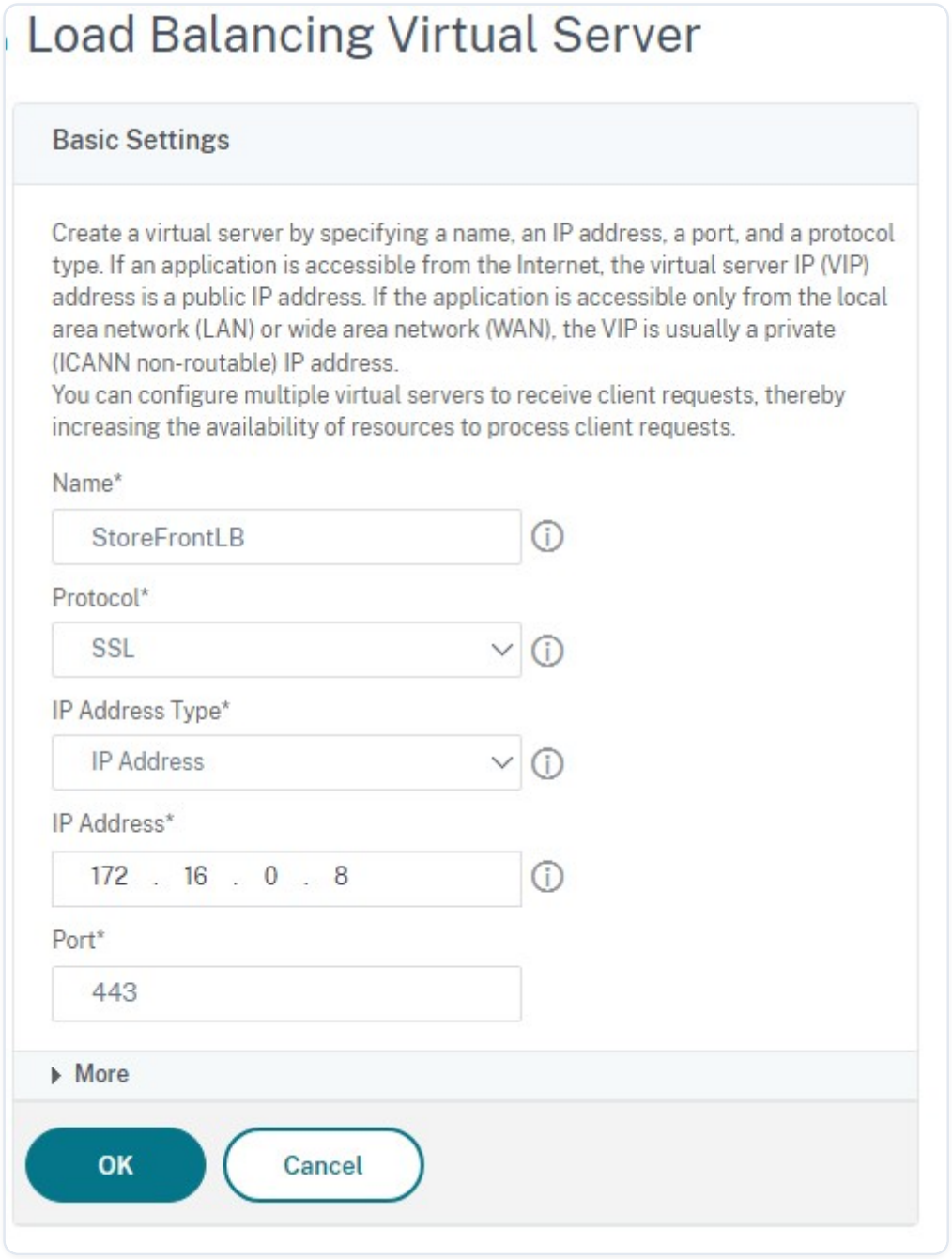


5. Add the **Settings** section. Select **Insert Client IP Header** and enter a header name of **X-Forwarded-For**. This allows the Client IP Address to be used in Citrix Virtual Apps and Desktops Policies.

Create a load balancing virtual server for user traffic

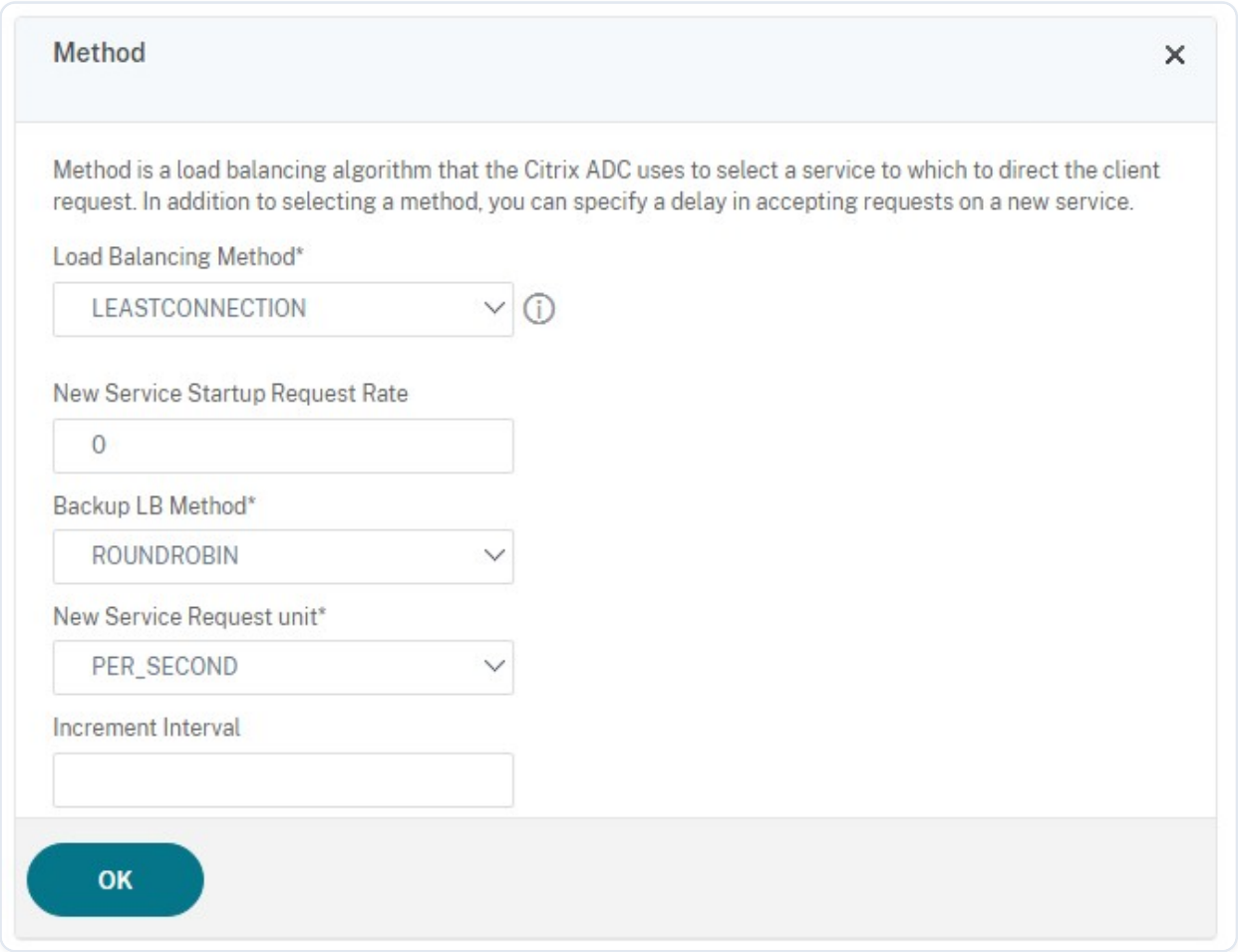
1. Log on to the NetScaler ADC appliance management GUI.
2. Select **Traffic Management > Load Balancing > Virtual Servers > Add** to create a new virtual server.
3. Enter a name, choose a protocol of SSL and enter the **Port**. Click OK to create the Virtual Server.

© 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.

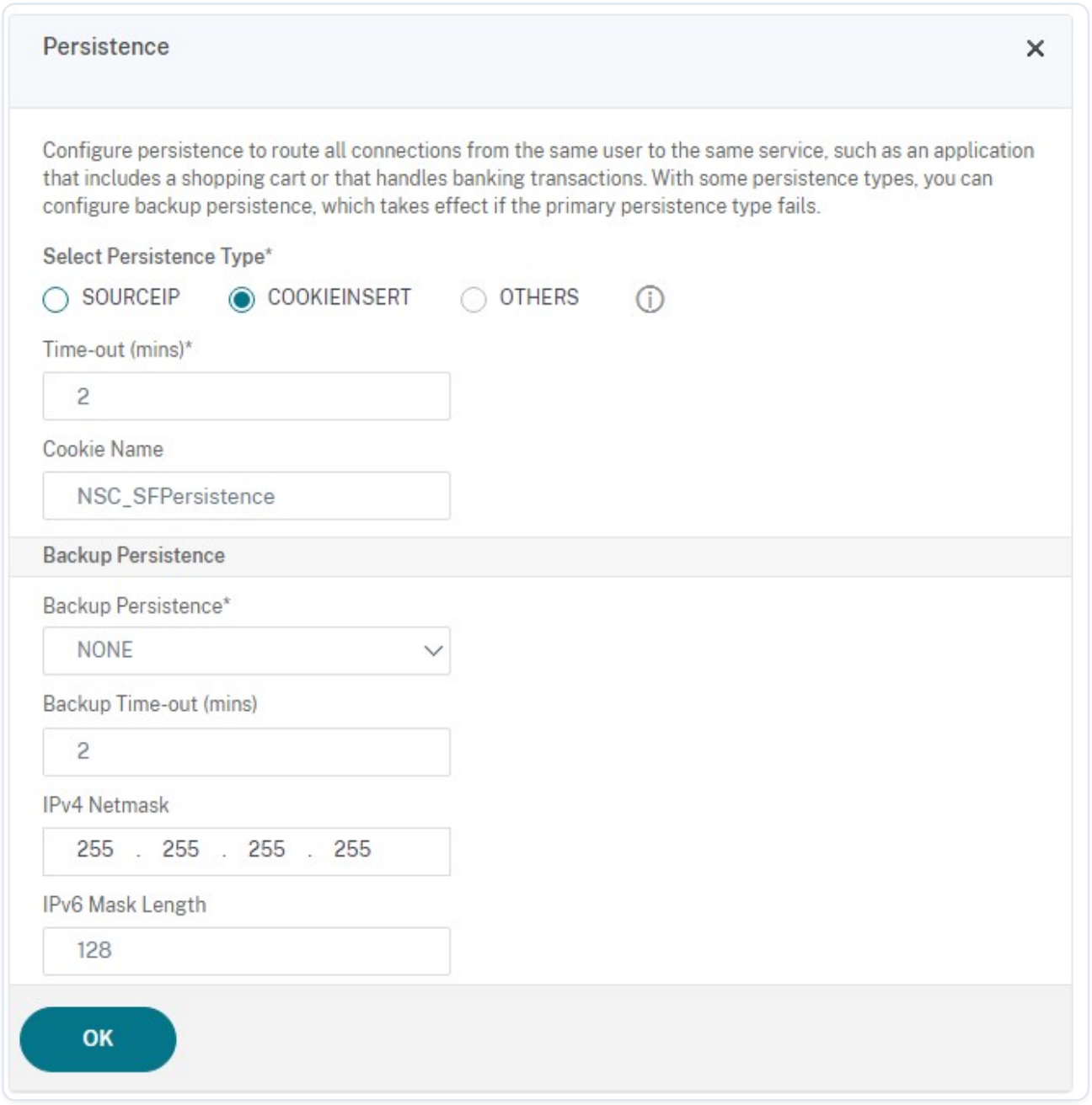
   c. Name the cookie. For example, **NSC_SFPersistence**, as this makes it easy to identify during debugging.

   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.

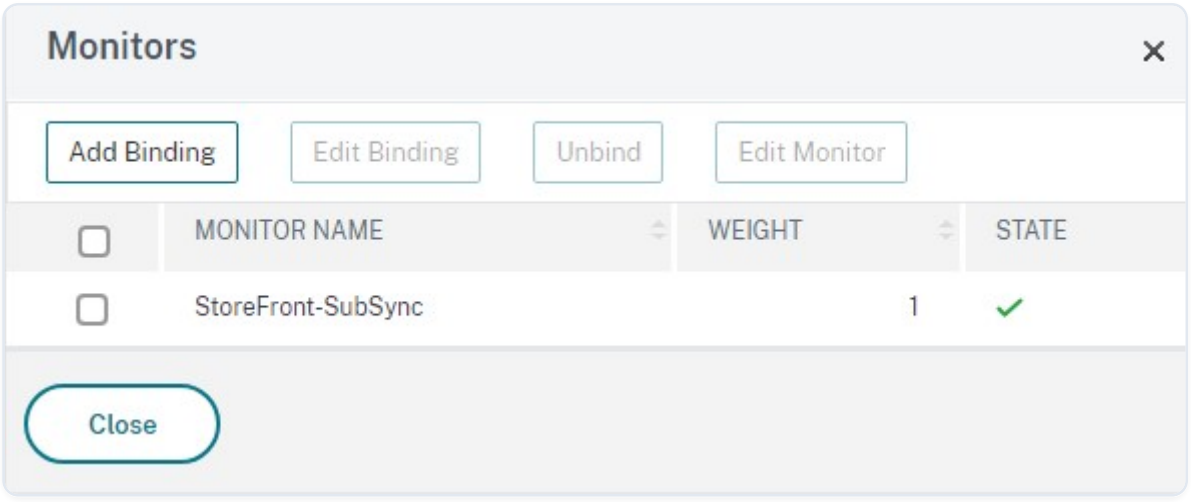
© 1997–2026 Citrix Systems, Inc. All rights reserved.

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**.

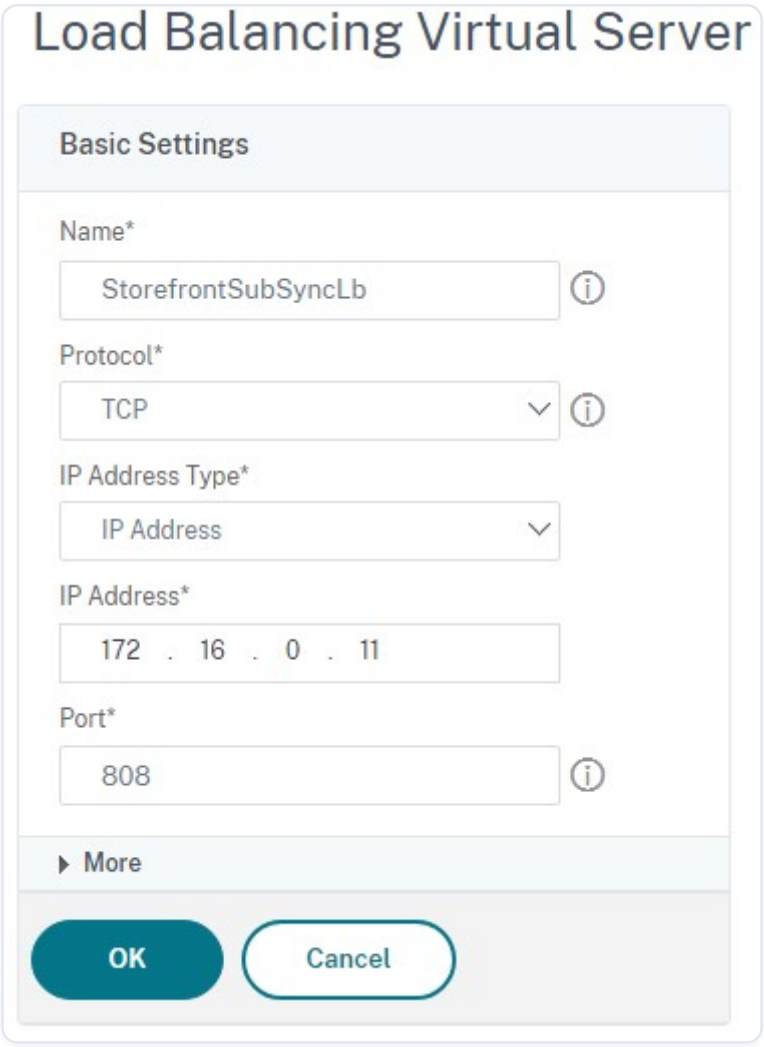


Create a load balancing virtual server for subscription synchronization

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:

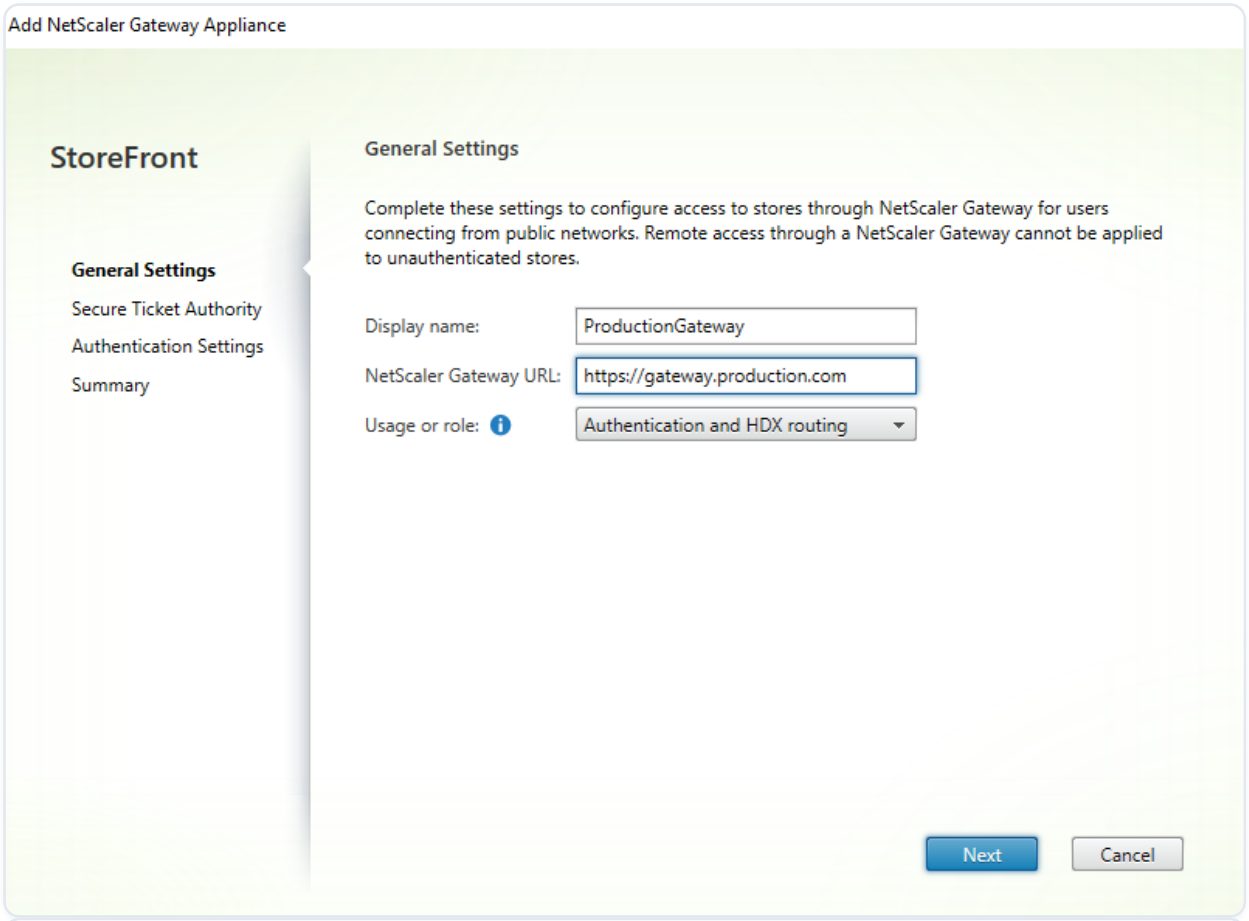
- StoreFront, Citrix Virtual App and Desktops and VDAs are all on the `development.com` domain.
- Authentication to the Citrix Receiver for Web site occurs using a development\testuser1 account and password.
- There is no trust relationship between the two domains.

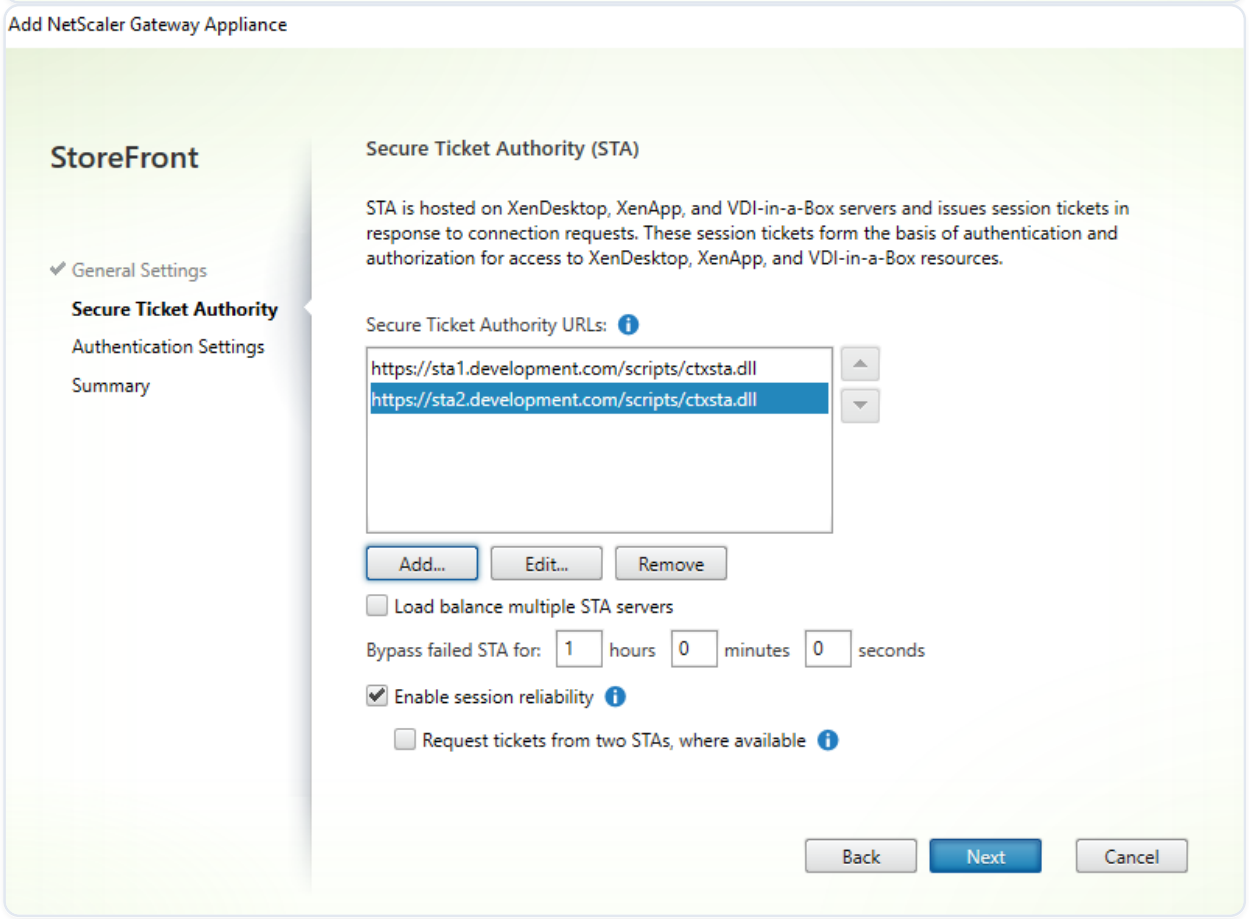
Configure a Citrix Gateway for the store

To configure a Citrix Gateway for the store:

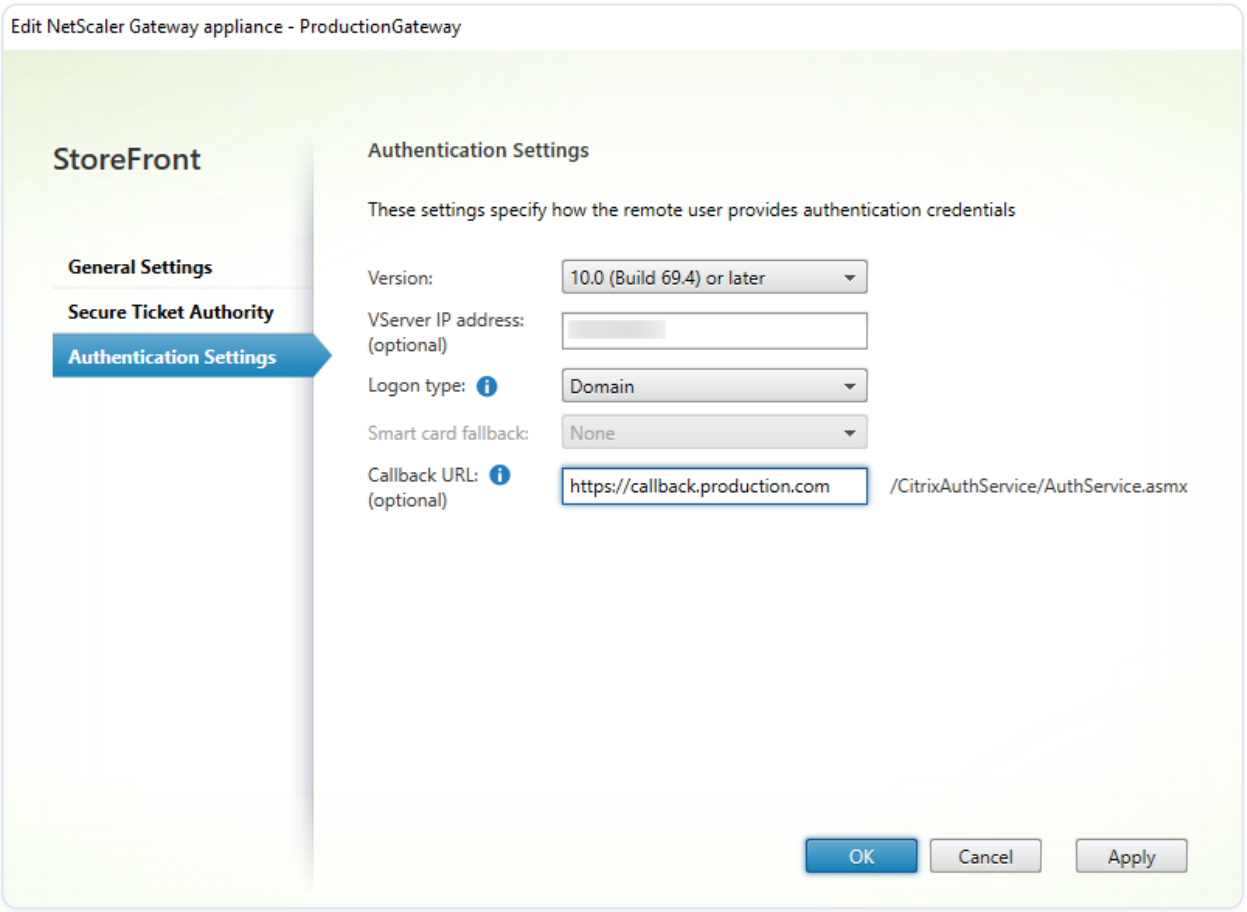
1. Select **Stores** in the left pane of the Citrix StoreFront management console, and in the **Actions** pane, click **Manage Citrix Gateways**.
2. On the Manage Citrix Gateways screen, click **Add**.
3. Complete the General Settings, Secure Ticket Authority, and Authentication steps.

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





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



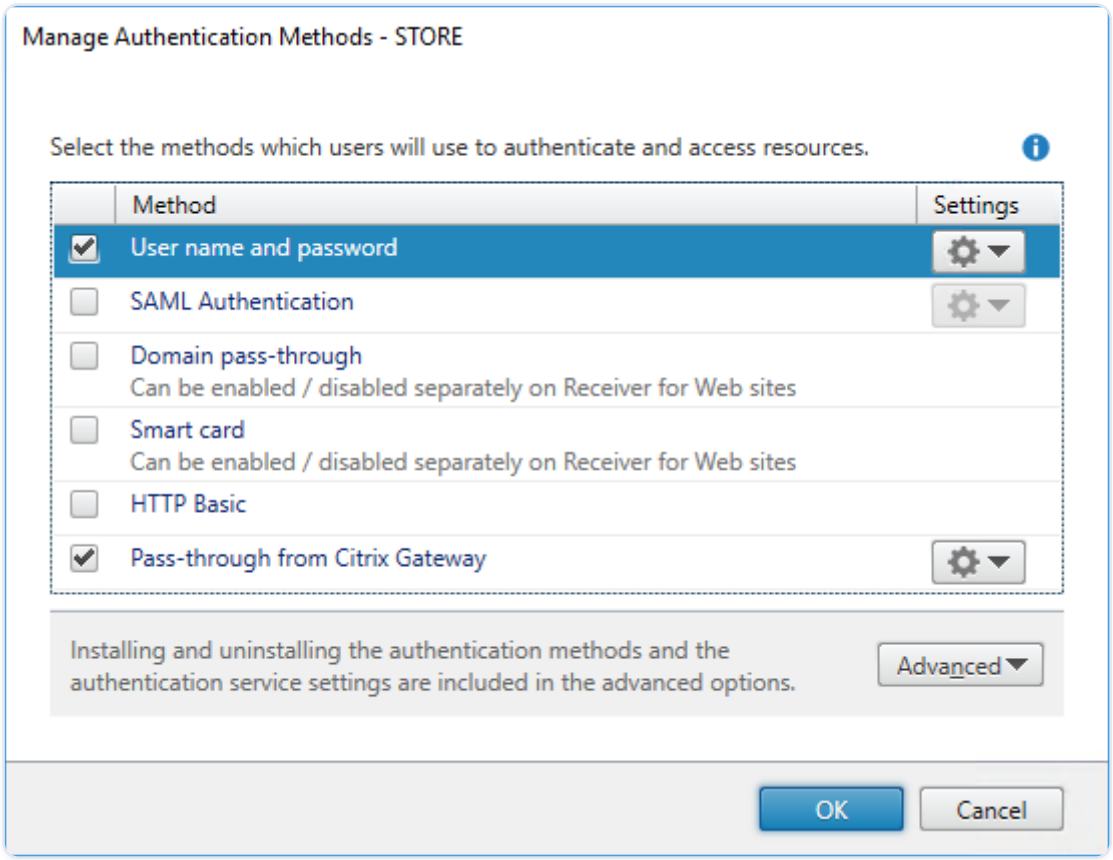
NOTE:

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**.

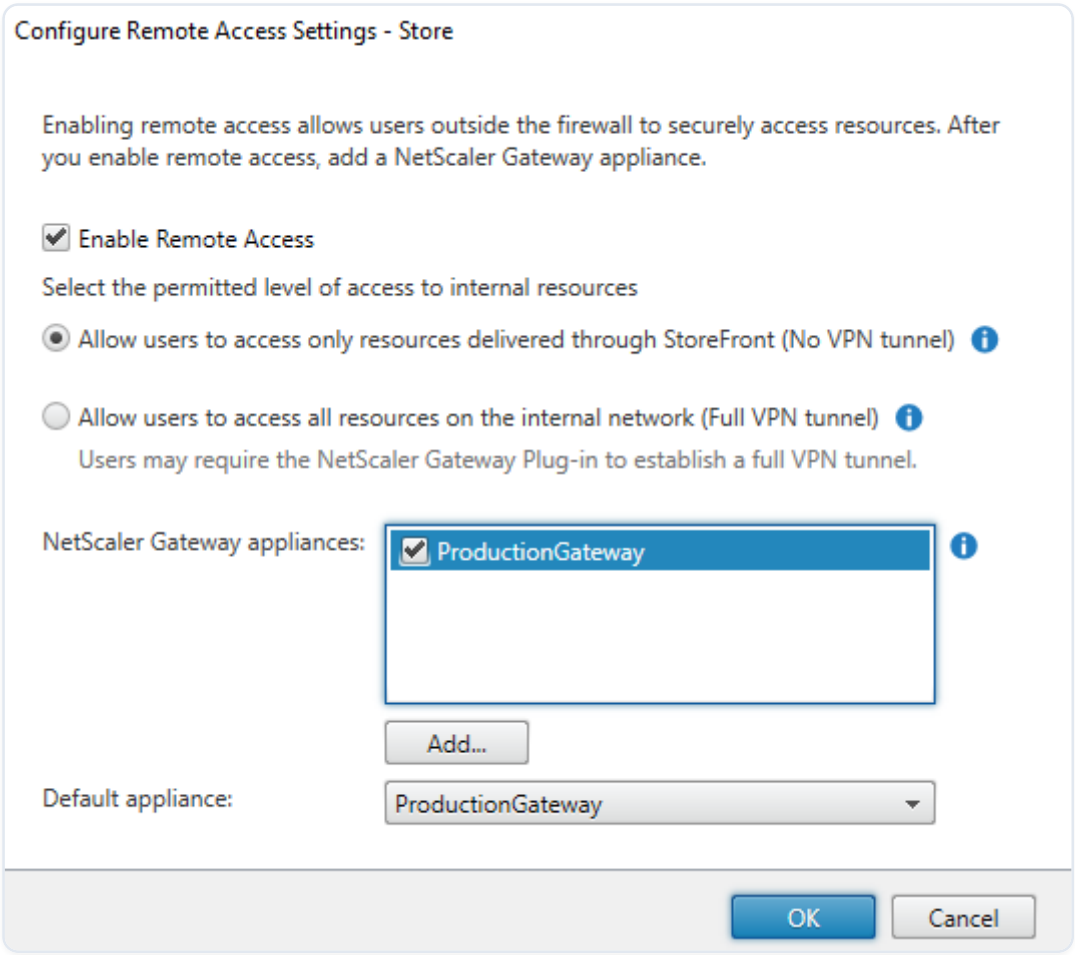
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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.

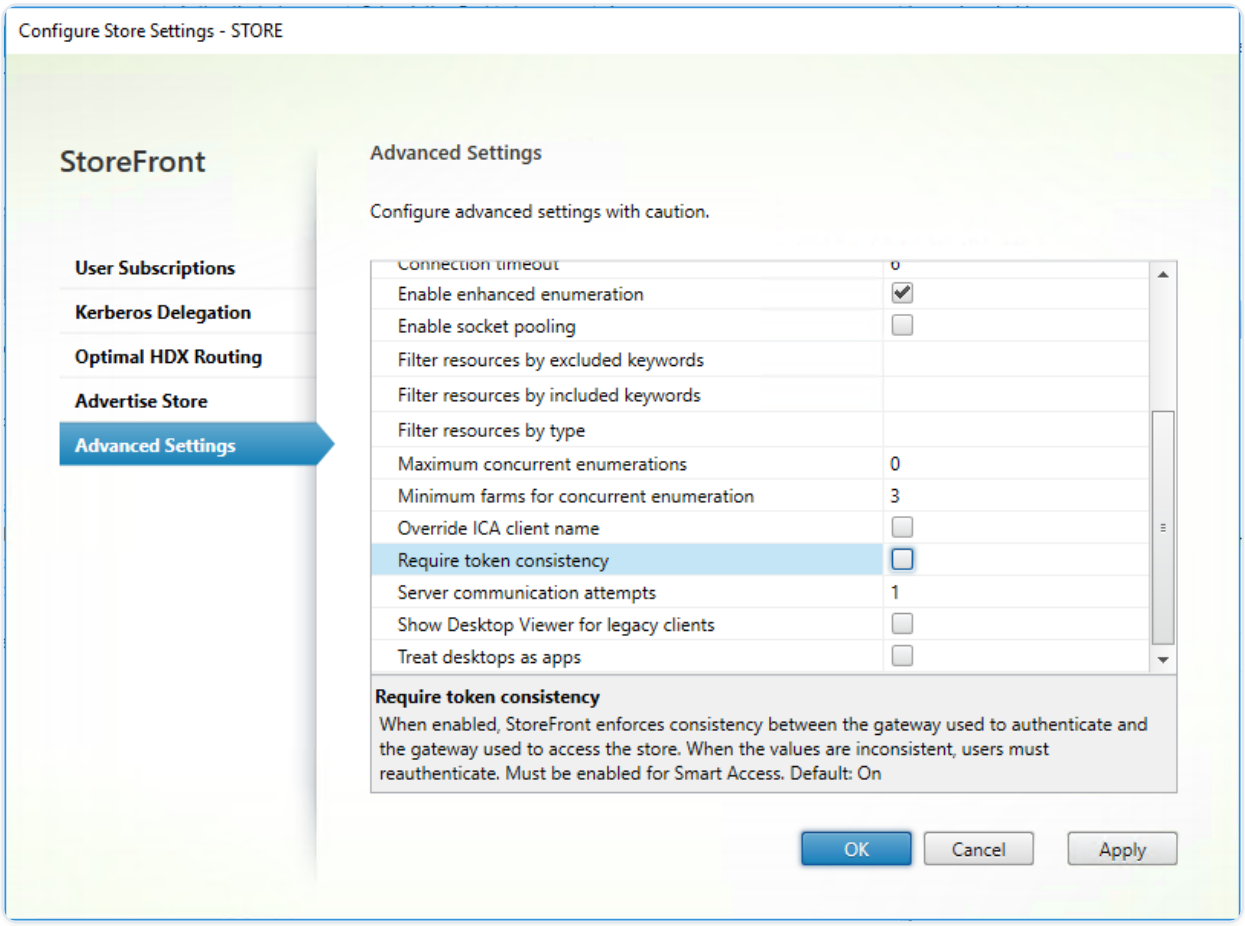
© 1997–2026 Citrix Systems, Inc. All rights reserved.



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

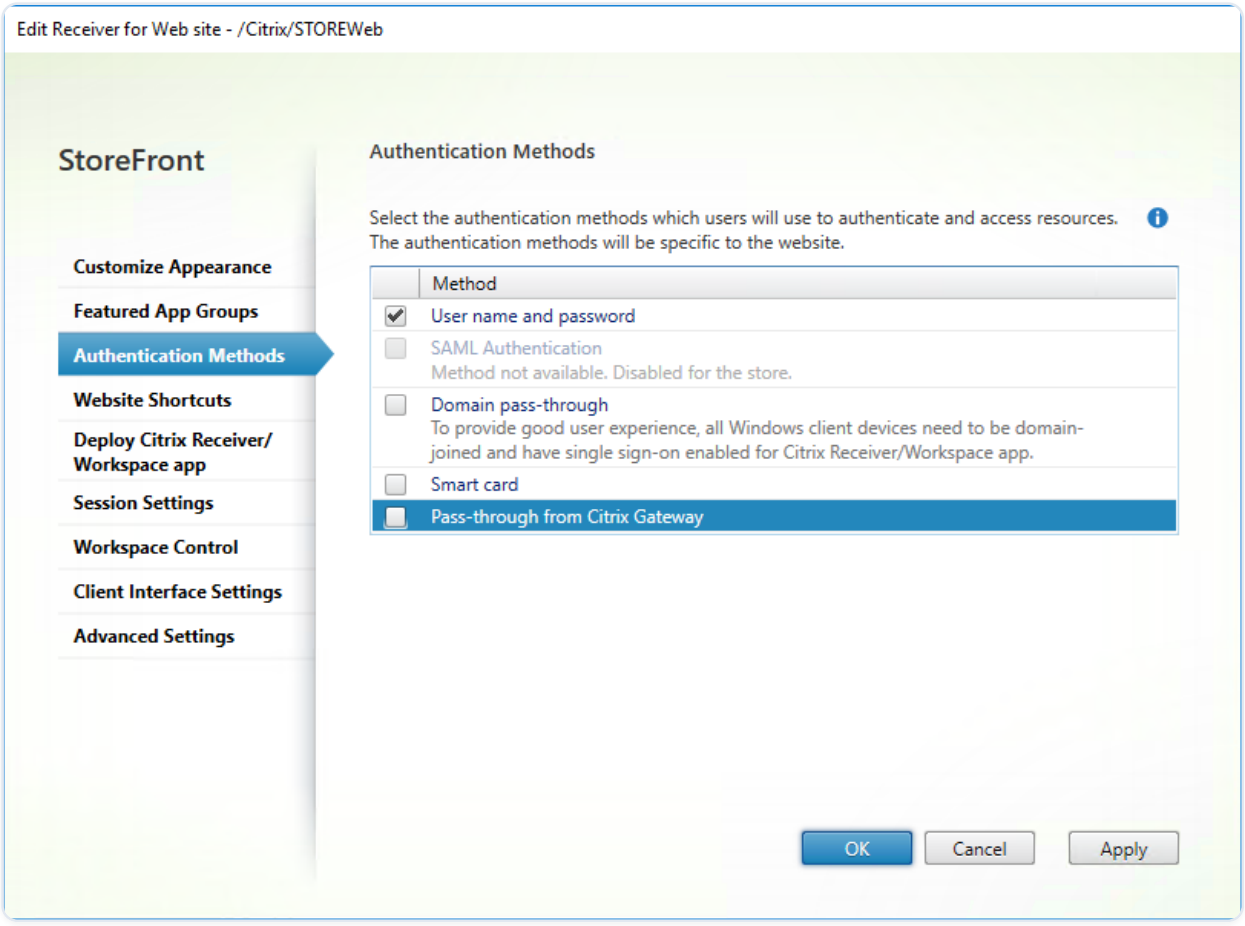
IMPORTANT:

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.

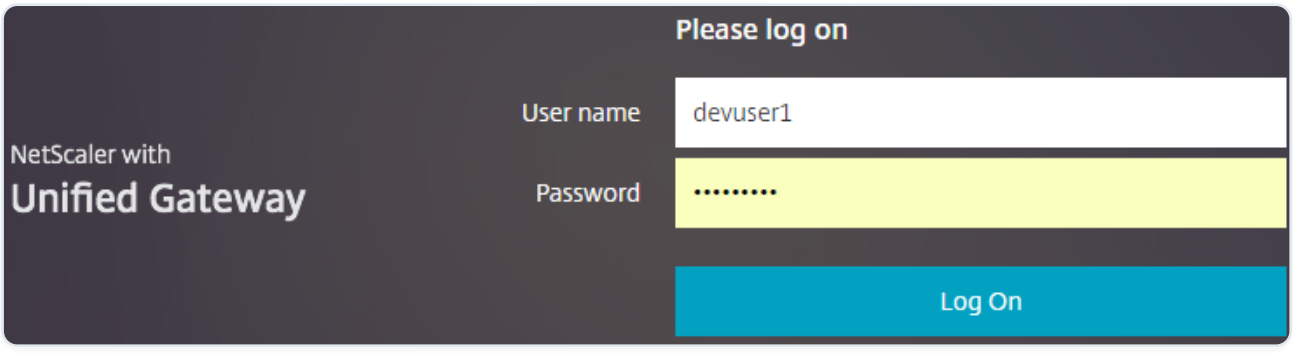
© 1997–2026 Citrix Systems, Inc. All rights reserved.

3. In the **Actions** pane, click **Manage Receiver for Web Sites**.
4. In Authentication Methods, clear **Pass-through from Citrix Gateway**.
5. Click **OK**.



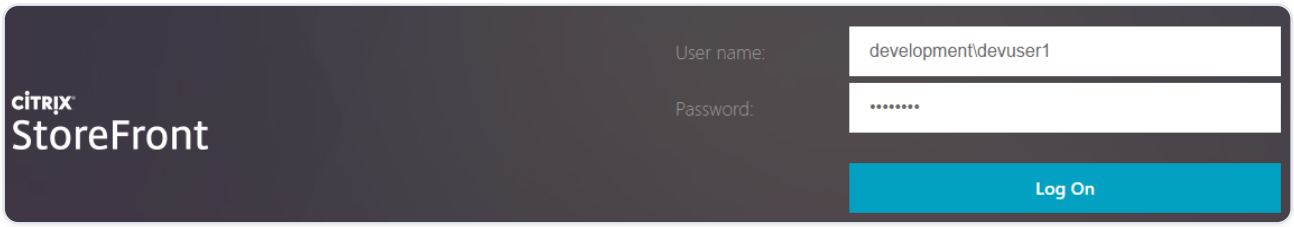
Log on to Gateway using a `production.com` user and credentials

To test, log on to Gateway using a `production.com` user and credentials.



After logon, the user is prompted to enter `development.com` credentials.

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

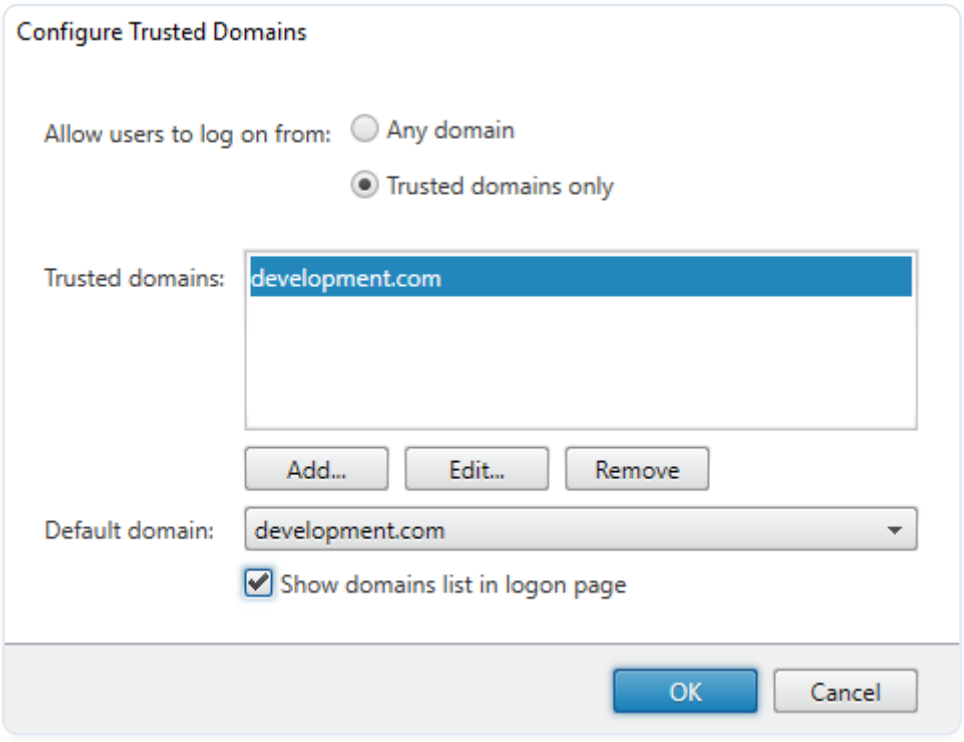


Add a trusted domain drop-down list in StoreFront (optional)

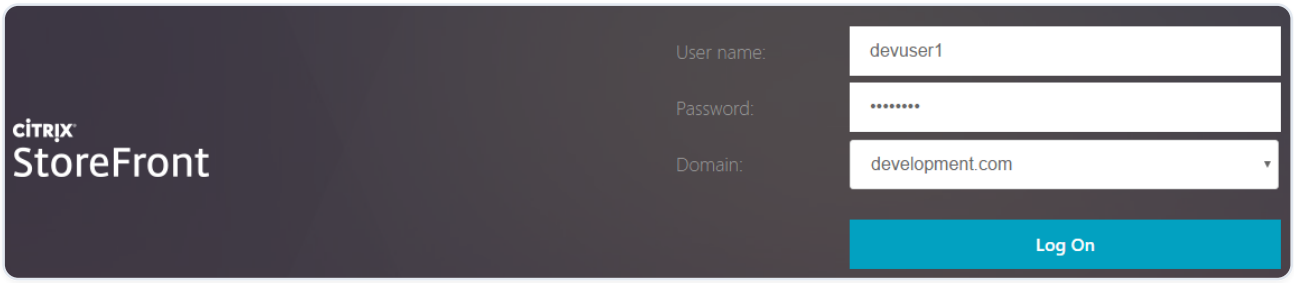
This setting is optional, but it may help prevent the user from accidentally entering the wrong domain to authenticate through the Citrix Gateway.

If the user name is the same for both domains, entering the wrong domain is more likely. New users may also be used to leaving out the domain when they log on through the Citrix Gateway. Users may then forget to enter domain\username for the second domain when they are prompted to log on to the Receiver for Web site.

1. Select **Stores** in the left pane of the Citrix StoreFront management console, and in the **Actions** pane, click **Manage Authentication Methods**.
2. Select the drop-down arrow next to **User name and password**.
3. Click **Add** to add `development.com` as a trusted domain, and select the **Show domains list in logon page** check box.
4. Click **OK**.



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



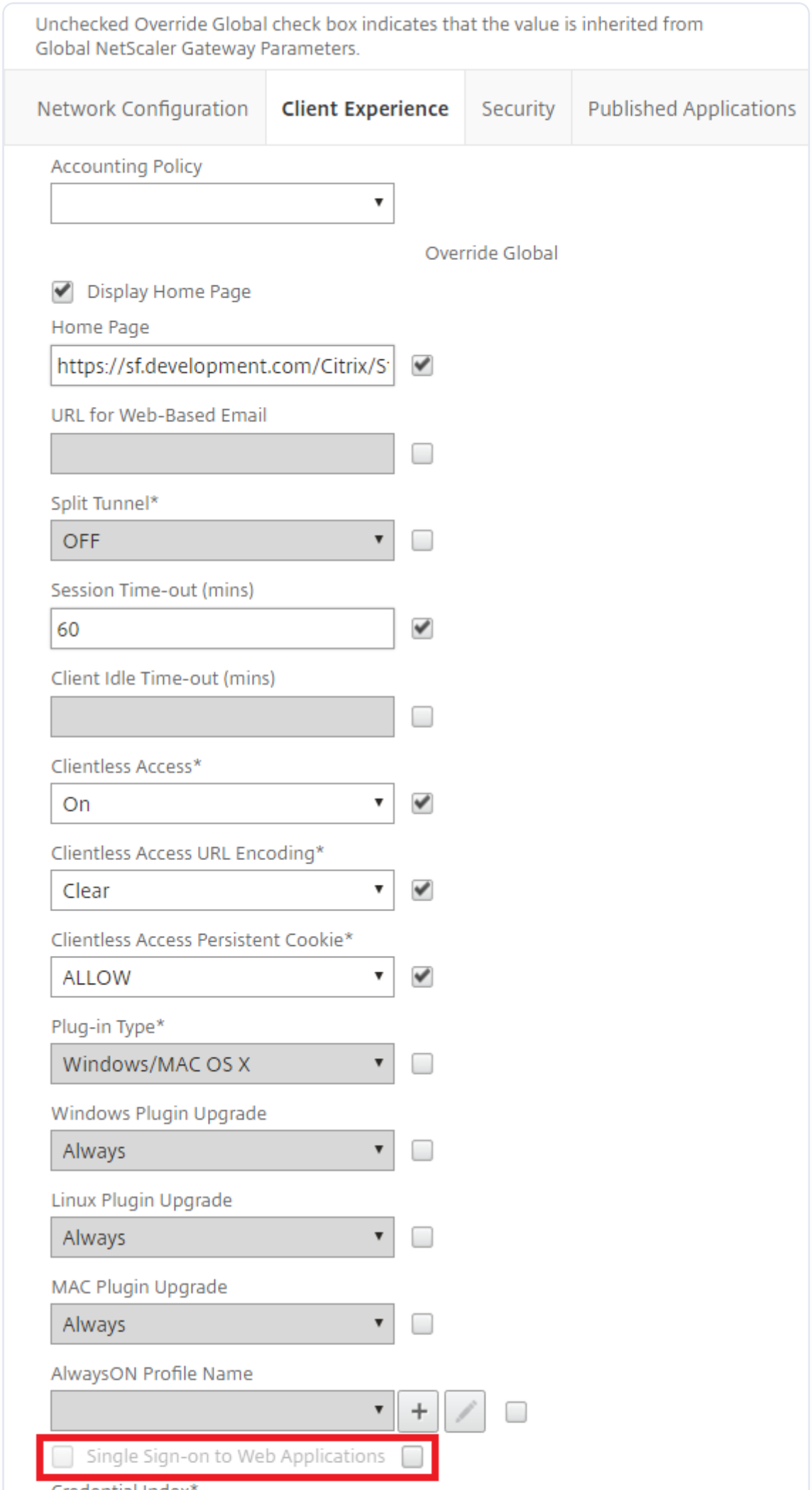
NOTE:

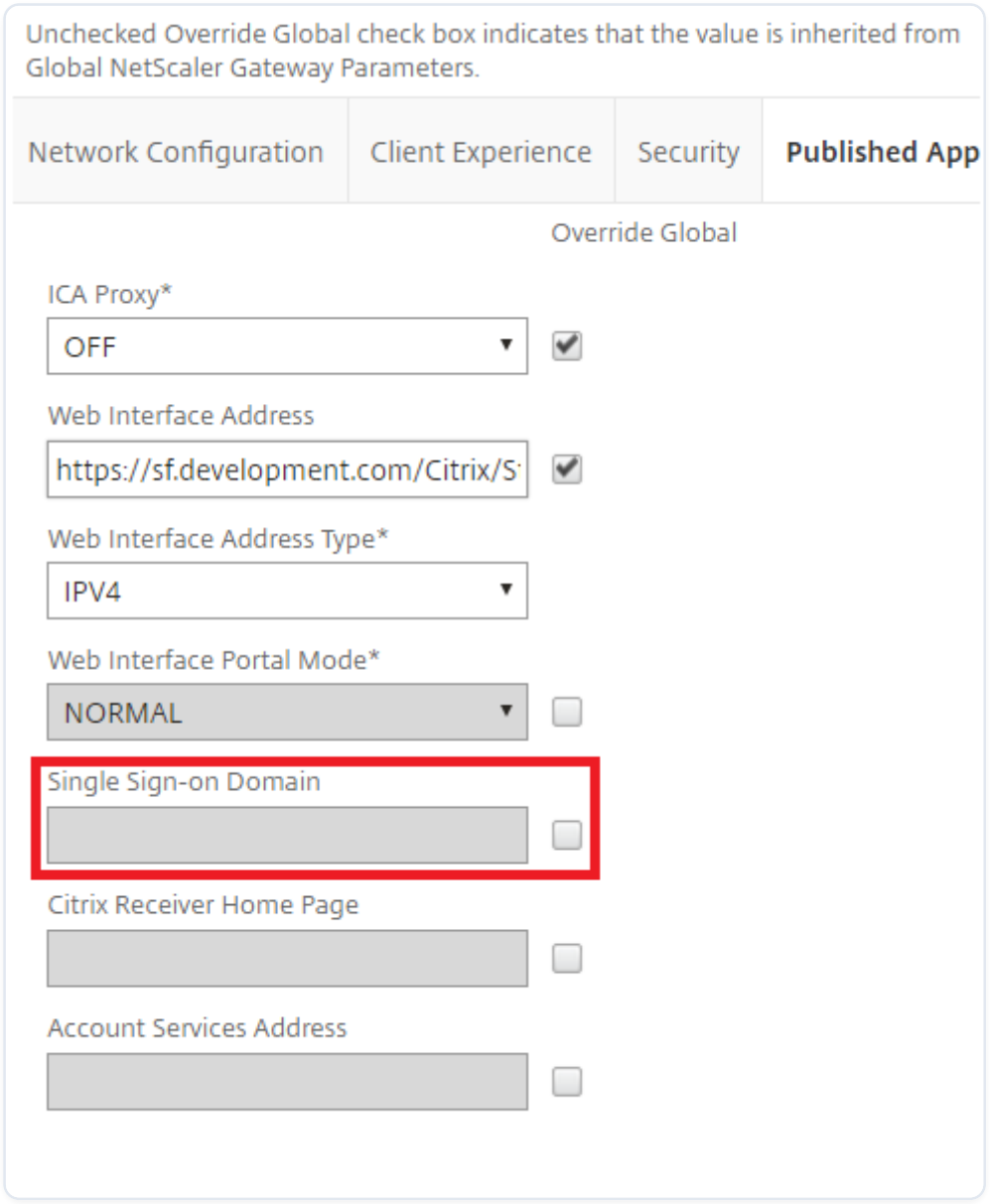
Browser password caching is not recommended in this authentication scenario. If users have different passwords for the two different domain accounts, password caching can lead to a poor experience.

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:

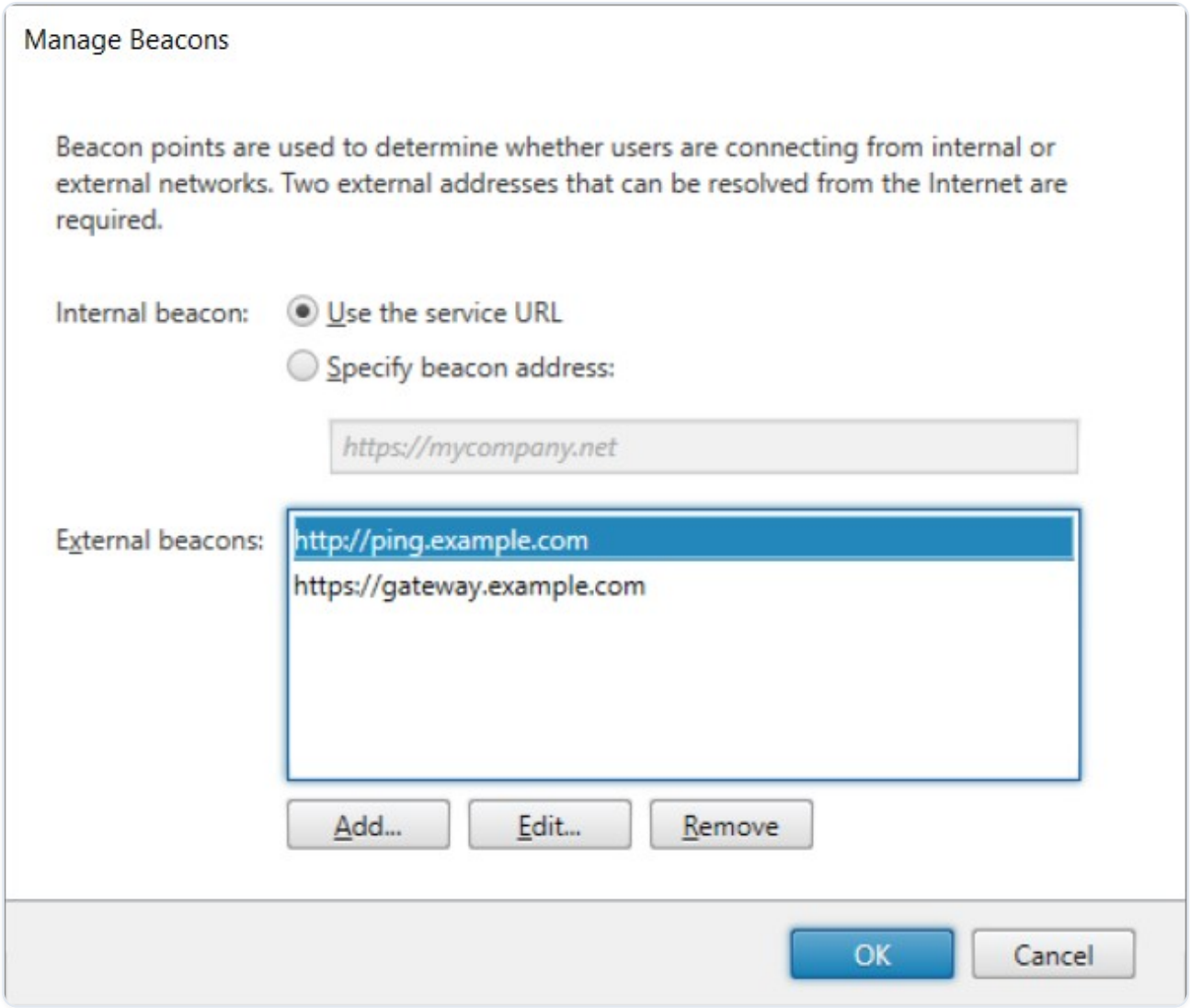
`http://ping.citrix.com` is no longer available and should not be used.

Do not use third party websites that you do not own as an external beacon. Instead use websites controlled by your organization.

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

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

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 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.

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

- 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 SDK

To get the current beacons use Get-STFRoamingBeacon.

To add a beacon use Set-STFRoamingBeacon.

To set the beacons to their defaults, use Clear-STFRoamingBeacon.

Create a single FQDN used internally and externally

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.

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

For example you could use the following URLs:

- `https://storefront.example.com` as the single URL used for users to access StoreFront. When inside the network it resolves to the StoreFront server or load balancer. When outside the network it resolves to the gateway.
- `https://storefrontcb.example.com` as the callback URL. When inside your network this resolves to the gateway.This is only required for smart access or password-less authentication. You must ensure that the certificate on the gateway includes this address as a SAN, or use a wildcard certificate.

Server Group base URL

Change the base URL to be the single URL. See Change the base URL for a deployment.

StoreFront beacons for locally installed Citrix Workspace app

Locally installed Citrix Workspace™ app attempts to contact beacon points and uses the responses to determine whether users are connected to local or public networks.

By default, StoreFront uses the server group base URL as the internal beacon URL. In this configuration, the same URL is valid both internally and externally so cannot be used as a beacon. Therefore, you must set the internal beacon to a URL that you know is only accessible internally.

See Configure beacon.

External DNS

- storefront.example.com resolves to the externally facing IP of the Citrix Gateway Virtual Server.

Internal DNS

- storefront.example.com resolves to the storefront load balancer or single StoreFront server IP.
- storefrontcb.example.com resolves to the gateway vServer VIP. If a firewall exists between the DMZ and the enterprise local network, allow for this.

Require Citrix Workspace™ app to connect through a gateway

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

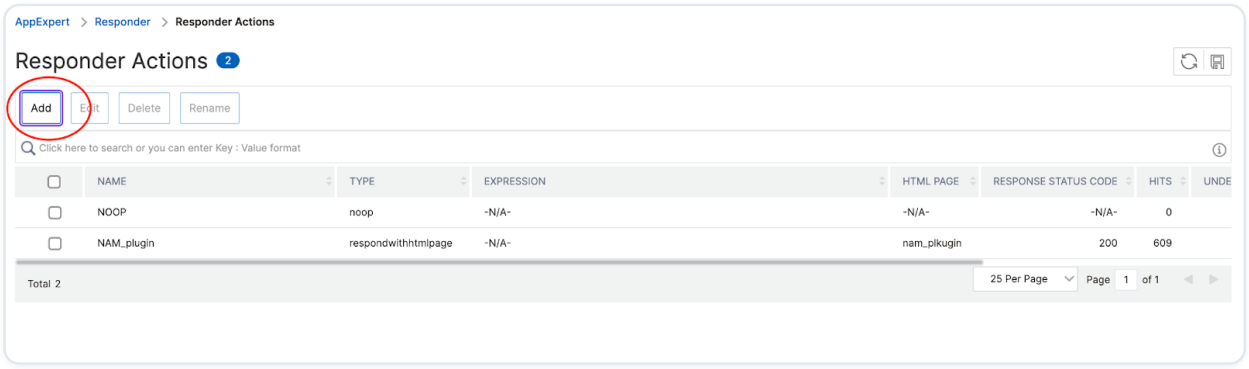
To deploy the plug-in to your gateway:

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

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.

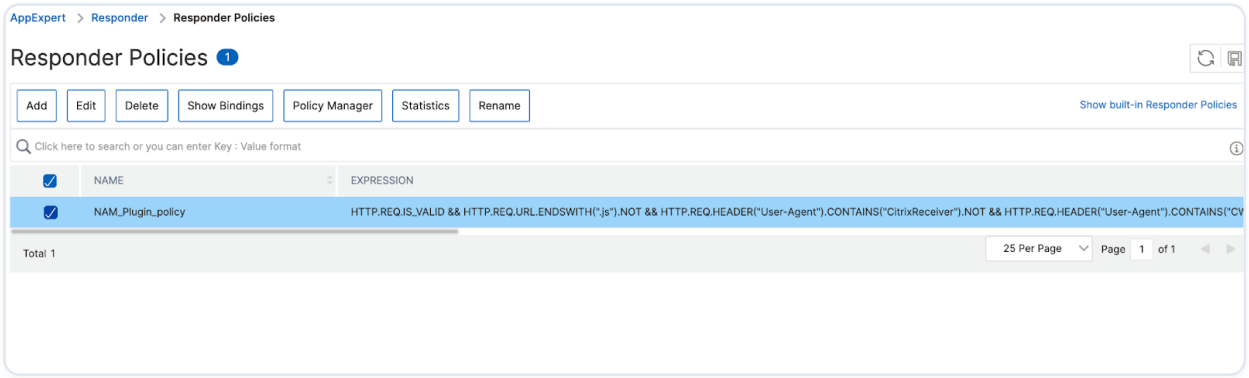


3. Configure the responder action:

   Type: Respond with HTML page

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

4. Create a responder policy.



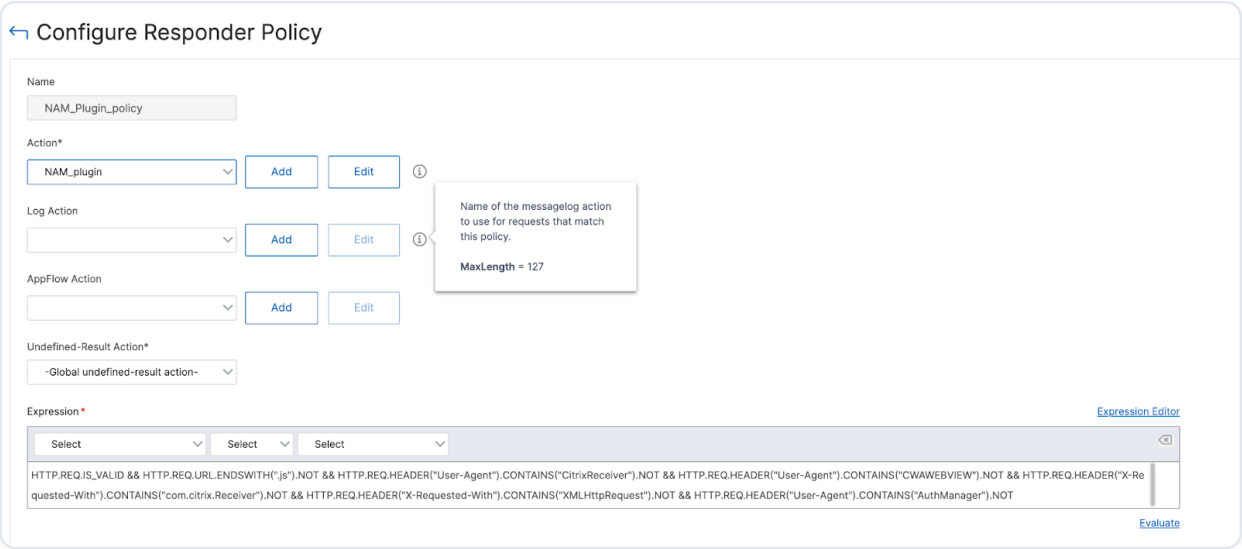
5. Configure the responder policy:

   Action: The name of the action you created above.

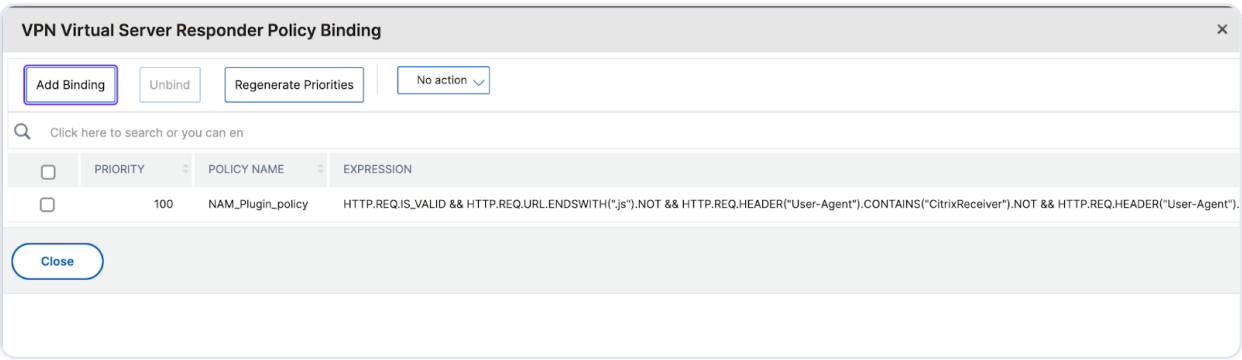
   Expression: `HTTP.REQ.IS_VALID && HTTP.REQ.URL.ENDSWITH(".js").NOT && HTTP.REQ.HEADER("User-Agent").CONTAINS("CitrixReceiver").NOT &&`

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

```
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
```

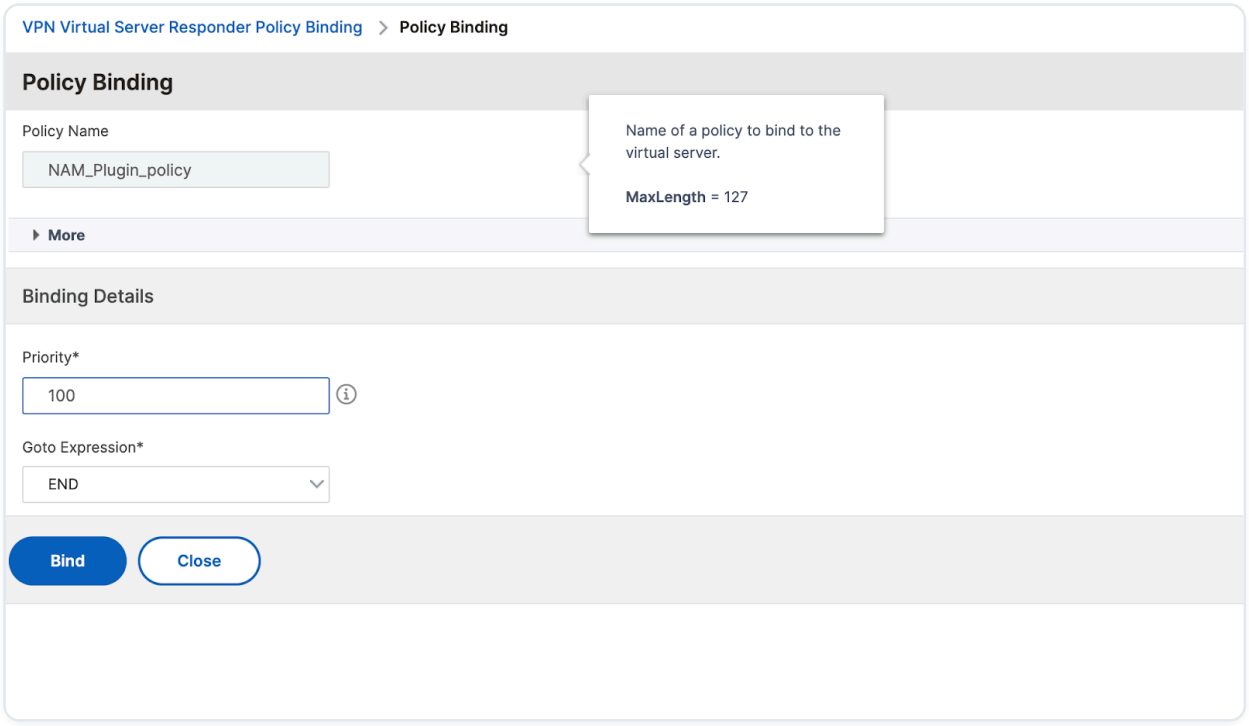


6. Navigate to the virtual server where you want to bind the responder policy.



7. Bind the policy you created.

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



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
```

3. Bind the policy to the VPN vserver

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

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

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

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

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

PARAMETER	DESCRIPTION
	base URL from the exporting server. Example: `https://<importingserver>.example.com`

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:

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

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

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

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.

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

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

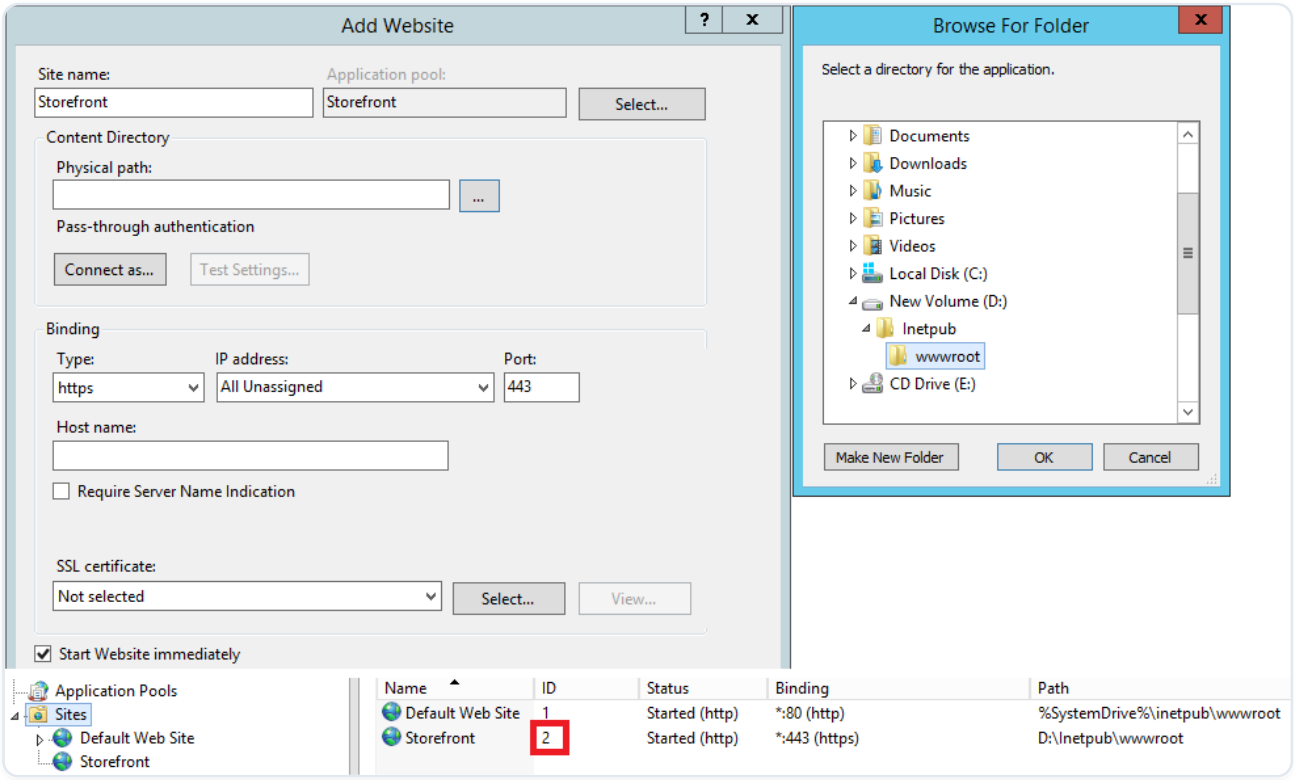
Copy the backup.zip file to the desktop of server B.

```
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\wwwrooot`.



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**.

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

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.

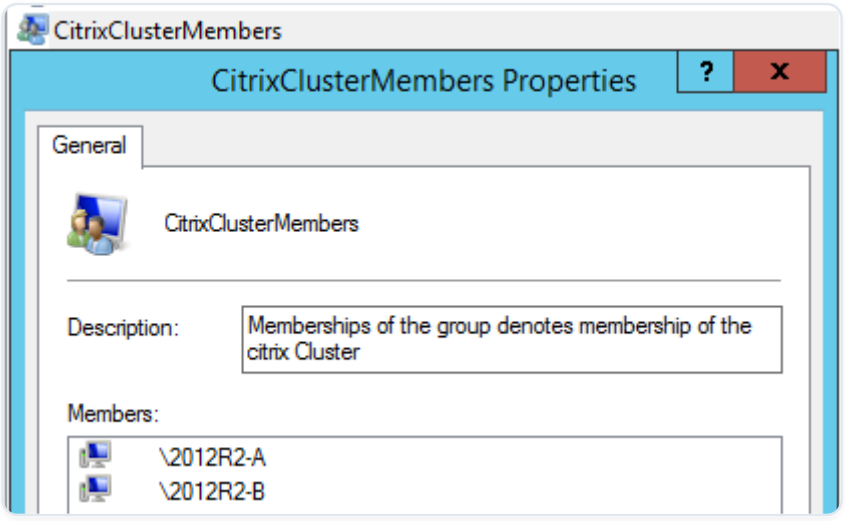
```
Import-STFConfiguration -configurationZip
"$env:userprofile\desktop\backup.ctxzip" -HostBaseURL "https://
serverB.example.com"
```

Server group scenarios

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

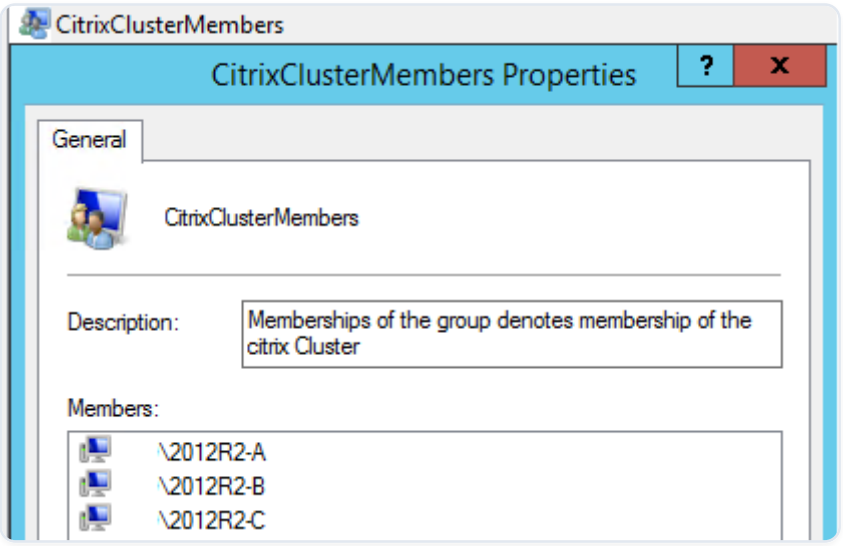
A previous configuration backup was taken while only two StoreFront servers, 2012R2-A and 2012R2-B, were members of the server group. Within the backup archive is a record of the **CitrixClusterMembership** at the time the backup was taken containing only the two original servers 2012R2-A and 2012R2-B. 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 = "Pa55w0rd"

$Password = $Password | ConvertTo-SecureString -asPlainText -Force

$CredObject = New-Object System.Management.Automation.PSCredential($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 = "Pa55w0rd"
```

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

```
$Password = $Password | ConvertTo-SecureString -asPlainText -Force

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



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

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

User experience

Users can view the stores either in a web browser or Citrix Workspace app. See User access.

StoreFront provides the following user experiences:

Modern user experience

The modern user experience is consistent with Citrix Workspace. It incorporates Activity Manager for managing your sessions and improved searching. Prior to CU2, the modern experience is available as a preview and not recommended for use in production environments.

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.
- The Workspace Control feature that lets end users connect back to their sessions from a remote device is not available.
- Users cannot change their password.
- Deep customizations using JavaScript and css with the StoreFront™ Client UI Customization API.

For more information, see Modern experience

Classic user 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.

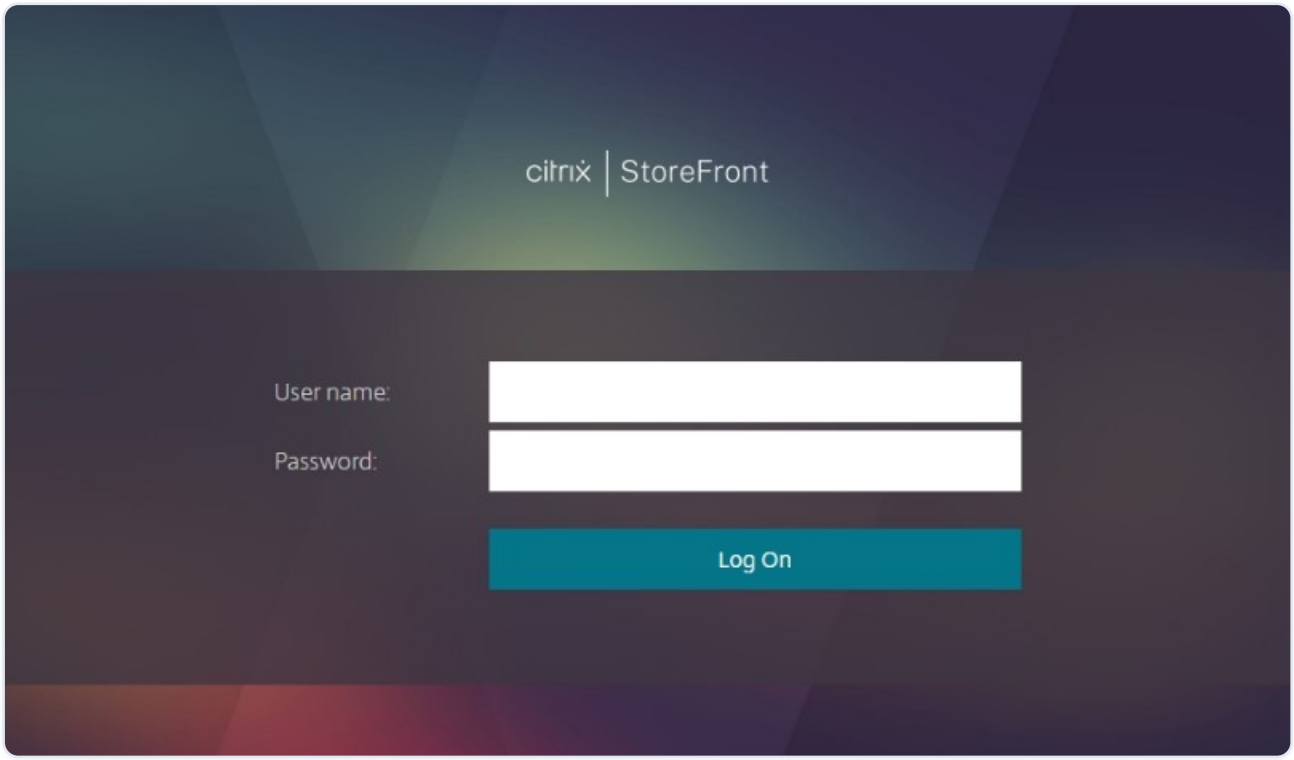
© 1997–2026 Citrix Systems, Inc. All rights reserved.

Classic experience

This section describes how users can access and interact with their stores using the classic experience, previously known as the unified 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

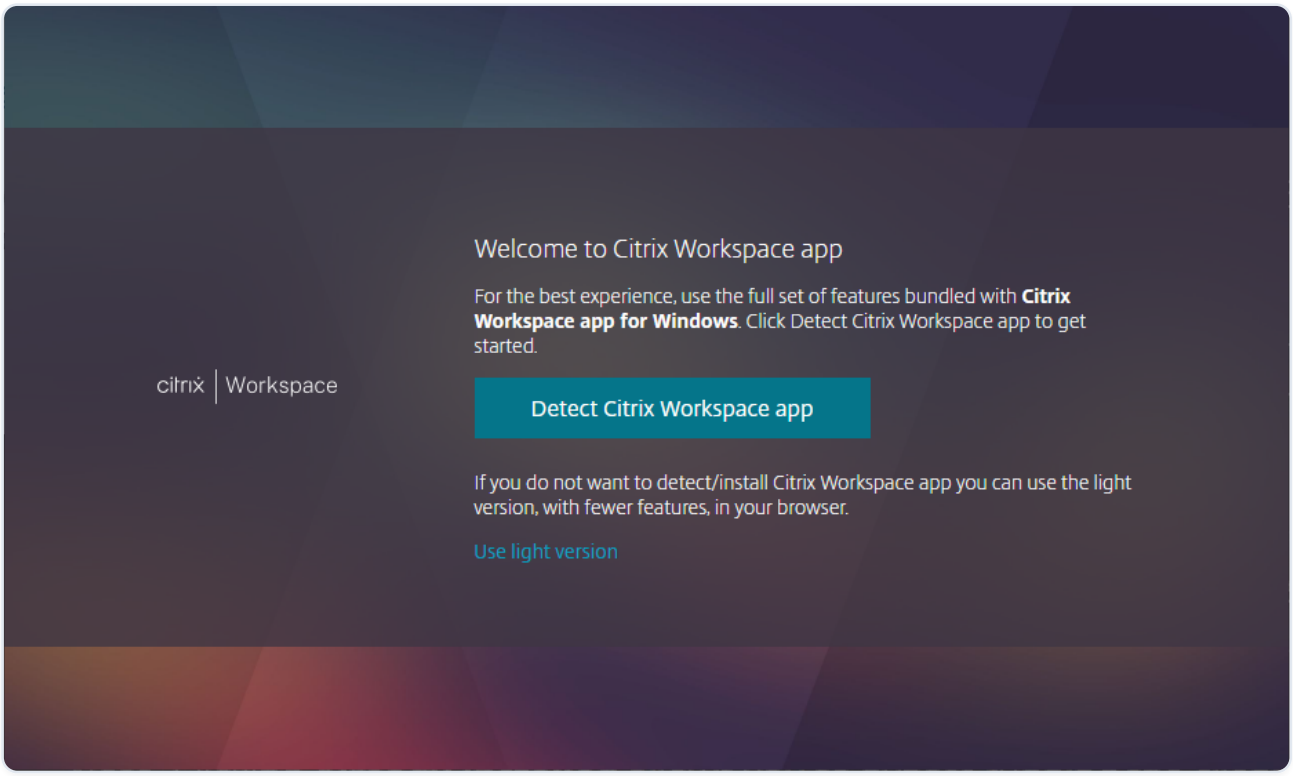
NOTE:

This section only applies when accessing the store through a web browser, and the deployment option is set to **Install locally** or **Use Receiver for HTML5 if local Receiver is unavailable**. This step may occur before or after log on depending configuration.

If Citrix web extensions 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 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.

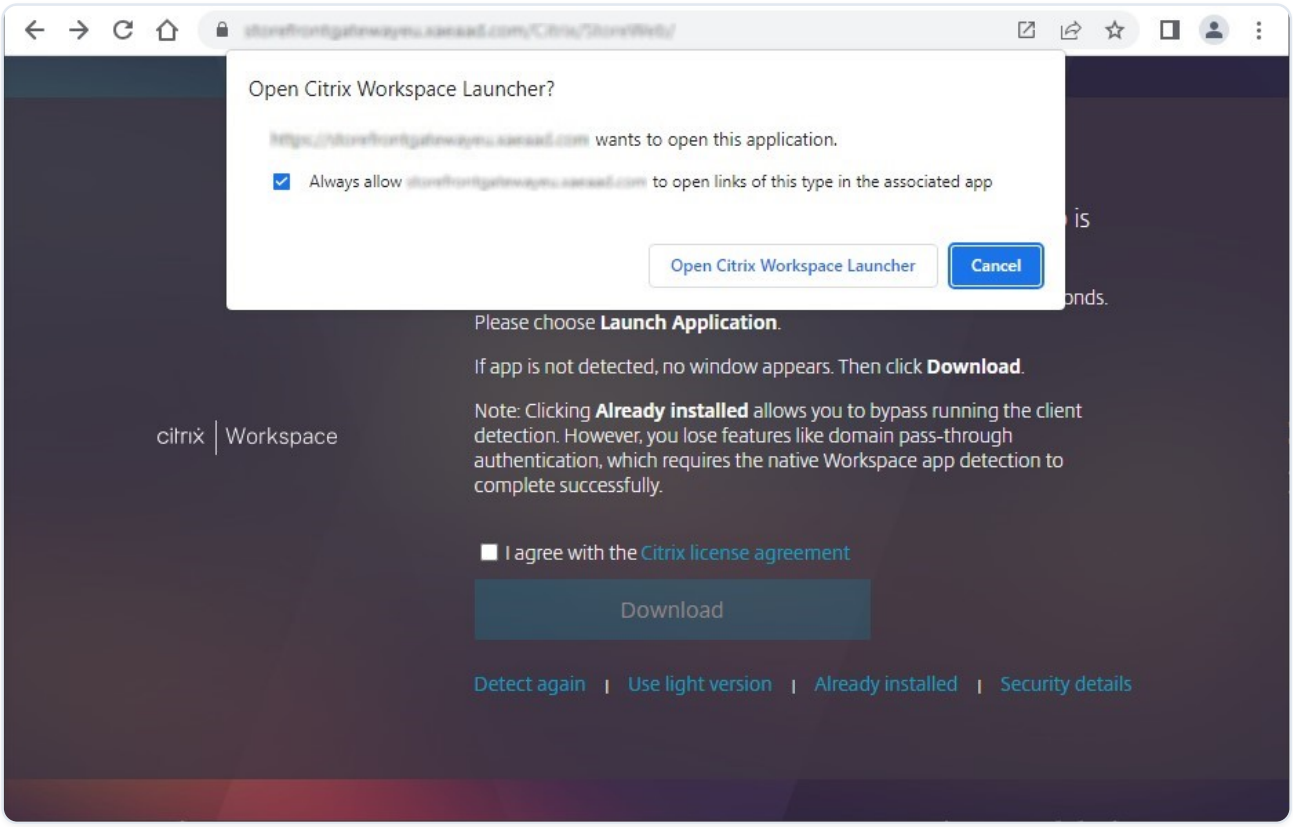


They can either:

- Select **Detect Citrix Workspace app** to launch resources in the locally installed Citrix Workspace app. This is recommended for the best experience.
- Select **Use light version** to always launch resources within the browser. This option is only available if the deployment option is set to **Use Receiver for HTML5 if local Receiver is unavailable**.

When the user selects **Detect Citrix Workspace app**, it attempts to open **Citrix Workspace Launcher** which is a component of Citrix Workspace app. If Citrix Workspace app is installed then their browser pops up a window asking to run the **Citrix Workspace Launcher**. They should select **Open Citrix Workspace Launcher**, **Open link**, **Open**, or **Always open** (depending on the browser). It is recommended they also tick **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.

© 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 light version** - Skips Workspace app detection and always opens resources in the web browser. To show this option, set the Deployment option to **Use Receiver for HTML5 if local Receiver is unavailable**.
- **Already installed** - 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.

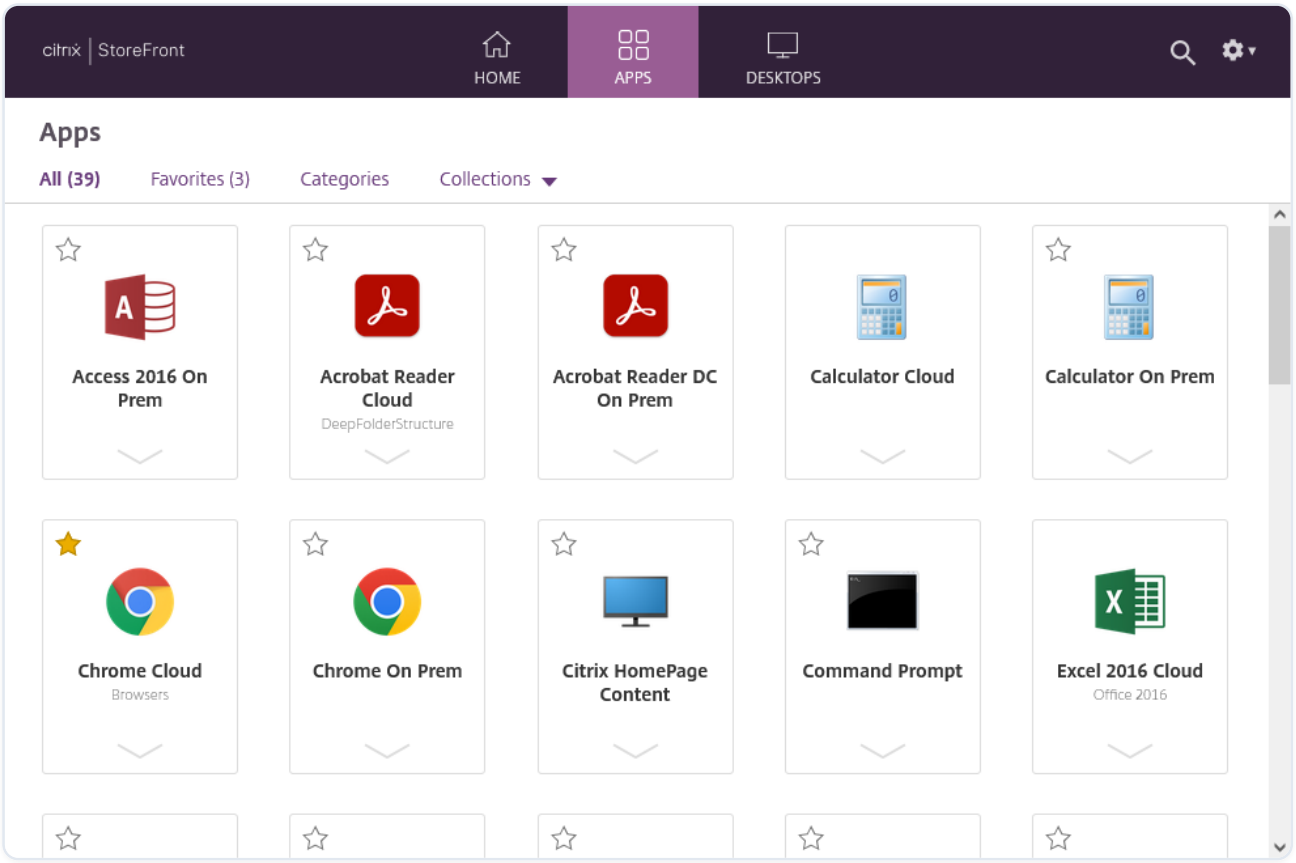


Apps tab

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.

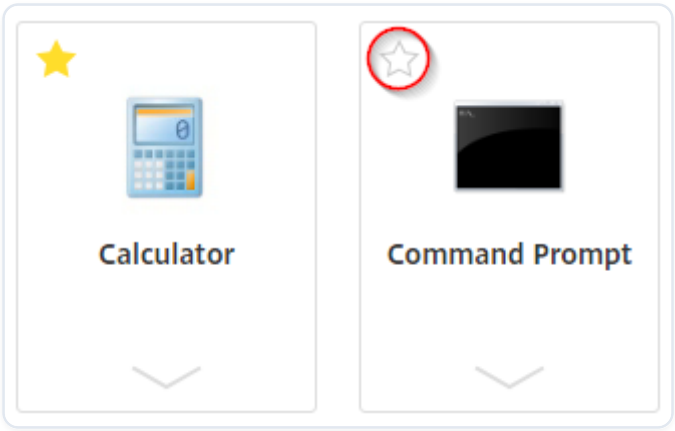
App and desktop tiles

Click on an icon to launch the app or desktop.

Favorites

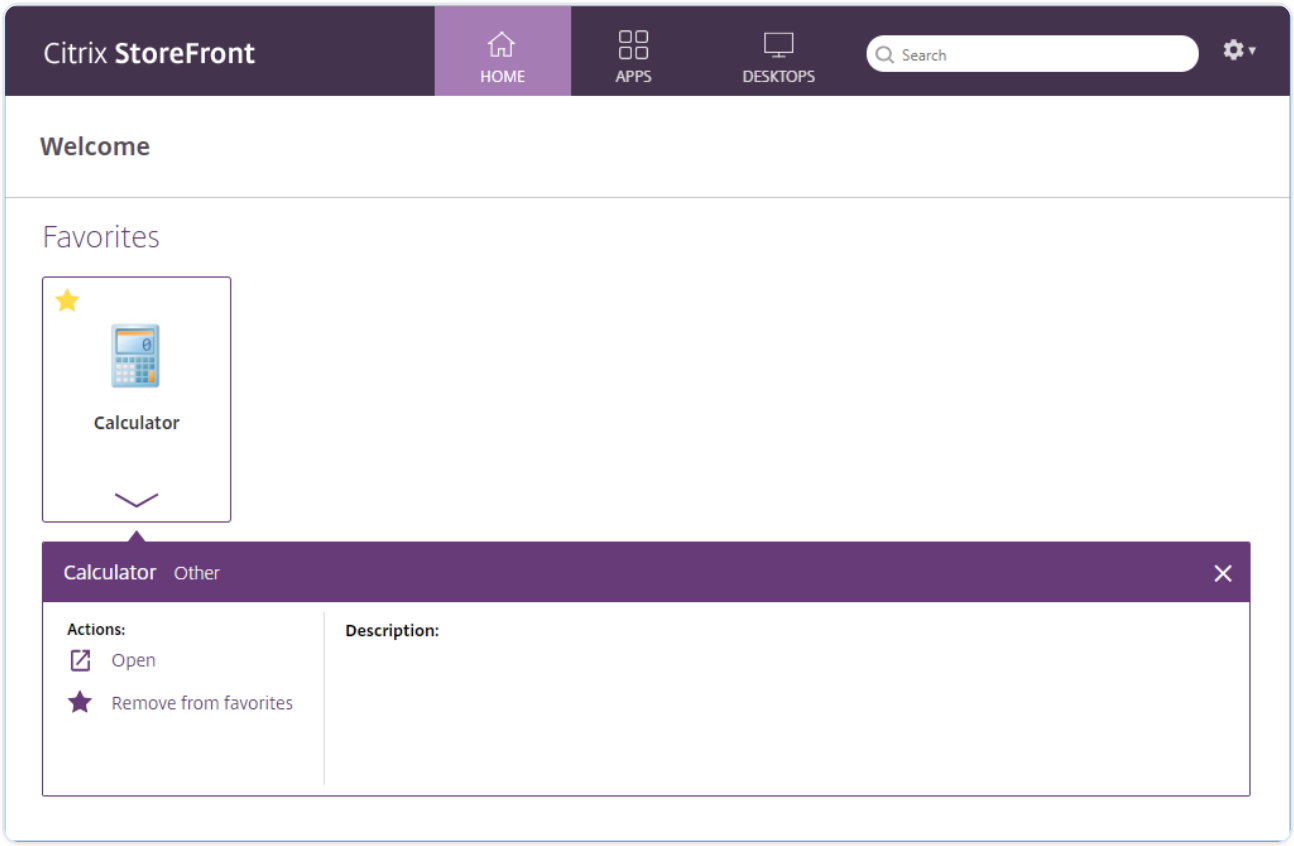
If favorites are enabled then the user can select star on a resource's tile to make it a favorite:

© 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.

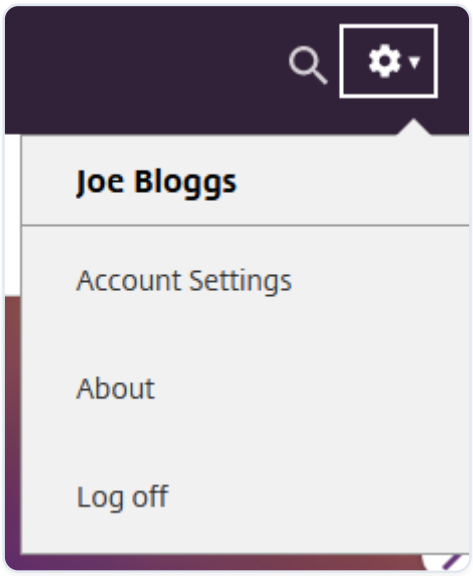
Search

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.

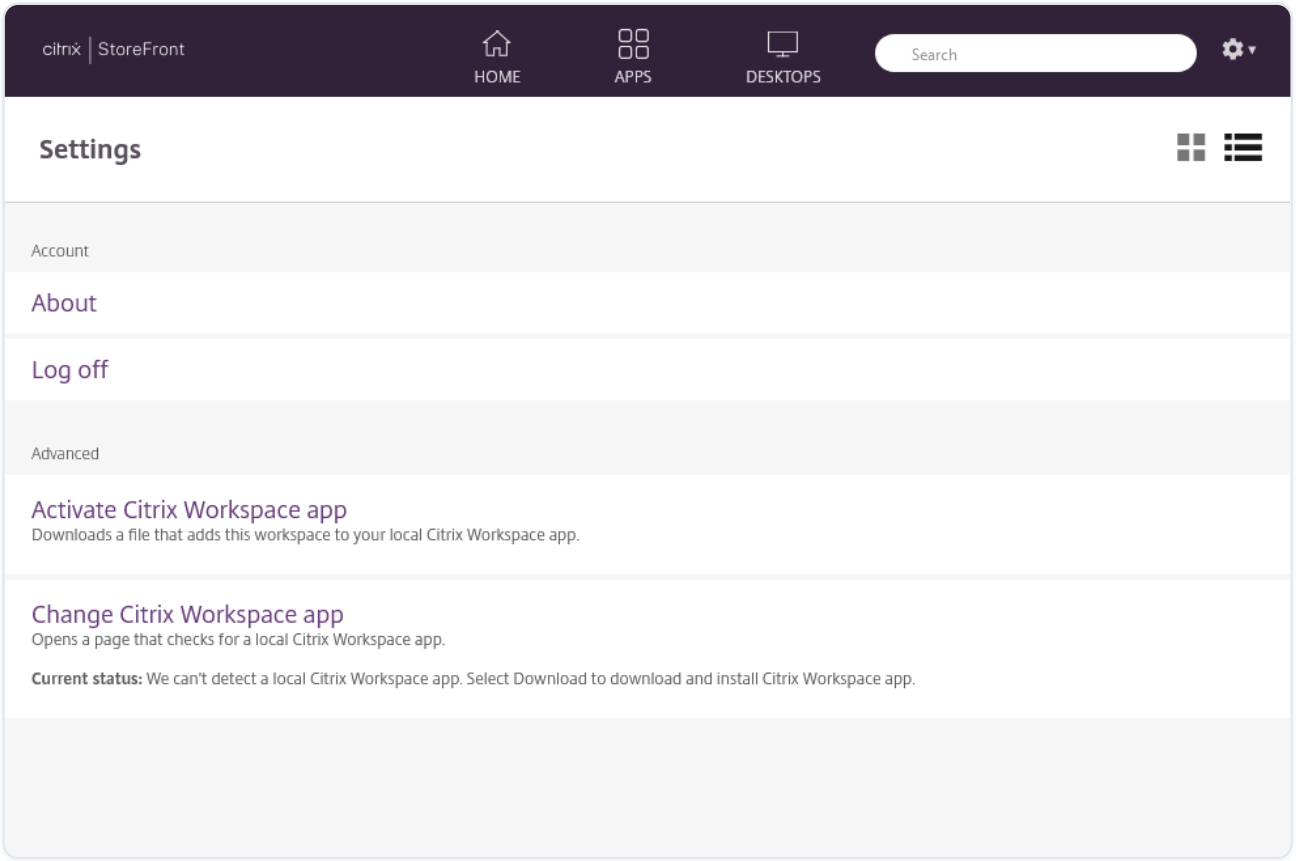


The settings menu has the following options:

- **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

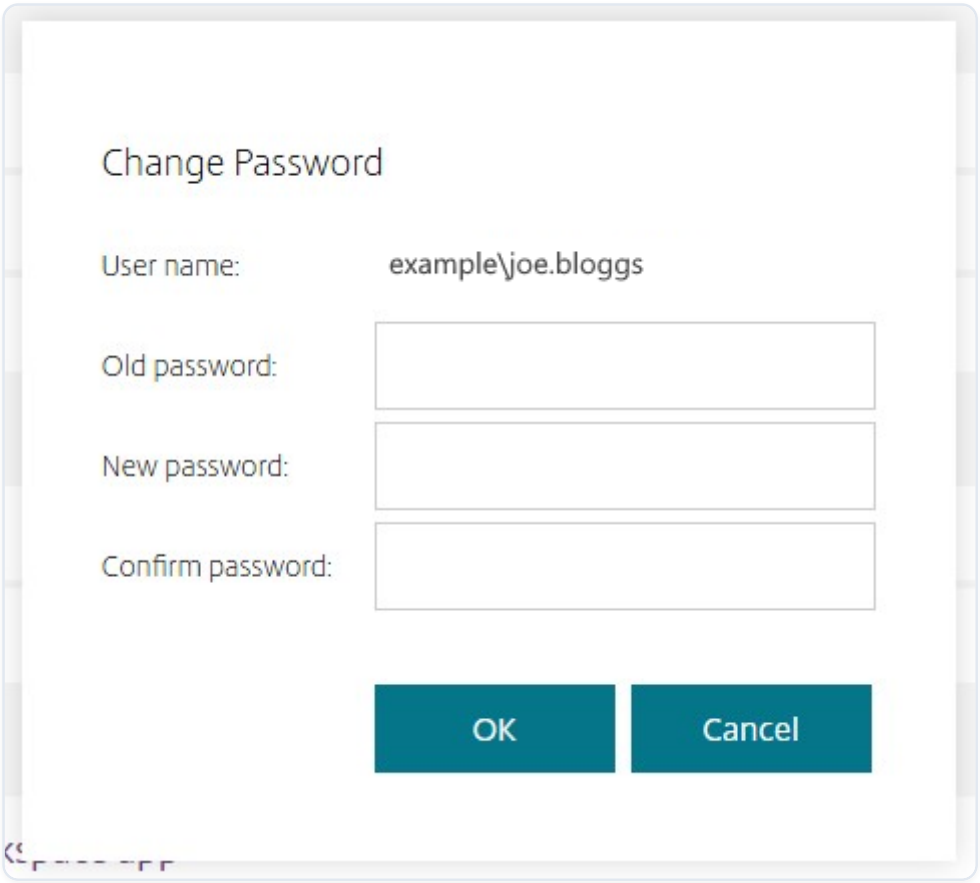


The account settings page may have the following sections.

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 Citrix Workspace app. Opens a page that checks for a locally installed Citrix Workspace app. This also allows users to switch between launching resources using the locally installed Citrix Workspace app, and launching them in a web browser.

© 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.

Modern experience

This section describes how users can access and interact with their stores using the modern experience, previously known as the next generation experience. The modern experience is not enabled by default. To enable it, see UI experience.

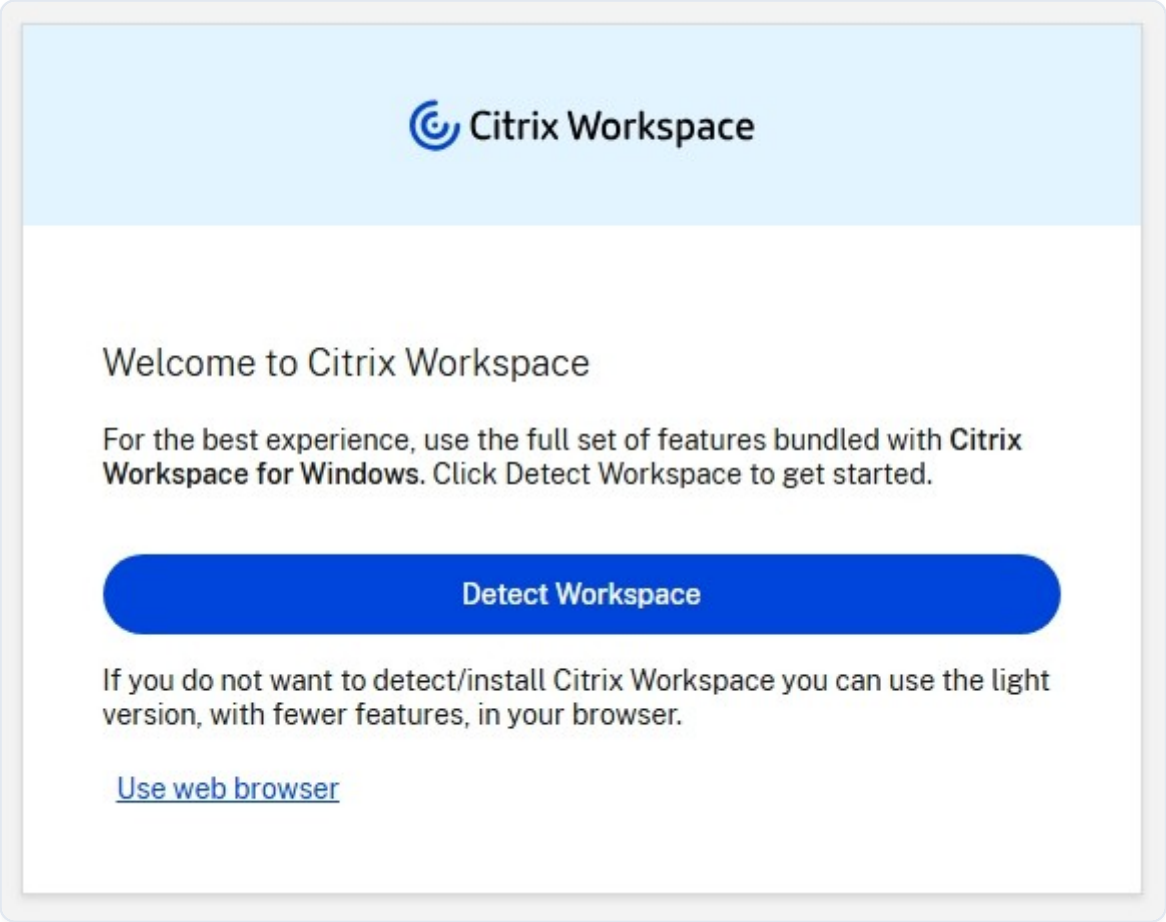
Citrix Workspace™ app detection

NOTE:

This step only applies when accessing the store through a web browser, and the Deployment option is set to **Install locally** or **Use Receiver for HTML5 if local Receiver is unavailable**. This step may occur before or after log in depending configuration.

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 Account settings page.
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.

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

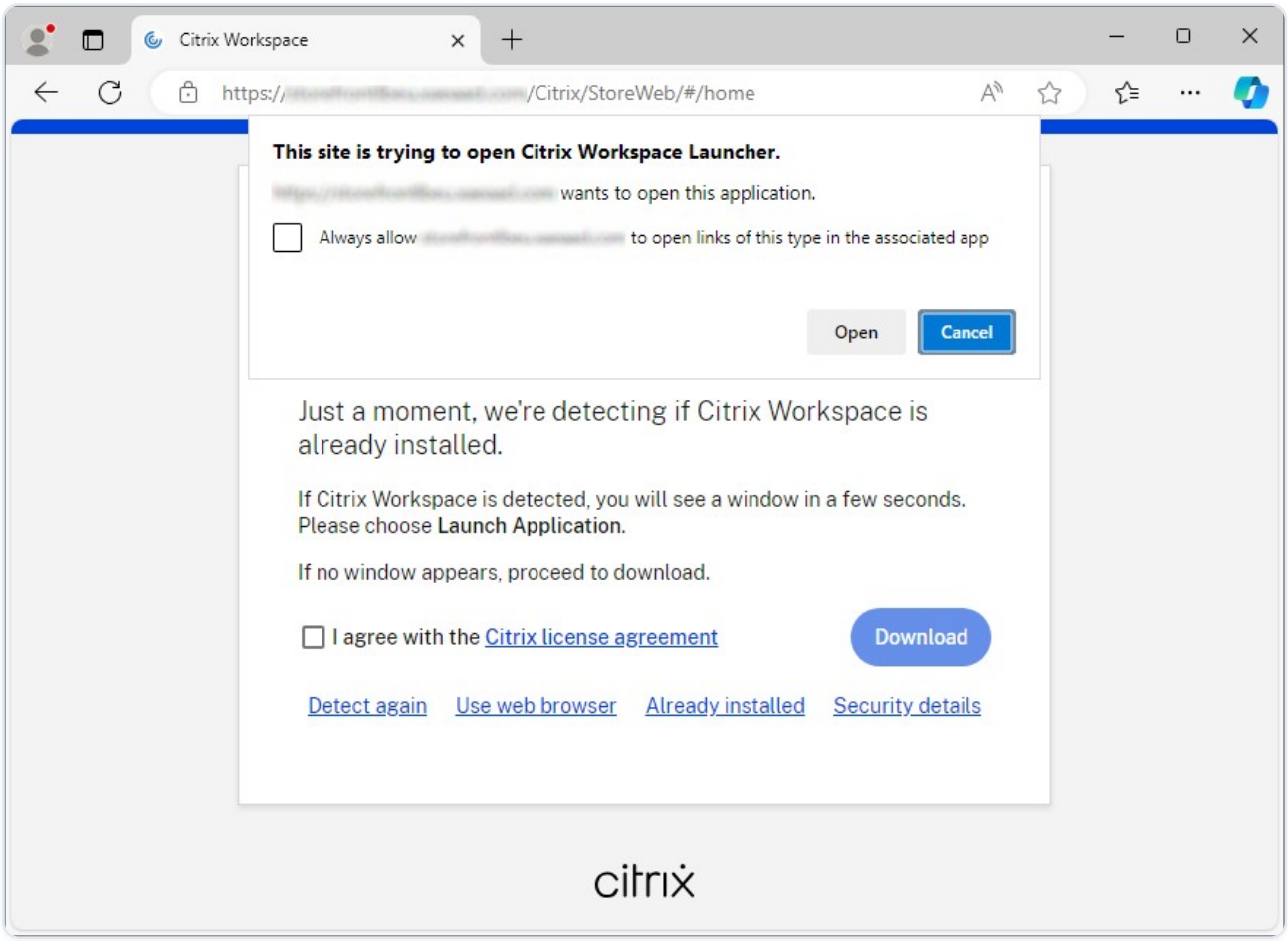


They can either:

- Select **Detect Citrix Workspace app** if they wish to launch resources in the locally installed Citrix Workspace app. This is recommended for the best experience.
- Select **Use web browser** to always launch resources within the browser. This option is only available if launch option is set to **Use Receiver for HTML5 if local Receiver is unavailable**.

When the user selects **Detect Citrix Workspace app**, the website 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.

© 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 resources in the locally installed Citrix Workspace app.

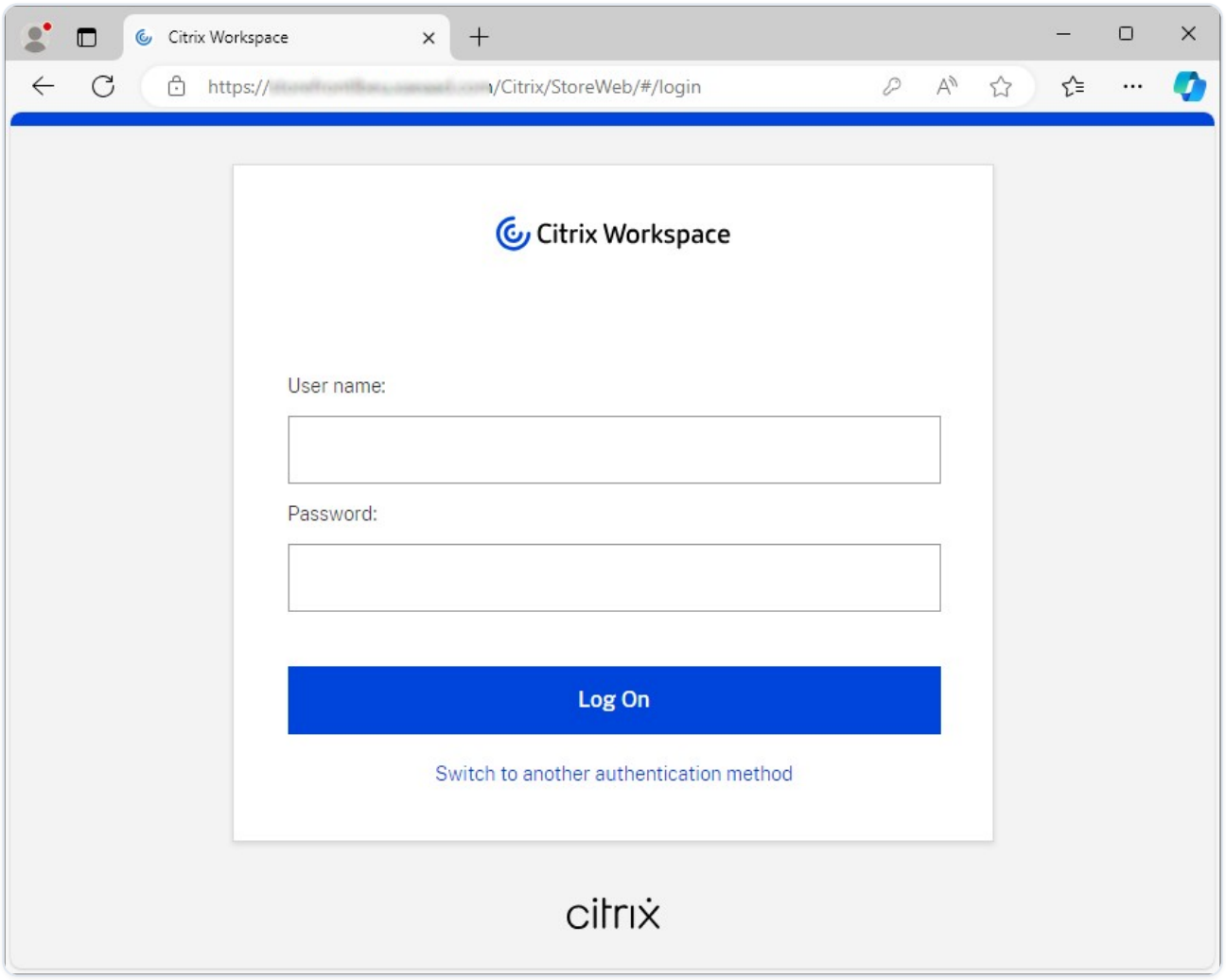
If Citrix Workspace app is not installed, or they cancel the launcher then depending on launch preferences they have the following options:

- **Download** - Downloads Citrix Workspace app from the Citrix website or from the StoreFront server.
- **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 Deployment option to **Use Receiver for HTML5 if local Receiver is unavailable**.
- **Already installed** - 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.

Log In

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.

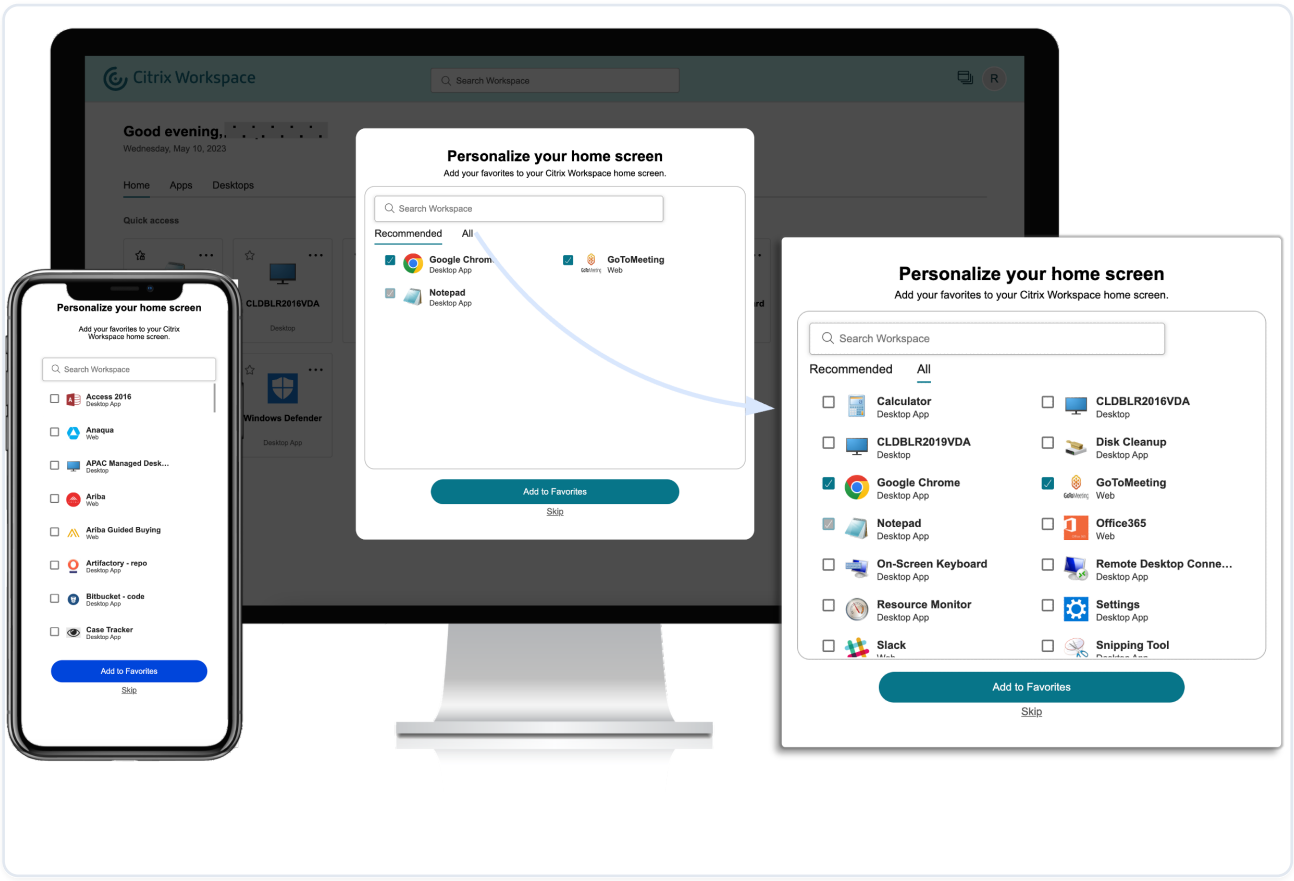
First-time user experience for Workspace app

When accessing the UI, for the first time, users are prompted with a pop-up where they can favorite multiple apps in one easy single step.

The first-time user experience is activated when users have more than 20 apps, and haven't added any of them to Favorites. The experience is supported on all browsers and native clients (Mac, Windows, Linux, and ChromeOS), and mobile devices (iOS and Android). To configure whether this window appears, see Display Personalize your home screen for first time users.

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

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

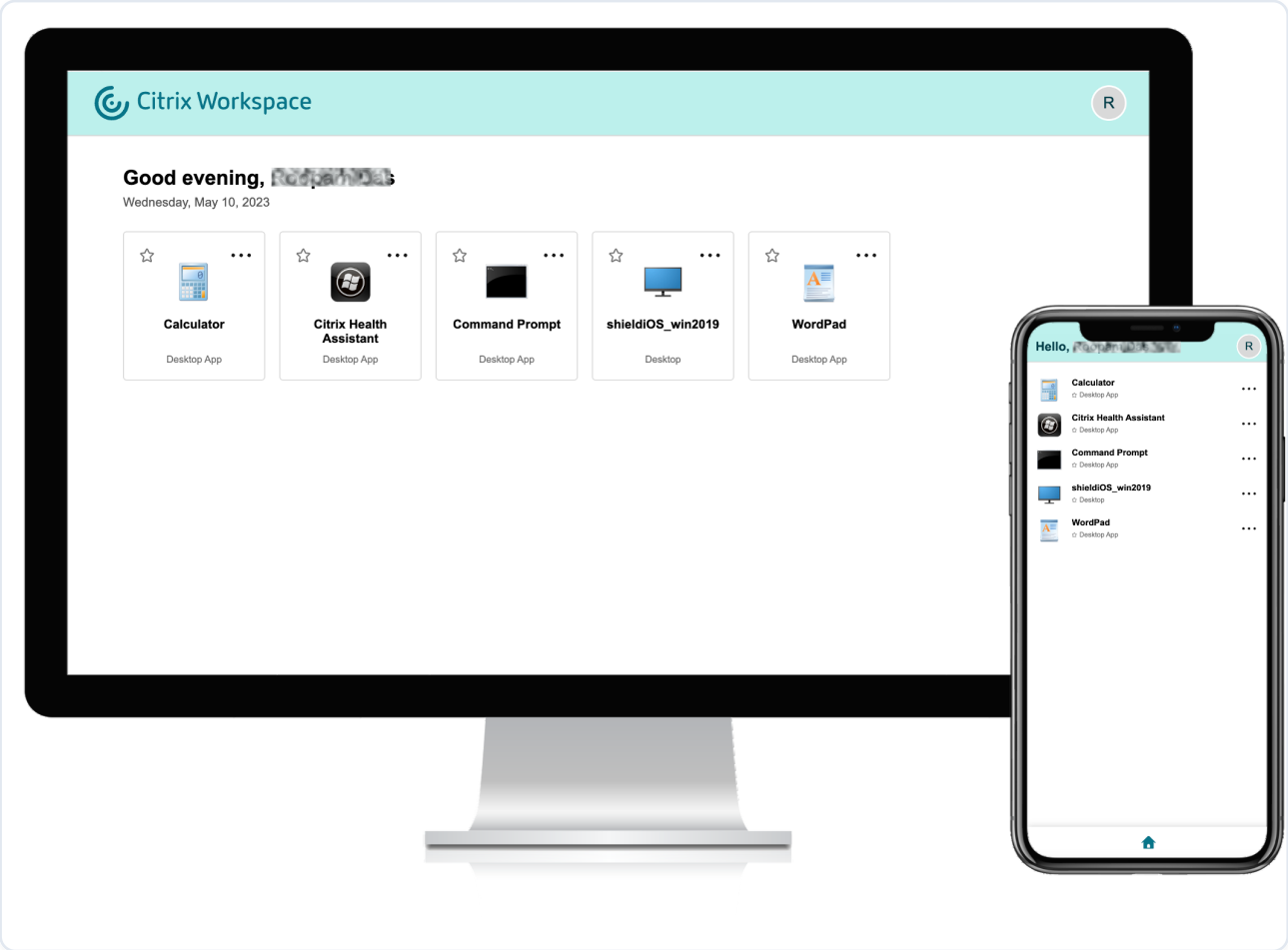
- The **Personalization** screen appears once per device and browser, and every time for incognito mode unless users mark a favorite.
- If the admin removes the mandatory or recommended tag from the apps, the apps in **Favorites** won't have any impact.
- If the end-user has not added any apps to **Favorites**, the **Personalization** screen appears each time the workspace app is opened. To avoid this:
  - 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.

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

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.



Full view

If users have more than 20 resources, up to three tabs are displayed - **Home**, **Apps** and **Desktops**. When a user logs in they land on the **Home** tab. The **Apps** and **Desktops** tabs are displayed if resources of those types exist.

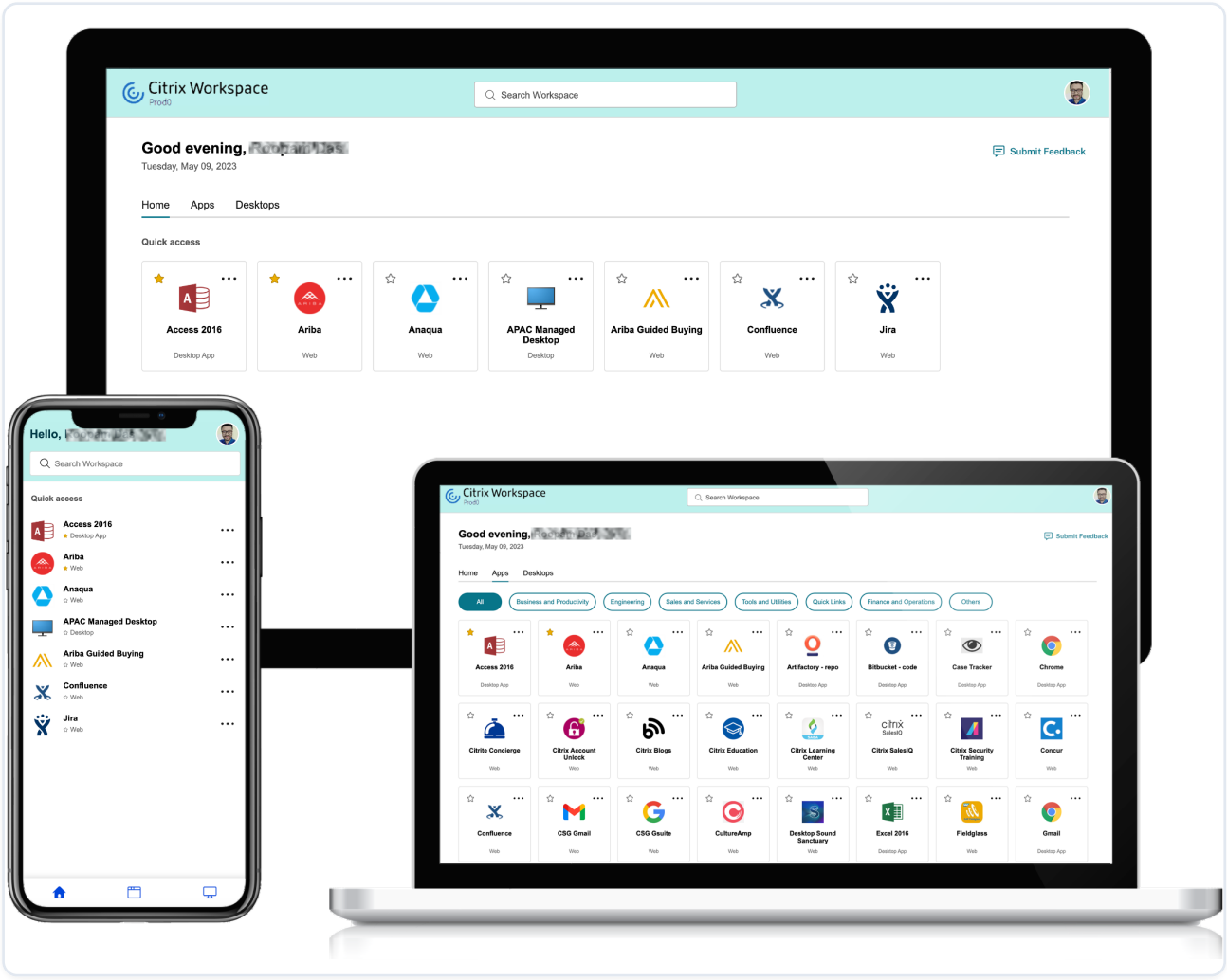
Home tab

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.

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

Apps tab

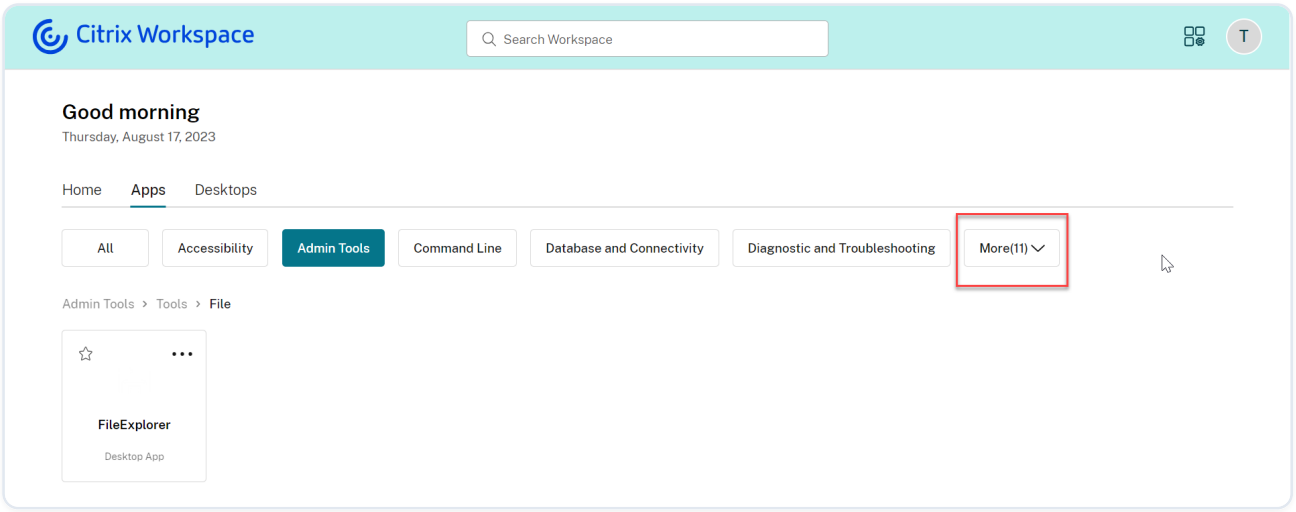
On the **Apps** tab, favorites appear first, followed by all the other apps in an alphabetical order. If the admin has created categories and attached the apps to them, then the various categories appear, and users can select the category of the apps that they want to view.



For each application you can define a category. The category represents the folder structure that appears on the screen for end users. For example, consider an app for which the folder is defined as `Optimisation tools/Cleaning`. Now, to access this app, end users must go to Optimisation tools > Cleaning, where Optimisation tools is a category and Cleaning is it's sub-category. For more information about configuring categories, see Applications.

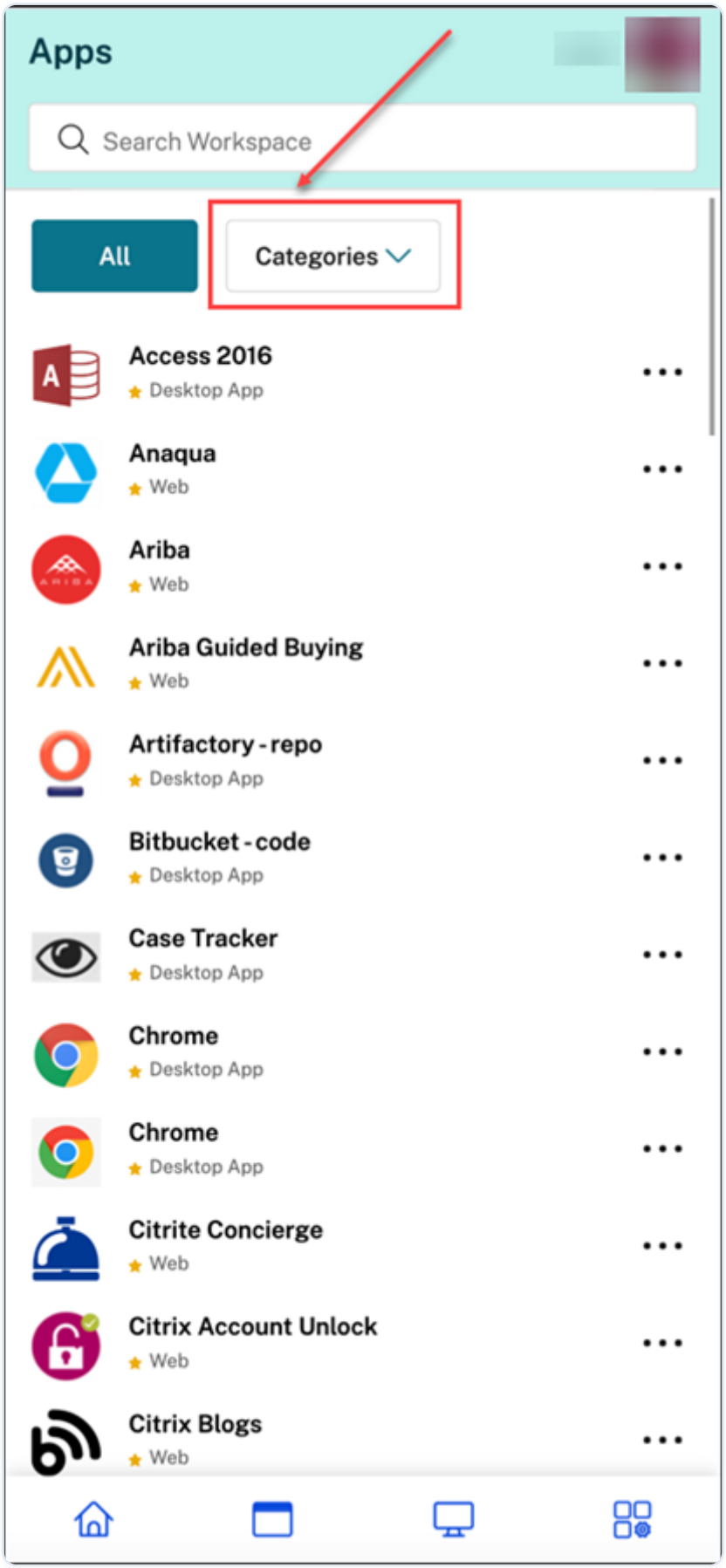
When the number of primary categories created by the admins exceeds the available space on the user's screen, the user interface adjusts based on the screen size, and dynamically moves categories under the **More** dropdown. The navigation breadcrumbs are also displayed to the users.

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



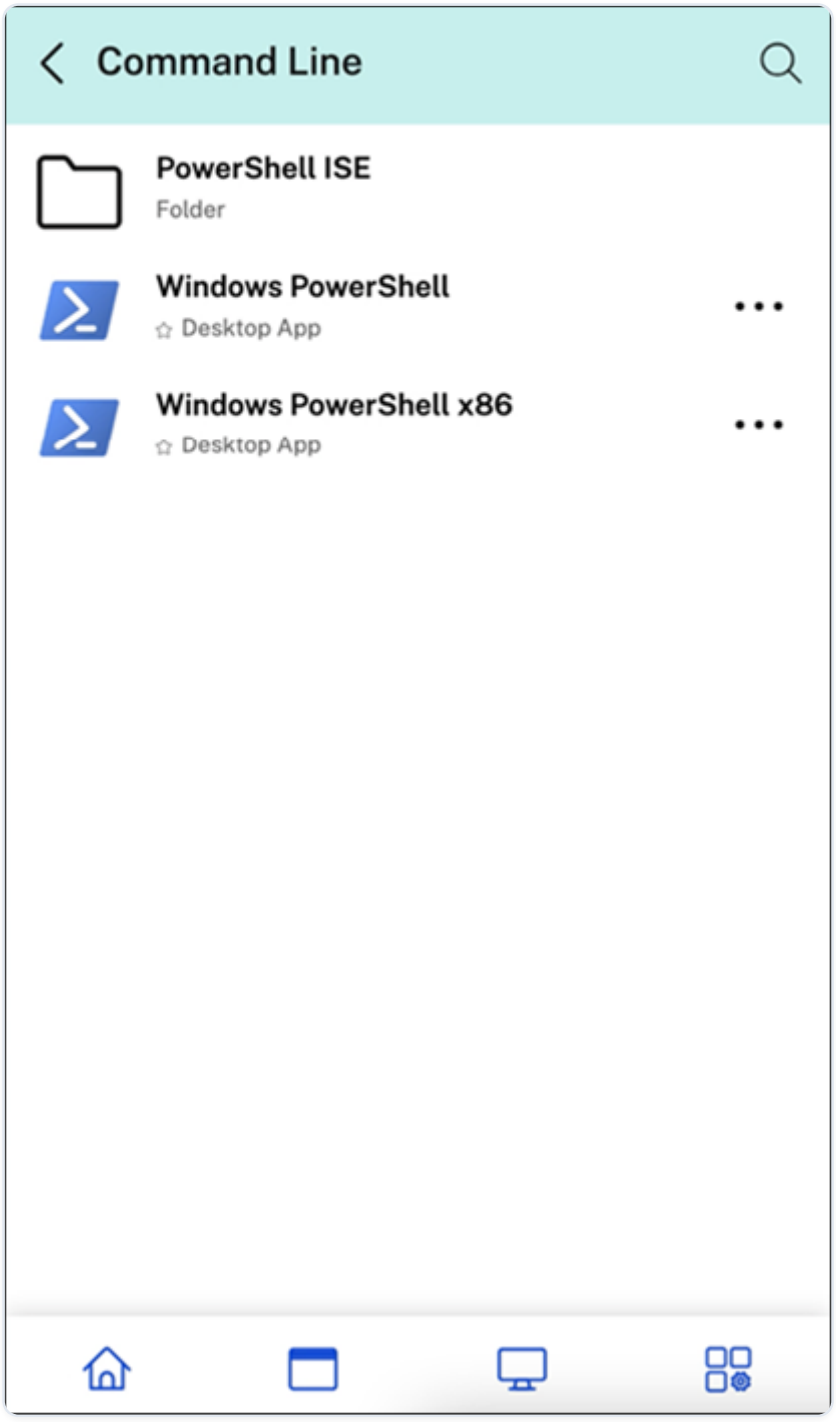
On mobile platforms, navigate to the Apps tab and click the **Categories** dropdown to view a list of available categories. Sub-categories are displayed as folders that might contain further sub-folders or applications as per the admin configuration.

© 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.

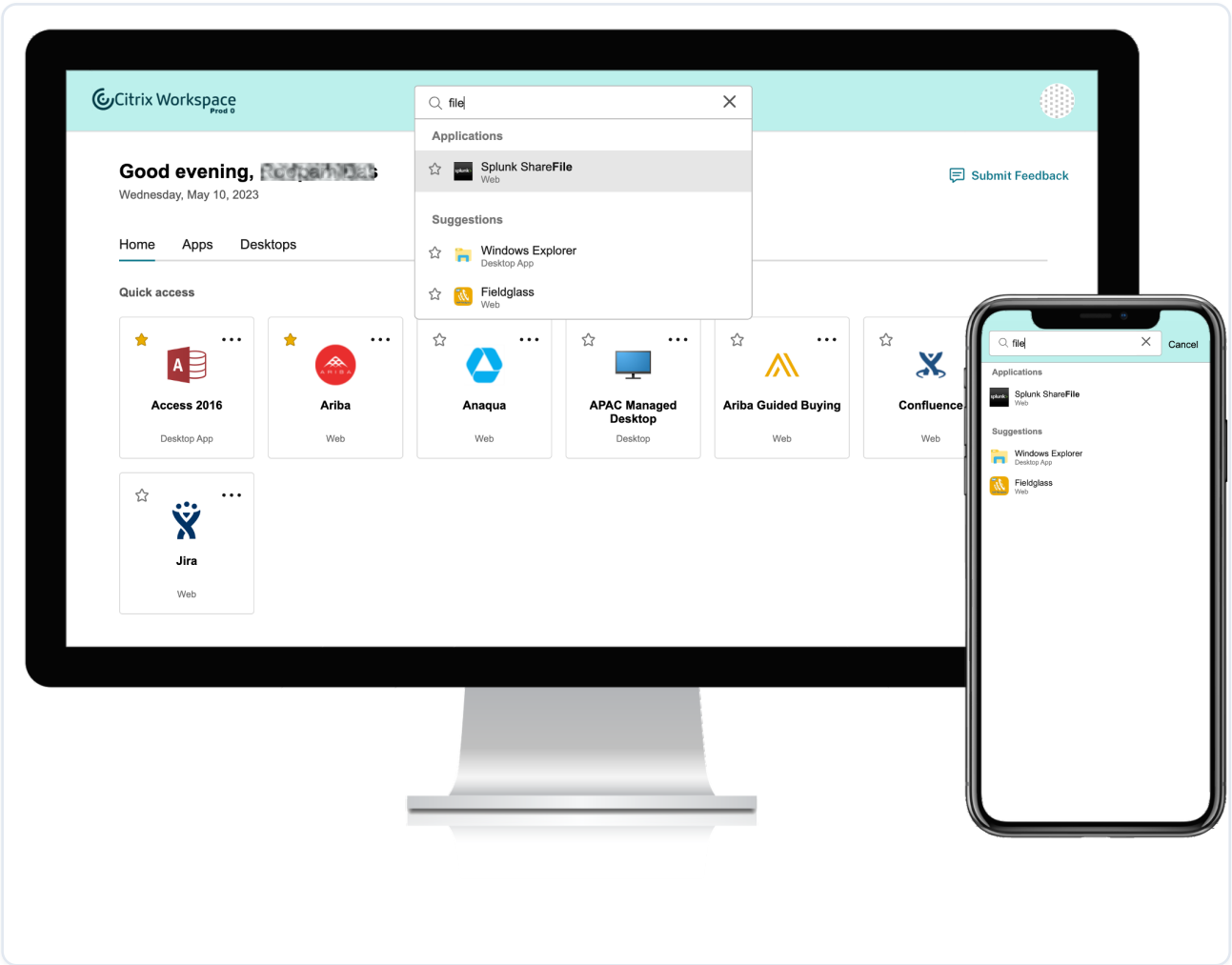
© 1997–2026 Citrix Systems, Inc. All rights reserved.

- **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 feature

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.

Account 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.

Apps and Desktops Launch Preference

This displays whether apps launch in the web browser, or in Citrix Workspace app, or by downloading and ICA file that the user can open in Citrix Workspace app.

The user can select **Verify connection** to open the Citrix Workspace app detection screen.

Download Workspace Configuration

Users can download a file that configures Citrix Workspace app to connect to the store.

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.

Activity Manager requires Citrix Desktops as a Service or Citrix Virtual Apps and Desktops™ 2311 or higher.

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 Configure custom themes.

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.

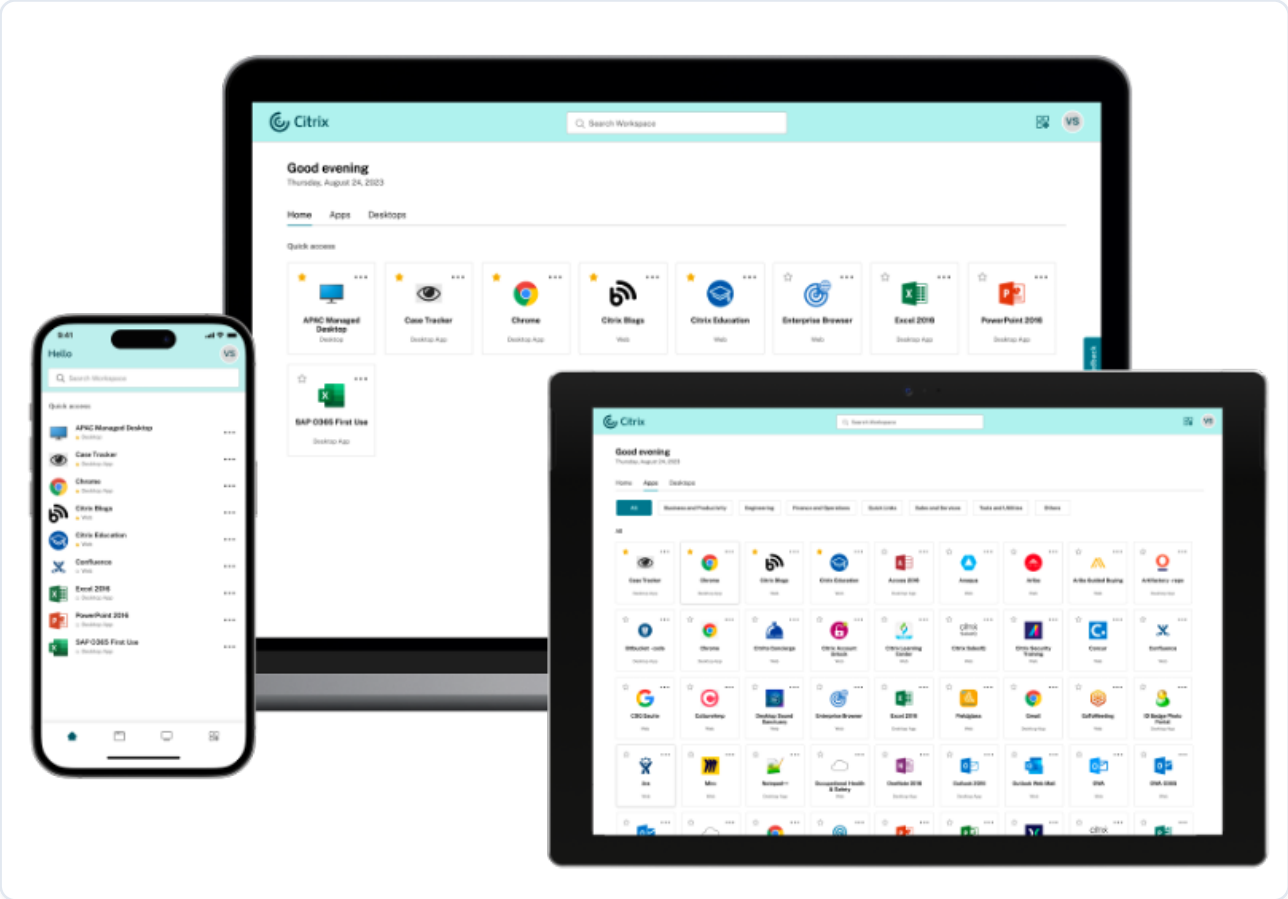
To control whether the **Activity manager** button is displayed, see Display Activity manager.

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

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**.



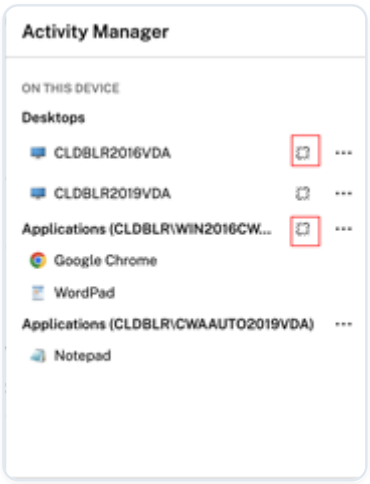
Users can perform the following actions on an app or desktop by clicking the respective ellipsis(...) button.

- **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 Quit**: 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.

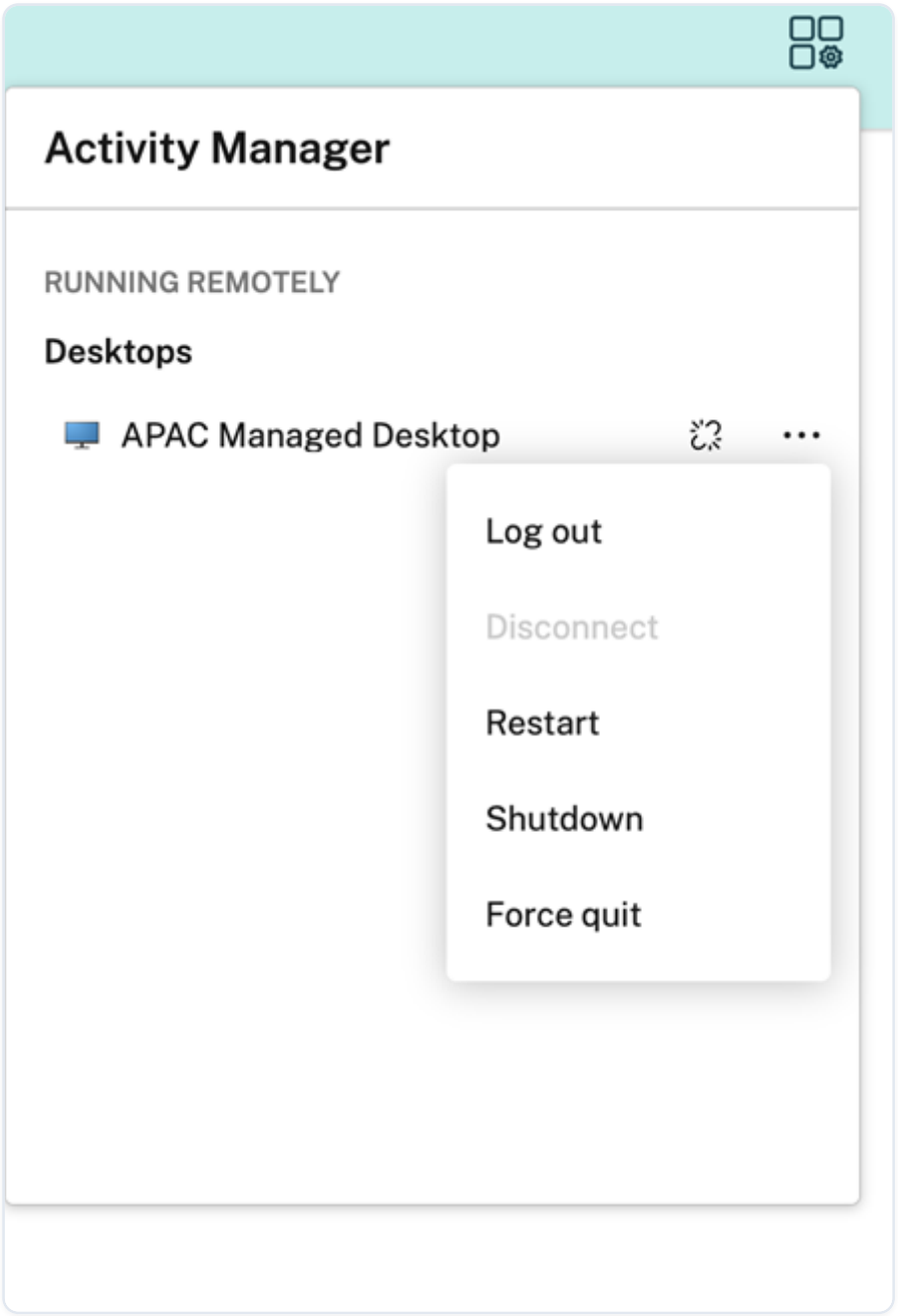
Disconnected apps and desktops

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 you are signed into Citrix workspace through a browser, and disconnect a local session, the session is first displayed under On this device. However, once you close and reopen Activity Manager, the disconnected session is moved under Running Remotely.
- If you are signed into Citrix Workspace app through a native device, and disconnect a local session, the disconnected session disappears from the list. However, once you close and reopen Activity Manager again, the disconnected session is moved under Running Remotely.

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

StoreFront SDK

Citrix StoreFront provides an SDK based on a number of Microsoft Windows PowerShell version 2.0 modules. With the SDK, you can perform the same tasks as you would with the StoreFront MMC console, together with tasks you cannot do with the console alone.

NOTE:

The PowerShell SDK is not compatible with PowerShell 6 or higher.

For the SDK Reference, see StoreFront SDK.

Use the SDK

The SDK comprises of a number of PowerShell snap-ins installed automatically by the installation wizard when you install and configure various StoreFront components.

To access and run the cmdlets:

1. 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 SDK cmdlets within scripts, set the execution policy in PowerShell to RemoteSigned. For more information about PowerShell execution policy, see Microsoft documentation.

Get started with the SDK

To create a script, perform the following steps:

1. Take one of the provided SDK examples installed by StoreFront into the **%ProgramFiles%\Citrix\Receiver StoreFront\PowerShellSDK\Examples** folder.

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

2. To help you customize your own script. review the example script to understand what each part is doing. For more information, see the example use case, which explains in detail the script's actions.
3. Convert and adapt the example scripts to turn them into a script that is more consumable. To do this:
    - Use the PowerShell ISE or a similar tool to edit the script.
    - Use variables to assign values that are to be reused or modified.
    - Remove any commands that are not required.
    - Note that StoreFront cmdlets can be identified by the prefix STF.
    - Use the **Get-Help** cmdlet supplying the cmdlet name and **-Full** parameter for more information on a specific command.

Examples

NOTE:

When creating a script, to ensure you always get the latest enhancements and fixes, Citrix® recommends you follow the procedure described above rather than copying and pasting the example scripts.

EXAMPLES	DESCRIPTION
Create a Simple Deployment	Script: creates a simple deployment with a StoreFront controller configured with a single XenDesktop server.
Create a Remote Access Deployment	Script: builds on the previous script to add remote access to the deployment.
Create a Remote Access Deployment with Optimal Launch Gateway	Script: builds on the previous script to add preferred optimal launch gateways for a better user experience.

Example: Create a simple deployment

The following example shows how to create a simple deployment configured with one XenDesktop® controller.

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

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

NOTE:

To ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described in this document, rather than copying and pasting the example script.

Understand the script

This section explains what each part of the script produced by StoreFront is doing. This will help you with the customization of your own script.

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

```
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,
```

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

```
    [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

    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 iin preparation for adding the required StoreFront services. **-Confirm:$false** supresses the requirement to confirm the deployment can procede.

```
\# Determine if the deployment already exists

$existingDeployment = Get-STFDeployment

if(-not $existingDeployment)

{
```

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

```
    \# 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

    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
```

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

```
appended with Auth

    $authentication = Add-STFAuthenticationService
$authenticationVirtualPath

}

else

{

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

}
```

- Creates the new store service configured with one XenDesktop controller with the servers defined in the array **$XenDesktopServers** at the specified virtual path if one does not already exist.

```
\# 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

{
```

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

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

        -SSLRelayPort $SSLRelayPort -TransportType $TransportType

}
```

- Adds a Citrix Receiver™ for Web service 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

{
```

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

```
    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

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

NOTE:

To ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described in this document, rather than copying and pasting the example script.

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

Understand the script

This section explains what each part of the script produced by StoreFront is doing. This will help you with the customization of your own script.

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

```
Param(

    [Parameter(Mandatory=$true)]

    [Uri]$HostbaseUrl,

    [Parameter(Mandatory=$true)]

    [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,
```

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

```
    [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

\# 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"
```

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

```
& $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.

```
\# 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.

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

```
\# 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

\# 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

}
```

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

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

NOTE:

To ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described in this document, rather than copying and pasting the example script.

Understand the script

This section explains what each part of the script produced by StoreFront is doing. This will help you with the customization of your own script.

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

```
Param(

    [Parameter(Mandatory=$true)]

    [Uri]$HostbaseUrl,

    [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,

    [Parameter(Mandatory=$true)]

    [Uri]$OptimalGatewayUrl,

    [Parameter(Mandatory=$true)]

    [string[]]$OptimalGatewaySTAUrls,

    [Parameter(Mandatory=$true)]

    [string]$OptimalGatewayName

)
```

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

```
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 \`

    -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.

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

```
\# 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 farm 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
```

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

Troubleshoot StoreFront

Installation Logs

When StoreFront is installed or uninstalled, the following log files are created by the StoreFront installer in the *C:\Windows\Temp\StoreFront* directory. The file names reflect the components that created them and include time stamps.

- Citrix-DeliveryServicesRoleManager-*.log—Created when StoreFront is installed interactively.
- Citrix-DeliveryServicesSetupConsole-*.log—Created when StoreFront is installed silently and when StoreFront is uninstalled, either interactively or silently.
- CitrixMsi-CitrixStoreFront-x64-*.log—Created when StoreFront is installed and uninstalled, either interactively or silently.

Event Logs

StoreFront supports Windows event logging for the authentication service, stores, and Receiver for Web sites. Any events that are generated are written to the StoreFront application log, which can be viewed using Event Viewer under either **Application and Services Logs > Citrix Delivery Services** or **Windows Logs > Application**. You can control the number of duplicate log entries for a single event by editing the configuration files for the authentication service, stores, and Receiver for Web sites.

Log throttling

1. Use a text editor to open the *web.config* file for the authentication service, store, or Receiver for Web site, which are typically located in the C:\inetpub\wwwroot\Citrix\Authentication\, C:\inetpub\wwwroot\Citrix\storename\, and C:\inetpub\wwwroot\Citrix\storenameWeb\ directories, respectively, where storename is the name specified for the store when it was created.
2. Locate the following element in the file.

   ```
   <logger duplicateInterval="00:01:00" duplicateLimit="10">
   ```

   By default, StoreFront is configured to limit the number of duplicate log entries to 10 per minute.

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

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.

PowerShell and management console logs

Configuration changes made through PowerShell or the management console are logged at `C:\Program Files\Citrix\Receiver StoreFront\Admin\logs`. The log file names contain command actions and subjects, along with time stamps that can be used to differentiate command sequences.

Diagnostics logging

StoreFront writes diagnostics logs to `c:\Program Files\Citrix\Receiver StoreFront\admin\trace`

By default, messages of level **Error**, **Warning**, and **Info** are logged. In most cases this includes sufficient information to diagnose any issues.

You can enable additional verbose logging for troubleshooting purposes. This is only required if requested by Citrix® support. This may have an impact on performance so you should revert the `TraceLevel` to `Info` once troubleshooting is complete.

To enable Verbose logging:

1. Using an account with local administrator permissions, start Windows PowerShell
2. Enter command:

   ```
   Set-STFDiagnostics -All -TraceLevel "Verbose" -confirm:$False
   ```

   This enables "Verbose" logging for all services, without prompting for confirmation. When this command is entered it restarts the Storefront services. Wait for the PowerShell prompt to return to verify that that the services have finished restarting. While these services are restarting, the StoreFront server will not be accessible by users.

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

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
```

You can further customize the diagnostics logging:

- StoreFront writes a separate log file for each service. By default, each log file is up to 200Mb and StoreFront writes up to five log files per service before purging old log files. If you need to customize the size or number of logs written then you can do this using the `-FileSizeKb` and `-FileCount` parameters.
- Change the level of detail logged using `-TraceLevel`. Allowed values are `Off`, `Error`, `Warning`, `Info`, or `Verbose`.
- Using the parameter `-All` sets the logging parameters for all services. You can customize logging for an individual service using `-Service [Service name]`

For more information on the `Set-STFDiagnostics` cmdlet, see the StoreFront PowerShell SDK documentation.

Launch.ica file logging

When a user launches an app or desktop, StoreFront generates a file called launch.ica that Workspace app reads to determine how to connect to the app or desktop. Depending on configuration this file may be stored in memory so not directly accessible. To diagnose launch errors it can be useful to view the contents of launch.ica.

To enable logging of the launch.ica file on the client PC, complete the following steps:

1. Navigate to the following registry key by using the registry editor:

   32-bit Systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

   64-bit Systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

2. Set the following two string key values:

   - LogFile="path to the log file"
   - LogICAFile=true

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

For example:

```
LogFile=C:\ica\ica.log

LogICAFile=true
```

Note:

The use of an ICA file in your environment for anything other than troubleshooting purposes is further outlined in CTX200126.

© 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 Jorik Tangelder <j.tangelder@gmail.com>;

Licensed under the MIT license

jQuery MouseWheel

Copyright (c) 2011 Brandon Aaron (http://brandonaaron.net)

Licensed under the MIT License (LICENSE.txt).

WPF Toolkit 3.5

WPF Toolkit Copyright (c) 2006-2014 Microsoft

MS-PL license

Extended WPF Toolkit 3.0

Copyright (C) 2007-2013 Xceed Software Inc.

This program is provided to you under the terms of the Microsoft Public License (Ms-PL).

For more features, controls, and fast professional support, pick up the Plus Edition at `<http://xceed.com/wpf_toolkit>`

Stay informed: follow @datagrid on Twitter

WiX Toolset

Copyright (c) Outercurve Foundation. Common Public License Version 1.0.

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

CLR Security

Copyright (c) Microsoft Corporation. Microsoft Limited Permissive License (MS-LPL)

Stack Exchange Redis 1.1

StackExchange.Redis.StrongName 1.1 `<https://stackexchange.github.io/StackExchange.Redis>` Copyright (c) 2014 Stack Exchange

Licensed under the MIT license

Newtonsoft JSON

Copyright (c) 2007 James Newton-King

Licensed under the MIT license.

jQuery JavaScript Library v3.7.0

(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

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

VelocityJS.org (1.5.0)

velocity-animate (C) 2014-2017 Julian Shapiro.

Licensed under the MIT license. See LICENSE file in the project root for details.

slick.js - 1.8.0

The MIT License (MIT)

Copyright (c) 2013-2016

jQuery UI Touch Punch 0.2.3

Copyright 2011–2014, Dave Furfero

Dual licensed under the MIT or GPL Version 2 licenses.

Microsoft .NET 8

The MIT License (MIT)

Copyright (c) .NET Foundation and Contributors

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:
```

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

```
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

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.
```

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

"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 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.

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

> "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
> (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

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

```
   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
   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
```

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

```
   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
   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
```

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

```
(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
    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
```

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

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 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,

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

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 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

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

```
   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
   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
```

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

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

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

```
(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.



(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.
```

Common Public License Version 1.0

THE ACCOMPANYING PROGRAM IS PROVIDED UNDER THE TERMS OF THIS COMMON PUBLIC LICENSE (“AGREEMENT”). ANY USE, REPRODUCTION OR DISTRIBUTION OF THE PROGRAM CONSTITUTES RECIPIENT’S ACCEPTANCE OF THIS AGREEMENT.

1.Definitions of Contribution

(a) In the case of the initial Contributor, the initial code and documentation distributed under this Agreement.

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

(b) In the case of each subsequent Contributor:

```
- Changes to the Program

- Additions to the Program; where such changes and/or additions to the
Program originate from and are distributed by that particular Contributor.
A Contribution ‘originates’ from a Contributor if it was added to the
Program by such Contributor itself or anyone acting on such Contributor’s
behalf. Contributions do not include additions to the Program which: (a)
are separate modules of software distributed in conjunction with the
Program under their own license agreement, and (b) are not derivative
works of the Program. “Contributor” means any person or entity that
distributes the Program. “Licensed Patents ” mean patent claims licensable
by a Contributor which are necessarily infringed by the use or sale of its
Contribution alone or when combined with the Program. “Program” means the
Contributions distributed in accordance with this Agreement. “Recipient”
means anyone who receives the Program under this Agreement, including all
Contributors.
```

2.Grant of Rights

(a) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free copyright license to reproduce, prepare derivative works of, publicly display, publicly perform, distribute and sublicense the Contribution of such Contributor, if any, and such derivative works, in source code and object code form.

(b) Subject to the terms of this Agreement, each Contributor hereby grants Recipient a non-exclusive, worldwide, royalty-free patent license under Licensed Patents to make, use, sell, offer to sell, import and otherwise transfer the Contribution of such Contributor, if any, in source code and object code form. This patent license shall apply to the combination of the Contribution and the Program if, at the time the Contribution is added by the Contributor, such addition of the Contribution causes such combination to be covered by the Licensed Patents. The patent license shall not apply to any other combinations which include the Contribution. No hardware per se is licensed hereunder.

(c) Recipient understands that although each Contributor grants the licenses to its Contributions set forth herein, no assurances are provided by any Contributor that the Program does not infringe the patent or other intellectual property rights of any other entity. Each Contributor disclaims any liability to Recipient for claims brought by any other entity based on infringement of intellectual property rights or otherwise. As a condition to exercising the rights and licenses granted hereunder, each Recipient hereby assumes sole responsibility to secure any other intellectual property rights

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

needed, if any. For example, if a third party patent license is required to allow Recipient to distribute the Program, it is Recipient's responsibility to acquire that license before distributing the Program.

(d) Each Contributor represents that to its knowledge it has sufficient copyright rights in its Contribution, if any, to grant the copyright license set forth in this Agreement.

3.Requirements

A Contributor may choose to distribute the Program in object code form under its own license agreement, provided that:

(a) It complies with the terms and conditions of this Agreement.

(b) Its license agreement:

```
  - Effectively disclaims on behalf of all Contributors all warranties and
conditions, express and implied, including warranties or conditions of
title and non-infringement, and implied warranties or conditions of
merchantability and fitness for a particular purpose.

  - Effectively excludes on behalf of all Contributors all liability for
damages, including direct, indirect, special, incidental and consequential
damages, such as lost profits.

  - States that any provisions which differ from this Agreement are
offered by that Contributor alone and not by any other party.

  - States that source code for the Program is available from such
Contributor, and informs licensees how to obtain it in a reasonable manner
on or through a medium customarily used for software exchange. When the
Program is made available in source code form:



     i. It must be made available under this Agreement.

     ii. A copy of this Agreement must be included with each copy of the
Program. Contributors may not remove or alter any copyright notices
contained within the Program. Each Contributor must identify itself as the
originator of its Contribution, if any, in a manner that reasonably allows
subsequent Recipients to identify the originator of the Contribution.
```

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

4.Commercial Distribution

Commercial distributors of software may accept certain responsibilities with respect to end users, business partners and the like. While this license is intended to facilitate the commercial use of the Program, the Contributor who includes the Program in a commercial product offering should do so in a manner which does not create potential liability for other Contributors. Therefore, if a Contributor includes the Program in a commercial product offering, such Contributor (“Commercial Contributor”) hereby agrees to defend and indemnify every other Contributor (“Indemnified Contributor”) against any losses, damages and costs (collectively “Losses”) arising from claims, lawsuits and other legal actions brought by a third party against the Indemnified Contributor to the extent caused by the acts or omissions of such Commercial Contributor in connection with its distribution of the Program in a commercial product offering. The obligations in this section do not apply to any claims or Losses relating to any actual or alleged intellectual property infringement.In order to qualify, an Indemnified Contributor must:

(a) Promptly notify the Commercial Contributor in writing of such claim.

(b) Allow the Commercial Contributor to control, and cooperate with the Commercial Contributor in, the defense and any related settlement negotiations. The Indemnified Contributor may participate in any such claim at its own expense. For example, a Contributor might include the Program in a commercial product offering, Product X. That Contributor is then a Commercial Contributor. If that Commercial Contributor then makes performance claims, or offers warranties related to Product X, those performance claims and warranties are such Commercial Contributor’s responsibility alone. Under this section, the Commercial Contributor would have to defend claims against the other Contributors related to those performance claims and warranties, and if a court requires any other Contributor to pay any damages as a result, the Commercial Contributor must pay those damages.

5.NO WARRANTY EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE PROGRAM IS PROVIDED ON AN “AS IS” BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, EITHER EXPRESS OR IMPLIED INCLUDING, WITHOUT LIMITATION, ANY WARRANTIES OR CONDITIONS OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Each Recipient is solely responsible for determining the appropriateness of using and distributing the Program and assumes all risks associated with its exercise of rights under this Agreement, including but not limited to the risks and costs of program errors, compliance with applicable laws, damage to or loss of data, programs or equipment, and unavailability or interruption of operations.

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

6.DISCLAIMER OF LIABILITY EXCEPT AS EXPRESSLY SET FORTH IN THIS AGREEMENT, NEITHER RECIPIENT NOR ANY CONTRIBUTORS SHALL HAVE ANY LIABILITY FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION LOST PROFITS), 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 OR DISTRIBUTION OF THE PROGRAM OR THE EXERCISE OF ANY RIGHTS GRANTED HEREUNDER, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

7.GENERAL If any provision of this Agreement is invalid or unenforceable under applicable law, it shall not affect the validity or enforceability of the remainder of the terms of this Agreement, and without further action by the parties hereto, such provision shall be reformed to the minimum extent necessary to make such provision valid and enforceable. If Recipient institutes patent litigation against a Contributor with respect to a patent applicable to software (including a cross-claim or counterclaim in a lawsuit), then any patent licenses granted by that Contributor to such Recipient under this Agreement shall terminate as of the date such litigation is filed. In addition, if Recipient institutes patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Program itself (excluding combinations of the Program with other software or hardware) infringes such Recipient’s patent(s), then such Recipient’s rights granted under Section 2(b) shall terminate as of the date such litigation is filed. All Recipient’s rights under this Agreement shall terminate if it fails to comply with any of the material terms or conditions of this Agreement and does not cure such failure in a reasonable period of time after becoming aware of such noncompliance. If all Recipient’s rights under this Agreement terminate, Recipient agrees to cease use and distribution of the Program as soon as reasonably practicable. However, Recipient’s obligations under this Agreement and any licenses granted by Recipient relating to the Program shall continue and survive. Everyone is permitted to copy and distribute copies of this Agreement, but in order to avoid inconsistency the Agreement is copyrighted and may only be modified in the following manner. The Agreement Steward reserves the right to publish new versions (including revisions) of this Agreement from time to time. No one other than the Agreement Steward has the right to modify this Agreement. IBM is the initial Agreement Steward. IBM may assign the responsibility to serve as the Agreement Steward to a suitable separate entity. Each new version of the Agreement will be given a distinguishing version number. The Program (including Contributions) may always be distributed subject to the version of the Agreement under which it was received. In addition, after a new version of the Agreement is published, Contributor may elect to distribute the Program (including its Contributions) under the new version. Except as expressly stated in Sections 2(a) and 2(b) above, Recipient receives no rights or licenses to the intellectual property of any Contributor under this Agreement, whether expressly, by implication, estoppel or otherwise. All rights in the Program not expressly granted under this Agreement are reserved. This

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

Agreement is governed by the laws of the State of New York and the intellectual property laws of the United States of America. No party to this Agreement will bring a legal action under this Agreement more than one year after the cause of action arose. Each party waives its rights to a jury trial in any resulting litigation.

Microsoft Limited Permissive License (MS-LPL)

Microsoft Limited Public License (Ms-LPL)

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 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.

4.Platform Limitation

The licenses granted in sections 2(a) & 2(b) extend only to the software or derivative works that you create that run on a Microsoft Windows operating system product.

© 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
08 May 2026	Release of StoreFront 2402 LTSR Cumulative Update 4	For details, see What's new.
26 Aug 2025	Release of StoreFront 2402 LTSR Cumulative Update 3	For details, see What's new.
07 Feb 2025	Release of StoreFront 2402 LTSR Cumulative Update 2	For details, see What's new.
30 Sep 2024	Known issue in StoreFront 2402 LTSR Cumulative Update 1	For details, see Known issue.
20 Aug 2024	Release of StoreFront 2402 LTSR Cumulative Update 1	For details, see What's new.
25 Mar 2024	Release of StoreFront 2402 LTSR	Release of StoreFront 2402 LTSR. For more information, see What's new.

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