StoreFront 1912 LTSR

Contents

What's new 3

Cumulative Update 5 (CU5) 4

Fixed issues in 1912 LTSR CU5 4

Cumulative Update 4 (CU4) 5

Fixed issues in 1912 LTSR CU4 5

Cumulative Update 3 (CU3) 7

Fixed issues in 1912 LTSR CU3 7

Cumulative Update 2 (CU2) 8

Fixed issues in 1912 LTSR CU2 9

Cumulative Update 1 (CU1) 10

Fixed issues in 1912 LTSR CU1 10

What's new 11

Fixed issues in 1912 LTSR 13

Known issues 13

Third party notices 15

System requirements 15

Plan your StoreFront deployment 22

User access options 27

User authentication 35

Optimize the user experience 46

StoreFront high availability and multi-site configuration 50

Install, set up, upgrade, and uninstall 54

Create a new deployment 77

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Join an existing server group 84

Reset a server to factory defaults 85

Migrate Web Interface features to StoreFront 87

Configure server groups 93

Configure authentication and delegation 96

Configure the authentication service 97

XML service-based authentication 105

Configure Kerberos constrained delegation for XenApp 6.5 107

Configure smart card authentication 111

Configure the password expiry notification period 116

Configure and manage stores 117

Create or remove a store 118

Create an unauthenticated store 124

Export store provisioning files for users 127

Advertise and hide stores to users 127

Manage the resources made available in stores 128

Manage remote access to stores through Citrix Gateway 130

Certificate Revocation List (CRL) checking 133

Configure two StoreFront stores to share a common subscription datastore 143

Manage subscription data for a store 144

Store subscription data using Microsoft SQL Server 150

Advanced store settings 171

Manage a Citrix Receiver for Web site 177

Create a Citrix Receiver for Web site 178

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Configure Citrix Receiver for Web sites 179

Support for the unified user experience 185

Create and manage featured apps 210

Configure workspace control 212

Configure Citrix Workspace app for HTML5 use of browser tabs 213

Configure user access 213

Configure StoreFront to launch applications and desktops in Windowed Mode 217

Configure communication and session time-out 218

Set up highly available multi-site stores 221

Integrate with Citrix Gateway and Citrix ADC 239

Add a Citrix Gateway connection 242

Import a Citrix Gateway 244

Configure Citrix Gateway connection settings 253

Load balancing with Citrix ADC appliance 256

Configure two URLs for the same Citrix Gateway 274

Configure Citrix ADC and StoreFront for Delegated Forms Authentication (DFA) 285

Authenticate using different domains 288

Configure beacon points 299

Create a single Fully Qualified Domain Name (FQDN) to access a store internally and externally 301

Advanced configurations 320

Configure Resource Filtering 320

Configure using configuration files 322

Configure StoreFront using the configuration files 322

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Configure Citrix Receiver for Web sites using the configuration files 328

Secure your StoreFront deployment 330

Export and import the StoreFront configuration 339

StoreFront SDK 349

Troubleshoot StoreFront 364

© 1999–2022 Citrix Systems, Inc. All rights reserved.

What's new

March 8, 2022

StoreFront 1912 LTSR

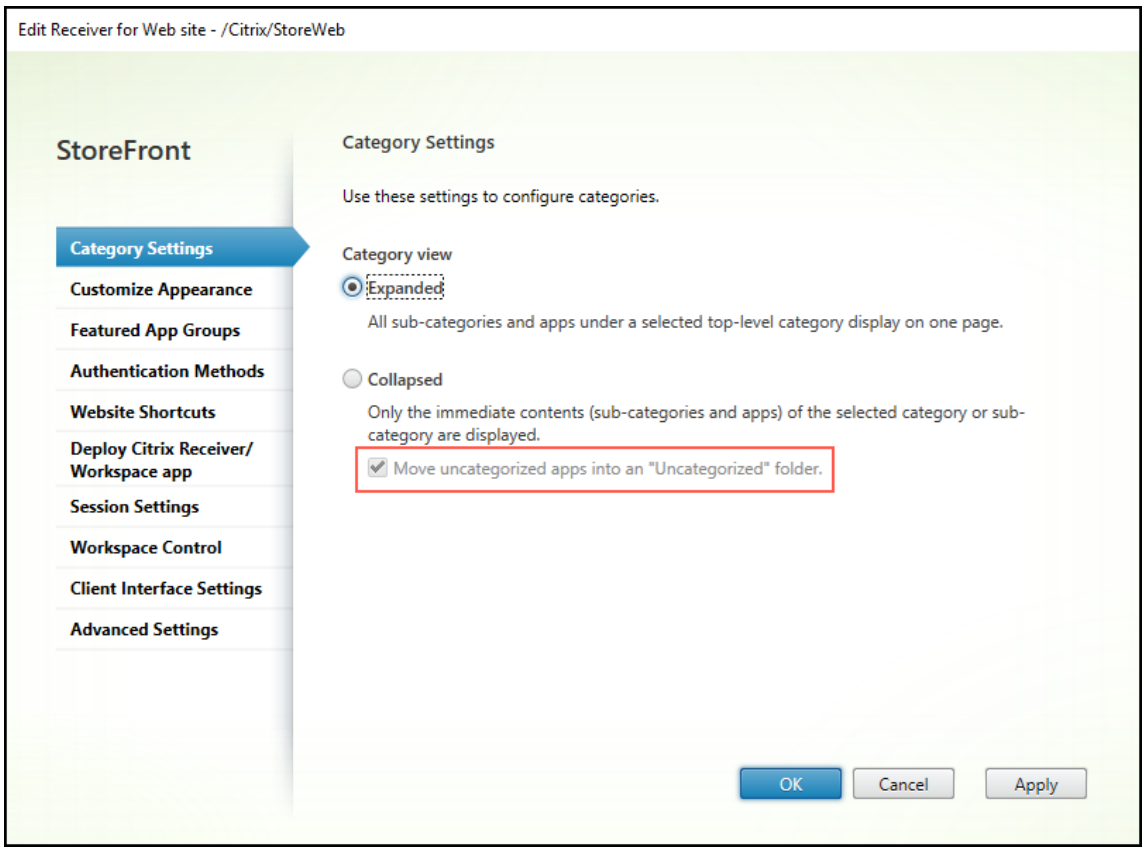
Cumulative Update 5 (CU5) is the most recent update to StoreFront 1912 LTSR.

Categories view for Unified user experience

In the collapsed mode of the **Categories** section, uncategorized apps are no longer placed in the **Uncategorized** folder. Instead, they appear directly under the first layer of the category folders. With this feature, you have faster access to the applications and an enhanced user experience.

To enable these settings, do the following steps:

1. Go to **Manage Receiver for Web sites > Configure > Categories Settings**.
2. Select the Collapsed section of the Category view.
3. Clear the **Move uncategorized apps into an Uncategorized folder** checkbox.



© 1999–2022 Citrix Systems, Inc. All rights reserved.

Upload StoreFront identity to broker via a header

With this feature, you can determine if specific calls are received from Delivery Controller Monitors on Citrix Gateway, or the Advanced Health Check feature on the StoreFront store. This information helps provide alerts to administrators on common misconfiguration.

Administrators can disable this feature by using the following PowerShell script on a StoreFront server: `Add-STFFeatureState -Name "Citrix.StoreFront.Wing.UploadServerIdentity"-IsEnabled $False`

Cumulative Update 5 (CU5)

March 7, 2022

Release date: 09 March, 2022.

About this release

StoreFront 1912 LTSR Cumulative Update 5 (CU5) fixes four issues reported since the CU4 release of the 1912 LTSR.

StoreFront 1912 LTSR Cumulative Update 4 (CU4)

StoreFront 1912 LTSR Cumulative Update 3 (CU3)

StoreFront 1912 LTSR Cumulative Update 2 (CU2)

StoreFront 1912 LTSR Cumulative Update 1 (CU1)

StoreFront 1912 LTSR (initial release)

Known issues in this release

Citrix Product Subscription Advantage Eligibility Dates

Fixed issues in 1912 LTSR CU5

February 23, 2022

Compared to: StoreFront 1912 LTSR CU4

StoreFront 1912 CU5 includes the following fixed issues:

- When you log on to Citrix Workspace app from the same workstation as the previous user, incorrect applications might be listed in tabs **All** and **Favorites**. [CVADHELP-18149]

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- When StoreFront site aggregation is enabled, application launches and filtering based on keywords might fail. [CVADHELP-18362]
- You can enable or disable the option to move uncategorized apps in the Web Receiver collapsed category mode into an 'Uncategorized' folder. [CVADHELP-18692]
- With this fix, you can determine whether you receive specific calls from Delivery Controller Monitors on Citrix Gateway or the Advanced Health Check feature on the StoreFront store. This information helps provide alerts to administrators on common misconfiguration.

  Administrators can disable this feature using the following PowerShell script on a StoreFront server: **Add-STFFeatureState -Name "Citrix.StoreFront.Wing.UploadServerIdentity" -IsEnabled $False** [CVADHELP-18810]

Cumulative Update 4 (CU4)

November 3, 2021

Release date: November 03, 2021

About this release

StoreFront 1912 LTSR Cumulative Update 4 (CU4) fixes eight issues reported since the CU3 release of the 1912 LTSR.

StoreFront 1912 LTSR Cumulative Update 3 (CU3)

StoreFront 1912 LTSR Cumulative Update 2 (CU2)

StoreFront 1912 LTSR Cumulative Update 1 (CU1)

StoreFront 1912 LTSR (initial release)

Known issues in this release

Citrix Product Subscription Advantage Eligibility Dates

Fixed issues in 1912 LTSR CU4

October 28, 2021

Compared to: StoreFront 1912 LTSR CU3

StoreFront 1912 LTSR CU4 contains all fixes included in the 1912 LTSR initial release, CU1 release, CU2 release, CU3 release, and the following new fixes:

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- When you attempt to launch a user session using Citrix StoreFront services API, the parameters passed to the launch request might be incorrect. [CVADHELP-16834]
- SAML authentication might fail on the Citrix Workspace app that is connected internally to a StoreFront. [CVADHELP-17295]
- This fix is an enhancement to StoreFront supporting the Local Host Cache feature in Citrix Virtual Apps and Desktops service deployment. This enhancement allows users to launch resources from locations where connectors are not added to the StoreFront as Delivery Controllers when the service is not in the cloud outage mode. [CVADHELP-17385]
- StoreFront includes a Cross Site Request Forgery (CSRF) token in the query string of a few URLs. A security concern might arise because the tokens might be retained in the browser history or in the logs of intermediate devices, such as proxy servers.

  With this fix, you can disable CSRF token usage for the following URL request.

  ```
  Add-STFFeatureState -Name "Citrix.DeliveryServices.WebUI.CsrfValidation
  .IgnoreOnSpecificRequests"-IsEnabled $True
  ```

  > **Note:**
  >
  > If the feature toggle is **ON**, you must remove CSRF tokens from the URLs in all WebAPI-based customizations.

  [CVADHELP-17671]
- If you select Source for Receivers/Workspace app as the Citrix Website using the Deploy Citrix Receiver/Workspace app option, the Citrix Receivers/Workspace app downloads from an insecure site. As a result, the latest Google Chrome browser updates block the download. [CVADHELP-18083]
- Upgrading StoreFront from version 7.15 LTSR CU2 to version 1912 LTSR CU3 might fail. Also, uninstalling StoreFront using the Windows Control Panel might fail with this error message:

  Uninstalling Citrix StoreFront failed with exit code: 9

  [CVADHELP-18172]
- When switching accounts to log on to Citrix Workspace app on the same client, icons of featured app groups might launch incorrect applications. For example, if the user clicks the icon of application **A** on Citrix Workspace app, application **B** might launch. Also, the detail box of application A displays the information of application B. [CVADHELP-18221]
- Highlighted tabs in Citrix Receiver for Web sites ignore the 'Link color' value specified in the Customize Appearance tab of the Edit Receiver for Web site dialog. Instead, highlighted tabs display in purple, [LCM-9536]

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Cumulative Update 3 (CU3)

May 12, 2021

Release date: May 12, 2021

About this release

StoreFront 1912 LTSR Cumulative Update 3 (CU3) fixes 10 issues reported since the CU2 release of the 1912 LTSR.

StoreFront 1912 LTSR Cumulative Update 2 (CU2)

StoreFront 1912 LTSR Cumulative Update 1 (CU1)

StoreFront 1912 LTSR (initial release)

Known issues in this release

Citrix Product Subscription Advantage Eligibility Dates

Fixed issues in 1912 LTSR CU3

July 15, 2021

Compared to: StoreFront 1912 LTSR CU2

StoreFront 1912 LTSR CU3 contains all fixes included in the 1912 LTSR initial release, CU1 release, CU2 release, and the following new fixes:

- When you log on to StoreFront, this error message might appear:

  Cannot Complete Your Request

  The issue occurs when enumerating applications with verbose logging enabled and any of the enumerated applications with a command-line argument contains a **{**. [CVADHELP-16227]

- The StoreFront does not hide apps from **All Apps** that appear in a featured category through the customization code described in Support for the unified user experience. [CVADHELP-16577]

- When you launch more than 10 applications using Internet Explorer, an extra scroll bar might appear. [CVADHELP-16605]

- With socket pooling enabled, attempts to log on to StoreFront might fail with this error message:

  Cannot Complete your Request

  The issue occurs when there is a TCP dynamic port exhaustion.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

[CVADHELP-16625]

- After upgrading StoreFront from version 7.15 LTSR CU4, VDI desktops with the same host name might appear in random order instead of serial order. [CVADHELP-16723]
- Attempts to launch a provisioned VDI desktop from the Delivery Group with the App Protection feature enabled might fail. The following behaviors might be observed:
  - When you launch the desktop using Citrix Workspace app for Windows, a spinning circle appears until the StoreFront times out.
  - When you launch the desktop using Citrix Workspace app for Mac, this error message appears:

    Cannot Complete your Request

  [CVADHELP-16800]
- After installing or upgrading StoreFront to version 1912 LTSR CU2, joining the StoreFront server group might fail. Also, configuration changes might not propagate to the other servers. [CVADHELP-17107]
- The Secure Ticket Authority update of the Citrix Gateway object might not get reflected in the Store Service's web.config file when the **Usage or role** of the Citrix Gateway is selected as **HDX routing only** or **Authentication and HDX routing**. The issue occurs when multiple optimal gateways are configured. [CVADHELP-17112]
- Clicking a website shortcut for the first time through Citrix Receiver utilizing SAML authentication might require multiple attempts. [CVADHELP-17137]

Cumulative Update 2 (CU2)

November 24, 2020

Release date: November 19, 2020

About this release

StoreFront 1912 LTSR Cumulative Update 2 (CU2) fixes nine issues reported since the CU1 release of the 1912 LTSR.

StoreFront 1912 LTSR Cumulative Update 1 (CU1)

StoreFront 1912 LTSR (initial release)

Known issues in this release

Citrix Product Subscription Advantage Eligibility Dates

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Fixed issues in 1912 LTSR CU2

November 17, 2020

Compared to: StoreFront 1912 LTSR CU1

StoreFront 1912 LTSR CU2 contains all fixes included in the 1912 LTSR initial release, the CU1 release, and the following new fixes:

- StoreFront stores have been using the unified user experience since StoreFront 1903. Some customers have reported that the way unified experience displays sub-categories in the Categories view is suboptimal for their business processes, and that it confuses their users. At this release, the Citrix StoreFront management console provides an option for stores to use a 'collapsed' Categories view instead.

  Collapsed Categories view hides the contents of any sub-categories until they are opened, and provides 'breadcrumb trail' navigation. For more information on the collapsed Categories view, and details of configuring it, see Support for the unified user experience. The **SetSTFWebReceiverUserInterface** PowerShell command has a new `CategoryViewCollapsed` parameter to control the categories view, see Citrix StoreFront 1912 SDK PowerShell Modules. [LCM-8241]

- When a custom config file is present in the store folder, the custom file might replace the content of the web.config file in the store folder. The issue occurs when you upgrade StoreFront. [CVADHELP-13485]

- In the StoreFront console, attempts to add domain names that contain an underscore (_) to a trusted domain list might fail. [CVADHELP-14213]

- Citrix StoreFront might fail to enumerate applications. The issue occurs when StoreFront connects to a Delivery Controller that has a certificate chain with an unsupported Certificate Policies extension. [CVADHELP-14328]

- Applications protected by app protection policies are not enumerated on StoreFront web stores. The issue occurs if you add more than two store sites on supported Citrix Workspace app versions. [CVADHELP-14637]

- When you attempt to launch an application using its shortcut, the application appears as undefined and the **Install** button appears for non-Citrix Endpoint Management applications. [CVADHELP-14808]

- On macOS, client detection might fail with an error: The URL cannot be opened. When you click the **Detect Receiver** button, StoreFront redirects the client to the error message. [CVADHELP-15073]

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- Attempts to launch a session using Citrix Workspace app for Mac might fail. The issue occurs when the session is from a delivery group with the app protection feature enabled. [CVADHELP-15751]
- On a StoreFront store, top-level applications might be listed under a subcategory in the Categories view. [CVADHELP-16179]

Cumulative Update 1 (CU1)

May 12, 2020

Release date: May 7, 2020

About this release

StoreFront 1912 LTSR Cumulative Update 1 (CU1) fixes more than eight issues reported since the initial release of the 1912 LTSR.

StoreFront (initial release)

Known issues in this release

Citrix Product Subscription Advantage Eligibility Dates

Fixed issues in 1912 LTSR CU1

September 9, 2020

Compared to: StoreFront 1912 LTSR initial release

StoreFront 1912 LTSR CU1 contains all fixes included in the 1912 LTSR initial release, plus the following, new fixes:

- Security Assertion Markup Language (SAML) authentication might fail when you use a third-party application as an Identity Provider (IdP). The following error message appears:

  `There was a failure with the mapped account.` [CVADHELP-13396]
- When you log on to StoreFront, application enumeration might take a long time to complete. The issue occurs if you type your user name in `domain\username` format and user authentication is delegated to Delivery Controllers. [CVADHELP-13891]

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- After you refresh Citrix Workspace app, the **Details** options that let you see the details of each app might disappear. If you log on or add the account information for the first time, the issue does not occur on initial refresh. But, the issue occurs on subsequent refreshes. [CVADHELP-13949]
- Non-English language versions of the StoreFront metainstaller might display some strings incorrectly. [CVADHELP-14030]
- When the connection between the Citrix Cloud Connector and the Citrix Virtual Apps and Desktops service is lost, attempts to launch published applications or desktops through StoreFront might fail. [CVADHELP-14075]
- Connections through Citrix Gateway might fail with the following error message:

  `Cannot Complete Request.`

  The issue occurs after you use the PowerShell command to add the Global Server Load Balancing (GSLB) URL. [CVADHELP-14354]
- When you install a Delivery Controller, StoreFront might not be installed by default. To install it, use the Citrix StoreFront option from the Citrix Virtual Apps and Desktops metainstaller. [LCM-7335]
- This release contains a fix which addresses a security vulnerability. For more information, see Knowledge Center article CTX277455. [LCM-7272]

What's new

May 1, 2020

What's new in 1912 LTSR

Version 1912 of StoreFront includes the following new features and enhancements:

StoreFront Protocol Handler Support now includes Chrome devices with Workspace app for Android

When users on Chrome devices open a Citrix Receiver for Web site, with Citrix Workspace app for Android 1912 or higher installed, the browser automatically opens ICA files using Citrix Workspace app for Android at launch.

The client detection work flow for Android—which determines whether Citrix Workspace app for Android is installed—is now identical to Citrix Workspace app for Windows and Citrix Workspace app for

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Mac when the Chrome browser is used on Chrome devices. In previous releases, users on Chrome devices were required to manually open a downloaded ICA file first.

Support for app protection policies

StoreFront 1912 supports app protection policies to enhance security when other Citrix components, such as Citrix Workspace app and Citrix Virtual Apps and Desktops delivery controllers, also support the app protection feature. App protection policies are set at the Delivery Group level, and Citrix Virtual Apps and Desktops determines whether app protection policies are used. You need to manually enable the app protection feature within StoreFront. When StoreFront receives requests containing the HTTP header X-Citrix-AppProtection-Capable from a Citrix Workspace app that supports app protection policies, StoreFront automatically sends a smart access tag to Citrix Virtual Apps and Desktops indicating that it supports app protection policies. For details of configuring Delivery Groups with app protection policies, see App protection.

To enable app protection on a StoreFront server, run the following PowerShell command on the StoreFront server: `Add-STFFeatureState -Name "Citrix.StoreFront.AppProtectionPolicy.Control"-IsEnabled $True`. (In a multiple-server StoreFront deployment, you must manually propagate these changes to all the other servers in the server group. See Propagate local changes to a server group.)

To verify that the feature is enabled on a StoreFront server, use the following PowerShell command:
`Get-STFFeatureState -Name "Citrix.StoreFront.AppProtectionPolicy.Control`.

Desktop Appliance sites no longer supported

StoreFront support for users to access desktops on Desktop Appliance sites was announced as deprecated in Citrix Virtual Apps and Desktops 7 1811. At this release, Desktop Appliance sites are no longer supported, and we recommend using Citrix Workspace app Desktop Lock for all non-domain-joined use cases.

> **Warning:**
>
> When you upgrade to StoreFront 1912, any Desktop Appliance sites in your deployment are automatically removed. See Upgrade StoreFront.

StoreFront PowerShell SDK

The StoreFront PowerShell SDK has been republished as version 1912. You can no longer create or manage Desktop Appliance sites using PowerShell.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Fixed issues in 1912 LTSR

May 2, 2020

The following issues have been fixed since version 1909:

- On-Prem StoreFront cannot add launch gateway for web links in MMC. [WSP-4368]
- LCM-6351: Old registry keys of CitrixPrivilegedService_x64.msi were not removed after upgrade DDC. [WSP-4785]
- If VMware VMTools v10.3.x is installed on your StoreFront server when you attempt to upgrade StoreFront to version 1906 using the Citrix Virtual Apps and Desktops 7 1906 meta-installer, the upgrade fails. StoreFront is upgraded successfully by the stand-alone StoreFront 1906 installer, but StoreFront 1906 is not added to the Windows Add/Remove Programs List. [WSP-4895]
- Customisation to truncate long app names no longer works in X1.1 Purple UI. [WSP-4899]
- Upgrades that include 2.6, 3.0.1, 3.5, 3.8 in their upgrade history to 3.12 CU* and above may fail if the KCD service is in Stopped state. [WSP-5160]
- Update `http://downloadplugins.citrix.com` to deliver Citrix Workspace app instead of end-of-life Citrix Receivers. [WSP-5303]

Known issues

February 22, 2022

Known issues in StoreFront 1912 CU5

There are no new known issues in Cumulative Update 5.

Known issues in StoreFront 1912 CU4

There are no new known issues in Cumulative Update 5.

Known issues in StoreFront 1912 CU3

- Import and export of StoreFront configurations between different product versions isn't possible. The StoreFront 1912 LTSR initial release and the later Cumulative Updates are considered to be different product versions for this limitation. For example, import and export configuration between StoreFront 1912 LTSR initial release and 1912 LTSR initial release, or between StoreFront

© 1999–2022 Citrix Systems, Inc. All rights reserved.

versions 1912 LTSR CU1 and 1912 LTSR CU1 is also possible. But not between versions 1912 LTSR CU2 and 1912 LTSR CU3. [LCM-7104]

- Highlighted tabs in Citrix Receiver for Web sites ignore the 'Link color' value specified in the **Customize Appearance** tab of the **Edit Receiver for Web site** dialog. Instead, highlighted tabs display in purple (#985d94).

  As a workaround, specify the desired color. Add the following lines to the CSS style sheet in the custom folder of your store web (for example C:\inetpub\wwwroot\Citrix\StoreWeb\custom\style.css): [LCM-9536]

```
.theme-header-selection-color.selected
{
 background-color:<desired color>;  }

<!--NeedCopy-->
```

Known issues in StoreFront 1912 CU2

- Attempts to join a StoreFront server to an existing server group, which is using a supported OS with German, Spanish, or French locale settings, fail. Join attempts succeed with server groups using supported OS and other locale settings. [CVADHELP-17107]
- Applications in a StoreFront store fail to enumerate and launch and an SSL connection error is reported. This issue occurs if the delivery controller is installed on Windows Server 2016 or Windows Server 2019, and StoreFront is installed on Windows Server 2012 R2. To resolve this issue, the cipher suite order list must include the TLS_ECDHE_* cipher suites and these cipher suites must precede any other cipher suites. [LCM-9305]
- Applications in a StoreFront store fail to enumerate and launch, and an SSL connection error is reported. It happens if you use the Citrix ADC load balancing feature to distribute the load to the delivery controller servers. And StoreFront is using HTTPS to communicate with the load balancing delivery controller services. To resolve this issue, the cipher suite order list on Citrix ADC must include only the `TLS_ECDHE_\*` cipher suites. If you have assigned a delivery controller server as STA Server in Citrix ADC or StoreFront which is outside your site, the cipher suite order list on StoreFront must also include the TLS_ECDHE_* cipher suites AND these cipher suites must precede any other cipher suites. [LCM-9308]

Known issues in StoreFront 1912 CU1

No new known issues have been observed in Cumulative Update 1.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Known issues in StoreFront 1912

- Subscription propagation between members of a StoreFront server group fails in the following case: When you disable TLS 1.0 in Windows, and the Windows Server is using the .NET 4.5 Framework server. By default, the .NET 4.5 Framework uses TLS 1.0 only. A workaround for this issue is to upgrade the .NET Framework on the server to 4.7 or later (which use TLS 1.2 by default). [STF-2413]
- A known third-party issue exists with smart card authentication and Microsoft Edge. To work around this issue, use Internet Explorer. [DNA-47809]
- Workspace control reconnects to only one app session instead of all the apps in the workspace. This issue is seen if using Chrome to access the Receiver for Web site. To work around this issue, click Connect on each disconnected app. [DNA-25140, DNA-22561]
- When StoreFront is installed on Windows Server 2012 R2, it fails to register with the Citrix Analytics service (CAS). It happens when the C++ run time software components aren't already installed. The StoreFront stand-alone installer does not install these components. A simple work-around is to install C++ run time before or after StoreFront is installed. [WSP-4412]

Third party notices

May 1, 2020

StoreFront might include third party software licensed under the terms defined in the following document:

StoreFront Third Party Notices (PDF Download)

System requirements

November 8, 2021

When planning your installation, Citrix recommends at least 6 GB of RAM for the StoreFront server. The subscription store service requires a minimum of 5 MB disk space, plus approximately 8 MB for every 1000 application subscriptions. All other hardware specifications must meet the minimum requirements for the installed operating system.

> **Note:**

© 1999–2022 Citrix Systems, Inc. All rights reserved.

> Upgrading to the latest current release from an older current release that is now End of Life is not supported. For more information see CTX200356.

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

- Windows Server 2019 Datacenter and Standard editions
- Windows Server 2016 Datacenter and Standard editions
- Windows Server 2012 R2 Datacenter and Standard editions

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. All the servers in a multiple server deployment must run the same operating system version with the same locale settings.

StoreFront server groups containing mixtures of operating system versions and locales are not supported. There is no limit of the number of servers in a StoreFront server group. However, from a capacity perspective based on simulations, there is no advantage of server groups containing more than three servers. 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 minimum latency criteria. See Scalability.

Before you can install StoreFront, Windows PowerShell (version 4.0 or later) and Microsoft Management Console (version 3.0 or later) must be installed on the web server. These are both default components of Windows Server.

The StoreFront installer checks that the following prerequisites are installed and enabled before installing StoreFront. By default these prerequisites are provided as feature packages by the OS. If the StoreFront installer detects that any of these prerequisites are missing or disabled, they are automatically installed and enabled:

- Microsoft .NET Framework (version 4.5.1 or later)
- Microsoft ASP.NET (version 4.5 or later)
- Microsoft Visual C++ 2017 (x64) Runtime (v141)
- Microsoft Internet Information Services (IIS)

  IIS is added by the web server 'Windows Server' role, with its version dependent on the chosen operating system. For reference, the StoreFront installer adds the following IIS roles:

  - Web-Static-Content
  - Web-Default-Doc
  - Web-Http-Errors
  - Web-Http-Redirect
  - Web-Http-Logging
  - Web-Mgmt-Console

© 1999–2022 Citrix Systems, Inc. All rights reserved.

  - Web-Scripting-Tools
  - Web-Windows-Auth
  - Web-Basic-Auth
  - Web-AppInit
  - Web-Asp-Net45
  - Net-Wcf-Tcp-PortSharing45

  The relative path to StoreFront in IIS must be the same on all the servers in a server group.

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

- TCP ports 80 and 443 are used for HTTP and HTTPS communications, respectively, and must be accessible from both inside and outside the corporate network.
- TCP port 808 is used for communications between StoreFront servers and must therefore be accessible.
- A TCP port randomly selected from all unreserved ports is used for communications between the StoreFront servers in a server group. When you install StoreFront, a Windows Firewall rule is configured enabling access to the StoreFront executable. However, since the port is assigned randomly, you must ensure that any firewalls or other devices on your internal network do not block traffic to any of the unassigned TCP ports.
- TCP port 8008 is used by Citrix Workspace app for HTML5, or supported versions of Citrix Receiver and Citrix Workspace app, where enabled, for communications from local users on the internal network to the servers providing their desktops and applications.

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

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 server requirements

StoreFront stores aggregate desktops and applications from the following products.

- Citrix Virtual Apps and Desktops 7 1912 LTSR

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- Citrix Virtual Apps and Desktops 7 1909
- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp and XenDesktop 7.15 LTSR *
- XenApp and XenDesktop 7.6 LTSR *

* For more information about using this Current Release (CR) in a Long Term Service (LTSR) environment and other frequently asked questions, see Knowledge Center article.

Citrix Gateway requirements

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

- Citrix Gateway 13.0
- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1

Citrix Workspace app for HTML5 requirements

To enable users to access desktops and applications using Citrix Workspace app for HTML5 running on Receiver for Web sites, the following additional requirements apply.

For internal network connections, Citrix Workspace app for HTML5 enables access to desktops and applications provided by the following products.

- Citrix Virtual Apps and Desktops 7 1912 LTSR
- Citrix Virtual Apps and Desktops 7 1909
- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp and XenDesktop 7.15 LTSR
- XenApp and XenDesktop 7.6 LTSR

> **Note:**
>
> Citrix Workspace app for HTML5 only launches desktops and apps using internal network connections when secure connections to the VDAs hosting those resources have been configured. You cannot use HTTP connections to the VDAs that host the apps and desktops.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

For remote users outside the corporate network, Citrix Workspace app for HTML5 enables access to desktops and applications through the following versions of Citrix Gateway and NetScaler Gateway.

- Citrix Gateway 13.0
- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1

For users connecting through Citrix Gateway, Citrix Workspace app for HTML5 enables access to desktops and applications provided by the following products.

- Citrix Virtual Apps and Desktops 7 1912 LTSR
- Citrix Virtual Apps and Desktops 7 1909
- Citrix Virtual Apps and Desktops 7 1906
- Citrix Virtual Apps and Desktops 7 1903
- Citrix Virtual Apps and Desktops 7 1811
- Citrix Virtual Apps and Desktops 7 1808
- XenApp and XenDesktop 7.15 LTSR
- XenApp and XenDesktop 7.6 LTSR

User device requirements

StoreFront provides a number of different options for users to access their desktops and applications. Citrix Workspace app users can either access stores through Citrix Workspace app, or use a web browser to log on to a Citrix Receiver for Web site for the store. For users who cannot install Citrix Workspace app but who have an HTML5-compatible web browser, you can provide access to desktops and applications directly within the web browser by enabling Citrix Workspace app for HTML5 on your Citrix Receiver for Web site.

Users with PCs running the Citrix Desktop Lock, along with older Citrix clients that cannot be upgraded, must connect through the XenApp Services URL for the store.

To deliver Microsoft Application Virtualization (App-V) sequences to users, you also require a supported version of the Microsoft Application Virtualization Desktop Client. For more information, see Managing Streamed Applications. Users cannot access offline applications or App-V sequences through Citrix Receiver for Web sites.

Using Citrix Workspace app to access StoreFront stores

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

You can connect to StoreFront stores through Citrix Gateway using the Citrix Gateway plug-in, ICA proxy or clientless VPN (cVPN). See Unified user experience.

Accessing stores through Citrix Receiver for Web sites

To access Citrix Receiver for Web sites from both internal network connections and through Citrix Gateway, use latest version of the following browsers:

On Windows

- Internet Explorer 11
- MS Edge (based on Chromium)
- Google Chrome
- Mozilla Firefox

On Mac

- Safari
- Google Chrome
- Mozilla Firefox

On Linux

- Google Chrome
- Mozilla Firefox

Connections through Citrix Gateway can be made using the Citrix Gateway plug-in, ICA proxy or clientless VPN (cVPN). Additionally, specific versions of Citrix Gateway are required to enable connections from outside the corporate network. For more information, see Infrastructure requirements.

Launching resources through Citrix Receiver for Web sites

Citrix Receiver for Web sites support launches either via a natively installed Citrix Workspace app, or via Citrix Workspace app for HTML5. All of the browsers listed above are HTML5 compliant and support HTML5 resource launches. Depending on your Receiver for Web configuration, it is possible for end users to switch between the two launch methods.

Accessing stores through XenApp Services URLs

You 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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

3.4 Enterprise and older clients that only support connections via PNAgent. Connections through Citrix Gateway, where supported, can be made using both the Citrix Gateway plug-in and clientless access.

Smart card requirements

Using Citrix Receiver for Windows 4.x, and Citrix Workspace app 1808 for Windows or later, 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.

Authenticating through Citrix Gateway

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

- Citrix Gateway 13.0
- Citrix Gateway 12.1
- NetScaler Gateway 12.0
- NetScaler Gateway 11.1

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 browsing to Citrix Receiver for Web sites in HTML5-compatible browsers. Citrix Analytics service data is supplied when launching resources using either the

© 1999–2022 Citrix Systems, Inc. All rights reserved.

native Citrix Workspace app or using HTML5.
- 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.

Plan your StoreFront deployment

March 2, 2021

StoreFront employs Microsoft .NET technology running on Microsoft Internet Information Services (IIS) to provide enterprise app stores that aggregate resources and make them available to users. StoreFront integrates with your Citrix Virtual Apps and Desktops deployments, providing users with a single, self-service access point for their desktops and applications.

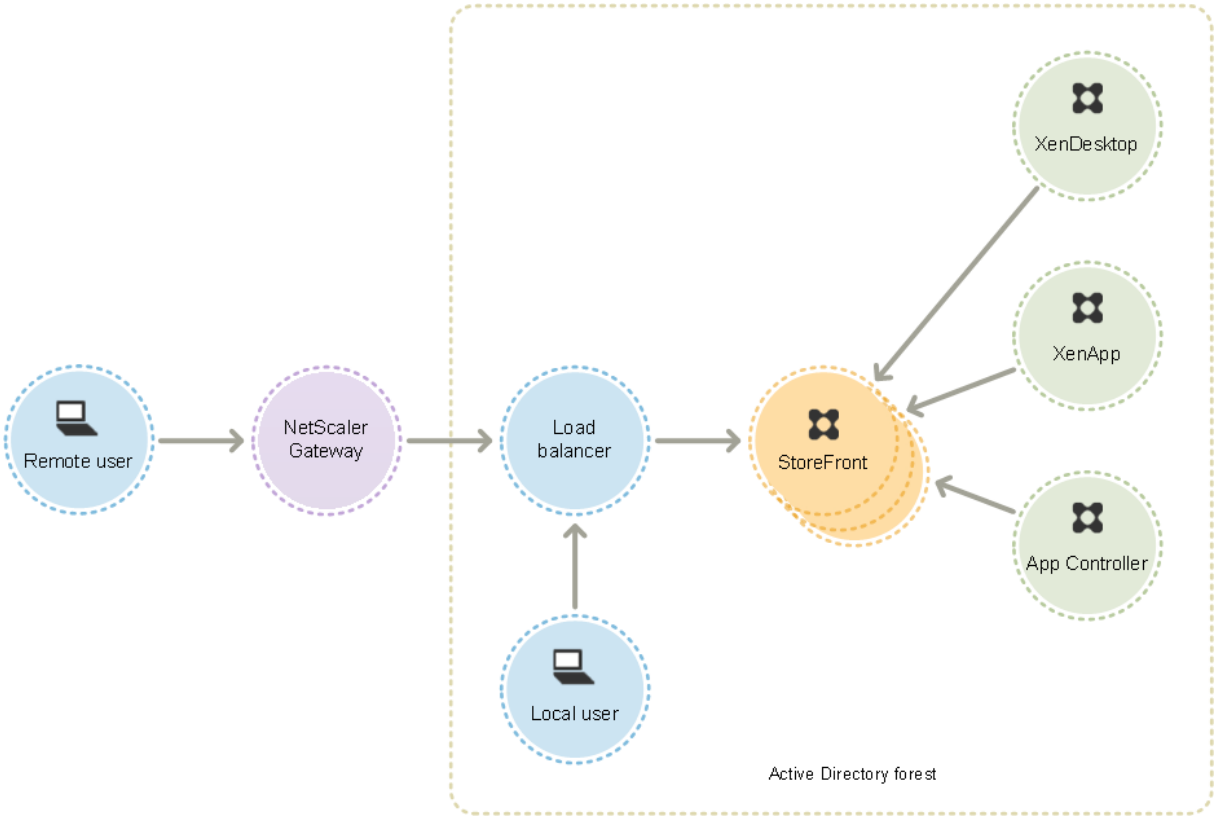
StoreFront comprises the following core components:

- The authentication service authenticates users to Microsoft Active Directory, ensuring that users do not need to log on again to access their desktops and applications. For more information, see User authentication.
- Stores enumerate and aggregate desktops and applications from Citrix Virtual Apps and Desktops. Users access stores through Citrix Workspace app, Citrix Receiver for Web sites, and XenApp Services URLs. For more information, see User access options.
- The subscription store service records details of users' application subscriptions and updates their devices to ensure a consistent roaming experience. For more information about enhancing the experience for your users, see Optimize the user experience.

StoreFront can be configured either on a single server or as a multiple server deployment. Multiple server deployments not only provide additional capacity, but also greater availability. The modular architecture of 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.

The figure shows a typical StoreFront deployment.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



Load balancing

For multiple server deployments, external load balancing through, for example, Citrix ADC or Windows Network Load Balancing is required. Configure the load balancing environment for failover between servers to provide a fault-tolerant deployment. For more information about load balancing with Citrix ADC , see Load Balancing. For more information about Windows Network Load Balancing, see https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831698(v=ws.11).

Active load balancing of requests sent from StoreFront to Citrix Virtual Desktops sites and Citrix Virtual Apps farms is recommended for deployments with thousands of users or where high loads occur, such as when a large number of users log on over a short period of time. Use a load balancer with built-in XML monitors and session persistency, such as Citrix ADC .

If you deploy SSL-terminating load balancer or if you need to troubleshoot, you can use the PowerShell cmdlet **Set-STFWebReceiverCommunication**.

Syntax:

```
Set-STFWebReceiverCommunication [-WebReceiverService] <
    WebReceiverService> [[-Loopback] <On | Off | OnUsingHttp>] [[-
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
        LoopbackPortUsingHttp] <Int32>]
```

The valid values are:

- **On** - This is the default value for new Citrix Receiver for Web sites. Citrix Receiver for Web uses the schema (HTTPS or HTTP) and port number from the base URL but replaces the host with the loopback IP address to communicate with StoreFront Services. This works for single server deployments and deployments with a non SSL-terminating load balancer.
- **OnUsingHttp** - Citrix Receiver for Web uses HTTP and the loopback IP address to communicate with StoreFront Services. If you are using an SSL-terminating load balancer, select this value. You must also specify the HTTP port if it is not the default port 80.
- **Off** - This turns off loopback and Citrix Receiver for Web uses the StoreFront base URL to communicate with StoreFront Services. If you perform an in-place upgrade, this is the default value to avoid disruption to your existing deployment.

For example, if you are using an SSL-terminating load balancer, your IIS is configured to use port 81 for HTTP and the path of your Citrix Receiver for Web site is /Citrix/StoreWeb, you can run the following command to configure the Citrix Receiver for Web site:

```
1 $wr = Get-STFWebReceiverService -VirtualPath /Citrix/StoreWeb
2 Set-STFWebReceiverCommunication -WebReceiverService $wr -Loopback
     OnUsingHttp -LoopbackPortUsingHttp 81
```

> **Note:**
>
> Switch off loopback to use any web proxy tool like Fiddler to capture the network traffic between Citrix Receiver for Web and StoreFront Services.

Active Directory considerations

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.

User connections

In a production environment, Citrix recommends using HTTPS to secure communications between StoreFront and users' devices. To use HTTPS, StoreFront requires that the IIS instance hosting the authentication service and associated stores is configured for HTTPS. In the absence of the appropriate

© 1999–2022 Citrix Systems, Inc. All rights reserved.

IIS configuration, StoreFront uses HTTP for communications. You can change from HTTP to HTTPS at any time, provided the appropriate IIS configuration is in place.

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

Multiple Internet Information Services (IIS) websites

StoreFront enables 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. This can be used, for example, to allow multiple Storefront URLs and certificates to bind on the same StoreFront server group.

Start by creating two websites, in addition to the default web site. After creating multiple websites in IIS, use the PowerShell SDK to create a StoreFront deployment in each of those IIS websites. For more information about creating websites in IIS, see Create a Web Site.

> **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.

Example: To create two IIS website deployments—one for applications and one for desktop

```
Add-STFDeployment -SiteID 1 -HostBaseURL "https://www.storefront.app.com"
Add-STFDeployment -SiteID 2 -HostBaseURL "https://www.storefront.desktop.com"
```

StoreFront disables the management console when it detects multiple sites and displays a message to that effect.

For more information, see Before installing and configuring.

Scalability

The number of Citrix Workspace app users supported by a StoreFront server group depends on the hardware you use and on the level of user activity. Based on simulated activity where users log on, enumerate 100 published applications, and start one resource, expect a single StoreFront server with

© 1999–2022 Citrix Systems, Inc. All rights reserved.

the minimum recommended specification of two virtual CPUs running on an underlying dual Intel Xeon L5520 2.27 Ghz processor server to enable up to 30,000 user connections per hour.

Expect a server group with two similarly configured servers in the group to enable up to 60,000 user connections per hour; three nodes up to 90,000 connections per hour; four nodes up to 120,000 connections per hour; five nodes up to 150,000 connections per hour; six nodes up to 175,000 connections per hour.

The throughput of a single StoreFront server can also be increased by assigning more virtual CPUs to the system, with four virtual CPUs enabling up to 55,000 user connections per hour and eight virtual CPUs enabling 80,000 connections per hour.

The minimum recommended memory allocation for each StoreFront server is described in System requirements. When using Citrix Receiver for Web, assign an additional 700 bytes per-resource, per-user in addition to the base memory allocation. Here "resource" means a published application or desktop assign to the user. Similarly, when using Citrix Workspace app, design environments to allow an extra 700 bytes per-resource, per-user in addition to the base memory requirements for this version of StoreFront.

For example, if one application and two desktops are assigned to a user and provide access for three users, the minimum additional memory would be:

```
(700 Byte x 1 "application" + 700 Byte x 2 "desktops" )x 3 "users" /1000 =
6.3 KB.<!--NeedCopy-->
```

As your usage patterns might be different than those simulated above, your servers might support more or fewer numbers of users connections per hour.

> **Important:**
>
> 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.
>
> StoreFront server groups containing mixtures of operating system versions, or mixtures of operating system languages or locale configurations, are not supported.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Timeout considerations

Occasionally, network issues or other problems can occur between a StoreFront store and the servers that it contacts, causing delays or failures for users. You can use the timeout settings for a store to tune this behavior. If you specify a short timeout setting, StoreFront quickly abandons a server and tries another one. This is useful if, for example, you have configured multiple servers for failover purposes.

If you specify a longer timeout, StoreFront waits longer for a response from a single server. This is beneficial in environments where network or server reliability is uncertain and delays are common.

Citrix Receiver for Web also has a timeout setting, which controls how long a Citrix Receiver for Web site waits for a response from the store. Set this timeout setting to a value at least as long as the store timeout. A longer timeout setting allows for better fault tolerance, but users might experience long delays. A shorter timeout setting reduces delays for users, but they might experience more failures.

For information about setting timeouts, see Communication time-out duration and server retry attempts and Communication time-out duration and retry attempts.

User access options

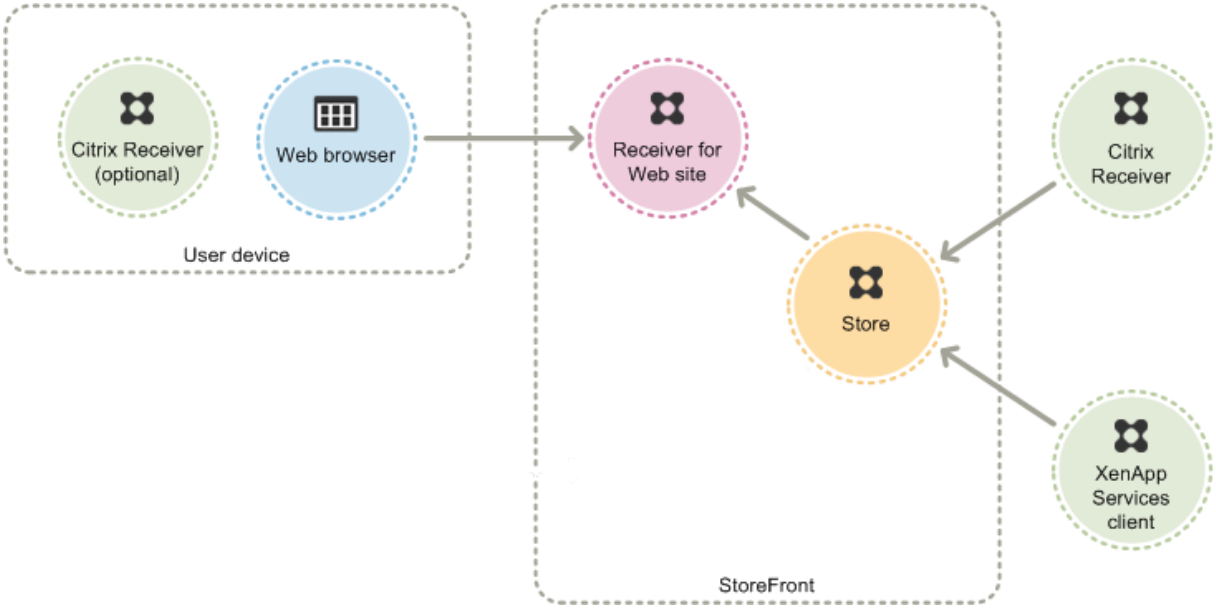
November 24, 2021

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

- Citrix Receiver or Citrix Workspace app - Users with compatible versions of Citrix Receiver or Citrix Workspace app can access StoreFront stores within the Citrix Receiver or Citrix Workspace app user interface. This provides the best user experience and the greatest functionality.
- Citrix Receiver for Web sites - Users with compatible web browsers can access StoreFront stores by browsing to Citrix Receiver for Web sites. By default, users also require a compatible version of Citrix Receiver or Citrix Workspace app to access their desktops and applications. However, you can configure your Citrix Receiver for Web sites to enable users with HTML5-compatible browsers to access their resources without installing Citrix Receiver or Citrix Workspace app. When you create a new store, a Citrix Receiver for Web site is created for the store by default.
- XenApp Services URLs - Users of domain-joined desktop appliances and repurposed PCs running the Citrix Desktop Lock, along with users who have older 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.

The figure shows the options for users to access StoreFront stores:

© 1999–2022 Citrix Systems, Inc. All rights reserved.



Citrix Receiver or Citrix Workspace app

Accessing stores from within the Citrix Receiver or Citrix Workspace app user interface provides the best user experience and the greatest functionality. For the Citrix Receiver or Citrix Workspace app versions that can be used to access stores in this way, see System Requirements. References to "Citrix Workspace app" in this document also represent the supported versions of Citrix Receiver unless otherwise noted.

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

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 Configure and install using command-line parameters in the Citrix Receiver for Windows or Citrix Workspace app for Windows documenta-

© 1999–2022 Citrix Systems, Inc. All rights reserved.

> tion.

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, Citrix Receiver for Web sites offer users a provisioning file for the single store for which the site is configured. You could instruct your users to visit the Receiver for Web sites 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 Mac OS, you can use the Citrix Receiver for Mac or 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.

Manual configuration

More advanced users can create new accounts by entering store URLs into Citrix Workspace app. For more information, see the Citrix Workspace app documentation.

Email-based account discovery

Users who install Citrix Workspace app on a device for the first time can set up accounts by entering their email addresses, provided that they download Citrix Workspace app from the Citrix website or a Citrix Workspace app download page hosted within your internal network. You configure Service Location (SRV) locator resource records for Citrix Gateway or StoreFront on your Microsoft Active Directory Domain Name System (DNS) server. Users do not need to know the access details for their stores, instead they enter their email addresses during the Citrix Workspace app initial configuration process. Citrix Workspace app contacts the DNS server for the domain specified in the email address and obtains the details you added to the SRV resource record. Users are then presented with a list of stores that they can access through Citrix Workspace app.

Configure 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 by entering their email addresses. Provided that they

© 1999–2022 Citrix Systems, Inc. All rights reserved.

download Citrix Workspace app from the Citrix website or a Citrix Workspace app download page hosted within your internal network, users do not need to know the access details for their stores when they install and configure Citrix Workspace app. Email-based account discovery is available if Citrix Workspace app is downloaded from any other location, such as a Receiver for Website. Note that *ReceiverWeb.exe* or *ReceiverWeb.dmg* downloaded from Citrix Receiver for Web does not prompt users to configure a store. Users can still use Add Account and enter their email address

During the initial configuration process, Citrix Workspace app prompts users to enter either an email address or a store URL. When a user enters an email address, Citrix Workspace app contacts the Microsoft Active Directory Domain Name System (DNS) server for the domain specified in the email address to obtain a list of available stores from which the user can select.

To enable Citrix Workspace app to locate available stores on the basis of users' email addresses, you configure Service Location (SRV) locator resource records for Citrix Gateway or StoreFront on your DNS server. As a fallback, you can also deploy StoreFront on a server named "discoverReceiver.domain," where domain is the domain containing your users' email accounts. If no SRV record is found in the specified domain, Citrix Workspace app searches for a machine named "discoverReceiver" to identify a StoreFront server.

You must install a valid server certificate on the Citrix Gateway appliance or StoreFront server to enable email-based account discovery. The full chain to the root certificate must also be valid. For the best user experience, install a certificate with a Subject or Subject Alternative Name entry of discoverReceiver.domain,where domain is the domain containing your users' email accounts. Although you can use a wildcard certificate for the domain containing your users' email accounts, you must first ensure that the deployment of such certificates is permitted by your corporate security policy. Other certificates for the domain containing your users' email accounts can also be used, but users will see a certificate warning dialog box when Citrix Workspace app first connects to the StoreFront server. Email-based account discovery cannot be used with any other certificate identities.

To enable email-based account discovery for users connecting from outside the corporate network, you must also configure Citrix Gateway with the StoreFront connection details. For more information, see Connecting to StoreFront by Using Email-Based Discovery.

Add an SRV record to your DNS server

1. On the Windows **Start** screen, click **Administrative Tools** and, in the **Administrative Tools** folder, click **DNS**.
2. In the left pane of **DNS Manager**, select your domain in the forward or reverse lookup zones. Right-click the domain and select **Other New Records**.
3. In the **Resource Record Type** dialog box, select **Service Location (SRV)** and then click **Create Record**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

4. In the **New Resource Record** dialog box, enter in the **Service** box the host value **_citrixreceiver**.
5. Enter in the **Protocol** box the value **_tcp**.
6. In the **Host offering this service** box, specify 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.
7. If you configured an SRV record for your Citrix Gateway appliance, add the StoreFront connection details to Citrix Gateway in a session profile or global setting.

Citrix Receiver for Web sites

Users with compatible web browsers can access StoreFront stores by browsing to Citrix Receiver for Web sites. When you create a new store, a Citrix Receiver for Web site is automatically created for the store. The default configuration for Citrix Receiver for Web sites requires that users install a compatible version of Citrix Workspace app to access their desktops and applications. For more information about the Citrix Workspace app and web browser combinations that can be used to access Citrix Receiver for Web sites, see User device requirements.

By default, when a user accesses a Citrix Receiver for Web site from a computer running Windows or Mac OS X, the site attempts to determine whether Citrix Workspace app is installed on the user's device. If Citrix Workspace app cannot be detected, the user is prompted to download and install it for their platform. The default download location is the Citrix website, but you can also copy the installation files to the StoreFront server and provide users with these local files instead. Storing the Citrix Workspace app installation files locally enables you to configure the site to offer users with older clients the option to upgrade to the version on the server. For more information about configuring deployment of Citrix Receiver for Windows or Citrix Workspace app for Windows and Citrix Receiver for Mac or Citrix Workspace app for Mac, see Configure Citrix Receiver for Web sites.

Citrix Workspace app for HTML5

Citrix Workspace app for HTML5 is a component of StoreFront that is integrated by default with Citrix Receiver for Web sites. You can enable Citrix Workspace app for HTML5 on your Citrix Receiver for Web sites so that users who cannot install Citrix Workspace app can still access their resources. With Citrix Workspace app for HTML5, users can access desktops and applications directly within HTML5-compatible web browsers without needing to install Citrix Workspace app. When a site is created,

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Citrix Workspace app for HTML5 is disabled by default. For more information about enabling Citrix Workspace app for HTML5, see Configure site behavior for users without Citrix Workspace app.

To access their desktops and applications using Citrix Workspace app for HTML5, users must access the Citrix Receiver for Web site with an HTML5-compatible browser. For more information about the operating systems and web browsers that can be used with Citrix Workspace app for HTML5, see User device requirements.

Citrix Workspace app for HTML5 can be used by both users on the internal network and remote users connecting through Citrix Gateway. For connections from the internal network, Citrix Workspace app for HTML5 only supports access to desktops and applications provided by a subset of the products supported by Citrix Receiver for Web sites. Users connecting through Citrix Gateway can access resources provided by a wider range of products if you chose Citrix Workspace app for HTML5 as an option when configuring StoreFront. Specific versions of Citrix Gateway are required for use with Citrix Workspace app for HTML5. For more information, see Infrastructure requirements.

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

By default, Citrix Workspace app for HTML5 starts desktops and applications in a new browser tab. However, when users start resources from shortcuts using Citrix Workspace app for HTML5, the desktop or application replaces the Citrix Receiver for Web site in the existing browser tab rather than appearing in a new tab. You can configure Citrix Workspace app for HTML5 so that resources are always started in the same tab as the Receiver for Web site. For more information, see Configure Citrix Workspace app for HTML5 use of browser tabs.

Resource shortcuts

You can generate URLs that provide access to desktops and applications available through Citrix Receiver for Web sites. 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 Receiver for Web site, where they log on if they have not already done so. The Citrix Receiver for Web site automatically starts the resource. In the case of applications, users are also subscribed to the application if they have not subscribed previously. For more information about generating resource shortcuts, see Configure Citrix Receiver for Web sites.

As with all desktops and applications accessed from Citrix Receiver for Web sites, users must either have installed Citrix Workspace app, or be able to use Citrix Workspace app for HTML5 to access resources through shortcuts. The method used by a Citrix Receiver for Web site depends on the site

© 1999–2022 Citrix Systems, Inc. All rights reserved.

configuration, on whether Citrix Workspace app can be detected on users' devices, and on whether an HTML5-compatible browser is used. 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 Receiver for Web site to the Local intranet or Trusted sites zones in Internet Explorer to avoid this extra step. By default, both workspace control and automatic desktop starts are disabled when users access Citrix Receiver for Web sites through shortcuts.

When you create an application shortcut, ensure that no other applications available from the Citrix Receiver for Web site 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 Citrix Receiver for Web site, 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. However, for users connecting through Citrix Gateway, websites hosting shortcuts are not validated because the URLs are not passed to StoreFront. To ensure that remote users can only access application shortcuts on trusted internal websites, configure Citrix Gateway to restrict user access to only those specific sites. For more information, see http://support.citrix.com/article/CTX123610.

Customize your sites

Citrix Receiver for Web sites provide a mechanism for customizing the user interface. You can customize strings, the cascading style sheet, and the JavaScript files. You can also add a custom pre-logon or post-logon screen, and add language packs.

Important considerations

Users accessing stores through a Citrix Receiver for Web site benefit from many of the features available with store access within Citrix Workspace app, such as application synchronization. When you decide whether to use Citrix Receiver for Web sites to provide users with to access your stores, consider the following restrictions.

- Only a single store can be accessed through each Citrix Receiver for Web site.
- Citrix Receiver for Web sites cannot initiate Secure Sockets Layer (SSL) virtual private network (VPN) connections. Users logging on through Citrix Gateway without a VPN connection cannot access web applications for which App Controller requires that such a connection is used.
- Subscribed applications are not available on the Windows Start screen when accessing a store through a Citrix Receiver for Web site.
- File type association between local documents and hosted applications accessed through Citrix Receiver for Web sites is not available.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- Offline applications cannot be accessed through Citrix Receiver for Web sites.
- Citrix Receiver for Web sites do not support Citrix Online products integrated into stores. Citrix Online products must be delivered with App Controller or made available as hosted applications to enable access through Citrix Receiver for Web sites.
- Citrix Workspace app for HTML5 can be used over HTTPS connections if the VDA is XenApp 7.6 or XenDesktop 7.6 and has SSL enabled or if the user is connecting using Citrix Gateway.
- To use Citrix Workspace app for HTML5 with Mozilla Firefox over HTTPS connections, users must type `about:config` in the Firefox address bar and set the `network.websocket.allowInsecureFromHTTPS` preference to true.

XenApp Services URLs

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 Receiver for Windows documentation.

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

Important considerations

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

- You cannot modify the XenApp Services URL for a store.
- You cannot modify XenApp Services URL settings by editing the configuration file, config.xml.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- 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.

User authentication

October 22, 2020

StoreFront supports a number of different authentication methods for users accessing stores; although, not all are available depending on the user access method and their network location. For security reasons, some authentication methods are disabled by default when you create your first store. For more information about enabling and disabling user authentication methods, see Create and configure the authentication service.

User name and password

Users enter their credentials and are authenticated when they access their stores. Explicit authentication is enabled by default. All user access methods support explicit authentication.

When a user employs Citrix Gateway to access Citrix Receiver for Web, Citrix Gateway handles the logon and password change at expiration. Users can make elective password changes with the Citrix Receiver for Web UI. After an elective password change, the Citrix Gateway session terminates and the user must log on again. Citrix Receiver for Linux or Citrix Workspace app for Linux users can change only expired passwords.

SAML authentication

Users authenticate to a SAML Identity Provider and are automatically logged on when they access their stores. StoreFront can support SAML authentication directly within the corporate network, without the need to go through Citrix Gateway. StoreFront supports only Service Provider Initiated (SP-initiated) sign-in, but does not support Identity Provider Initiated (IdP-initiated) sign-in.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

SAML (Security Assertion Markup Language) is an open standard used by identity and authentication products such as Microsoft AD FS (Active Directory Federation Services). With the integration of SAML authentication through StoreFront, administrators can allow users to, for example, log on once to their corporate network and then get single sign-on to their published apps.

Requirements:

- Implementation of the Citrix Federated Authentication Service (FAS). Unless FAS is installed there is no Single sign-on (SSO) authentication when users launch an app or desktop, and they therefore need to enter their credentials every time.
- SAML 2.0-compliant identity providers (IdPs):
  - Microsoft AD FS v4.0 (Windows Server 2016) using SAML bindings only (not WS-Federation bindings). For more information, see AD FS Deployment and AD FS Operations.
  - Microsoft AD FS v3.0 (Windows Server 2012 R2)
  - Citrix Gateway (configured as an IdP)
- Configure SAML authentication in StoreFront using the StoreFront management console in a new deployment (see Create a new deployment), or in an existing deployment (see Configure the authentication service). You can also configure SAML authentication using PowerShell cmdlets, see StoreFront SDK.
- Citrix Receiver (4.6 and later) or Citrix Workspace app for Windows, or Citrix Receiver for Web.

Using SAML authentication with Citrix Gateway is currently supported with Receiver for Web sites.

Domain pass-through

Users authenticate to their domain-joined Windows computers, and their credentials are used to log them on automatically when they access their stores.

When you install StoreFront, domain pass-through authentication is disabled by default. You can enable domain pass-through authentication for users connecting to stores through Citrix Workspace app and XenApp Services URLs. Citrix Receiver for Web sites support domain pass-through authentication for Internet Explorer, Microsoft Edge, Mozilla Firefox, and Google Chrome on domain-joined Windows client machines.

To enable domain pass-through authentication

1. Install Citrix Receiver for Windows or Citrix Workspace app for Windows or the Citrix Online plug-in for Windows on user devices. Ensure that pass-through authentication is enabled.
2. In the Citrix Receiver for Web site node in the administration console, enable domain pass-through authentication.
3. Configure SSON on Citrix Receiver for Windows or Citrix Workspace app for Windows, described in Configure domain pass-through authentication. Citrix Workspace app for HTML5 does not

© 1999–2022 Citrix Systems, Inc. All rights reserved.

support domain pass-through authentication.

4. Windows' default behavior is "Automatic logon only in the Intranet zone." For Internet Explorer, Mozilla Firefox and Google Chrome, either configure your Citrix Receiver for Web sites as Intranet sites using the Internet Options, or enable automatic logon for the Trusted zone. For Microsoft Edge you must configure your Citrix Receiver for Web sites as Intranet sites.

5. For Mozilla Firefox, modify the browser advanced settings to trust the Citrix Receiver for Windows or Citrix Workspace app for Windows URI.

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

   a) Start Firefox, enter **about:config** in the address field and select "I accept the risk!"
   b) Type **ntlm** to the search box.
   c) Double-click on "network.automatic-ntlm-auth.trusted-uris" and type the Citrix Receiver for Windows or Citrix Workspace app for Windows site URL to the pop-up dialog.
   d) Click **OK**.

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 Citrix Workspace app or Citrix Receiver for Web sites. For more information about configuring StoreFront for Citrix Gateway, see Add a Citrix Gateway connection.

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

- **Security token.** Users log on to Citrix Gateway using passcodes that are derived from tokencodes generated by security tokens combined, in some cases, with personal identification numbers. If you enable pass-through authentication by security token only, ensure that the resources you make available do not require additional or alternative forms of authentication, such as users' Microsoft Active Directory domain credentials.
- **Domain and security token.** Users logging on to Citrix Gateway are required to enter both their domain credentials and security token passcodes.
- **Client certificate.** Users log on to Citrix Gateway and are authenticated based on the attributes of the client certificate presented to Citrix Gateway. Configure client certificate authentication to enable users to log on to Citrix Gateway using smart cards. Client certificate authentication can also be used with other authentication types to provide double-source authentication.

StoreFront uses the Citrix Gateway authentication service to provide pass-through authentication for remote users so that they only need to enter their credentials once. However, by default, pass-through

© 1999–2022 Citrix Systems, Inc. All rights reserved.

authentication is only enabled for users logging on to Citrix Gateway with a password. To configure pass-through authentication from Citrix Gateway to StoreFront for smart card users, delegate credential validation to Citrix Gateway. For more information, see Create and configure the authentication service.

Users can connect to stores within Citrix Workspace app with pass-through authentication through a Secure Sockets Layer (SSL) virtual private network (VPN) tunnel using the Citrix Gateway plug-in. Remote users who cannot install the Citrix Gateway plug-in can use clientless access to connect to stores within Citrix Workspace app with pass-through authentication. To use clientless access to connect to stores, users require a version of Citrix Workspace app that supports clientless access.

Additionally, you can enable clientless access with pass-through authentication to Citrix Receiver for Web sites. To do this, configure Citrix Gateway to act as a secure remote proxy. Users log on to Citrix Gateway directly and use the Citrix Receiver for Web site to access their applications without needing to authenticate again.

Users connecting with clientless access to App Controller resources can only access external software-as-a-service (SaaS) applications. To access internal web applications, remote users must use the Citrix Gateway plug-in.

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 multidomain 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 on the basis of Citrix Gateway session policies. For more information about SmartAccess, see How SmartAccess works for Citrix Virtual Apps and Desktops.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Smart cards

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

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

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

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

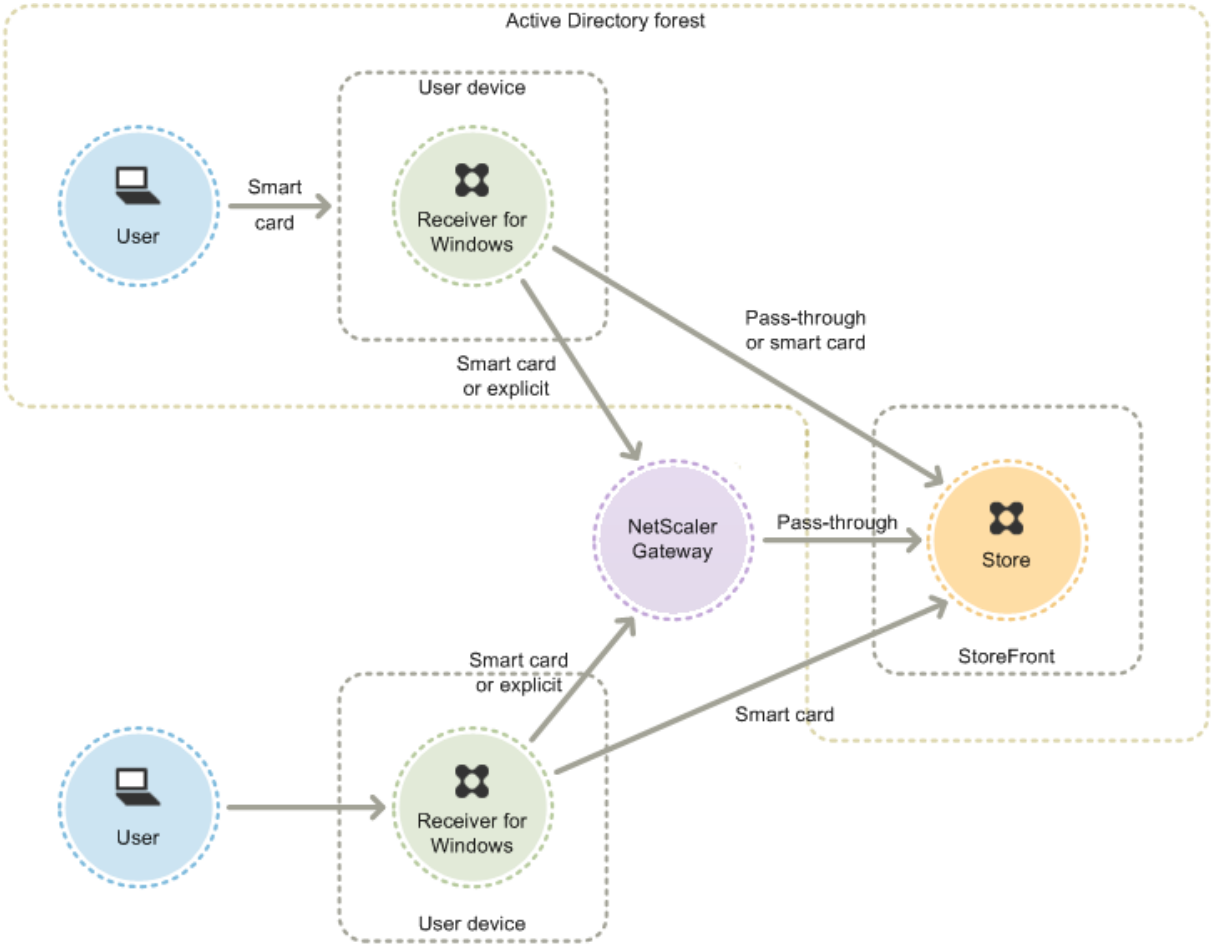
The configuration of smart card authentication with StoreFront depends on the user devices, the clients installed, and whether the devices are domain-joined. In this context, domain-joined means devices that are joined to a domain within the Active Directory forest containing the StoreFront servers.

Use smart cards with Citrix Receiver for Windows or Citrix Workspace app for Windows

Users with devices running Citrix Receiver for Windows or Citrix Workspace app for Windows can authenticate using smart cards, either directly or through Citrix Gateway. Both domain-joined and non-domain-joined devices can be used, although the user experience is slightly different.

The figure shows the options for smart card authentication through Citrix Receiver for Windows or Citrix Workspace app for Windows.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



For local users with domain-joined devices, you can configure smart card authentication so that users are only prompted for their credentials once. Users log on to their devices using their smart cards and PINs and, with the appropriate configuration in place, are not prompted for their PINs again. Users are silently authenticated to StoreFront and also when they access their desktops and applications. To achieve this, you configure Citrix Receiver for Windows or Citrix Workspace app for Windows for pass-through authentication and enable domain pass-through authentication to StoreFront.

Users log on to their devices and then authenticate to Citrix Receiver for Windows or Citrix Workspace app for Windows using their PINs. There is no further PIN prompts when they try to start apps and desktops

Because users of non-domain-joined devices log on to Citrix Receiver for Windows or Citrix Workspace app for Windows directly, you can enable users to fall back to explicit authentication. If you configure both smart card and explicit 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.

Users connecting through Citrix Gateway must log on using their smart cards and PINs at least twice to access their desktops and applications. This applies to both domain-joined and non-domain-joined

© 1999–2022 Citrix Systems, Inc. All rights reserved.

devices. Users authenticate using their smart cards and PINs, and, with the appropriate configuration in place, are only prompted to enter their PINs again when they access their desktops and applications. To achieve this, you enable pass-through with Citrix Gateway authentication to StoreFront and delegate credential validation to Citrix Gateway. Then, create an additional Citrix Gateway virtual server through which you route user connections to resources. In the case of domain-joined devices, you must also configure Citrix Receiver for Windows or Citrix Workspace app for Windows for pass-through authentication.

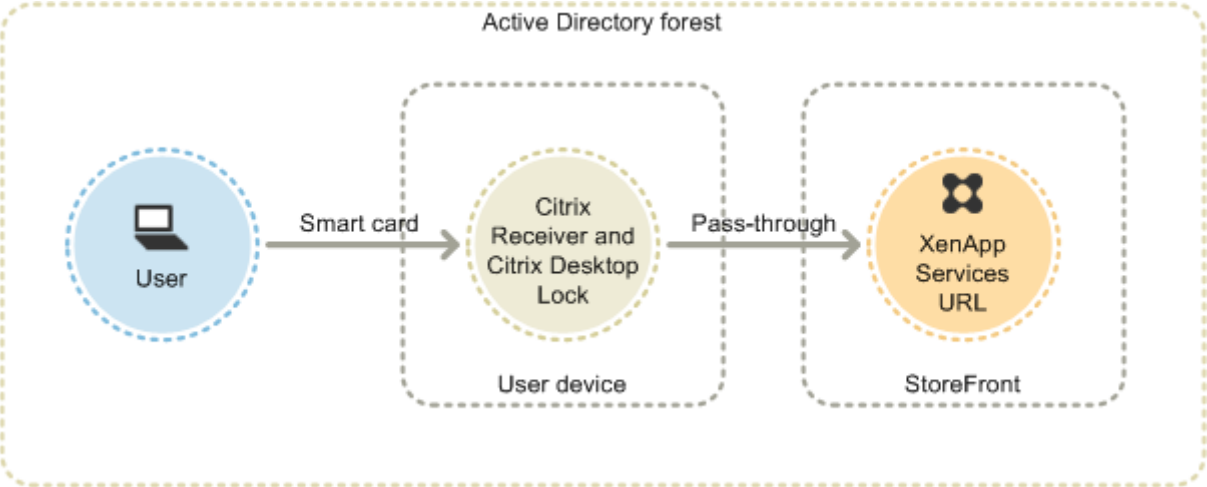
> **Note:**
>
> If you are using Citrix Receiver for Windows or Citrix Workspace app for Windows, you can set up a second vServer and use the optimal gateway routing feature to remove the need for PIN prompts when starting apps and desktops.

Users can log on to Citrix Gateway using either their smart cards and PINs, or with explicit credentials. This enables you to provide users with the option to fall back to explicit authentication for Citrix Gateway logons. Configure pass-through authentication from Citrix Gateway to StoreFront and delegate credential validation to Citrix Gateway for smart card users so that users are silently authenticated to StoreFront.

Use smart cards with XenApp Services URLs

Users of PCs running the Citrix Desktop Lock can authenticate using smart cards. Unlike other access methods, pass-through of smart card credentials is automatically enabled when smart card authentication is configured for a XenApp Services URL.

The figure shows smart card authentication from a domain-joined device running the Citrix Desktop Lock.



Users log on to their devices using their smart cards and PINs. The Citrix Desktop Lock then silently authenticates users to StoreFront through the XenApp Services URL. Users are automatically authen-

© 1999–2022 Citrix Systems, Inc. All rights reserved.

ticated when they access their desktops and applications, and are not prompted for their PINs again.

Use smart cards with Citrix Receiver for Web

You can enable smart card authentication to Citrix Receiver for Web from the StoreFront Administration Console.

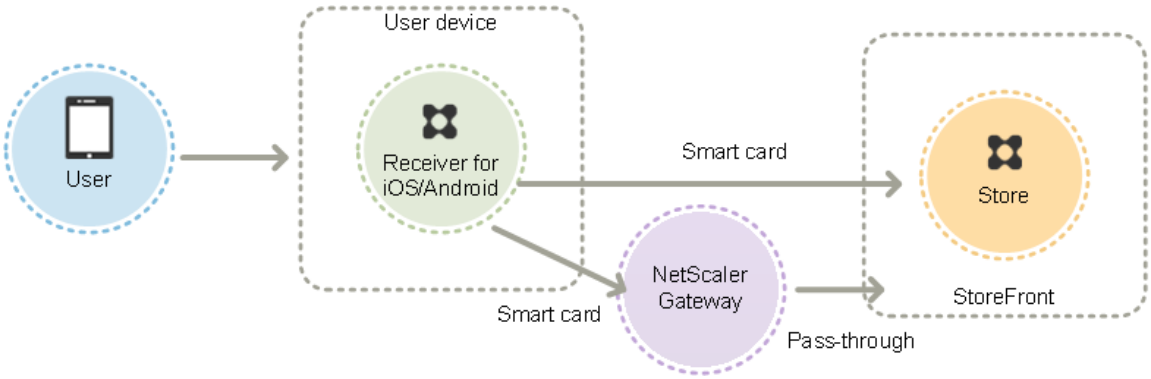
1. Select the Citrix Receiver for Web node in the left panel.
2. Select the site you want to use smart card authentication.
3. Select the Choose Authentication Methods task in the right panel.
4. Check the Smart card checkbox in the popup dialog screen and click OK.

If you enable pass-through with smart card authentication to Citrix Virtual Apps and Desktops for Citrix Receiver for Windows or 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 Receiver for Windows or 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.

Use smart cards with Citrix Workspace app for iOS and Android

Users with devices running Citrix Workspace app for iOS and Android can authenticate using smart cards, either directly or through Citrix Gateway. Non-domain-joined devices can be used.



In the case of devices on the local network, the minimum number of logon prompts that users can receive is two. When users authenticate to StoreFront or initially create the store, they are prompted

© 1999–2022 Citrix Systems, Inc. All rights reserved.

for the smart card PIN. With the appropriate configuration in place, users are prompted to enter their PINs again only when they access their desktops and applications. To achieve this, you enable smart card authentication to StoreFront and install smart card drivers on the VDA.

With these Citrix Workspace apps, you have the option of specifying smart cards OR domain credentials. If you created a store to use smart cards and you want to connect to the same store using domain credentials, you must add a separate store without turning on smart cards.

Users connecting through Citrix Gateway must log on using their smart cards and PINs at least twice to access their desktops and applications. Users authenticate using their smart cards and PINs, and, with the appropriate configuration in place, are only prompted to enter their PINs again when they access their desktops and applications. To achieve this, you enable pass-through with Citrix Gateway authentication to StoreFront and delegate credential validation to Citrix Gateway. Then, create an additional Citrix Gateway virtual server through which you route user connections to resources.

Users can log on to Citrix Gateway using either their smart cards and PINs or with explicit credentials, depending on how you specified the authentication for the connection. Configure pass-through authentication from Citrix Gateway to StoreFront and delegate credential validation to Citrix Gateway for smart card users so that users are silently authenticated to StoreFront. If you want to change the authentication method, you must delete and recreate the connection.

Use smart cards with Citrix Receiver for Linux or Citrix Workspace app for Linux

Users with devices running Citrix Receiver for Linux or Citrix Workspace app for Linux can authenticate using smart cards in a similar way to users of non-domain-joined Windows devices. Even if the user authenticates to the Linux device with a smart card, Citrix Receiver for Linux or Citrix Workspace app for Linux has no mechanism to acquire or reuse the PIN entered.

Configure the server side components for smart cards the same way you configure them for use with the Citrix Receiver for Windows or Citrix Workspace app for Windows. Refer to Configure smart card authentication and for instructions on using smart cards, see Citrix Receiver for Linux.

The minimum number of logon prompts that users can receive is one. Users log on to their devices and then authenticate to Citrix Receiver for Linux or Citrix Workspace app for Linux using their smart cards and PINs. Users are not prompted to enter their PINs again when they access their desktops and applications. To achieve this, you enable smart card authentication to StoreFront.

Because users log on to Citrix Receiver for Linux or Citrix Workspace app for Linux directly, you can enable users to fall back to explicit authentication. If you configure both smart card and explicit 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.

Users connecting through Citrix Gateway must log on using their smart cards and PINs at least once to access their desktops and applications. Users authenticate using their smart cards and PINs and,

© 1999–2022 Citrix Systems, Inc. All rights reserved.

with the appropriate configuration in place, are not prompted to enter their PINs again when they access their desktops and applications. To achieve this, you enable pass-through with Citrix Gateway authentication to StoreFront and delegate credential validation to Citrix Gateway. Then, create an additional Citrix Gateway virtual server through which you route user connections to resources.

Users can log on to Citrix Gateway using either their smart cards and PINs, or with explicit credentials. This enables you to provide users with the option to fall back to explicit authentication for Citrix Gateway logons. Configure pass-through authentication from Citrix Gateway to StoreFront and delegate credential validation to Citrix Gateway for smart card users so that users are silently authenticated to StoreFront.

Smart cards for Citrix Receiver for Linux or Citrix Workspace app for Linux are not supported with the XenApp Services Support sites.

Once smart card support is enabled for both the server and Citrix Workspace app, provided the application policy of the smart card certificates allow it, you can use smart cards for the following purposes:

- Smart card logon authentication. Use smart cards to authenticate users to Citrix Virtual Apps and Desktops servers.
- Smart card application support. Enable smart card-aware published applications to access local smart card devices.

Use smart cards with XenApp Services Support

Users logging on to XenApp Services Support sites to start applications and desktops can authenticate using smart cards without depending on specific hardware, operating systems, and Citrix Workspace apps. When a user accesses a XenApp Services Support site and successfully enters a smart card and PIN, PNA determines the user identity, authenticates the user with StoreFront, and returns the available resources.

For pass-through and smart card authentication to work, you must enable Trust requests sent to the XML service.

Use an account with local administrator permissions on the Delivery Controller to start Windows PowerShell and, at a command prompt, enter the following commands to enable the Delivery Controller to trust XML requests sent from StoreFront. The following procedure applies to XenApp 7.5 through 7.8 and XenDesktop 7.0 through 7.8.

1. Load the Citrix cmdlets by typing `asnp Citrix*.` (including the period).
2. Type `Add-PSSnapin citrix.broker.admin.v2`.
3. Type `Set-BrokerSite -TrustRequestsSentToTheXmlServicePort $True`.
4. Close PowerShell.

For information about configuring the XenApp Services Support smart card authentication method, see Configure authentication for XenApp Services URLs.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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 web page, using their smart cards and PINs to authenticate at each step. Pass-through authentication to StoreFront with the Citrix Gateway plug-in is not 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 additional 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 Receiver for Windows or 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 Receiver for Windows or Citrix Workspace app for Windows users with domain-joined devices accessing stores through Citrix Gateway, this setting applies to all users of the store. To enable pass-through authentication for some users and require others to log on to their desktops and applications, you must create separate stores for each group of users. Then, direct your users to the appropriate store for their method of authentication.
- Only one authentication method can be configured for each XenApp Services URL and only one URL is available per store. If you need to enable other types of authentication in addition to smart card authentication, you must create separate stores, each with a XenApp Services URL, for each authentication method. Then, direct your users to the appropriate store for their method of authentication.
- When StoreFront is installed, the default configuration in Microsoft Internet Information Services (IIS) only requires that client certificates are presented for HTTPS connections to the certificate authentication URL of the StoreFront authentication service. IIS does not request client certificates for any other StoreFront URLs. This configuration enables you to provide smart card

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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 cannot connect through Citrix Gateway and cannot fall back to explicit authentication. Users must log on again if they remove their smart cards from their devices.

Optimize the user experience

October 1, 2020

StoreFront includes features designed to enhance the user experience. These features are configured by default when you create new stores and their associated Citrix Receiver for Web sites, and XenApp Services URLs.

Workspace control

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.

Workspace control is enabled by default for Citrix Receiver for Web sites and connections to stores through XenApp Services URLs. 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, either through the Citrix Receiver for Web site or the XenApp Services URL, 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 Citrix Receiver for Web sites, the same browser must be used to log on, start the applications, and log off.

Workspace control for XenApp Services URLs cannot be configured or disabled. For more information about configuring workspace control for Citrix Receiver for Web sites, see Configure workspace control.

Use of workspace control on Citrix Receiver for Web sites is subject to the following requirements and restrictions.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- Workspace control is not available when Citrix Receiver for Web sites are accessed from hosted desktops and applications.
- For users accessing Citrix Receiver for Web sites from Windows devices, workspace control is only enabled if the site can detect that Citrix Workspace app is installed on users' devices or if Citrix Workspace app for HTML5 is used to access resources.
- To reconnect to disconnected applications, users accessing Citrix Receiver for Web sites through Internet Explorer must add the site to the Local intranet or Trusted sites zones.
- If there is only one desktop available for a user on a Citrix Receiver for Web site that is configured to start single desktops automatically when the user logs on, that user's applications are not reconnected, regardless of the workspace control configuration.
- Users must disconnect from their applications using the same browser that was originally used to start them. Resources started using a different browser, or started locally from the desktop or Start menu using Citrix Workspace app, cannot be disconnected or shut down by Citrix Receiver for Web sites.

Content redirection

Where users have subscribed to the appropriate application, content redirection enables local files on users' devices to be opened using subscribed applications. To enable redirection of local files, associate the application with the required file types in Citrix Virtual Apps and Desktops. File type association is enabled by default for new stores. For more information, see Disable file type association.

User changed password

You can enable Citrix Receiver for Web site users logging on with Microsoft Active Directory domain credentials 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.

Users logging on to Desktop Appliance sites can only change expired passwords, even if you enable users to change their passwords at any time. Desktop Appliance sites do not provide controls to enable users to change their passwords after they have logged on.

When you create the authentication service, the default configuration prevents Citrix Receiver for Web site 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. StoreFront must be able to contact the domain controller to change users' 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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

that reserves user password change functions for internal use only, ensure that none of the stores are accessible from outside your corporate network.

Citrix Receiver for Web site desktop and application views

When both desktops and applications are available from a Citrix Receiver for Web site, the site displays separate desktop and application views by default. Users see the desktop view first when they log on to the site. Regardless of whether applications are also available from a Citrix Receiver for Web site, if only a single desktop is available for a user, the site starts that desktop automatically when the user logs on. You can configure which views appear for your sites and prevent Citrix Receiver for Web sites from automatically starting desktops for users. For more information, see Configure how resources are displayed for users.

The behavior of the views on Citrix Receiver for Web sites depends on the types of resources being delivered. For example, users must subscribe to applications before they appear in the application view, whereas all the desktops available to a user are automatically displayed in the desktop view. For this reason, users cannot remove desktops from the desktop view and cannot reorganize them by dragging and dropping the icons. When desktop restarts are enabled by the Citrix Virtual Desktops administrator, controls that enable users to restart their desktops are provided in the desktop view. If users have access to multiple instances of a desktop from a single desktop group, Citrix Receiver for Web sites differentiate the desktops for users by appending numerical suffixes to the desktop names.

For users connecting to stores within Citrix Workspace app, or through XenApp Services URLs, the way in which desktops and applications are displayed, and their behavior, is determined by the Citrix client being used.

Additional recommendations

When delivering applications with Citrix Virtual Apps and Desktops, 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 Create a Delivery Group application.

- Categorize applications to make it easier for users to find what they need when browsing through the available resources. Application categories you assign to applications in Citrix Virtual Apps and Desktops Studio appear as categories in Citrix Workspace app and Citrix Receiver for Web. You could, for example, categorize applications by type, or create categories for different user roles in your organization.
- Ensure that you include meaningful descriptions when you deliver applications, as these descriptions are visible to users in Citrix Workspace app.
- You can specify that all users have a core set of applications that cannot be removed from the Citrix Workspace app home screen by appending the string `KEYWORDS:Mandatory` to the ap-

© 1999–2022 Citrix Systems, Inc. All rights reserved.

plication description. Users can still use the self-service UI to add more applications or remove nonmandatory applications.

- You can automatically subscribe all users of a store to an application by appending the string `KEYWORDS:Auto` to the description you provide when you deliver the application. When users log on to the store, the application is automatically provisioned without users needing to manually subscribe.
- To automatically subscribe all users of a store to a web or software-as-a-service (SaaS) application managed by App Controller, select the **App is available in Citrix Receiver or Citrix Workspace app to all users automatically** check box when you configure the application settings.
- Advertise Citrix Virtual Apps and Desktops applications to users or make commonly used applications easier to find by listing them in the Featured list in Citrix Workspace app. To do this, append the string `KEYWORDS:Featured` to the application description.

  > **Note:**
  >
  > Multiple keywords must be separated by spaces only; for example, `KEYWORDS:Auto Featured`.

- By default, Citrix Virtual Apps and Desktops hosted shared desktops are treated like other desktops by Citrix Receiver for Web sites. To change this behavior, append the string `KEYWORDS:TreatAsApp` to the desktop description. The desktop is displayed in the application views of Citrix Receiver for Web sites rather than the desktop views and users are required to subscribe before they can access the desktop. In addition, the desktop is not automatically started when the user logs on to the Citrix Receiver for Web site and is not accessed with the Desktop Viewer, even if the site is configured to do this for other desktops.
- For Windows users, you can specify that the locally installed version of an application should be used in preference to the equivalent delivered instance if both are available. To do this, append the string `KEYWORDS:prefer="application"` to the application description, where *application* is either one or more complete words in the name of the local application as given by the shortcut file name, or the absolute path including the executable file name to the local application from the *\Start Menu* folder. When a user subscribes to an application with this keyword, Citrix Workspace app searches for the specified name or path on the user's device to determine whether the application is already installed locally. If the application is found, Citrix Workspace app subscribes the user to the delivered application, but does not create a shortcut. When the user starts the delivered application from Citrix Workspace app, the locally installed instance runs instead. For more information, see Configuring application delivery.
- In Citrix Virtual Apps and Desktops, when users launch a published application from within a published desktop, administrators can control whether the application is launched in that desktop session or as a published application in the same Delivery Group. Use a PowerShell cmdlet

© 1999–2022 Citrix Systems, Inc. All rights reserved.

on the Broker Service and a policy setting in Citrix Receiver for Windows (vPrefer) to control this behavior. This feature works with Citrix Receiver for Windows or Citrix Workspace app for Windows launches of published apps only. It cannot be used to launch an app locally if the published app is launched through the StoreFront site in a web browser. In previous releases, "double-hop" application launch control required the use of the `KEYWORDS:Prefer` tag in Studio.The `KEYWORDS:Prefer` tag can still be used. If both the KEYWORDS and the vPrefer method have been configured, vPrefer takes precedence.

For more information, see CTX232210, the Applications article in Citrix Virtual Apps and Desktops, and the Citrix Receiver for Windows documentation.

StoreFront high availability and multi-site configuration

April 29, 2020

StoreFront includes a number of features that combine to enable load balancing and failover between the deployments providing resources for stores. You can also specify dedicated disaster recovery deployments for increased resiliency. These features enable you to configure StoreFront deployments distributed over multiple sites to provide high availability for your stores. For more information, see Set up highly available multi-site store configurations.

Resource 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.

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. App Controller applications cannot be aggregated. When a user starts an aggregated resource, StoreFront determines the most appropriate instance of that resource for the user on the basis of server availability, whether the user already has an active session, and the ordering you specified in your configuration.

StoreFront dynamically monitors servers that fail to respond to requests on the basis that such servers are either overloaded or temporarily unavailable. Users are directed to resource instances on other

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

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

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

Map users to resources

By default, users accessing a store see an aggregate of all the resources available from all the deployments configured for that store. To provide different resources for different users, you can configure separate stores or even separate StoreFront deployments. However, when you set up highly available multi-site configurations, you can provide access to particular deployments on the basis of users' membership of Microsoft Active Directory groups. This enables you to configure different experiences for different user groups through a single store.

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

Alternatively, you can create a deployment for power users that provides the same resources as your

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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.

Subscription synchronization

If you enable your users to access the same applications from similar stores in different StoreFront deployments, users' application subscriptions must be synchronized between the server groups. Otherwise, users who subscribe to an application in a store on one StoreFront deployment might need to resubscribe to the application when they log on to a different server group. To provide a seamless experience for users moving between separate StoreFront deployments, you can configure periodic synchronization of users' application subscriptions between stores in different server groups. Choose between regular synchronization at a specific interval or schedule synchronization to occur at particular times throughout the day. For more information, see Configure subscription synchronization.

Dedicated disaster recovery resources

You can configure specific disaster recovery deployments that are not used unless all other deployments are unavailable. Typically, disaster recovery deployments are not colocated with the main deployments, provide only a subset of the resources that are normally available, and might offer a degraded user experience. When you specify that a deployment is to be used for disaster recovery, the deployment will not be used for load balancing or failover. Users cannot access desktops and applications provided by disaster recovery deployments unless all the other deployments for which the disaster recovery deployments are configured become unavailable.

When access to any other deployment is re-established, users cannot start more disaster recovery resources, even if they are already using such a resource. Users running disaster recovery resources are not disconnected from those resources when access to other deployments is restored. However, they cannot start disaster recovery resources again once they have exited these resources. Similarly, StoreFront does not attempt to reuse existing sessions with disaster recovery deployments if any other deployments have subsequently become available.

Optimal Citrix Gateway routing

If you have configured separate Citrix Gateway appliances for your deployments, StoreFront enables you to define the optimal appliance for users to access each of the deployments providing resources for a store. For example, if you create a store that aggregates resources from two geographical locations, each with a Citrix Gateway appliance, users connecting through an appliance in one location can start a desktop or application in the other location. However, by default, the connection to the

© 1999–2022 Citrix Systems, Inc. All rights reserved.

resource is then routed through the appliance to which the user originally connected and must therefore traverse the corporate WAN.

To improve the user experience and reduce network traffic over the WAN, you can specify the optimal Citrix Gateway appliance for each of your deployments. With this configuration, user connections to resources are automatically routed through the appliance local to the deployment providing the resources, regardless of the location of the appliance through which the user accesses the store.

Optimal Citrix Gateway routing can also be used in the special case where local users on the internal network are required to log on to Citrix Gateway for endpoint analysis. With this configuration, users connect to the store through the Citrix Gateway appliance, but there is no need to route the connection to the resource through the appliance as the user is on the internal network. In this case, you enable optimal routing, but do not specify an appliance for the deployment, so user connections to desktops and applications are routed directly and not through Citrix Gateway. Note that you must also configure a specific internal virtual server IP address for the Citrix Gateway appliance. Additionally, specify an inaccessible internal beacon point so that Citrix Workspace app is always prompted to connect to Citrix Gateway, regardless of the user's network location.

Citrix Gateway global server load balancing

StoreFront supports Citrix Gateway deployments configured for global server load balancing with multiple appliances configured with a single fully qualified domain name (FQDN). For user authentication and to route user connections through the appropriate appliance, StoreFront must be able to distinguish between the appliances. Because the appliance FQDN cannot be used as a unique identifier in a global server load balancing configuration, you must configure StoreFront with unique IP addresses for each of the appliances. Typically, this is the IP address of the Citrix Gateway virtual server.

For information about load balancing, see Load balancing with Citrix ADC.

Important considerations

When you decide whether to set up highly available multi-site configurations for your stores, consider the following requirements and restrictions.

- Desktops and applications must have the same name and path on each server to be aggregated. In addition, the properties of aggregated resources, such as names and icons, must be the same. If this is not the case, users could see the properties of their resources change when Citrix Workspace app enumerates the available resources.
- Assigned desktops, both pre-assigned and assigned-on-first-use, should not be aggregated. Ensure that Delivery Groups providing such desktops do not have the same name and path in sites that you configure for aggregation.
- App Controller applications cannot be aggregated.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- If you configure synchronization of users' application subscriptions between stores on separate StoreFront deployments, the stores must have the same name in each server group. In addition, both server groups must reside within the Active Directory domain containing your users' accounts or within a domain that has a trust relationship with the user accounts domain.
- StoreFront only provides access to backup deployments for disaster recovery when all the primary sites in the equivalent deployment set are unavailable. If a backup deployment is shared between multiple equivalent deployment sets, all the primary sites in each of the sets must be unavailable before users can access the disaster recovery resources.

Install, set up, upgrade, and uninstall

February 9, 2022

Before installing and configuring

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

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

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

2. If not already present, StoreFront requires Microsoft .NET Framework, which can be downloaded from Microsoft. You must have Microsoft .NET installed before you can install StoreFront.

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

   To use Citrix ADC for load balancing, you define a virtual server to proxy your StoreFront servers. For more information on configuring Citrix ADC for load balancing, see Load balancing with Citrix ADC.

   a) Ensure that load balancing is enabled on your Citrix ADC appliance.

   b) For each StoreFront server, create individual HTTP or SSL load balancing services, as appropriate, using the StoreFront monitor type.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

c) Configure the services to insert the client IP address into the X-Forwarded-For HTTP header of requests forwarded to StoreFront, overriding any global policies.

StoreFront requires users' IP addresses to establish connections to their resources.

d) Create a virtual server and bind the services to the virtual server.

e) On the virtual server, configure persistence using either the **Client IP** or **Cookie Insert** method. Ensure the Time To Live (TTL) is sufficient to enable users to stay logged on to the server as long as required.

Persistence ensures that only the initial user connection is load balanced, after which subsequent requests from that user are directed to the same StoreFront server.

4. Optionally, enable the following features.

   - .NET Framework Features > .NET Framework, ASP.NET

   Optionally, enable the following roles and their dependencies on the StoreFront server.

   - Web Server (IIS) > Web Server > Common HTTP Features > Default Document, HTTP Errors, Static Content, HTTP Redirection
   - Web Server (IIS) > Web Server > Health and Diagnostics > HTTP Logging
   - Web Server (IIS) > Web Server > Security > Request Filtering, Windows Authentication
   - Web Server (IIS) > Web Server > Application Development > .NET Extensibility, Application Initialization, ASP.NET, ISAPI Extensions, ISAPI Filters

   The StoreFront installer checks that all the preceding features and server roles are enabled.

5. 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.

6. Optionally, configure Microsoft Internet Information Services (IIS) for HTTPS if you plan to use HTTPS to secure communications between StoreFront and users' devices.

   HTTPS is required for smart card authentication. By default, Citrix Workspace app requires HTTPS connections to stores. To configure IIS so that you can use an HTTPS hostbaseURL in StoreFront, create an HTTPS binding to the default website and link it to the StoreFront server certificate. For more information about adding HTTPS binding to an IIS site, see Secure your StoreFront deployment.

7. Optionally, configure Transport Layer Security (TLS).

8. Ensure your firewalls and other network devices permit access to TCP port 80 or 443, as appropriate, from both inside and outside the corporate network. In addition, ensure that any

© 1999–2022 Citrix Systems, Inc. All rights reserved.

firewalls or other devices on your internal network do not block traffic to any of the unassigned TCP ports.

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

9. If you plan to use multiple Internet Information Services (IIS) websites, after creating the websites in IIS, use the PowerShell SDK to create a StoreFront deployment in each of those IIS websites. For more information, see Multiple Internet Information Services (IIS) websites.

   > **Note:**
   >
   > StoreFront disables the management console when it detects multiple sites and displays a message to that effect.

10. Use the Citrix StoreFront management console to configure your server.

Install StoreFront

> **Important**
>
> - To avoid potential errors and data loss when installing StoreFront, ensure that all applications are closed and no other tasks or operations are running on the target system.
> - From StoreFront 1912 LTSR CU1 onwards, to install StoreFront in a custom location for the first time, you must install from the command prompt using the -INSTALLDIR argument to specify the location. See To install StoreFront at a command prompt.

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

   Before the components are installed, the following roles are enabled if they are not already configured on the server.

   - Web Server (IIS) > Web Server > Common HTTP Features > Default Document, HTTP Errors, Static Content, HTTP Redirection
   - Web Server (IIS) > Web Server > Health and Diagnostics > HTTP Logging

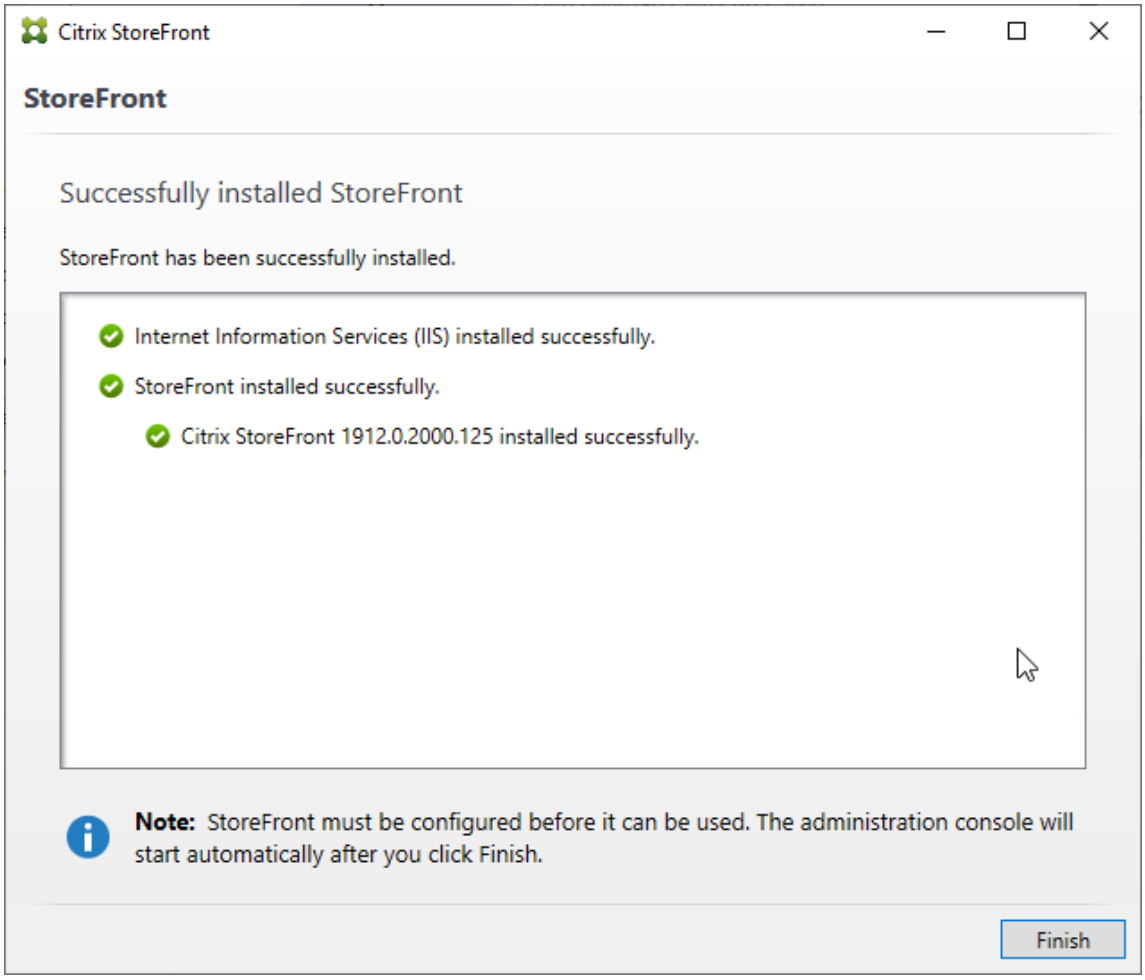
© 1999–2022 Citrix Systems, Inc. All rights reserved.

- Web Server (IIS) > Web Server > Security > Request Filtering, Windows Authentication
- Web Server (IIS) > Management Tools > IIS Management Console, IIS Management Scripts and Tools

The following features are also enabled if they are not already configured.

- .NET Framework Features > .NET Framework, ASP.NET

8. When the installation is complete, click **Finish**. The Citrix StoreFront management console starts automatically. You can also open StoreFront from the Start screen.



> **Note:**
>
> From StoreFront 1912 LTSR CU1 onwards a restart is required after StoreFront installation.

9. In the Citrix StoreFront management console, click **Create a new deployment**.
   a) Specify the URL of the StoreFront server in the **Base URL** box.
   b) On the **Store Name** page, specify a name for your store, and click **Next**.

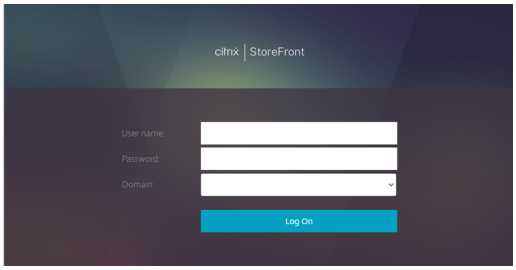
On the **Delivery Controllers** page, enter details of the Citrix Virtual Apps and Desktops deployments that that provide the resources you want to make available in the store.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

1. Set the **Transport type** and the **Port**, such as HTTP and port 80, or HTTPS and port 443, and click **OK**.
2. On the **Remote Access** page, select None. If you are using Citrix Gateway, select No VPN Tunnel and enter your gateway details.
3. On the **Remote Access** page, select Create. Once the store has been created, click **Finish**.

Your store is now available for users to access through the Citrix Receiver for Web site, which enables users to access their desktops and apps through a webpage.

The URL for users to access the Citrix Receiver for Web site for the new store is displayed. For example: `example.net/Citrix/StoreWeb/`. Log on and you access the new user interface in Citrix Workspace app.



To install StoreFront at a command prompt

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

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

Use the **-silent** argument to silently install StoreFront and its prerequisites. By default, StoreFront is installed at C:\Program Files\Citrix\Receiver StoreFront. However, you can specify a different installation location using the -INSTALLDIR argument, where *installationlocation* is the

© 1999–2022 Citrix Systems, Inc. All rights reserved.

directory in which to install StoreFront. The installation location must be a fully qualified pathname to an existing drive on the local file system, for example, “C:\ABC”. Valid characters are a–z A–Z 0–9 . ~ \ - ( ) _ and white space. Installing into a subdirectory of a user profile folder is not allowed. 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.

By default, if a Citrix Receiver for Web site cannot detect Citrix Workspace app on a Windows or macOS X device, the user is prompted 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 Receiver for Windows or 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.

CEIP

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 the Registry Editor can be solved. Use the 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
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
Value: 0 = disabled, 1 = enabled
<!--NeedCopy-->
```

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

Using PowerShell, the following cmdlet disables enrollment in CEIP:

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

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

CEIP data collected from StoreFront

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

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Data	Description
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 Citrix Cloud customer and you have an on-premises StoreFront deployment, you can configure StoreFront so that data is sent to the Citrix Analytics service in Citrix Cloud. When configured, Citrix Workspace app—and Citrix Receiver for Web sites accessed from HTML5-compatible 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 the following addresses at port 443 for this feature to work properly and consume the Citrix Cloud services:
>
> - `https://*.cloud.com`
> - `https://*.citrixdata.com`

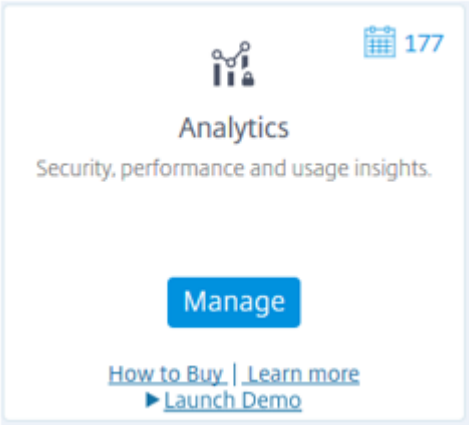
Download the configuration file from Citrix Analytics

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

1. Log on to Citrix Cloud (`https://citrix.cloud.com/`) using an administrator account.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

2. Select a Citrix Cloud customer.
3. Open the Citrix Analytics service management console by clicking **Manage**.



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

Example configuration file

```
{

  "customerId": "<yourcloudcustomer>",
  "enablementService": " https://api.analytics.cloud.com /casvc/<
     yourcloudcustomer>/ctxana/v1/cas/<yourcloudcustomer>/XenDesktop/<
     deviceid>/dsconfigdata",
  "cwsServiceKey": "PFJTPn ··· ··· .. T4=",
  "enablementServiceStatus": " https://api.analytics.cloud.com /casvc/<
     yourcloudcustomer>/ctxana/v1/cas/storefront/config",
  "instanceId": "d98f21d0-56e0-11e9-ba52-5136d90862fe",
  "name": "CASSingleTenant"
 }

<!--NeedCopy-->
```

where

customerId is the unique ID for the current Citrix Cloud customer.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

cwsServiceKey is a unique key identifying the current Citrix Cloud customer account.

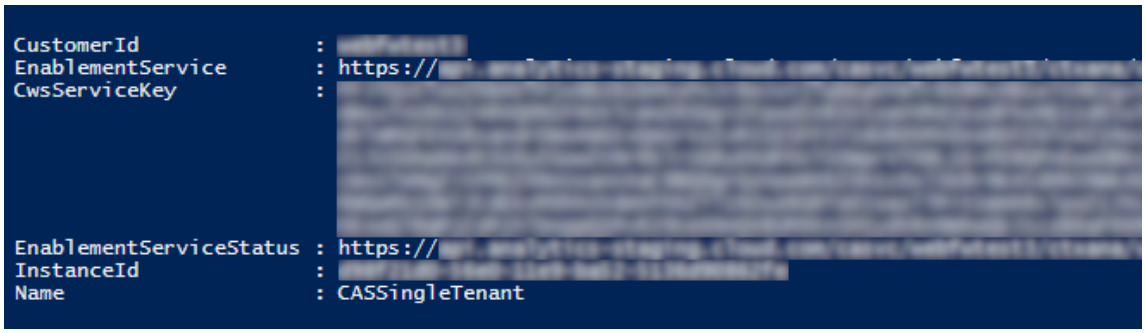
instanceID is a generated ID used to sign (secure) requests made from Citrix Workspace app to Citrix Analytics. If you register multiple StoreFront servers or server groups with Citrix Cloud, then each one has a unique instanceID.

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
<!--NeedCopy-->
```

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



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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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:

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

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
<!--NeedCopy-->
```

Stop sending data to Citrix Analytics from StoreFront

1. Open PowerShell ISE and select **Run as Administrator**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

2. Run the following commands:

   ```
   Remove-STFCasConfiguration
   ```

   ```
   Get-STFCasConfiguration
   ```

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

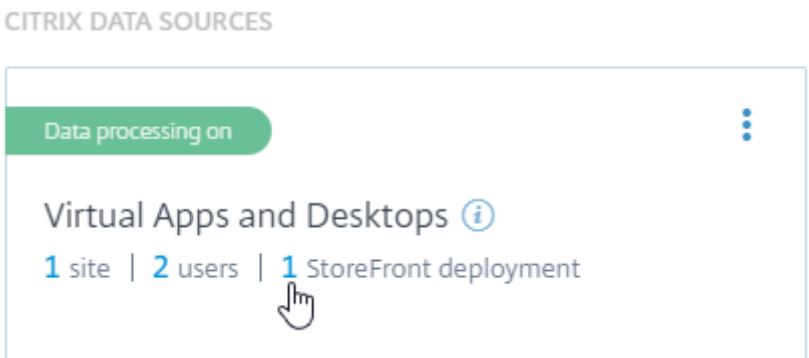
3. If you are performing these actions on a StoreFront server group, propagate the change and remove the imported Citrix Analytics data from all members of the server group. On one server in the server group, run the following command:

   ```
   Publish-STFServerGroupConfiguration
   ```

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

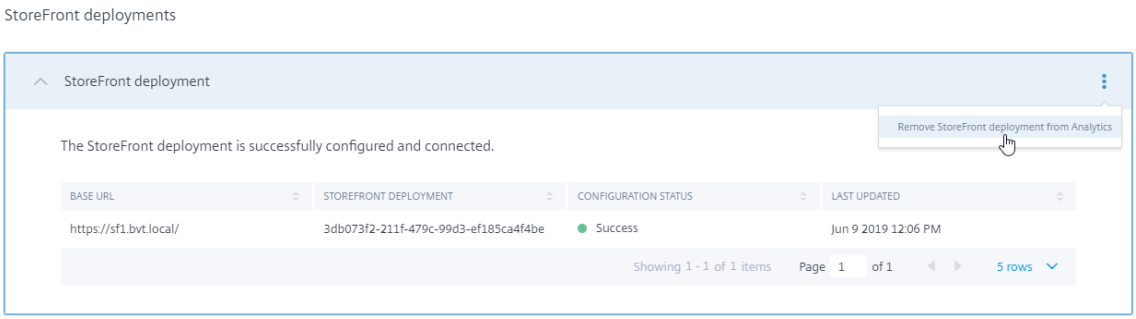
   ```
   Get-STFCasConfiguration
   ```

5. Log on to Citrix Cloud (`https://citrix.cloud.com/`) using an administrator account.
6. Select a Citrix Cloud 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**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



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

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

If StoreFront is placed on a host webserver behind a web proxy, registration with Citrix Analytics fails. 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**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

2. Set `$Stores = @("Store","Store2")` to include the stores you want 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"
$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\"))
        {

            Write-Host "Creating $env:UserProfile\desktop\$Store\directory for backup..." -ForegroundColor "Yellow"
            New-Item -Path "$env:UserProfile\desktop\$Store\" -
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
                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"

        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
        {

```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
            $ProxyServer = ("HTTP://$ProxyFQDN"+":"+$ProxyPort)
         }


        $XMLObject = (Get-Content $StoreConfigPath) -as [Xml]

        # Create 3 elements
        $SystemNet = $XMLObject.CreateNode("element","system.net",
            "")
        $DefaultProxy = $XMLObject.CreateNode("element","
            defaultProxy","")
        $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"
    IISReset /RESTART
 }


Set-StoreProxyServer -Stores $Stores -ProxyFQDN $ProxyFQDN -
    ProxyPort $ProxyPort
# OR
Set-StoreProxyServer -Stores $Stores -ProxyIP $ProxyIP -ProxyPort
    $ProxyPort
<!--NeedCopy-->
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

```
        </dependentAssembly>
    </assemblyBinding>
</runtime>
<system.net>
    <defaultProxy>
    <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
       bypassonlocal="true" />
    </defaultProxy>
</system.net>
</configuration>
<!--NeedCopy-->
```

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

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

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

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

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

```
<system.net>
    <defaultProxy>
    <proxy proxyaddress="HTTP://proxyserver.example.com:8888"
       bypassonlocal="true" />
    </defaultProxy>
</system.net>
<!--NeedCopy-->
```

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
<system.net>
    <defaultProxy>
    <proxy proxyaddress="HTTP://10.0.0.1:8888" bypassonlocal="true
        " />
    </defaultProxy>
</system.net>
<!--NeedCopy-->
```

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

```
<runtime>
<gcServer enabled="true" />
<assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
    <dependentAssembly>
    <assemblyIdentity name="System.Web.MVC" publicKeyToken="31
        BF3856AD364E35" culture="neutral" />
    <bindingRedirect oldVersion="0.0.0.0-5.0.0.0" newVersion="
        5.0.0.0" />
    </dependentAssembly>
    <dependentAssembly>
    <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30
        ad4fe6b2a6aeed" 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>
<!--NeedCopy-->
```

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

Upgrade StoreFront

> **Warnings:**
>
> When you upgrade to StoreFront 1912, any Desktop Appliance sites in your deployment are au-

© 1999–2022 Citrix Systems, Inc. All rights reserved.

> tomatically removed. If you need to preserve your Desktop Appliance sites, do not upgrade. As an alternative, Citrix recommends using Citrix Workspace app Desktop Lock for all non-domain-joined use cases.
>
> When you upgrade to StoreFront 1912 CU2, the order of TLS cipher suites must be reconfigured on the Controller or StoreFront to ensure applications in a StoreFront store enumerate and launch correctly. For more information, see Known issues and Transport Layer Security (TLS).

Upgrading preserves your StoreFront configuration and leaves users' application subscription data intact so that users do not need to resubscribe to all of their applications. By contrast, uninstalling StoreFront removes StoreFront and associated services, sites, application subscription data (on standalone servers), and associated configuration.

Good to know

- 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.
- Upgrading to the latest StoreFront current release or LTSR release, from an older release that is now End of Life, is not supported. For more information see CTX200356.
- StoreFront does not support multiple server deployments containing different product versions, so all servers in a server group must be upgraded to the same version before you grant access to the deployment.
- StoreFront does not support multiple server deployments containing different server OSs, so all servers in a server group must be on the same Windows Server OS.
- Concurrent upgrade is not supported for multiple server deployments, servers must be upgraded sequentially.
- Any stores which use the classic user experience are updated to use the unified experience when you upgrade to this version of StoreFront. We recommend that you make users aware of the new experience which the upgrade introduces, described in Unified user experience. If you have customized the unified experience, your customizations are preserved when you upgrade to this version of StoreFront. Check that the appearance of your customizations is still suitable with the new unified experience.
- Before the StoreFront upgrade runs it performs some pre-upgrade checks. If any pre-upgrade check fails, the upgrade does not start and you are notified of the failures. Your StoreFront installation remains unchanged. After fixing the cause of the failures, rerun the upgrade.
- If the StoreFront upgrade itself fails, your existing StoreFront installation may lose its initial configuration. Restore your StoreFront installation to a functional state then rerun the upgrade. To restore StoreFront to a functional state consider the following approaches:
  - restoring the VM snapshot you created before the upgrade,
  - importing the StoreFront configuration you exported before the upgrade (see Export and import the StoreFront configuration),

© 1999–2022 Citrix Systems, Inc. All rights reserved.

  - performing the troubleshooting advice in Troubleshoot StoreFront upgrade issues.
- Any StoreFront upgrade failures which occur from the Citrix Virtual Apps and Desktops metainstaller are reported in a dialog, with a link to the relevant failure log.

Get ready to upgrade

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

- Plan your backup strategy before upgrading.
- If you have made modifications to files in `C:\inetpub\wwwroot\Citrix\<StoreName>\App_Data`, such as default.ica and usernamepassword.tfrm, back them up for each store. After the upgrade you can restore them to reinstate your modifications.
- Close all other applications on the StoreFront server.
- Close the StoreFront management console.
- Close all command line and PowerShell windows.
- Close all StoreFront-related folders such as C:\inetpub\wwwroot\Citrix\Store and C:\inetpub\wwwroot\Citrix This prevents Windows Explorer from taking an exclusive lock on them.
- Before upgrading a server, restart it to ensure that there are no exclusive locks on StoreFront files or folders. (Restarting the explorer process—for example by closing all instances of Windows explorer—is *not* enough).
- Run the upgrade immediately without starting any other programs on the server.
- Upgrade the server using an admin account with no other installations running and a minimum of other applications.

Upgrade a stand-alone StoreFront server

1. Disconnect users from the StoreFront deployment to prevent them from accessing the servers while the upgrade is in progress. 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.
2. Back up the server by creating a VM snapshot.
3. Export the existing StoreFront configuration (recommended).
4. Run the installation file for this version of StoreFront.

To upgrade a StoreFront server group

Upgrading StoreFront server groups involves using one of the servers to remove the other servers from the group. The removed servers retain configuration related to the group, which can prevent

© 1999–2022 Citrix Systems, Inc. All rights reserved.

them being joined to a new server group. Before they can be reused to build new server groups, or as standalone StoreFront servers, they must be reset to factory defaults, or have StoreFront reinstalled on them.

Before upgrading a server group:

- Back up all servers in the group by creating VM snapshots. This allows you to quickly revert to a working three node server group if the upgrade does not go as planned.
- Export the existing StoreFront configuration (recommended). 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.

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

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

1. Back up all servers in the group by creating VM snapshots.
2. Export the existing StoreFront configuration from one server in the server group.
3. 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.
4. Use server A to remove servers B and C from the group.

   Servers B and C are now 'orphaned' from the server group.
5. Upgrade server A by running the installation file for this version of StoreFront.
6. Ensure that server A has been successfully upgraded.
7. On servers B and C, uninstall the currently installed version of StoreFront, then install the new version of StoreFront.
8. Join servers B and C to the upgraded server A to create an upgraded server group. This server group consists of one upgraded server (A) and two freshly installed servers (B and C).

   The Join existing server group process automatically propagates all configuration data and subscription data to new servers B and C.
9. Check that all servers are functioning correctly.
10. Enable user access to the upgraded server group by enabling the load balancing URL.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

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

1. Back up all servers in the group by creating VM snapshots.
2. Export the existing StoreFront configuration from one server in the server group.
3. Export subscription data from server A using **Export-STFStoreSubscriptions**, described in Manage subscription data for a store. This backup is necessary because servers are factory reset later in the process, which deletes subscription and configuration data.
4. Disable user access to server C by disabling the load balancer service that represents server C. This prevents users from connecting to server C during the upgrade process. Keep the load balanced service representing servers A and B enabled, so your users can continue to use them.
5. 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.
6. Reset the orphaned server C to factory defaults using **Clear-STFDeployment**.
7. 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.
8. Upgrade server C by running the installation file for this version of StoreFront. Server C now has an identical configuration to the old server group, and is upgraded to a new version of StoreFront.
9. 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.
10. Repeat steps 4, 5, 6 and 8 using server B. (Do not repeat step 9.) 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.
11. 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).
12. Enable the load balanced services for both server B and C so they can take over from server A.
13. Disable the load balanced service for server A so that users are directed to the newly upgraded servers B and C.
14. Repeat steps 6 and 8 using server A.
15. Join server A to server group B and C using the Join existing server group process. This gives a new three-node server group on the new StoreFront version (servers A, B, and C).
16. Enable the load balanced service for server A so that users are directed to all three upgraded servers A, B, and C.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

The server group upgrade process is now complete. Servers A, B, and C have identical configuration and subscription data from the original group.

> **Note:**
>
> During the brief period when server A is the only accessible server, subscriptions can be lost (step 10). This can cause the new server group to have a slightly outdated copy of the subscription database after upgrade, and any new subscription records to be lost.
>
> This has no functional impact because subscription data is not essential for users to be able to log on and launch resources. Users would, however, need to subscribe to a resource again after server A is factory reset and joined to the newly upgraded group. Although it is unlikely that more than a few subscription records would ever be lost, it is a possible consequence of upgrading a live StoreFront production environment with no downtime.

Configure StoreFront

> **Note:**
>
> During installation and upgrade, members of the local admin group are copied to an internal CitrixStoreFrontAdministrators group. This gives users who already belonged to the local admin group, when StoreFront was last installed or upgraded, the ability to use the StoreFront management console to configure StoreFront server groups and perform related propagation and replication tasks. If you later add users to the local admin group, you must manually copy them to the CitrixStoreFrontAdministrators group before they can use the StoreFront management console to configure StoreFront server groups and perform related propagation and replication tasks. If you add a currently logged in user to the CitrixStoreFrontAdministrators group, they need to log out and log in again to use the StoreFront management console.

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. Citrix recommends no more than 6 servers to a server group.

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 subscrip-

© 1999–2022 Citrix Systems, Inc. All rights reserved.

tion 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 admin console if it is open.
3. Close any PowerShell sessions that may have been used to manage StoreFront via its PowerShell SDK.
4. On the Windows **Start** screen or Apps screen, locate the **Citrix StoreFront** tile. Right-click the tile and click **Uninstall**.
5. In the **Programs and Features** dialog box, 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**.

Uninstall StoreFront using PowerShell

You can use the following PowerShell to trigger an MSI windows uninstall of StoreFront:

1. List all installed applications:

   ```
   Get-WmiObject -Class Win32_Product | Select-Object -Property Name<!--
   NeedCopy-->
   ```

2. If StoreFront is listed, then execute the following command:

   ```
   $storefront = Get-WmiObject -Class Win32_Product | Where-Object{ $_.
   Name -eq "<Storefront_Product_Name>"} <!--NeedCopy-->
   ```

3. Run `$storefront` to confirm it maps to the required product.

4. Run `$storefront.uninstall()`.

Create a new deployment

May 4, 2021

1. If the Citrix StoreFront management console is not already open after installation of StoreFront, on the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.

2. In the results pane of the Citrix StoreFront management console, click **Create a new deployment**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

3. Specify the URL of the StoreFront server or the load balancing environment for a multiple server deployment in the **Base URL** box.

   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.

4. Click **Next** to set up the authentication service, which authenticates users to Microsoft Active Directory.

   To use HTTPS to secure communications between StoreFront and users' devices, you must configure Microsoft Internet Information Services (IIS) for HTTPS. In the absence of the appropriate IIS configuration, StoreFront uses HTTP for communications.

   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. HTTPS is required for smart card authentication. You can change from HTTP to HTTPS at any time after configuring StoreFront, provided the appropriate IIS configuration is in place. For more information, see Configure server groups.

   You can change from HTTP to HTTPS at any time using the **Change Base URL** task in the StoreFront management console, provided that Microsoft Internet Information Services (IIS) is configured for HTTPS.

5. On the **Store Name** page, specify a name for your store, specify whether you want to allow only unauthenticated (anonymous) users access to the store, and click **Next**.

   StoreFront stores aggregate desktops and applications, making them available to users. Store names appear in Citrix Workspace app under users' accounts, so choose a name that gives users information about the content of the store.

6. On the **Delivery Controllers** page, list the infrastructure providing the resources that you want to make available in the store. To add desktops and applications to the store, follow the appropriate described in Add Citrix Virtual Apps and Desktops resources to the store. You can configure stores to provide resources from any mixture of Citrix Virtual Apps and Desktops deployments. Repeat the procedures, as necessary, to add all the deployments providing resources for the store.

7. When you have added all the required resources to the store, on the **Delivery Controllers** page, click **Next**.

8. On the **Remote Access** page, specify whether and how users connecting from public networks can access the internal resources.

   - To make the store available to users on public networks, check the **Enable remote access** box. If you leave this box unchecked, only local users on the internal network are able to access the store.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- To make only resources delivered through the store available through Citrix Gateway, select **Allow users to access only resources delivered through StoreFront (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 all other resources on the internal network available through a Secure Sockets Layer (SSL) virtual private network (VPN) tunnel, select **Allows users to access all resources on internal network (Full VPN tunnel).** Users require the Citrix Gateway plug-in to establish the VPN tunnel.

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

9. If you enabled remote access, **Citrix Gateway appliances** lists the deployments through which users can access the store. To add a Citrix Gateway deployment to this list, follow the appropriate procedure described in Provide remote access to the store through a Citrix Gateway appliance. Repeat the procedures, as necessary, to add further deployments.
10. In the **Citrix Gateway appliances** list, select the deployments through which users can access the store. If you enable access through multiple deployments, specify the **Default appliance** to be used to access the store. Click **Next**.
11. On the **Authentication Methods** page, select the methods your users will use to authenticate to the store and click **Next**. You can select from the following methods:
    - **Username and password**: Users enter their credentials and are authenticated when they access their stores.
    - **SAML Authentication**: Users authenticate to an Identity Provider and are automatically logged on when they access their stores.
    - **Domain pass-through†**: Users authenticate to their domain-joined Windows computers and their credentials are used to log them on automatically when they access their stores.
    - **Smart card†**: Users authenticate using smart cards and PINs when they access their stores.
    - **HTTP basic**: Users authenticate with the StoreFront server's IIS web server.
    - **Pass-through through Citrix Gateway**: Users authenticate to Citrix Gateway and are automatically logged on when they access their stores. This is automatically checked when the remote access is enabled.

    > **Note:**
    >
    > † Store authentication methods which do not propagate to the store's Citrix Receiver for Web sites. Configure these authentication methods independently for each Citrix Receiver for Web site using the **Manage Receiver for Web Sites** task described in Configure Citrix Receiver for Web sites.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

> The other store authentication methods described here do propagate to the store's Citrix Receiver for Web sites. (That is, a selection or deselection made here for the store dictates the setting used by all its Receiver for Web sites.)

12. On the **Configure Password Validation** page, select the Delivery Controllers to provide the password validation, click **Next**.
13. On the **XenApp Services URL** page, configure the XenApp Service URL for users who use PNAgent to access the applications and desktops.
14. After the store has been create, further options become available in the Citrix StoreFront management console. For more information, see Configure and manage stores.

Your store is now available for users to access with Citrix Workspace app, which must be configured with access details for the store. There are a number of ways in which you can provide these details to users to make the configuration process easier for them. For more information, see User access options.

Alternatively, users can access the store through the Citrix Receiver for Web site, which enables users to access their desktops and applications through a webpage. The URL for users to access the Citrix Receiver for Web site for the new store is displayed when you create the store.

When you create a new store, the XenApp Services URL is enabled by default. Users of domain-joined desktop appliances and repurposed PCs running the Citrix Desktop Lock, along with users who have older Citrix clients that cannot be upgraded, can access stores directly using the XenApp Services URL for the store. The XenApp Services URL 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 you specified for the store in Step 5.

To quickly add more servers to your deployment, select the option to join an existing server group when installing further instances of StoreFront.

Add Citrix Virtual Apps and Desktops resources to the store

Complete the following steps to make desktops and applications provided by Citrix Virtual Apps and Desktops available in the store that you create as part of the initial configuration of your StoreFront server. It is assumed that you have completed Steps 1 to 6 in the "Create a new deployment" procedure at the top of this article.

1. On the **Delivery Controllers** page, list the infrastructure providing the resources that you want to make available in the store. Click **Add**.
2. In the Add Delivery Controller dialog box, specify a **Display name** that will help you to identify the deployment and select a **Type** to indicate how the resources made available in the store are provided. Type defaults to Citrix Virtual Apps and Desktops. XenApp 6.5 is available as a

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Type, however it reached End of Life in June 2018, and is now covered by the Extended Support Program.

3. To make desktops and applications provided by Citrix Virtual Apps and Desktops and XenApp 6.5 available in the store, add the names or IP addresses of your servers to the **Servers** list. Specify multiple servers to enable fault tolerance, listing the entries in order of priority to set the failover sequence. For Citrix Virtual Apps and Desktops sites, give details of Delivery Controllers. In the case of XenApp 6.5 farms, list servers running the Citrix XML Service.

4. Select from the **Transport type** list 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 secure HTTP connections using Transport Layer Security (TLS), 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.
   - To send data over secure connections to XenApp 6.5 servers using the SSL Relay to perform host authentication and data encryption, select **SSL Relay**.

     > Note:
     >
     > If you are using HTTPS or the SSL Relay 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.

5. Specify the **Port** for StoreFront to use for connections to the servers. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. In the case of Citrix Virtual Apps and Desktops servers, the specified port must be the port used by the Citrix XML Service.

   In a Citrix Virtual Apps and Desktops *on-premises* environment, **Shared secret** lets you allow only approved StoreFront machines to communicate with Delivery Controllers by specifying a key. For information about key generation, see Manage security keys.

   In a Citrix Virtual Apps and Desktops *service* environment, **Shared secret** lets you allow only approved StoreFront machines to communicate with Citrix Cloud by specifying a key. For information about key generation, see Manage security keys.

6. If you are using the SSL Relay to secure connections between StoreFront and XenApp 6.5 servers, specify the TCP port of the SSL Relay in **SSL Relay port**. The default port is 443. Ensure that all the servers running the SSL Relay are configured to monitor the same port.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

7. Click **OK**. You can configure stores to provide resources from any mixture of Citrix Virtual Apps and Desktops deployments. To add further Citrix Virtual Desktops sites or Citrix Virtual Apps farms, repeat the procedure above. When you have added all the required resources to the store, return to Step 7 in the "Create a new deployment" procedure at the top of this article.

Provide remote access to the store through a Citrix Gateway appliance

Complete the following steps to configure remote access through a Citrix Gateway appliance to the store that you create as part of the initial configuration of your StoreFront server. It is assumed that you have completed Steps 1 to 9 in the "Create a new deployment" procedure at the top of this article.

1. On the **Remote Access** page of the StoreFront console Create Store dialog box, click **Add**.
2. In the Add Citrix Gateway Appliance dialog box, on the **General Settings** page, specify a **Display name** for the Citrix Gateway appliance 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 gateway. 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 or closest gateway to their location.
3. For **Citrix Gateway URL**, type the URL:port combination of the Citrix Gateway virtual server for your deployment. If a port is not specified, then the default `https://` port of 443 is used. It is not necessary to specify port 443 in the URL.

   For information about creating a single Fully Qualified Domain Name (FQDN) to access a store internally and externally, see Create a single Fully Qualified Domain Name (FQDN) to access a store internally and externally.
4. Select the **Usage or role** of the Citrix Gateway from the available options.
   - **Authentication and HDX routing:** The Citrix Gateway will be used for Authentication, as well as for routing any HDX sessions.
   - **Authentication Only:** The Citrix Gateway will be used for Authentication and not for any HDX session routings.
   - **HDX routing Only:** The Citrix Gateway will be used for HDX session routings and not for Authentication.
5. For all deployments where you are making resources provided by Citrix Virtual Apps and Desktops or XenApp 6.5 available in the store, on the **Secure Ticket Authority** page, add **Secure Ticket Authority (STA) URLs** for servers running the STA. Add URLs for multiple STAs to enable fault tolerance, listing the servers in order of priority to set the failover sequence.

   The STA is hosted on Citrix Virtual Apps and Desktops, or XenApp 6.5 servers and issues session tickets in response to connection requests. These session tickets form the basis of authentication and authorization for access to Citrix Virtual Apps and Desktops, or XenApp 6.5 resources.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Use the correct STA URL (such as `HTTPS://` or `HTTP://`) depending on how your Delivery Controllers are configured. The STA URL must also be identical to the one configured within Citrix Gateway on your virtual server.

In a Citrix Virtual Apps and Desktops *on-premises* environment, **Shared secret** lets you allow only approved StoreFront machines to communicate with Secure Ticket Authority (STA) by specifying a key. For information about key generation, see Manage security keys.

In a Citrix Virtual Apps and Desktops *service* environment, **Shared secret** lets you allow only approved StoreFront machines to communicate with Citrix Cloud by specifying a key. For information about key generation, see Manage security keys.

6. To ensure Citrix Virtual Apps and Desktops, or XenApp 6.5 keep disconnected sessions open while Citrix Workspace app attempts to reconnect automatically, select **Enable session reliability**.

7. If you configure multiple STAs and want to ensure that session reliability is always available, select **Request tickets from two STAs, where available**. Then StoreFront obtains session tickets from two different STAs and 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.

8. On the **Authentication Settings** page, type the **VServer IP address** (VIP) of the Citrix Gateway appliance.

   Use the private IP address for the Citrix Gateway virtual server rather than the public IP address that is NATed to the private IP address. Gateways are usually identified by StoreFront via their URLs. If you are using global server load balancing (GSLB), you must add the VIP to each gateway. This allows StoreFront to identify multiple gateways which all use the same URL (GSLB domain name) as distinct gateways. For example, three gateways may be configured for the store with the same URL such as `https://gslb.domain.com` but would each have unique VIPs configured such as 10.0.0.1, 10.0.0.2 and 10.0.0.3.

9. If you are adding an appliance running Citrix Gateway, select from the **Logon type** list the authentication method you configured on the appliance for Citrix Workspace app users.

   - If users are required to enter their Microsoft Active Directory domain credentials, select **Domain**.
   - If users are required to enter a tokencode obtained from a security token, select **Security token**.
   - If users are required to enter both their domain credentials and a tokencode obtained from a security token, select **Domain and security token**.
   - If users are required to enter a one-time password sent by text message, select **SMS authentication**.
   - If users are required to present a smart card and enter a PIN, select **Smart card**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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**.

10. If you are configuring StoreFront for Citrix Gateway and want to use Smart Access, then you must type a **Callback URL**. StoreFront automatically appends the standard portion of the URL. Enter the internally accessible URL of the appliance. StoreFront contacts the Citrix Gateway authentication service to verify that requests received from Citrix Gateway originate from that appliance.

    When using GSLB, we recommend that you configure unique callback URLs for each of your GSLB gateways. StoreFront must be able to resolve each of the unique Callback URLs to the private VIPs configured for each of the GSLB gateway virtual servers. For example, `emeagateway.domain.com`, `usgateway.domain.com` and `apacgateway.domain.com` should resolve to the correct gateway VIP.

11. Click **Create** to add your Citrix Gateway appliance to the list in the **Remote Access Settings** dialog box.

    Information about the configuration of your Citrix Gateway appliances is saved to the .cr provisioning file for the store. This enables Citrix Workspace app to send the appropriate connection request when contacting appliances for the first time.

12. Return to Step 10 in the "Create a new deployment" procedure at the top of this article.

Join an existing server group

April 15, 2021

There is no limit of the number of servers in a StoreFront server group. However, from a capacity perspective based on simulations, there is no advantage to server groups containing more than three servers.

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

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

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

© 1999–2022 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.

Reset a server to factory defaults

October 22, 2020

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

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

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

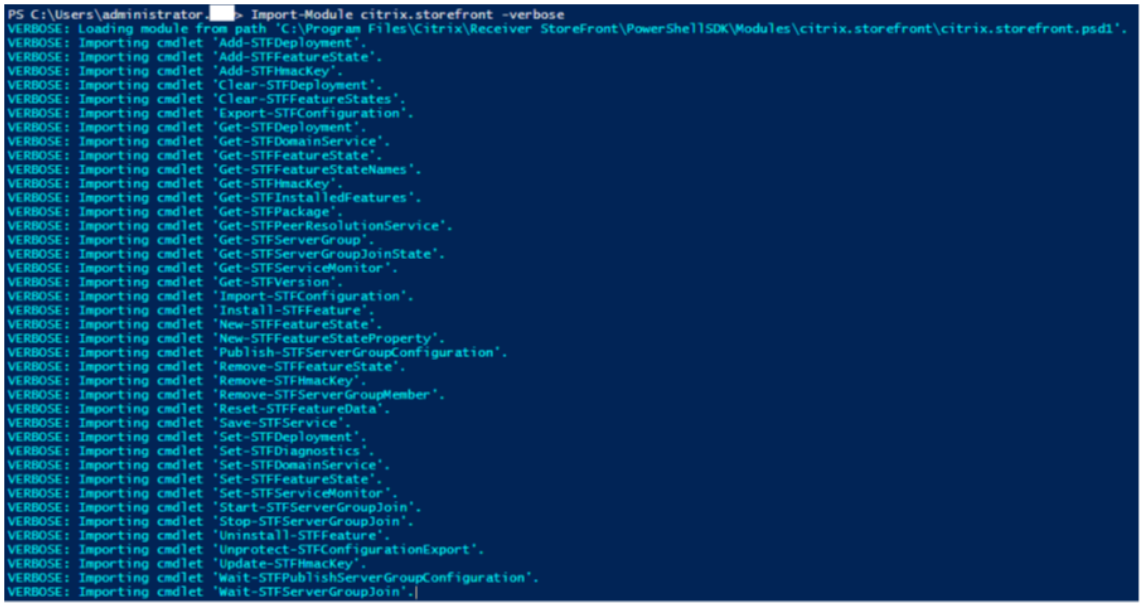
© 1999–2022 Citrix Systems, Inc. All rights reserved.

3. Set the PowerShell path:

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

4. Import the Citrix StoreFront module.

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

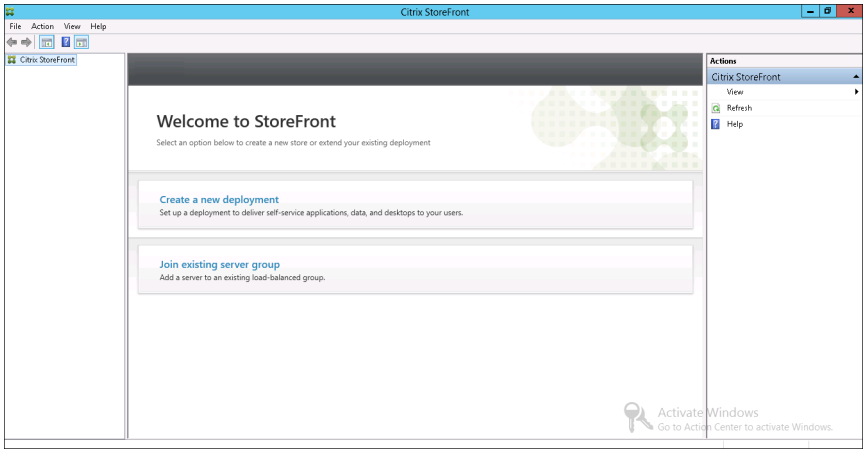


5. After the module is imported, run the **Clear-STFDeployment** command to reset the StoreFront server to the default settings:

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

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.



Migrate Web Interface features to StoreFront

April 29, 2020

Many of the Web Interface customizations have equivalents in StoreFront by using JavaScript tweaks, Citrix published APIs, or the StoreFront management console.

The table contains an overview of the customizations and basic information about how to achieve them.

Folder locations

- For script customizations, append the examples to the script.js file found in

  C:\inetpub\wwwroot\Citrix\StoreNameWeb\custom

- For style customization, append the example to the style.css file found in

  C:\inetpub\wwwroot\Citrix\StoreNameWeb\custom

- For dynamic content, add the dynamic context to a text file in

  C:\inetpub\wwwroot\Citrix\StoreNameWeb\customweb

- If you have a multiserver deployment, you can replicate any changes to other servers from the StoreFront administration console or by using PowerShell.

> **Note:**
>
> Web Interface enabled individual users to customize various settings. Currently, StoreFront does not have this ability, and while it is possible to add more extensive customization to support it, that is not the focus of this article.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Web Interface Feature	StoreFront Equivalent
Customization with the Management Console	
Layout-low graphics, Layout-full graphics, Allow users to choose	Not applicable. StoreFront auto detects and adjusts the UI to device screen.
Enable search, Disable search	Search is enabled by default. **To disable the search boxes on the desktop/web UI**, add the following style to style.css: `.search-container { display: none; }`. **To disable the search boxes on the phone UI**, add the following style to style.css: `##searchBtnPhone { display: none; }`
Enable refresh	Enabled by default (browser refresh).

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Web Interface Feature	StoreFront Equivalent
Enable return to last folder	Not enabled by default. To remember the current folder, and return to it on load, add the following to script.js: `CTXS.Extensions.afterDisplayHomeScreen = function(){ //check if view was saved last time CTXS.ExtensionAPI.localStorageGetItem("view", function (view){ if (view){ // if view was saved, change to it CTXS.ExtensionAPI.changeView(view); } if (view == "store"){ // if view is store, see if folder was saved CTXS.ExtensionAPI.localStorageGetItem("folder", function(folder){ if (folder != ""){ // if folder was saved, change to it CTXS.ExtensionAPI.navigateToFolder(folder); } }); } // set up monitoring of folder CTXS.Extensions.onFolderChange = function(folder){ CTXS.ExtensionAPI.localStorageSetItem("folder", folder); } ; // set up monitoring of view CTXS.Extensions.onViewChange = function(newview){ // don't retain search or appinfo views // instead, remember parent view. if ((newview != "appinfo")&&(newview != "search")){ CTXS.ExtensionAPI.localStorageSetItem("view", newview); } } ; }); } ;`
Enable hints	Citrix Workspace app makes very limited use of tooltips, as it is targeting touch and non-touch devices. You can add tooltips by custom script.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Web Interface Feature	StoreFront Equivalent
Icon view, Tree view, Details view, List view, Group view, Set Default view, (Low graphics) Icon view, (Low graphics) List view, (Low graphics) Default view	Citrix Workspace app has a different UI so these choices do not apply. You can use use the StoreFront management console to configure views. For more information see, Specify different views for applications and desktops.
Single tab UI, Tabbed UI (App tab, Desktop tab, Content tab, (Tab order))	The Citrix Workspace app UI is tabbed by default, with apps and content in one tab and desktops in the other. There is also an optional **Favorite** tab.
Header logo, Text color, Header background color, Header background image	Equivalents for colors and logos using the StoreFront administration console. Click **Customize Website Appearance** in the StoreFront administration console **Actions** pane and make your customizations on the screen that displays. You can set the header to a background image using a style customization. For example `.theme-header-bgcolor { background-image: url('spirals.png'); }`

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Web Interface Feature	StoreFront Equivalent
Pre-logon welcome message (Pre-locale) (Title,Text, Hyperlink, Button label)	By default, there is no separate pre-logon screen. This example script adds a click-through message box: `var doneClickThrough = false; // Before web login CTXS.Extensions. beforeLogon = function (callback){ doneClickThrough = true; CTXS. ExtensionAPI.showMessage({ messageTitle: ”Welcome!”, messageText: ”Only for \<a href=” http://www.WWc.com” target=”_blank ”\>WWCo Employees”, okButtonText: ” Accept”, okAction: callback }); } ; // Before main screen (for native clients)CTXS.Extensions. beforeDisplayHomeScreen = function (callback){ if (!doneClickThrough){ CTXS.ExtensionAPI.showMessage({ messageTitle: ”Welcome!”, messageText: ”Only for WWCo Employees”, okButtonText: ”Accept”, okAction: callback }); } else { callback(); } } ;`

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Web Interface Feature	StoreFront Equivalent
Logon screen title, Logon screen message, Logon screen system message	There are four areas for customization on the logon screen(s): top and bottom of screen (header and footer), and top and bottom of the logon box itself: `.customAuthHeader, .customAuthFooter .customAuthTop, .customAuthBottom { text-align: center; color: white; font-size: 16px; }`. Example script (static content): `\$('.customAuthHeader').html("Welcome to ACME");`. Example script (dynamic content): `function setDynamicContent(txtFile, element) { CTXS.ExtensionAPI.proxyRequest({ url: "customweb/"+txtFile, success: function(txt){ \$(element).html(txt); } } ); } setDynamicContent("Message.txt", ".customAuthTop");`. **Note:**: Do not explicitly include dynamic content in the script, or put it in the **custom** directory, because changes made here force all clients to reload the UI. Put dynamic content in the **customweb** directory.
Application screen welcome message, Application screen system message	See the examples for **CustomAuth** welcome screen above. See examples for dynamic content above. Use `##customTop` rather than `.customAuthTop` to place content on the home screen.
Footer text (all screens)	Example script: `##customBottom { text-align: center; color: white; font-size: 16px; } ** Example static content using a script: **\$('\##customBottom').html("Welcome to ACME");`

Features with no direct equivalent

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Web Interface Feature	StoreFront Equivalent
Logon screen without headers, Logon screen with headers (including messages)	There is no direct equivalent in StoreFront. However, you can create custom headers. See *Logon Screen Title* above.
User settings	By default, there are no user settings. You can add menus and buttons from JavaScript.
Workspace control	Equivalent functionality for administrator settings. The extension APIs allow significant additional flexibility. See http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/receiver-customization-api.html.
Deep Customizations (code)	
ICA File generation hooks and other call-routing customizations	Equivalent or better APIs. http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-customization-sdk.html
Authentication customizations	Equivalent or better APIs. http://www.citrix.com/go/citrix-developer/storefront-receiver-developer-community/store-authentication-sdks.html
JSP/ASP source access	There are no equivalent APIs on StoreFront, because the UI is not rendered in the same way. There are many JavaScript APIs to enable customization of the UI.

Configure server groups

September 1, 2021

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

You must configure servers comprising a StoreFront server group identically in terms of both StoreFront installation location and IIS website settings, such as physical path and site IDs.

Add a server to a server group

Use the Add Server task to obtain an authorization code to enable you to join a newly installed StoreFront server to your existing deployment. For more information about adding new servers to existing StoreFront deployments, see Join an existing server group. See the *Scalability* section of Plan your Storefront deployment to assess how many servers you need in your group.

Remove servers from a server group

Use the **Remove Server** task to delete servers from a multiple-server StoreFront deployment. You can remove any server in the group apart from the server on which you are running the task. Before removing a server from a multiple-server deployment, first remove the server from the load-balancing environment.

Before a removed StoreFront server can be added again, to the same or to a different server group, you must reset it to a factory default state. See Reset a server to factory defaults

Propagate local changes to a server group

Use the Propagate Changes task to update the configuration of all the other servers in a multiple-server StoreFront deployment to match the configuration of the current server. Propagation of configuration information is initiated manually so that you retain control over when and if the servers in the group are updated with configuration changes. While running this task, you cannot make any further changes until all the servers in the group have been updated.

> **Important:**
>
> Any changes made on other servers in the group are discarded during propagation. If you update the configuration of a server, propagate the changes to the other servers in the group to avoid losing those changes if you later propagate changes from different server in the deployment.

The information propagated between servers in the group includes the following:

- Contents of `C:\inetpub\wwwroot\Citrix\<Store>\App_Data` folder, such as the default.ica file.
- 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`.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- Contents of `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\contrib`.
- Contents of `C:\inetpub\wwwroot\Citrix\StoreWeb\Custom\custom folder`, such as copied images and customisation.js files.
- Contents of the Citrix Delivery Services certificate store, except any manually imported Certificate Revocation Lists (CRLs). (For details on distributing local CRLs, see Certificate Revocation List (CRL) checking.

> **Note:**
>
> Subscription data is synchronized with the other servers independently of the Propagate Changes mechanism. It happens automatically without the Propagate Changes task being initiated.

Change the base URL for a deployment

Use the **Change Base URL** task to modify the URL that 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. You can use this task to change from HTTP to HTTPS at any time, provided that Microsoft Internet Information Services (IIS) is configured for HTTPS, and you add an HTTPS binding to the default website. For more information, see Secure your StoreFront deployment.

Configure server bypass behavior

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

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

Considerations when specifying All failed bypass duration

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

To change the bypass parameters for a store

> **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 the other servers in the deployment are updated.

1. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and click **Manage Delivery Controllers** in the **Actions** pane.
3. Select a controller, click **Edit**, and then click **Settings** on the **Edit Delivery Controller** screen.
4. In Advanced Settings click **Settings**.
5. 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.

Configure authentication and delegation

April 29, 2020

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

Method	Detail
Configure the authentication service	The authentication service authenticates users to Microsoft Active Directory, ensuring that users do not need to log on again to access their desktops and applications.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Method	Detail
XML service-based authentication	When StoreFront is not in the same domain as Citrix Virtual Apps and Desktops, and it is not possible to put Active Directory trusts in place, you can configure StoreFront to use the Citrix Virtual Apps and Desktops XML Service to authenticate the user name and password credentials.
Kerberos constrained delegation for XenApp 6.5	Use the Configure Kerberos Delegation task to specify whether StoreFront uses single-domain Kerberos constrained delegation to authenticate to Delivery Controllers.
Smart card authentication	Set up smart card authentication for all the components in a typical StoreFront deployment.
Password expiry notification period	If you enable Citrix Receiver for Web site users to change their passwords at any time, local users whose passwords are about to expire are shown a warning when they log on.

Configure the authentication service

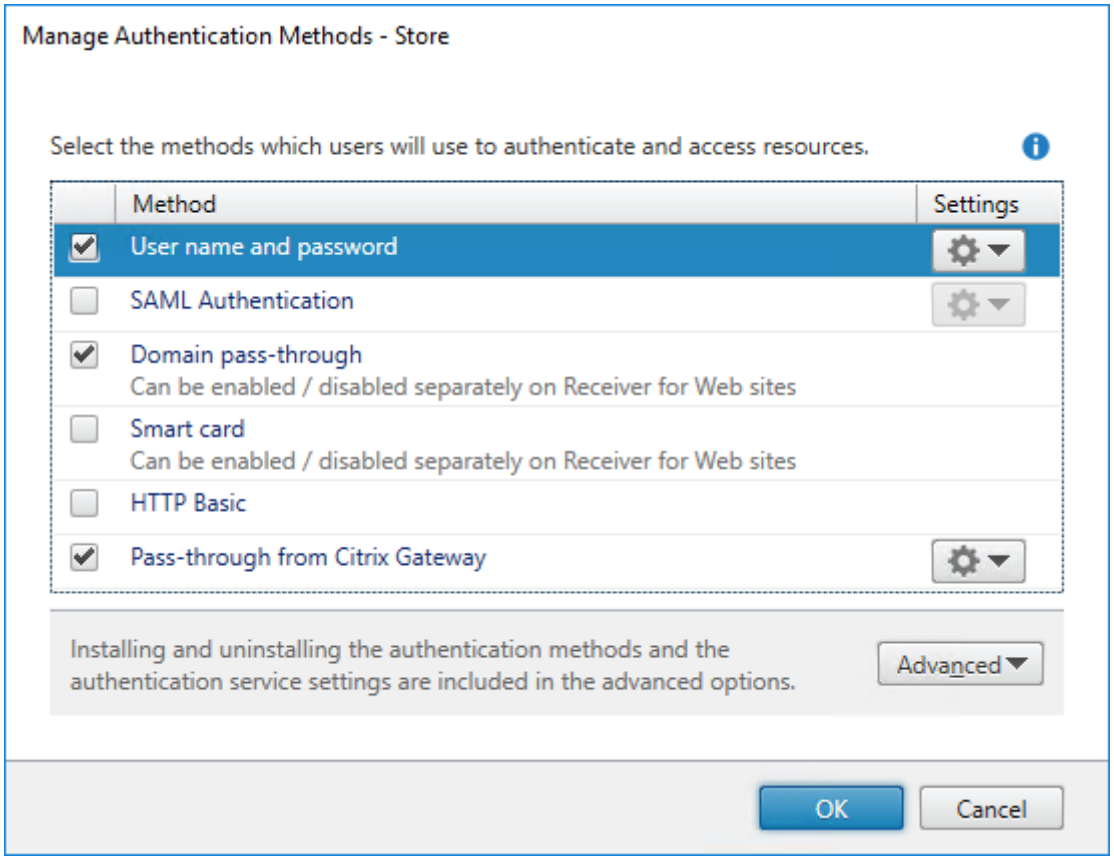
January 21, 2021

Manage authentication methods

You can enable or disable user authentication methods set up when the authentication service was created by selecting an authentication method in the results pane of the Citrix StoreFront management console and, in the Actions pane, clicking Manage Authentication Methods.

1. On the Windows Start screen or Apps screen, locate and click the Citrix **StoreFront** tile.
2. Select the **Store** node in the left pane of the Citrix StoreFront management console and, in the **Actions** pane, click **Manage Authentication Methods**.
3. Specify the access methods that you want to enable for your users.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



- Select the **Username and password** check box to enable explicit authentication. Users enter their credentials when they access their stores.
- Select the **SAML Authentication** check box to enable integration with a SAML Identity Provider. Users authenticate to an Identity Provider and are automatically logged when they access their stores. From the Settings drop-down menu:
  - Select **Identity Provider** to configure the trust to the Identity Provider.
  - Select **Service Provider** to configure the trust for the Service Provider. This information is required by the Identity Provider.
- Select **Domain pass-through** to enable pass-through of Active Directory domain credentials from users' devices. Users authenticate to their domain-joined Windows computers and are automatically logged on when they access their stores.

  To use domain pass-through authentication via Receiver for Web sites using Chrome or similar browsers, Citrix Receiver for Windows or Citrix Workspace app for Windows must be installed with the WebHelper component. WebHelper is installed by default with the Windows-based installer, but command-line installation requires installation using the `ADDLOCAL` parameter. To ensure users are not required to provide session credentials, domain pass-through authentication must be enabled when Citrix Receiver for Windows or Citrix Workspace app for Windows is installed on users' devices. See Citrix Workspace app for Windows documentation.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- Select **Smart card** to enable smart card authentication. Users authenticate using smart cards and PINs when they access their stores.
- Select **HTTP Basic** to enable HTTP Basic authentication. Users authenticate with the StoreFront server's IIS web server.
- Select **Pass-through from Citrix Gateway** to enable pass-through authentication from Citrix Gateway. Users authenticate to Citrix Gateway and are automatically logged on when they access their stores.

To enable pass-through authentication for smart card users accessing stores through Citrix Gateway, use the Configure Delegated Authentication task.

Configure trusted user domains

Use the Trusted Domains task to restrict access to stores for users logging on with explicit domain credentials, either directly or using pass-through authentication from Citrix Gateway.

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. 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**.
3. From the **User name and password > Settings** list, select **Configure Trusted Domains**.
4. Select **Trusted Domains only** and click **Add** to enter the name of a trusted domain. Users with accounts in that domain will be 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 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.
5. If you configure multiple trusted domains, select from the Default domain list the domain that is selected by default when users log on.
6. If you want to list the trusted domains on the logon page, select the Show domains list in logon page check box.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Enable users to change their passwords

Use the **Manage Password Options** task to enable Citrix Workspace app and Receiver for Web site users logging on with domain credentials to change their passwords. When you create the authentication service, the default configuration prevents Citrix Workspace app, and Citrix Receiver for Web site 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.

Citrix Workspace app and Citrix Receiver for Web both support password changes on expiration, as well as elective password changes.

Users accessing stores remotely (through Citrix Gateway), with Citrix Workspace app or Citrix Receiver for Web, can change their password when it expires. The Citrix Gateway option **Allow Password Change** must be enabled (see Citrix Gateway documentation).

Users accessing stores directly (via StoreFront) can only change their password when it expires if the **Allow users to change passwords** option is selected, as follows:

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. In the left pane of the Citrix StoreFront management console Actions pane, select the **Stores** node and click **Manage Authentication Methods**.
3. In **User name and passwords > Settings** select **Manage Password Options**.
4. To allow users to change their passwords, select **Allow users to change passwords**. If you do not select this option, you must make your own arrangements to support users who cannot access their desktops and applications because their passwords have expired.
5. Specify when Citrix Receiver for Web site users, logging on with domain credentials, can change their passwords.
   - **Only when they expire** enables users to change their passwords only when the passwords have already expired. Users who cannot log on because their passwords have expired are redirected to the Change Password dialog box.
   - **At any time** enables users to change their passwords whenever they want. Local users whose passwords are about to expire are shown a warning when they log on. Password expiry warnings are only displayed to users connecting from the internal network. By default, the applicable Windows policy setting determines the notification period for a user. For more information about setting custom notification periods, see Configure the password expiry notification period. This is supported with Citrix Receiver for Web only.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

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

Self-Service Password Reset security questions

Self-Service Password Reset enables end users to have greater control over their user accounts. Once you configure Self-Service Password Reset, if end users have problems logging on to their systems, they can unlock their accounts or reset their passwords to something new by correctly answering several security questions.

When setting up Self-Service Password Reset, you specify which users are able to perform password resets and unlock their accounts using the management console. If you enable these features for the StoreFront, users might still be denied permission to perform these tasks based on the settings configured in the Self-Service Password Reset configuration console.

Self-Service Password Reset is available only to users accessing StoreFront using HTTPS connections. They cannot access StoreFront using an HTTP connection and have Self-Service Password Reset available. Self-Service Password Reset is available only when authenticating directly to StoreFront with a user name and password.

Self-Service Password Reset does not support UPN logons, such as `username@domain.com`.

Before configuring Self-Service Password Reset for a store, you must ensure that:

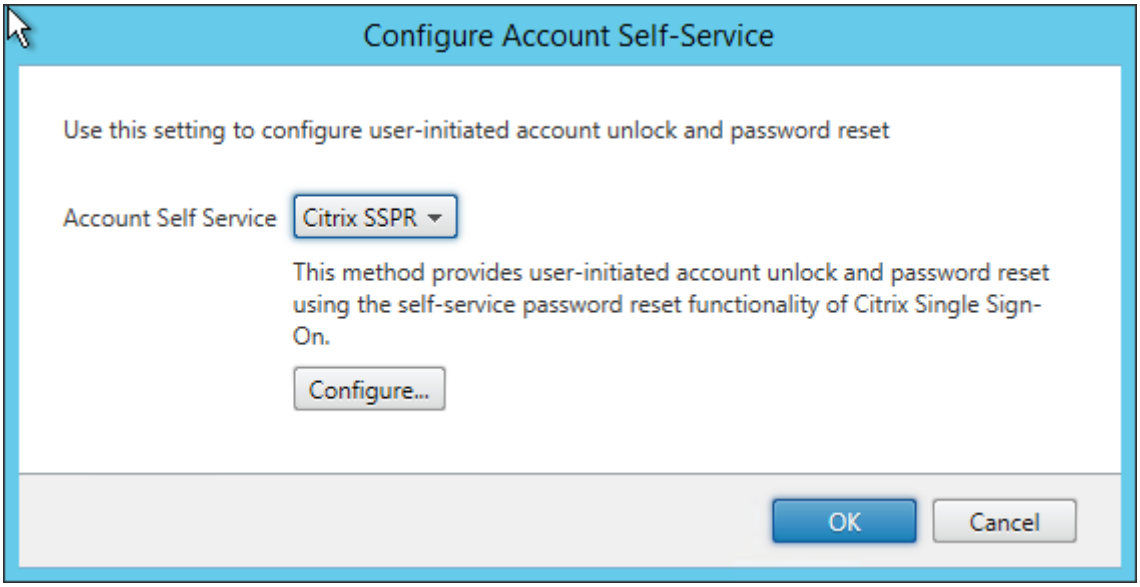
- The store is configured to use user name and password authentication.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- The store is configured to use only one Self-Service Password Reset. If StoreFront is configured to use multiple farms within the same or trusted domains, you must configure Self-Service Password Reset to accept credentials from all of those domains.
- The store is configured to allow users to change their password at any time if you want to enable password reset functionality.
- You must associate a StoreFront store with a Receiver for Web site.

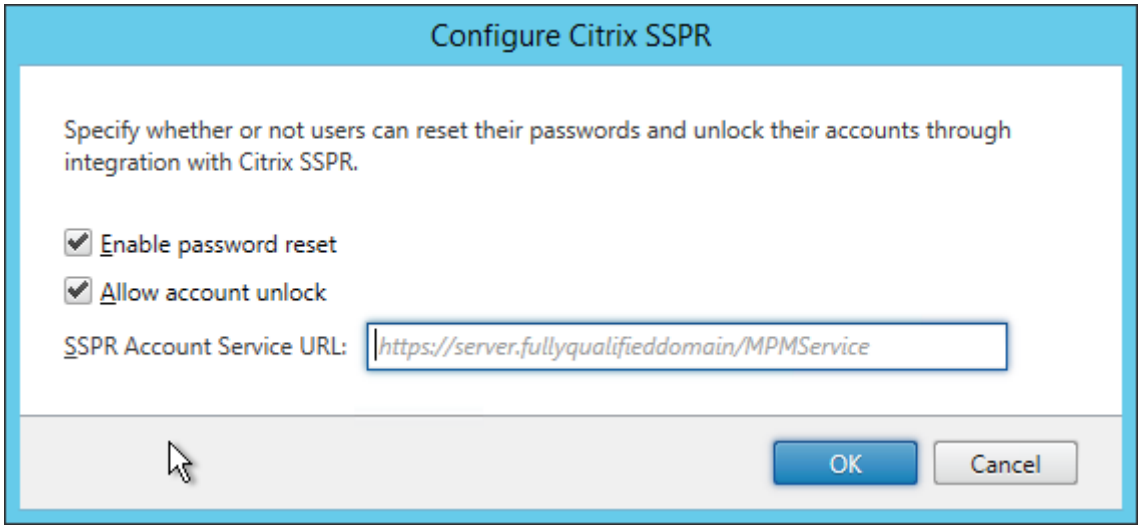
Before being able to use Self-Service Password Reset, you must install and configure it. It is available on the Citrix Virtual Apps and Desktops media. For information, see the Self-Service Password Reset documentation.

1. Enable Self-Service Password Reset support in StoreFront by selecting the **Stores** node in the left pane of the Citrix StoreFront management console and in the **Actions** pane, click **Manage Authentication Methods > User name and Password**, and choose **Manage Password Options** from the drop-down menu.
2. Choose when you want users to change passwords and click **OK**.
3. From the **User name and passwords** drop-down menu, choose **Configure Account Self-Service**, select **Citrix SSPR** from the drop-down menu, and click **OK**.
4. Specify whether or not users can reset their passwords and unlock their accounts with Self-Service Password Reset, add the Password Reset Service account URL, click **OK**, and then click **OK**.

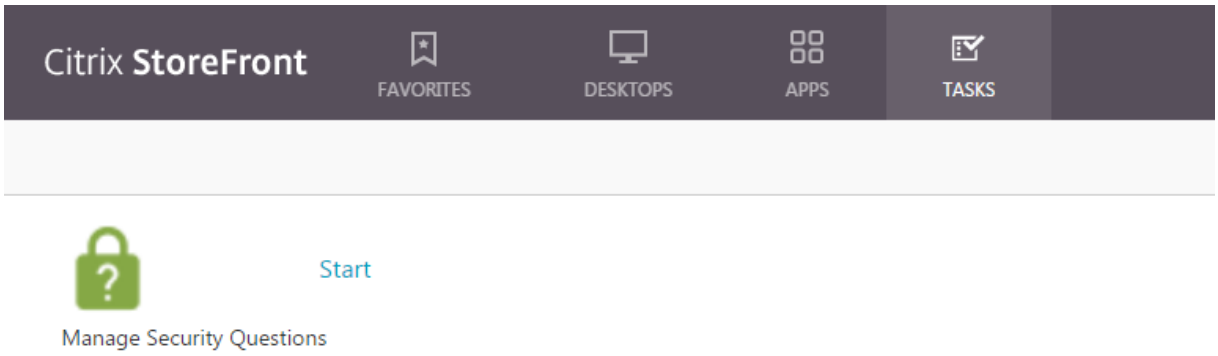


This option is available only when the StoreFront base URL is HTTPS (not HTTP) and the **Enable password reset** option is available only after you use **Manage Password Options** to allow users to change passwords at any time.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



The next time the user logs on to Citrix Workspace app, or Citrix Receiver for Web, security enrollment is available. After clicking **Start**, questions are displayed to which the user must specify answers.

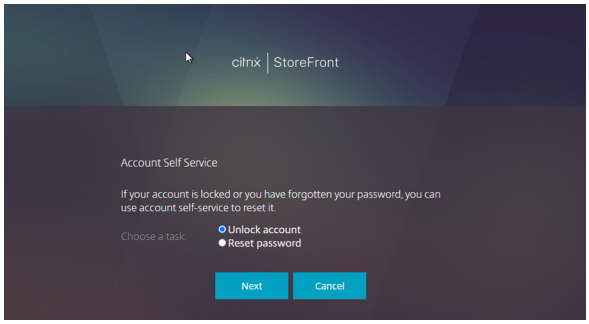


Once configured in StoreFront, users see the **Account Self-Service** link on the Citrix Receiver for Web logon screen (it displays as a button in other Citrix Workspace apps).

Clicking this link takes the user through a series of forms to first select between **Unlock account** and **Reset password** (if both are available).

After choosing a radio button and clicking **Next**, the next screen prompts for a domain and username (*domain\user*) if that information was not entered in the log on form. Note that account self-service does not support UPN log ons, such as `username@domain.com`.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



They are required to answer the security question. If all the answers match those supplied by the user, the requested operation (unlock or reset) is performed and the user is notified that it succeeded.

Shared authentication service settings

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

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

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

Delegate credential validation to Citrix Gateway

Use the Configure Delegated Authentication task to enable pass-through authentication for smart card users accessing stores through Citrix Gateway. This task is only available when Pass-through from Citrix Gateway is enabled and selected in the results pane.

When credential validation is delegated to Citrix Gateway, users authenticate to Citrix Gateway with their smart cards and are automatically logged on when they access their stores. This setting is disabled by default when you enable pass-through authentication from Citrix Gateway, so that pass-through authentication only occurs when users log on to Citrix Gateway with a password.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

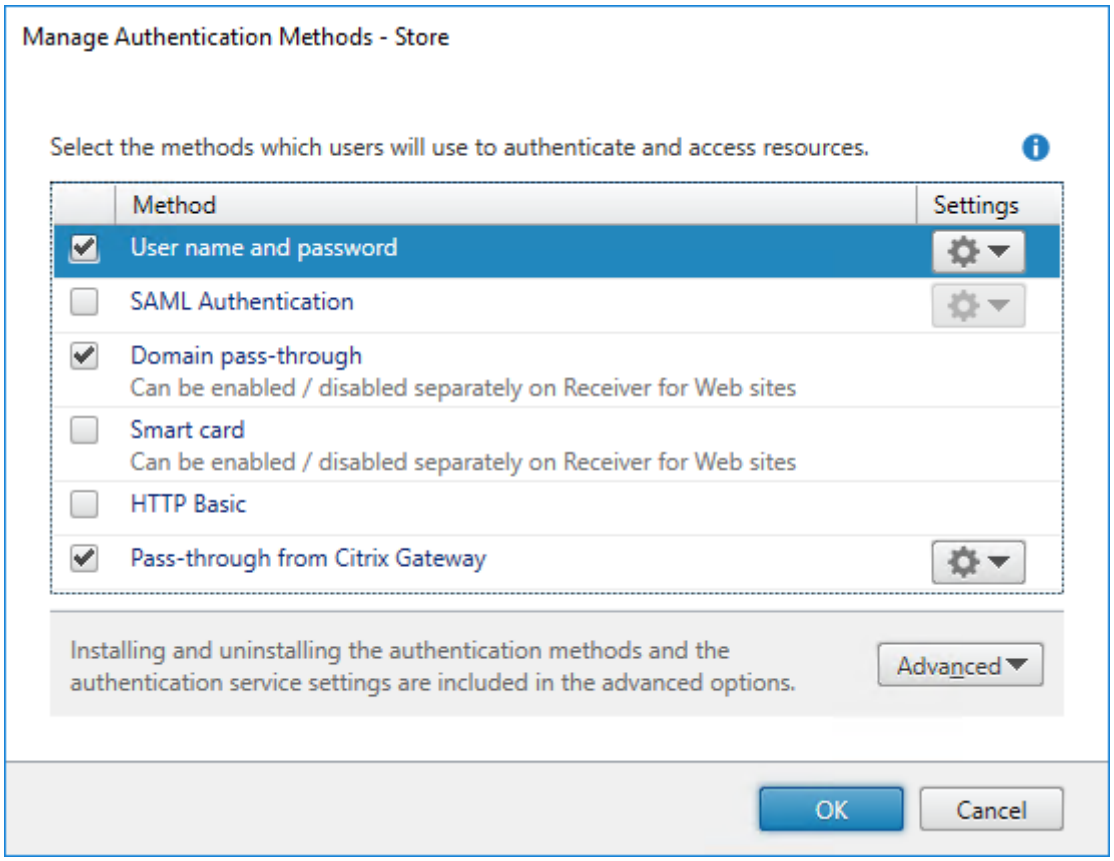
XML service-based authentication

October 22, 2020

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

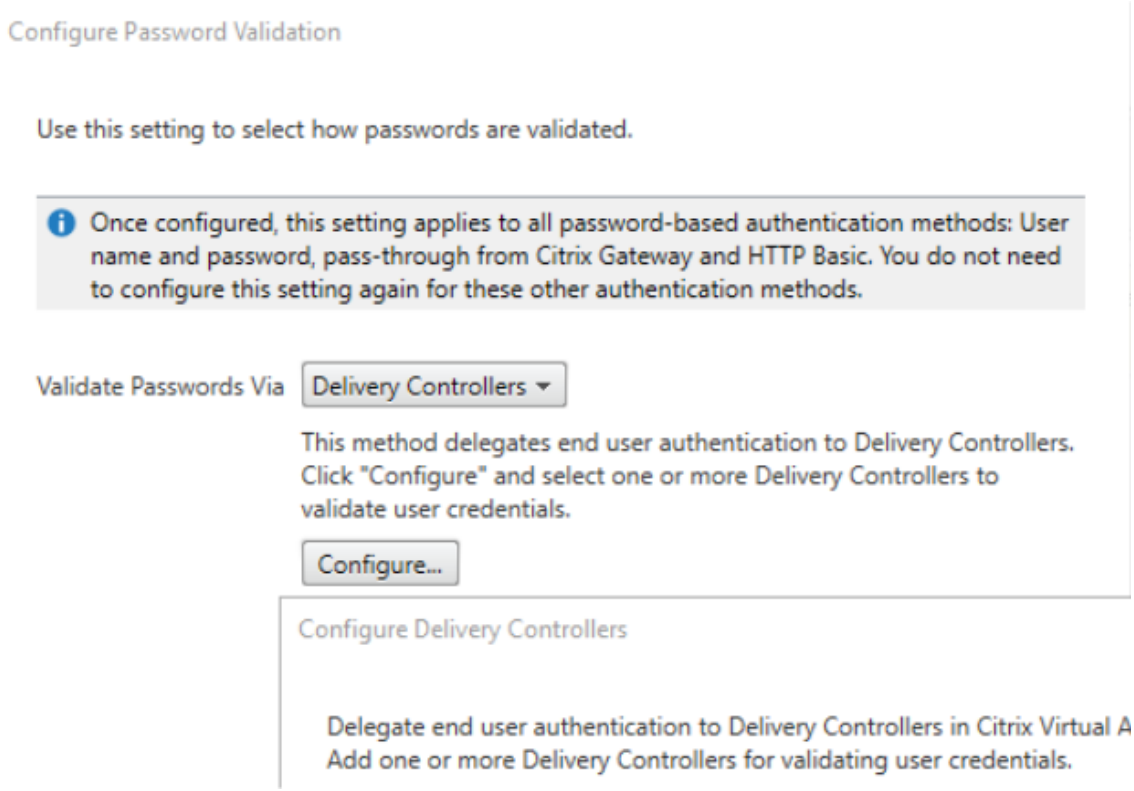
Enable XML service-based authentication

1. On the Windows **Start** screen or **Apps** screen, locate and click the Citrix StoreFront tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the Actions pane, click **Manage Authentication Methods**.
3. On the **Manage Authentication Methods** page, from the **User name and password > Settings** drop-down menu, select **Configure Password Validation**.



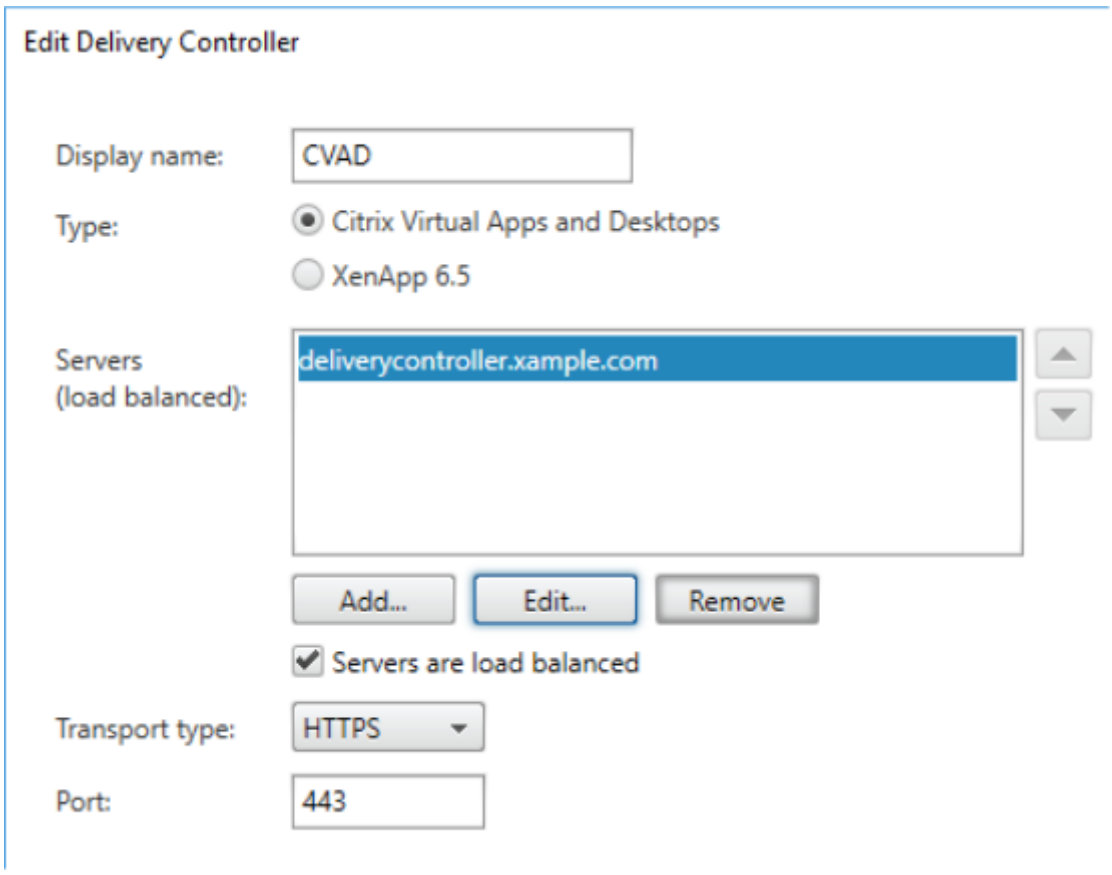
4. From the **Validation Password Via** list, select **Delivery Controllers**, and then click **Configure**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



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

© 1999–2022 Citrix Systems, Inc. All rights reserved.



Disable XML service-based authentication

1. On the Windows **Start** screen or **Apps** screen, locate and click the Citrix StoreFront tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the Actions pane, click **Manage Authentication Methods**.
3. On the **Manage Authentication Methods** page, from the **User name and password** > **Settings** list, select **Configure Password Validation**.
4. From the **Validation Password Via** drop-down menu, select **Active Directory**, and then click **OK**.

Configure Kerberos constrained delegation for XenApp 6.5

April 29, 2020

> Note:
>
> XenApp 6.5 has reached End of Life (EOL) and is now covered by the Extended Support Program.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Use the **Configure Store Settings** > **Kerberos delegation** task to specify whether StoreFront uses single-domain Kerberos constrained delegation to authenticate to Delivery Controllers.

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. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. 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,** and then click Kerberos Delegation.
3. Select Enable or Disable Kerberos delegation to authenticate to Delivery Controllers, respectively, enable or disable Kerberos constrained delegation.

Configure the StoreFront server for delegation

Follow this procedure when StoreFront is not installed on the same machine as Citrix Virtual Apps.

1. On the domain controller, open the MMC Active Directory Users and Computers snap-in.
2. On the **View** menu, click **Advanced Features**.
3. In the left pane, click the **Computers** node under the domain name and select the StoreFront server.
4. In the **Action** pane, click **Properties**.
5. On the **Delegation** tab, click **Trust this computer for delegation to specified services only** and **Use any authentication protocol**, and then click **Add**.
6. In the **Add Services** dialog box, click **Users or Computers**.
7. In the **Select Users or Computers** dialog box, type the name of the server running the Citrix Virtual Apps and Desktops XML Service in the **Enter the object names to select** box, click **OK**.
8. Select the HTTP service type from the list, click **OK**.
9. Apply the changes and close the dialog box.

Configure Citrix Virtual Apps server for delegation

Configure Active Directory Trusted Delegation for each Citrix Virtual Apps server.

1. On the domain controller, open the **MMC Active Directory Users and Computers** snap-in.
2. In the left pane, click the **Computers** node under the domain name and select the server running the Citrix Virtual Apps and Desktops XML Service that StoreFront is configured to contact.
3. In the **Action** pane, click **Properties**.
4. On the **Delegation** tab, click **Trust this computer for delegation to specified services only** and **Use any authentication protocol**, and then click **Add**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

5. In the **Add Services** dialog box, click **Users or Computers**.
6. In the **Select Users or Computers** dialog box, type the name of the server running the Citrix Virtual Apps and Desktops XML Service in the **Enter the object names to select** box, click **OK**.
7. Select the HOST service type from the list, click **OK**, and then click **Add**.
8. In the **Select Users or Computers** dialog box, type the name of the Domain Controller in the **Enter the object names to select box** and click **OK**.
9. Select the **cifs** and **ldap** service types from the list and click **OK**. Note: If two choices appear for the ldapservice, select the one that matches the FQDN of the domain controller.
10. Apply the changes and close the dialog box.

Important considerations

When you decide whether to use Kerberos constrained delegation, consider the following information.

- Key Notes:
  - You do not need ssonsvr.exe unless doing pass-through authentication (or smart card pin pass-through authentication) without Kerberos constrained delegation.
- Storefront and Citrix Receiver for Web domain pass-through:
  - You do not need ssonsvr.exe on the client.
  - You can set the Local username and password in the Citrix icaclient.adm template to anything (controls ssonsvr.exe function).
  - The icaclient.adm template Kerberos setting is required.
  - Add the Storefront Fully Qualified Domain Name (FQDN) to Internet Explorer trusted sites list. Check the Use local username box in the Internet Explorer security settings for the trusted zone.
  - The client must be in a domain.
  - Enable the Domain pass-through authentication method on the StoreFront server and enable for Citrix Receiver for Web.
- Storefront, Citrix Receiver for Web, and smart card authentication with PIN prompt:
  - You do not need ssonsvr.exe on the client.
  - Smart card authentication was configured.
  - You can set the Local username and password in the Citrix icaclient.adm template to anything (controls ssonsvr.exe function).
  - The icaclient.adm template Kerberos setting is required.
  - Enable the Smart card authentication method on the StoreFront server and enable for Citrix Receiver for Web.
  - To ensure smart card authentication is chosen, do not check the Use local username box in the Internet Explorer security settings for the StoreFront site zone.
  - The client must be in a domain.
- Citrix Gateway, StoreFront, Citrix Receiver for Web, and smart card authentication with PIN

© 1999–2022 Citrix Systems, Inc. All rights reserved.

prompt:

  - You do not need ssonsvr.exe on the client.
  - Smart card authentication was configured.
  - You can set the Local username and password in the Citrix icaclient.adm template to anything (controls ssonsvr.exe function).
  - The icaclient.adm template Kerberos setting is required.
  - Enable the Pass-through from Citrix Gateway authentication method on the StoreFront server and enable for Citrix Receiver for Web.
  - To ensure smart card authentication is chosen, do not check the Use local username box in the Internet Explorer security settings for the StoreFront site zone.
  - The client must be in a domain.
  - Configure Citrix Gateway for smart card authentication and configure an additional vServer for launch using StoreFront HDX routing to route the ICA traffic through the unauthenticated Citrix Gateway virtual server.

- Citrix Receiver for Windows or Citrix Workspace app for Windows (AuthManager), smart card authentication with PIN prompt, and StoreFront:
  - You do not need ssonsvr.exe on the client.
  - You can set the Local username and password in the Citrix icaclient.adm template to anything (controls ssonsvr.exe function).
  - The icaclient.adm template Kerberos setting is required.
  - The client must be in a domain.
  - Enable the Smart card authentication method on the StoreFront server.
- Citrix Receiver for Windows or Citrix Workspace app for Windows (AuthManager), Kerberos, and StoreFront:
  - You do not need ssonsvr.exe on the client.
  - You can set the Local username and password in the Citrix icaclient.adm template to anything (controls ssonsvr.exe function).
  - The icaclient.adm template Kerberos setting is required.
  - Check the Use local username box in the Internet Explorer security settings for the trusted zone.
  - The client must be in a domain.
  - Enable the Domain pass-through authentication method on the StoreFront server.
  - Ensure this registry key is set:

    > **Caution:**
    > 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.

    For 32-bit machines: HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\AuthManagerProtocols\integratedwin

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Name: SSONCheckEnabled
Type: REG_SZ
Value: true or false
For 64-bit machines: HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\AuthManagerProtocol
Name: SSONCheckEnabled
Type: REG_SZ
Value: true or false

Configure smart card authentication

November 25, 2020

This article gives an overview of the tasks involved in setting up smart card authentication for all the components in a typical StoreFront deployment. For more information and step-by-step configuration instructions, see the documentation for the individual products.

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.

> Note:
>
> In this article, mentions of "Citrix Workspace app" also represent the supported versions of Citrix Receiver unless otherwise noted.

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.
- Before continuing, 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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Configure Citrix Gateway

- On your Citrix Gateway appliance, install a signed server certificate from a certification authority. For more information, see Installing and Managing Certificates.
- On your Citrix Gateway appliance, install the root certificate of the certification authority issuing your smart card user certificates. For more information, see To install a root certificate on Citrix Gateway.
- Create and configure a virtual server for client certificate authentication. Create a certificate authentication policy, specifying SubjectAltName:PrincipalName for user name extraction from the certificate. Then, bind the policy to the virtual server and configure the virtual server to request client certificates. For more information, see Configuring and Binding a Client Certificate Authentication Policy.
- Bind the certification authority root certificate to the virtual server. For more information, see To add a root certificate to a virtual server.
- 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 virtual server. When you create the virtual server, disable client authentication in the Secure Sockets Layer (SSL) parameters. For more information, see Configuring smart card authentication.

  You must also configure StoreFront to route user connections to resources through this additional virtual server. Users log on to the first virtual server and the second virtual server is used for connections to their resources. When the connection is established, users do not need to authenticate to Citrix Gateway but are required to enter their PINs to log on to their desktops and applications. Configuring a second virtual server for user connections to resources is optional unless you plan to enable users to fall back to explicit authentication if they experience any issues with their smart cards.
- Create session policies and profiles for connections from Citrix Gateway to StoreFront and bind them to the appropriate virtual server. For more information, see Access to StoreFront Through Citrix Gateway.
- If you configured the virtual server used for connections to StoreFront to require client certificate authentication for all communications, you must create a further virtual server to provide the callback URL for StoreFront. This virtual server is used only by StoreFront to verify requests from the Citrix Gateway appliance and so does not need to be publically accessible. A separate virtual server is required when client certificate authentication is mandatory because StoreFront cannot present a certificate to authenticate. For more information, see Creating Virtual Servers.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Configure StoreFront

- You must use HTTPS for communications between StoreFront and users' devices to enable smart card authentication. Configure Microsoft Internet Information Services (IIS) for HTTPS by obtaining an SSL certificate in IIS and then adding HTTPS binding to the default website. For more information about creating a server certificate in IIS, see https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh831637(v=ws.11)#create-certificate-wizard. For more information about adding HTTPS binding to an IIS site, see https://docs.microsoft.com/en-us/previous-versions/orphan-topics/ws.11/hh831632(v=ws.11).

- If you want to require that client certificates are presented for HTTPS connections to all StoreFront URLs, configure IIS on the StoreFront server.

  When StoreFront is installed, the default configuration in IIS only requires that client certificates are presented for HTTPS connections to the certificate authentication URL of the StoreFront authentication service. This configuration is required to provide smart card users with the option to fall back to explicit authentication and, subject to the appropriate Windows policy settings, enable users to remove their smart cards without needing to reauthenticate.

  When IIS is configured to require client certificates for HTTPS connections to all StoreFront URLs, smart card users cannot connect through Citrix Gateway and cannot fall back to explicit authentication. Users must log on again if they remove their smart cards from their devices. To enable this IIS site configuration, the authentication service and stores must be colocated on the same server, and a client certificate that is valid for all the stores must be used. Moreover, this configuration where IIS is requiring client certificates for HTTPS connections to all StoreFront URLs, will conflict with authentication for Citrix Receiver for Web clients. For this reason, this configuration should be used when Citrix Receiver for Web client access is not required.

- Install and configure StoreFront. Create the authentication service and add your stores, as required. If you configure remote access through Citrix Gateway, do not enable virtual private network (VPN) integration. For more information, see Install and set up StoreFront.

- Enable smart card authentication to StoreFront for local users on the internal network. For smart card users accessing stores through Citrix Gateway, enable the pass-through with Citrix Gateway authentication method and ensure that StoreFront is configured to delegate credential validation to Citrix Gateway. If you plan to enable pass-through authentication when you install Citrix Receiver for Windows or Citrix Workspace app for Windows on domain-joined user devices, enable domain pass-through authentication. For more information, see Configure the authentication service.

  To allow Citrix Receiver for Web client authentication with smart cards, you must enable the authentication method per Citrix Receiver for Web site. For more information, see the Configure Citrix Receiver for Web sites instruction.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

If you want smart card users to be able to fall back to explicit authentication if they experience any issues with their smart cards, do not disable the user name and password authentication method.

- If you plan to enable pass-through authentication when you install Citrix Receiver for Windows or Citrix Workspace app for Windows on domain-joined user devices, edit the default.ica file for the store to enable pass-through of users' smart card credentials when they access their desktops and applications. For more information, see Enable pass-through with smart card authentication for Citrix Receiver for Windows or Citrix Workspace app for Windows.
- If you created an additional Citrix Gateway virtual server to be used only for user connections to resources, 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.
- To enable users of PCs running the Citrix Desktop Lock to authenticate using smart cards, enable pass-through with smart card authentication to your XenApp Services URLs. For more information, see Configure authentication for XenApp Services URLs.

Configure user devices

- Ensure that your vendor's smart card middleware is installed on all user devices.
- For users with repurposed PCs, install Receiver for Windows Enterprise using an account with administrator permissions. Configure Receiver for Windows with the XenApp Services URL for the appropriate store. Once you have confirmed that you can log on to the device with a smart card and access resources from the store, install the Citrix Desktop Lock. For more information, see To install the Desktop Lock.
- For all other users, install the appropriate version of Citrix Workspace app on the user device. To enable pass-through of smart card credentials to Citrix Virtual Apps and Desktops for users with domain-joined devices, use an account with administrator permissions to install Citrix Workspace app for Windows at a command prompt with the **/includeSSON** option. For more information, see Using command-line parameters.

  Ensure that Citrix Workspace app for Windows is configured for smart card authentication either through a domain policy or a local computer policy. For a domain policy, use the Group Policy Management Console to import the Citrix Workspace app for Windows Group Policy Object template file, icaclient.adm, onto the domain controller for the domain containing your users' accounts. To configure an individual device, use the Group Policy Object Editor on that device to configure the template. For more information, see Smart card.

  Enable the Smart card authentication policy. To enable pass-through of users' smart card credentials, select Use pass-through authentication for PIN. Then, to pass users' smart card cre-

© 1999–2022 Citrix Systems, Inc. All rights reserved.

dentials through to Citrix Virtual Apps and Desktops, enable the Local user name and password policy and select Allow pass-through authentication for all ICA connections. For more information, see ICA Settings Reference.

If you enabled pass-through of smart card credentials to Citrix Virtual Apps and Desktops for users with domain-joined devices, add the store URL to the Local intranet or Trusted sites zone in Internet Explorer. Ensure that Automatic logon with the current user name and password is selected in the security settings for the zone.

- Where necessary, provide users with connection details for the store (for users on the internal network) or Citrix Gateway appliance (for remote users) using an appropriate method. For more information about providing configuration information to your users, see ICA Settings Reference.

Enable pass-through with smart card authentication for Receiver for Windows or Citrix Workspace app for Windows

You can enable pass-through authentication when you install Receiver for Windows on domain-joined user devices. To enable pass-through of users' smart card credentials when they access desktops and applications hosted by Citrix Virtual Apps and Desktops, you edit the default.ica file for the store.

> **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. Use a text editor to open the default.ica file for the store, which is typically located in the C:\inetpub\wwwroot\Citrix\storename\App_Data\ directory, where storename is the name specified for the store when it was created.
2. To enable pass-through of smart card credentials for users who access stores without Citrix Gateway, add the following setting in the [Application] section.

   ```
   DisableCtrlAltDel=Off
   ```

   This setting applies to all users of the store. To enable both domain pass-through and pass-through with smart card authentication to desktops and applications, you must create separate stores for each authentication method. Then, direct your users to the appropriate store for their method of authentication.
3. To enable pass-through of smart card credentials for users accessing stores through Citrix Gateway, add the following setting in the [Application] section.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

`UseLocalUserAndPassword=On`

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

Configure the password expiry notification period

February 2, 2021

> **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.

If you enable Citrix Receiver for Web site users to change their passwords **At any time** (as described in Manage authentication methods), you can configure whether local users are reminded that their passwords are about to expire when they log on. By default, the notification period for a user is determined by the applicable Windows policy setting.

To set a custom notification period for all users, you can edit the web.config file for the authentication service.

- For a default store, edit `C:\inetpub\wwwroot\Citrix\Authentication\web.config`
- For a custom store, edit `C:\inetpub\wwwroot\Citrix\customAuth\web.config`

1. Search for the following explicit configuration:

```
<explicitBL authenticator="defaultDelegatedAuthenticator" requireAccountSIDs="true"
  hideDomainField="true" allowUserPasswordChange="Never" showPasswordExpiryWarning="Windows"
  passwordExpiryWarningPeriod="10" explicitJsonEnabled="true"
  allowZeroLengthPassword="false">
  <domainSelection default="">
    <clear />
  </domainSelection>
  <accountPolicy allowUnlockAccount="false" allowResetPassword="false" />
</explicitBL>
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

2. To disable password expiry notifications, use `showPasswordExpiryWarning="Never"`.
3. To set a custom notification period (for example 10 days before password expiry), use `showPasswordExpiryWarning="Custom"` and `passwordExpiryWarningPeriod="10"`.

> **Note:**
>
> StoreFront does not support Fine-Grained Password Policies in Active Directory.

Configure and manage stores

April 29, 2020

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

Task	Detail
Create or remove a store	Configure as many additional stores as you need.
Create an unauthenticated store	Configure additional unauthenticated stores to support access for unauthenticated (anonymous) users.
Export store provisioning files for users	Generate files containing connection details for stores, including any Citrix Gateway deployments and beacons configured for the stores.
Hide and advertise stores to users	Prevent stores being presented to users to add to their accounts when they configure Citrix Workspace app through email-based account discovery or FQDN.
Manage the resources made available in stores	Add and remove resources from stores.
Manage remote access to stores through Citrix Gateway	Configure access to stores through Citrix Gateway for users connecting from public networks.
Configure two StoreFront stores to share a common subscription datastore	Configure two stores to share a common subscription database.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Task	Detail
Advanced store settings	Configure advanced store settings.

Create or remove a store

May 4, 2021

Use the **Create Store** task to configure additional stores. 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.

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.

On the Store Name page, selecting **Allow only unauthenticated users to access this store** allows you to create an unauthenticated store which is anonymous, or unauthenticated. 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.)

> 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.

Add desktops and applications to the store

1. On the Windows Start screen or Apps screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the **Actions** pane, click **Create Store**.
3. On the **Store Name** page, specify a name for your store and click **Next**.

   Store names appear in Citrix Workspace app under users' accounts, so choose a name that gives users information about the content of the store.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

4. On the **Delivery Controllers** page, list the infrastructure providing the resources that you want to make available in the store. Click **Add**.
5. In the Add Delivery Controller dialog box, specify a **Display name** that will help you to identify the deployment. Specify **Type** to indicate how the resources made available in the store are provided. Type defaults to Citrix Virtual Apps and Desktops. XenApp 6.5 is available as a Type, however it reached End of Life in June 2018, and is now covered by the Extended Support Program.
6. To make desktops and applications provided by Citrix Virtual Apps and Desktops and XenApp 6.5 available in the store, add the names or IP addresses of your servers to the **Servers** list. Specify multiple servers to enable fault tolerance, listing the entries in order of priority to set the failover sequence. For Citrix Virtual Apps and Desktops sites, give details of Delivery Controllers. In the case of XenApp 6.5 farms, list servers running the Citrix XML Service.
7. Select from the **Transport type** list 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 secure HTTP connections using Transport Layer Security (TLS), 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.
   - To send data over secure connections to XenApp 6.5 servers using the SSL Relay to perform host authentication and data encryption, select **SSL Relay**.

     > Note:
     >
     > If you are using HTTPS or the SSL Relay 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.
8. Specify the **Port** for StoreFront to use for connections to the servers. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. In the case of Citrix Virtual Apps and Desktops servers, the specified port must be the port used by the Citrix XML Service.
9. If you are using the SSL Relay to secure connections between StoreFront and XenApp 6.5 servers, specify the TCP port of the SSL Relay in **SSL Relay port**. The default port is 443. Ensure that all the servers running the SSL Relay are configured to monitor the same port.

   In a Citrix Virtual Apps and Desktops *on-premises* environment, **Shared secret** lets you allow only approved StoreFront machines to communicate with Delivery Controllers by specifying a

© 1999–2022 Citrix Systems, Inc. All rights reserved.

key. For information about key generation and configuration, see Manage security keys.

In a Citrix Virtual Apps and Desktops *service* environment, **Shared secret** lets you allow only approved StoreFront machines to communicate with Citrix Cloud by specifying a key. For information about key generation and configuration, see Manage security keys.

10. Click **OK**. You can configure stores to provide resources from any mixture of Citrix Virtual Apps and Desktops deployments. Repeat Steps 4 to 10, as necessary, to list additional deployments providing resources for the store. When you have added all the required resources to the store, click **Next**.

11. On the **Remote Access** page, 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, select **Enable Remote Access**.
      - To make only resources delivered through the store available through Citrix Gateway, select **No VPN tunnel**. Users log on using either ICAProxy or clientless VPN (cVPN) to Citrix Gateway and do not need to use the Citrix Gateway plug-in to establish a full VPN.
      - To make the store and other resources on the internal network available through a Secure Sockets Layer (SSL) virtual private network (VPN) tunnel, select **Full VPN tunnel**. Users require the Citrix Gateway plug-in to establish the VPN tunnel.

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

12. If you enabled remote access, in the **Citrix Gateway appliances** list, select from the appliances (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 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. To add further appliances to the list, follow the process described in Provide remote access to the store through Citrix Gateway.

13. On the **Authentication Methods** page, select the methods your users will use to authenticate to the store and click **Next**. You can select from the following methods:

    - **Username and password**: Users enter their credentials and are authenticated when they access their stores.
    - **SAML Authentication**: Users authenticate to an Identity Provider and are automatically logged on when they access their stores.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- **Domain pass-through†**: Users authenticate to their domain-joined Windows computers and their credentials are used to log them on automatically when they access their stores.
- **Smart card†**: Users authenticate using smart cards and PINs when they access their stores.
- **HTTP basic**: Users authenticate with the StoreFront server's IIS web server.
- **Pass-through through Citrix Gateway**: Users authenticate to Citrix Gateway and are automatically logged on when they access their stores. This is automatically checked when the remote access is enabled.

> **Note:**
>
> † Store authentication methods which do not propagate to the store's Citrix Receiver for Web sites. Configure these authentication methods independently for each Citrix Receiver for Web site using the **Manage Receiver for Web Sites** task described in Configure Citrix Receiver for Web sites.
>
> The other store authentication methods described here do propagate to the store's Citrix Receiver for Web sites. (That is, a selection or deselection made here for the store dictates the setting used by all its Receiver for Web sites.)

14. On the **Configure Password Validation** page, select the Delivery Controllers to provide the password validation, click **Next**.
15. On the **XenApp Services URL** page, configure the URL for users who use PNAgent to access application and desktops and click **Create**.
16. When the store has been created, click **Finish**.

Accessing the store

Your store is now available for users to access with Citrix Workspace app, which must be configured with access details for the store. There are a number of ways in which you can provide these details to users to make the configuration process easier for them. For more information, see User access options.

Alternatively, users can access the store through the Receiver for Web site, which enables users to access their desktops and applications through a webpage. The URL for users to access the Receiver for Web site for the new store is displayed when you create the store.

When you create a new store, the XenApp Services URL is enabled by default. Users of PCs running the Citrix Desktop Lock, along with users who have older Citrix clients that cannot be upgraded, can access stores directly using the XenApp Services URL for the store. The XenApp Services URL has the form `http[s]://serveraddress/Citrix/storename/PNAgent/config.xml`, where **serveraddress** is the FQDN of the server or load balancing environment for your StoreFront deployment and **storename** is the name you specified for the store in Step 3.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Provide remote access to the store through Citrix Gateway

Complete the following steps to configure remote access through Citrix Gateway to the store that you created in the previous procedure. It is assumed that you have completed all the preceding steps.

1. On the **Remote Access** page of the **Create Store** wizard, click **Add**.
2. In the **Add Citrix Gateway Appliance** dialog, on the **General Settings** page, specify a **Display name** for the Citrix Gateway appliance 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 gateway. 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 or closest gateway to their location.
3. For **Citrix Gateway URL**, type the URL:port combination of the Citrix Gateway virtual server for your deployment. If a port is not specified, then the default `https://` port of 443 is used. It is not necessary to specify port 443 in the URL.

   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.
4. Select the **Usage or role** of the Citrix Gateway from the available options.
   - **Authentication and HDX routing:** The Citrix Gateway will be used for Authentication, as well as for routing any HDX sessions.
   - **Authentication Only:** The Citrix Gateway will be used for Authentication and not for any HDX session routings.
   - **HDX routing Only:** The Citrix Gateway will be used for HDX session routings and not for Authentication.
5. For all deployments where you are making resources provided by Citrix Virtual Apps and Desktops or XenApp 6.5 available in the store, on the **Secure Ticket Authority** page list the Secure Ticket Authority (STA) URLs for servers running the STA. Add URLs for multiple STAs to enable fault tolerance, listing the servers in order of priority to set the failover sequence.

   The STA is hosted on Citrix Virtual Apps and Desktops, or XenApp 6.5 servers and issues session tickets in response to connection requests. These session tickets form the basis of authentication and authorization for access to Citrix Virtual Apps and Desktops, or XenApp 6.5 resources. Use the correct STA URL (such as `HTTPS://` or `HTTP://`) depending on how your Delivery Controllers are configured. The STA URL must also be identical to the one configured within Citrix Gateway on your virtual server.

   In a Citrix Virtual Apps and Desktops *on-premises* environment, **Shared secret** lets you allow only approved StoreFront machines to communicate with Secure Ticket Authority (STA) by specifying a key. For information about key generation and configuration, see Manage security keys.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

In a Citrix Virtual Apps and Desktops *service* environment, **Shared secret** lets you allow only approved StoreFront machines to communicate with Citrix Cloud by specifying a key. For information about key generation, see Manage security keys.

6. Choose to set the Secure Ticket Authority to be load balanced. You can also specify the time interval after which the non-responding STAs are bypassed.

7. To ensure Citrix Virtual Apps and Desktops, or XenApp 6.5 keep disconnected sessions open while Citrix Workspace app attempts to reconnect automatically, select **Enable session reliability**.

8. If you configure multiple STAs and want to ensure that session reliability is always available, select **Request tickets from two STAs, where available**. Then StoreFront obtains session tickets from two different STAs and 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.

9. On the **Authentication Settings** page, type the **VServer IP address** (VIP) of the Citrix Gateway appliance.

   Use the private IP address for the Citrix Gateway virtual server rather than the public IP address that is NATed to the private IP address. Gateways are usually identified by StoreFront via their URLs. If you are using global server load balancing (GSLB), you must add the VIP to each gateway. This allows StoreFront to identify multiple gateways which all use the same URL (GSLB domain name) as distinct gateways. For example, three gateways may be configured for the store with the same URL such as `https://gslb.domain.com` but would each have unique VIPs configured such as 10.0.0.1, 10.0.0.2 and 10.0.0.3.

10. If you are adding an appliance running Citrix Gateway, select from the **Logon type** list the authentication method you configured on the appliance for Citrix Workspace app users.

    - If users are required to enter their Microsoft Active Directory domain credentials, select **Domain**.
    - If users are required to enter a tokencode obtained from a security token, select **Security token**.
    - If users are required to enter both their domain credentials and a tokencode obtained from a security token, select **Domain and security token**.
    - If users are required to enter a one-time password sent by text message, select **SMS authentication**.
    - If users are required to present a smart card and enter a PIN, select **Smart card**.

    If you configure smart card authentication with a secondary authentication method to which users can fall back if they experience any issues with their smart cards, select the secondary authentication method from the **Smart card fallback list**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

11. If you are configuring StoreFront for Citrix Gateway and want to use Smart Access, then you must type a **Callback URL**. StoreFront automatically appends the standard portion of the URL. Enter the internally accessible URL of the appliance. StoreFront contacts the Citrix Gateway authentication service to verify that requests received from Citrix Gateway originate from that appliance.

    When using GSLB, we recommend that you configure unique callback URLs for each of your GSLB gateways. StoreFront must be able to resolve each of the unique Callback URLs to the private VIPs configured for each of the GSLB gateway virtual servers. For example, `emeagateway.domain.com`, `usgateway.domain.com` and `apacgateway.domain.com` should resolve to the correct gateway VIP.

12. Click **Create** to add your Citrix Gateway appliance to the list in the **Remote Access Settings** dialog box.

    Information about the configuration of your Citrix Gateway appliances is saved to the .cr provisioning file for the store. This enables Citrix Workspace app to send the appropriate connection request when contacting appliances for the first time.

Remove a store

Use the Remove Store task to delete a store. When you remove a store, any associated Receiver for Web sites, and XenApp Services URLs are also deleted.

> **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.

Create an unauthenticated store

April 29, 2020

Use the Create Store task to configure additional unauthenticated stores to support access for unauthenticated (anonymous) users. You can create as many unauthenticated stores as you need; for example, you can create an unauthenticated store for a particular group of users or to group together a specific set of resources.

Remote access through a Citrix Gateway cannot be applied to unauthenticated stores.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

To create an unauthenticated store, you identify and configure communications with the servers providing the resources that you want to make available in the store.

> 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.

Add desktops and applications to the store

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. Select the Stores node in the left pane of the Citrix StoreFront management console and, in the Actions pane, click **Create Store**.
3. On the Store Name page, specify a name for your store, select **Allow only unauthenticated (anonymous) users to access this store**, and click **Next**.

   Store names appear in Citrix Receiver under users' accounts, so choose a name that gives users information about the content of the store.
4. On the **Delivery Controllers** page, list the infrastructure providing the resources that you want to make available in the store. Click **Add**.
5. In the **Add Delivery Controller** dialog box, specify a name that will help you to identify the deployment and indicate whether the resources that you want to make available in the store are provided by Citrix Virtual Apps and Desktops, or by XenApp 6.5. (Note XenApp 6.5 has reached End of Life (EOL) and is now covered by the Extended Support Program.) When assigning Delivery Controllers, ensure that you are only using those which support the anonymous apps feature. Configuring your unauthenticated store with Controllers that do not support this feature may lead to no anonymous apps being available from the store.

   To make desktops and applications provided by XenApp 6.5 farms available in the store, add the names of each individual server in the farm to the Servers list. Specify multiple servers to enable fault tolerance, listing the entries in order of priority to set the failover sequence. For Citrix Virtual Desktops sites, give details of Controllers. For XenApp 6.5 farms, list servers running the Citrix XML Service.
6. Select from the Transport type list 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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

servers.

- To send data over secure HTTP connections using Secure Sockets Layer (SSL) or Transport Layer Security (TLS), select **HTTPS**. If you select this option for Citrix Virtual Apps and Desktops servers, ensure that the Citrix XML Service is set to share its port with Microsoft Internet Information Services (IIS) and that IIS is configured to support HTTPS.

  > **Note:**
  >
  > If you are 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 connections using HTTP and 443 for HTTPS connections. In the case of Citrix Virtual Apps and Desktops servers, the specified port must be the port used by the Citrix XML Service.
8. Click **OK**. You can configure stores to provide resources from any mixture of Citrix Virtual Apps and Desktops deployments. Repeat Steps 4 to 9, as necessary, to list additional deployments providing resources for the store. When you have added all the required resources to the store, click **Create**.

Your unauthenticated store is now available for use. To enable user access to the new store, Citrix Workspace app must be configured with access details for the store. There are a number of ways in which you can provide these details to users to make the configuration process easier for them. For more information, see
User access options.

Alternatively, users can access the store through the Receiver for Web site, which enables users to access their desktops and applications through a web page. By default with unauthenticated stores, Receiver for Web displays the applications in a folder hierarchy that includes a breadcrumb path. The URL for users to access the Receiver for Web site for the new store is displayed when you create the store.

When you create a new store, the XenApp Services URL is enabled by default. Users of domain-joined desktop appliances and repurposed PCs running the Citrix Desktop Lock, along with users who have older Citrix clients that cannot be upgraded, can access stores directly using the XenApp Services URL for the store. The XenApp Services URL has the form `http[s]://serveraddress/Citrix/storename/PNAgent/config.xml`, where serveraddress is the FQDN of the server or load balancing environment for your StoreFront deployment and storename is the name you specified for the store in Step 3.

> Note:
>
> In StoreFront configurations where the *web.config* file has been configured with the parame-

© 1999–2022 Citrix Systems, Inc. All rights reserved.

> ter **LogoffAction="terminate"**, Citrix Receiver for Web sessions accessing this unauthenticated store will not terminate. Typically, the web.config file can be found at `C:\inetpub\wwwroot\Citrix\storename\`, where **storename** is the name specified for the store when it was created. To ensure these sessions terminate properly, the XenApp server being used by this store must have the Trust XML requests option enabled as shown in Configuring the Citrix XML Service Port and Trust.

Export store provisioning files for users

April 29, 2020

Use the **Export Multi-Store Provisioning File** and **Export Provisioning File** tasks to 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 obtain Citrix Workspace app provisioning files from Receiver for Web sites.

> 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. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile. Select the Stores node in the left pane of the Citrix StoreFront management console.
2. 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.
3. Click **Export** and **Save** the provisioning file with a .cr extension to a suitable location on your network.

Advertise and hide stores to users

April 29, 2020

Use the Hide Store task to prevent stores being 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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

must configure Citrix Workspace app with connection details for the store, either manually, using a setup URL, or with a provisioning file. To resume advertising a hidden store, use the Advertise Store task.

> 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. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. 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**.
3. On the **Advertise Store** page, select either **Advertise Store** or **Hide Store**.

Manage the resources made available in stores

April 29, 2020

Use the **Manage Delivery Controllers** task to add and remove from stores resources provided by Citrix Virtual Apps and Desktops, and to modify the details of the servers providing these 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.

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. Select the Stores node in the left pane of the Citrix StoreFront management console and, in the results pane, select a store. In the Actions pane, click **Manage Delivery Controllers**.
3. In the Manage Delivery Controllers dialog box:
   a) click **Add** to include desktops and applications from another Citrix Virtual Apps and Desktops deployment in the store.
   b) click **Edit** to modify the settings for a deployment.
   c) select an entry in the Delivery controllers list and click **Remove** to stop the resources provided by the deployment being available in the store.
4. In the Add Controller or Edit Controller dialog box, specify a **Display name** that will help you to identify the deployment.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

5. To make desktops and applications provided by Citrix Virtual Apps and Desktops available in the store, click **Add** to enter the name or IP address of a server. Depending on how the web.config file is configured, specifying multiple servers enables either load balancing or failover, as indicated in the dialog box. Load balancing is configured by default. If failover is configured, list the entries in order of priority to set the failover sequence. For Citrix Virtual Desktops sites, give details of Delivery Controllers. In the case of Citrix Virtual Apps farms, list servers running the Citrix XML Service. To modify the name or IP address of a server, select the entry in the Servers list and click **Edit**. Select an entry in the list and click **Remove** to stop StoreFront contacting the server to enumerate the resources available to the user.
6. We recommend that you select the option **Servers are load balanced** to ensure that load is distributed between all Delivery Controllers within the Citrix Virtual Apps and Desktops site. StoreFront selects a Delivery Controller at random from the Servers list during each launch and distributes the load across all servers in the Citrix Virtual Apps and Desktops site. If this option is not selected, the Servers list is treated as a failover list in priority order. In this case 100% of launches occur on the first Delivery Controller in the list. If that server goes offline, 100% of launches occur using the second in the list, and so on.
7. Select from the **Transport type** list 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 secure HTTP connections using Secure Sockets Layer (SSL) or Transport Layer Security (TLS), 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.
   - To send data over secure connections to Citrix Virtual Apps servers using the SSL Relay to perform host authentication and data encryption, select **SSL Relay**.

     > Note:
     > If you are using HTTPS or the SSL Relay to secure connections between StoreFront and your servers, ensure that the names you specify in Servers list match exactly (including the case) the names on the ertificates for those servers.
8. Specify the port for StoreFront to use for connections to the servers. The default port is 80 for connections using HTTP and the SSL Relay, and 443 for HTTPS connections. In the case of Citrix Virtual Apps and Desktops servers, the specified port must be the port used by the Citrix XML Service.
9. If you are using the SSL Relay to secure connections between StoreFront and Citrix Virtual Apps servers, specify the TCP port of the SSL Relay in the SSL Relay port box. The default port is 443. Ensure that all the servers running the SSL Relay are configured to monitor the same port.
10. Click **OK**. You can configure stores to provide resources from any mixture of Citrix Virtual Apps

© 1999–2022 Citrix Systems, Inc. All rights reserved.

and Desktops deployments. Repeat Steps 3 to 9, as necessary, to add or modify other deployments in the Delivery controllers list.

Manage remote access to stores through Citrix Gateway

February 12, 2021

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

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

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. 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**.
3. In the Configure Remote Access Settings dialog box, specify whether and how users connecting from public networks can access the store through Citrix Gateway.
   - To make the store unavailable to users on public networks, do not check **Enable remote access**. Only local users on the internal network will be able to access the store.
   - To enable remote access, check **Enable Remote Access**.
     - To make resources delivered through the store available through Citrix Gateway, select **No VPN tunnel**. Users log on using either ICAProxy or clientless VPN (cVPN) to Citrix Gateway and do not need to use the Citrix Gateway plug-in to establish a full VPN.
     - To make the store and other resources on the internal network available through a Secure Sockets Layer (SSL) virtual private network (VPN) tunnel, select **Full VPN tunnel**. Users require the Citrix Gateway plug-in to establish the VPN tunnel.

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

4. If you enabled remote access, select from the **Citrix Gateway appliances** list the deployments through which users can access the store. Any deployments you configured previously for this and other stores are available for selection in the list. If you want to add a further deployment to the list, click **Add**. Otherwise, continue to Step 14.

5. On the General Settings page, specify a **Display name** for the Citrix Gateway appliance 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 gateway. 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 or closest gateway to their location.

6. For **Citrix Gateway URL**, type the URL:port combination of the Citrix Gateway virtual server for your deployment. If a port is not specified, then the default `https://` port of 443 is used. It is not necessary to specify port 443 in the URL.

7. Select the usage of the Citrix Gateway from the available options.

   - **Authentication and HDX routing:** The Citrix Gateway will be used for Authentication, as well as for routing any HDX sessions.
   - **Authentication Only:** The Citrix Gateway will be used for Authentication and not for any HDX session routings.
   - **HDX routing Only:** The Citrix Gateway will be used for HDX session routings and not for Authentication.

8. For all deployments where you are making resources provided by Citrix Virtual Apps and Desktops or XenApp 6.5 available in the store, on the **Secure Ticket Authority** page list the Secure Ticket Authority (STA) URLs for servers running the STA. Add URLs for multiple STAs to enable fault tolerance, listing the servers in order of priority to set the failover sequence.

   The STA is hosted on Citrix Virtual Apps and Desktops, or XenApp 6.5 servers and issues session tickets in response to connection requests. These session tickets form the basis of authentication and authorization for access to Citrix Virtual Apps and Desktops, or XenApp 6.5 resources. Use the correct STA URL (such as `HTTPS://` or `HTTP://`) depending on how your Delivery Controllers are configured. The STA URL must also be identical to the one configured within Citrix Gateway on your virtual server.

   In a Citrix Virtual Apps and Desktops *on-premises* environment, **Shared secret** lets you allow only approved StoreFront machines to communicate with Secure Ticket Authority (STA) by specifying a key. For information about key generation and configuration, see Manage security keys.

   In a Citrix Virtual Apps and Desktops *service* environment, **Shared secret** lets you allow only approved StoreFront machines to communicate with Citrix Cloud by specifying a key. For information about key generation, see Manage security keys.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

9. Choose to set the Secure Ticket Authority to be load balanced. You can also specify the time interval after which the non-responding STAs are bypassed.

10. To ensure Citrix Virtual Apps and Desktops, or XenApp 6.5 keep disconnected sessions open while Citrix Workspace app attempts to reconnect automatically, select **Enable session reliability**.

11. If you configure multiple STAs and want to ensure that session reliability is always available, select **Request tickets from two STAs, where available**. Then StoreFront obtains session tickets from two different STAs and 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.

12. On the **Authentication Settings** page, type the **VServer IP address** (VIP) of the Citrix Gateway appliance.

    Use the private IP address for the Citrix Gateway virtual server rather than the public IP address that is NATed to the private IP address. Gateways are usually identified by StoreFront via their URLs. If you are using global server load balancing (GSLB), you must add the VIP to each gateway. This allows StoreFront to identify multiple gateways which all use the same URL (GSLB domain name) as distinct gateways. For example, three gateways may be configured for the store with the same URL such as `https://gslb.domain.com` but would each have unique VIPs configured such as 10.0.0.1, 10.0.0.2 and 10.0.0.3.

13. If you are adding an appliance running Citrix Gateway, select from the **Logon type** list the authentication method you configured on the appliance for Citrix Workspace app users.

    - If users are required to enter their Microsoft Active Directory domain credentials, select **Domain**.
    - If users are required to enter a tokencode obtained from a security token, select **Security token**.
    - If users are required to enter both their domain credentials and a tokencode obtained from a security token, select **Domain and security token**.
    - If users are required to enter a one-time password sent by text message, select **SMS authentication**.
    - If users are required to present a smart card and enter a PIN, select **Smart card**.

    If you configure smart card authentication with a secondary authentication method to which users can fall back if they experience any issues with their smart cards, select the secondary authentication method from the **Smart card fallback list**.

14. If you are configuring StoreFront for Citrix Gateway and want to use Smart Access, then you must type a **Callback URL**. StoreFront automatically appends the standard portion of the URL. Enter the internally accessible URL of the appliance. StoreFront contacts the Citrix Gateway

© 1999–2022 Citrix Systems, Inc. All rights reserved.

authentication service to verify that requests received from Citrix Gateway originate from that appliance.

When using GSLB, we recommend that you configure unique callback URLs for each of your GSLB gateways. StoreFront must be able to resolve each of the unique Callback URLs to the private VIPs configured for each of the GSLB gateway virtual servers. For example, `emeagateway.domain.com`, `usgateway.domain.com` and `apacgateway.domain.com` should resolve to the correct gateway VIP.

15. Click **Create** to add your Citrix Gateway appliance to the list in the **Remote Access Settings** dialog box.

    Information about the configuration of your Citrix Gateway appliances is saved to the .cr provisioning file for the store. This enables Citrix Workspace app to send the appropriate connection request when contacting appliances for the first time.

16. Repeat Steps 4 to 13, as necessary, to add more Citrix Gateway appliances to the Citrix Gateway appliances list. 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.

17. Click **OK** to save the configuation and close the Configure Remote Access dialog.

Certificate Revocation List (CRL) checking

October 22, 2020

Introduction

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

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

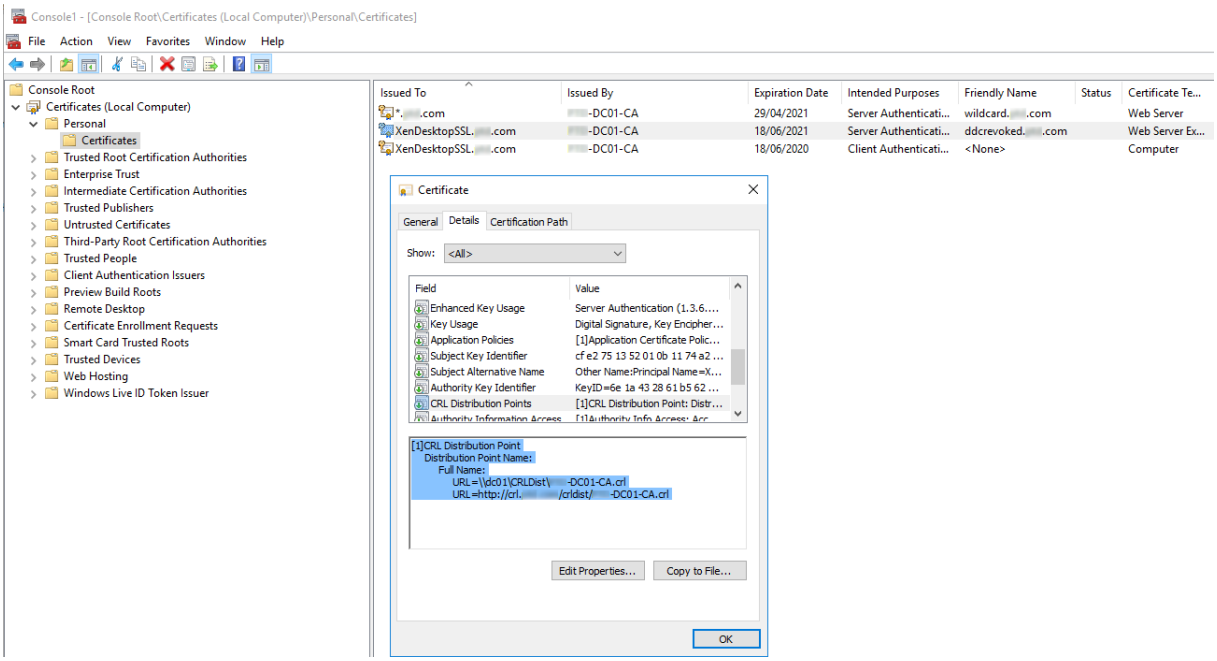
> **Note:**
>
> This topic is only relevant when HTTPS connections between StoreFront and Citrix Virtual Apps and Desktops delivery controllers are used. HTTP connections to delivery controllers do not require a certificate, so the -CertRevocationPolicy setting for the Store, described here, has no effect.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

> 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

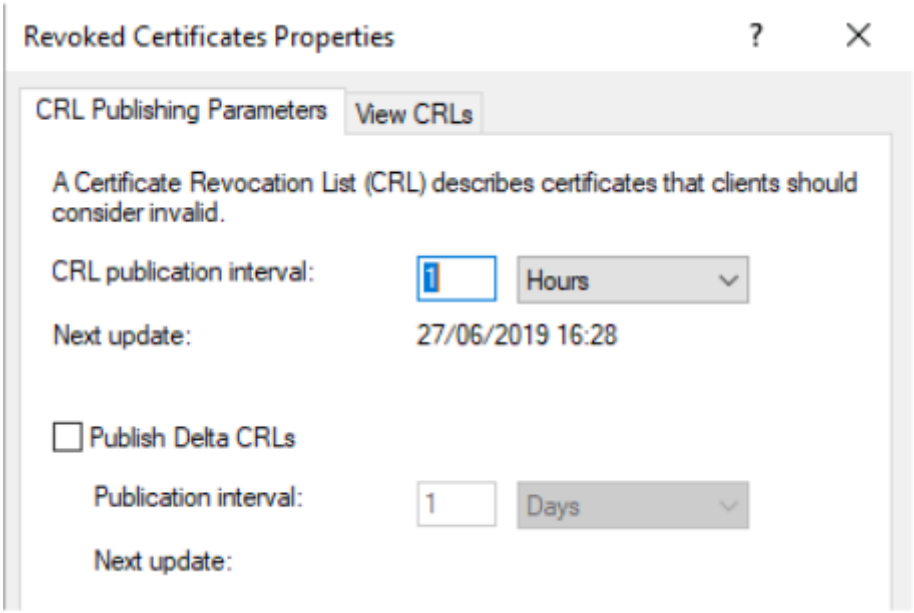
StoreFront does not enumerate resources from Citrix Virtual Apps and Desktops delivery controllers which are using revoked certificates whose serial numbers are listed in the published CRL. To detect which certificates have been revoked, StoreFront must be able to access the published CRL using one of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

© 1999–2022 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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

Certificate revocation policy settings

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

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

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

Configure a store for certificate revocation checking

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

```
$SiteID = 1
$StoreVirtualPath = "/Citrix/Store"
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
3 $StoreObject = Get-STFStoreService -SiteId $SiteID -VirtualPath
4 $StoreVirtualPath
5 Set-STFStoreFarmConfiguration -StoreService $StoreObject -
     CertRevocationPolicy
6 ”MustCheck”
```

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

```
1 (Get-STFStoreFarmConfiguration -StoreService $StoreObject).
     CertRevocationPolicy
```

Using locally imported CRLs on the StoreFront server

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

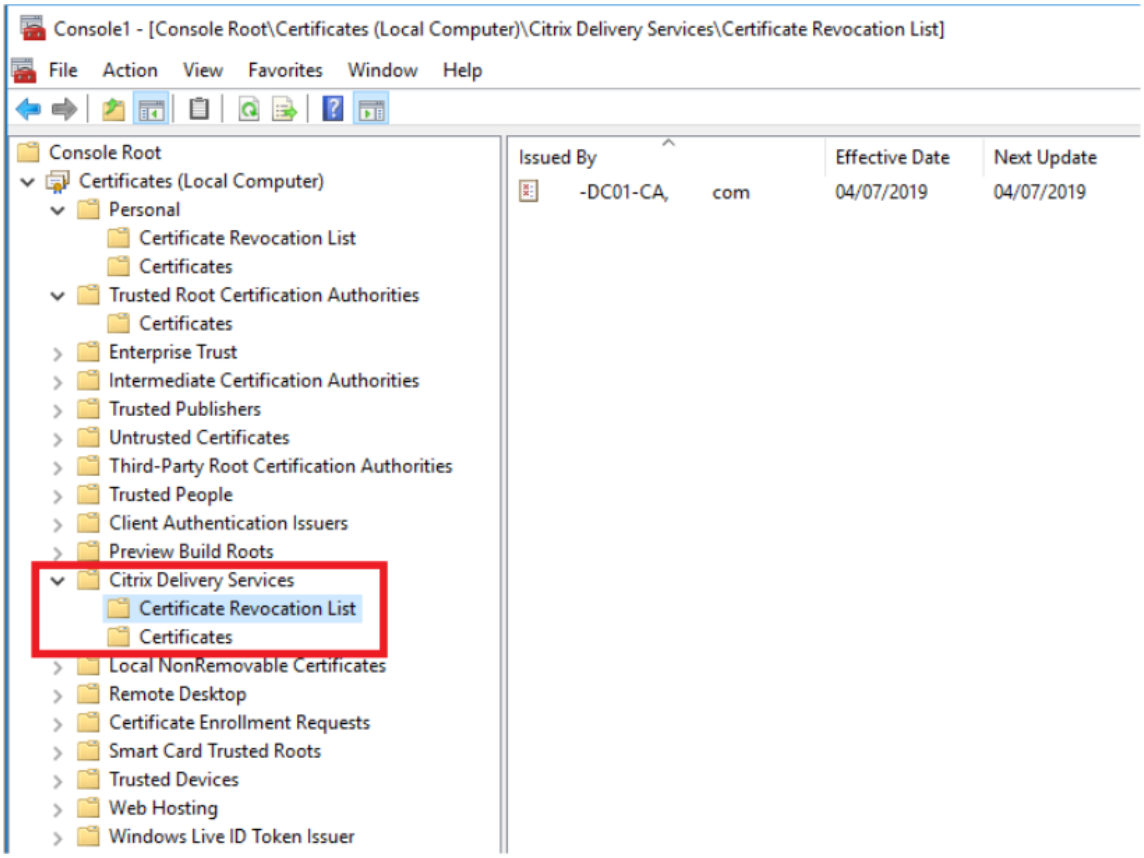
- They are difficult to manage and update in large enterprise deployments, where multiple StoreFront server groups may be involved.
- Manually updating CRLs on every StoreFront server, every time a certificate is revoked, is much less efficient than using CDP extensions and published CRLs on the entire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

© 1999–2022 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.
```

© 1999–2022 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 behaviour is desirable as active directory users should not be able to sign in to StoreFront if the certificate on the Citrix Virtual Apps and Desktops delivery controller, responsible for authenticating them, has been revoked.

To delegate user authentication to delivery controllers

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

Configure an XML authentication service for certificate revocation checking

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

> **Note:**
>
> StoreFront supports two models for mapping stores to an authentication service. The recommended approach is a one-to-one mapping between store and Authentication Service. In this case you must perform the steps in this section on all stores and their respective authentication services.
>
> Make sure that the certificate revocation mode is set to the same value for both the store and the authentication service. Alternatively, if the authentication configuration is identical for all stores, multiple stores can be configured to share a single authentication service.

The authentication service PowerShell cmdlets have no equivalent of **Set-STFStoreFarmConfiguration**, so a slightly different PowerShell approach is required. Use the same Certificate revocation policy settings describe in the earlier section.

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

© 1999–2022 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:

- On the StoreFront server type **Run**.
- Type **eventvwr** then press enter.
- In Applications and Services look for Citrix Delivery Services events.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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.ExplicitAuthenticationFailure,
Citrix.DeliveryServicesClients.Authentication, Version=3.20.0.0,
Culture=neutral, PublicKeyToken=null

General Authentication Failure

ExplicitResult.State: 5

AuthenticationControllerRequestUrl:
https://storefront.example.com/Citrix/StoreWeb/ExplicitAuth/LoginAttempt

ActionType: LoginAttempt

at
Citrix.Web.AuthControllers.Controllers.ExplicitAuthController.GetExplicitAuthResult(ActionType
type, Dictionary`2 postParams)
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Configure two StoreFront stores to share a common subscription datastore

April 29, 2020

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

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

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

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

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

The subscription data for each Store is located in:

```
C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore
\1__Citrix_<StoreName>
```

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

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

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

```
<subscriptionsStoreClient enabled="true">
<clientEndpoint uri="net.pipe://localhost/Citrix/Subscriptions/1
    __Citrix_Internal" authenticationMode="windows" transferMode="
    Streamed">
<clientCertificate thumbprint="0" />
</clientEndpoint>
</subscriptionsStoreClient>
<!--NeedCopy-->
```

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

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

Manage subscription data for a store

June 8, 2021

Manage subscription data 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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

> backup of your existing subscription data before making changes so that rollback to a previous state is possible.

Purge subscription data

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

1. Stop the Citrix Subscriptions Store service on the StoreFront server. If the Citrix Subscriptions Store service is running, it is not possible to delete subscription data for any of your stores.
2. Locate the subscription store folder on the StoreFront server: `C:\Windows\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore\1__Citrix_<StoreName>`
3. Delete the contents of the subscription store folder, but do not delete the folder itself.
4. Restart the Citrix Subscriptions Store service on the StoreFront server.

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

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

```
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

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

        Stop-Service -displayname $SubsService

        Remove-Item $SubsPath -Force -Verbose

        Start-Service -displayname $SubsService

        Get-Service -displayname $SubsService
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
 }


    Remove-SubscriptionData -Store "YourStore"
<!--NeedCopy-->
```

Export subscription data

You can back up Store subscription data by exporting it as a tab-separated .txt file using the following PowerShell cmdlet.

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

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

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

Restore subscription data

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

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

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

For more information on Restore-STFStoreSubscriptions, see https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Restore-STFStoreSubscriptions/

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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. Export the existing subscription data from any of the three servers.
2. Stop the Subscriptions Store service on servers StoreFrontB and C. This action prevents the servers from sending or receiving subscription data during the update of StoreFrontA.
3. Purge the subscription data from servers StoreFrontB and C. This prevents mismatch of the restored subscription data.
4. Restore the data on StoreFrontA using the **Restore-STFStoreSubscriptions** cmdlet. It is not necessary to stop the Subscriptions Store service, or to purge the subscription data on StoreFrontA (it is overwritten during the restore operation).
5. Restart the Subscriptions Store service on servers StoreFrontB and StoreFrontC. The servers can then receive a copy of the data from StoreFrontA.
6. Wait for synchronization to occur between all servers. The time required depends on the number of records that exist on StoreFrontA. If all servers are on a local network connection, synchronization normally occurs quickly. Synchronization of subscriptions across a WAN connection may take longer.
7. Export the data from StoreFrontB and C to confirm that the synchronization has completed, or view the Store Subscription counters.

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>"

```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

For more information on Import-STFStoreSubscriptions, see https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Import-STFStoreSubscriptions/

Subscription data file details

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

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

where:

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

Example

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Size of subscription data on the StoreFront server disk

Subscription Datastore Size	
No of Records	Size MB
0	6.02
1000	7.02
10000	40.00
100000	219.00
200000	358.00
500000	784.00
800000	1213.02
1000000	1497.15
1300000	1919.15
1500000	2205.15
1700000	2487.15
2000000	2915.15

Size of import and export .txt files

Subscriptions Import/Export.txt	
No of Records	Size MB
0	0.00
1000	0.13
10000	1.30
100000	12.80
200000	25.60
500000	64.10
800000	102.00
1000000	128.00
1300000	166.00
1500000	192.00
1700000	218.00
2000000	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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

View the Subscription Counters using PowerShell

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

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

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

Get-Counter -Counter "\Citrix Subscription Store Synchronization\Number
     Subscriptions Transferred"
<!--NeedCopy-->
```

Store subscription data using Microsoft SQL Server

November 18, 2020

> **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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Failures to connect to the SQL server instance used by StoreFront to store the subscription data due to network outages do not render the StoreFront deployment unusable. Outages only result in a temporarily degraded user experience; users cannot add, remove, or view favorite resources until the connection to SQL server is restored. Resources can still be enumerated and launched during the outage. The expected behavior is the same as if the Citrix Subscription Store service were to stop while using ESENT.
>
> **Tip:**
>
> Resources configured with KEYWORDS:Auto or KEYWORDS:Mandatory behave the same way when using both ESENT or SQL. New SQL subscription records are created automatically when a user first logs on if either KEYWORD is included in the user's resources.

Advantages of ESENT and SQL server

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

ESENT	SQL
SQL unnecessary when subscription management is not needed. If the subscription data will never need updating, ESENT is likely to meet customer needs.	Single copy of the subscription data shared by all members of the server group so less chance of data differences between servers or data syncing issues.

Disadvantages of ESENT and SQL server

ESENT	SQL
No easy means to manage subscription data easily and in a granular manner. Requires subscription manipulations to be done in exported .txt files. The whole subscription database must be exported and re imported. Potentially thousands of records may need to be changed using find and replace techniques, which is labor intensive and potentially error prone.	Requires basic SQL expertise and infrastructure. Can require an SQL license to be purchased, which increases total cost of ownership of StoreFront deployment. Although a Citrix Virtual Apps and Desktops database instance can also be shared with StoreFront to reduce costs.
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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

> database if you want to support user subscriptions. The method of storing the subscription data is set at the store level within StoreFront.

Citrix recommended all store databases reside on the same Microsoft SQL server instance to reduce management complexity and reduce the scope for misconfiguration.

Multiple stores can share the same database, provided they are all configured to use the same identical connection string. It does not matter if they use different delivery controllers. The disadvantage of multiple stores sharing a database is that there is no way to tell which store each subscription record corresponds to.

A combination of the two data storage methods is technically possible on a single StoreFront deployment with multiple stores. It is possible to configure one store to use ESENT and another to use SQL. This is not recommended due to increased management complexity and the scope for misconfiguration.

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

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

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

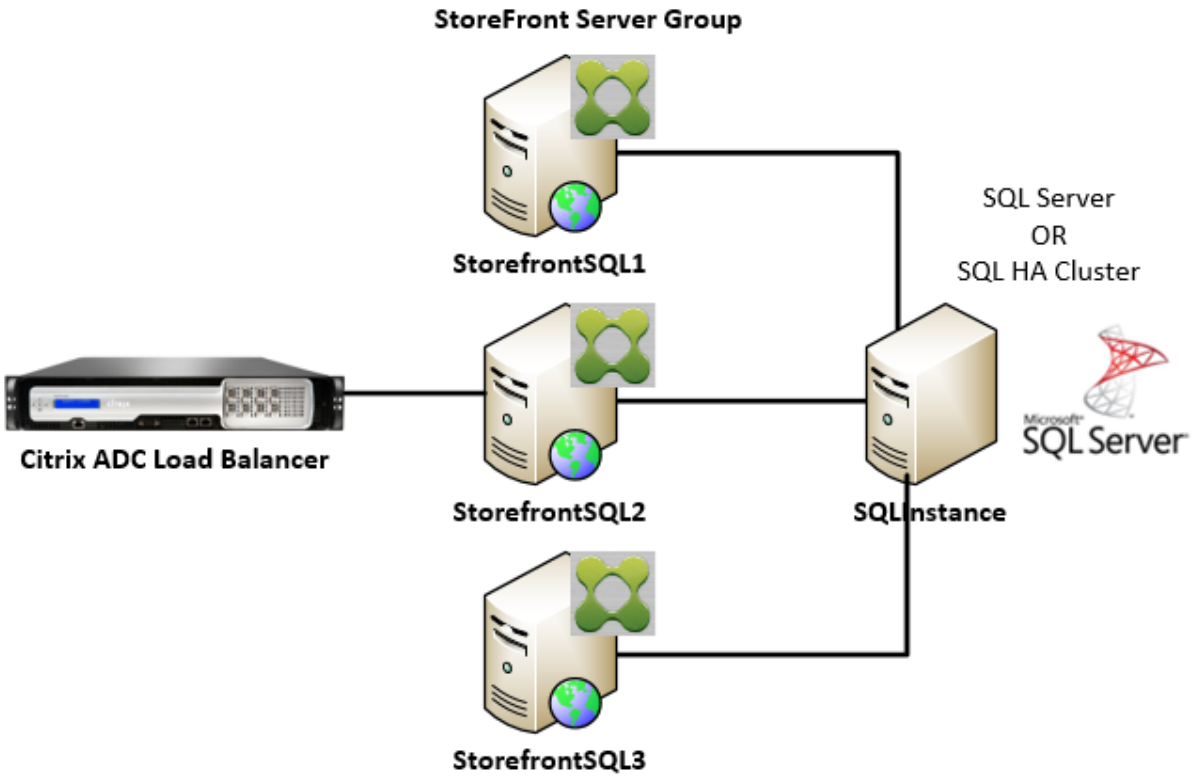
Scenario 2: Single StoreFront Server and a local Microsoft SQL server instance installed

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

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

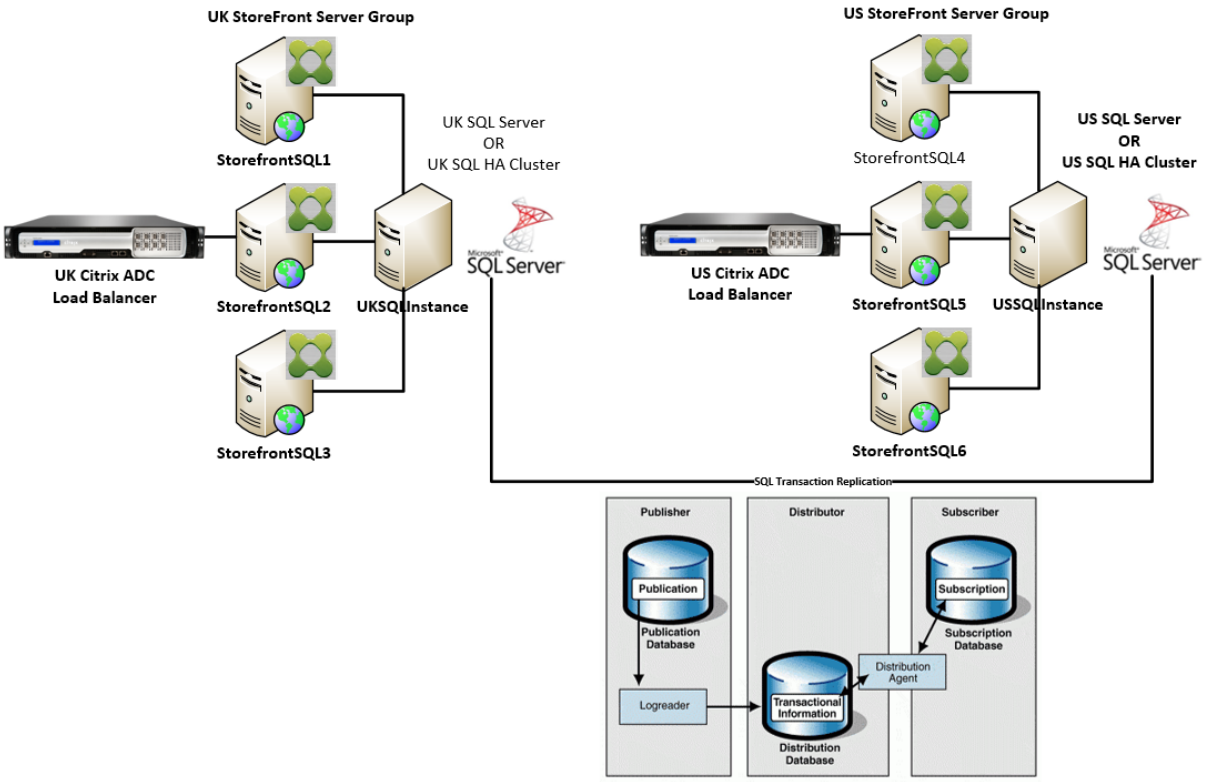


Scenario 4: Multiple StoreFront server groups and a dedicated Microsoft SQL server instance in each data center per server group

> **Note:**
>
> This is an advanced configuration. Only attempt it if you are an experienced SQL server administrator familiar with transaction replication, and you have the necessary skills to deploy it successfully.

This is the same as scenario 3, but extends it to situations where multiple StoreFront server groups are required in different remote data centers. Citrix Administrators may choose to synchronize subscription data between different server groups in the same or different data centers. Each server group in the data center connects to its own dedicated Microsoft SQL server instance for redundancy, failover, and performance. This scenario requires considerable extra Microsoft SQL server configuration and infrastructure. It relies entirely on Microsoft SQL technology to replicate the subscription data and its SQL transactions.

© 1999–2022 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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- **Create-ImportSubscriptionDataSP.sql** – creates a stored procedure to import the data transformed by Transform-SubscriptionDataForStore.ps1. Run this script once on the SQL server after you have created the database schema using Create-StoreSubscriptionsDB-2016.sql.

Configure the StoreFront server's local security group on the SQL Server

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

Create a local security group called `<SQLServer>\StoreFrontServers` on the Microsoft SQL server, and add the virtual accounts for the `IIS APPPOOL\DefaultAppPool` and `IIS APPPOOL\Citrix Receiver for Web` to allow the locally installed StoreFront to read and write to SQL. This security group is referenced in the .SQL script that creates the store subscription database schema, so ensure that the group name matches.

You can download the script Add-LocalAppPoolAccounts.ps1 to help you.

Install StoreFront before running the *Add-LocalAppPoolAccounts.ps1* script. The script depends on the ability to locate the `IIS APPPOOL\Citrix Receiver for Web` virtual IIS account, which does not exist until StoreFront has been installed and configured. `IIS APPPOOL\DefaultAppPool` is created automatically by installing the IIS webserver role.

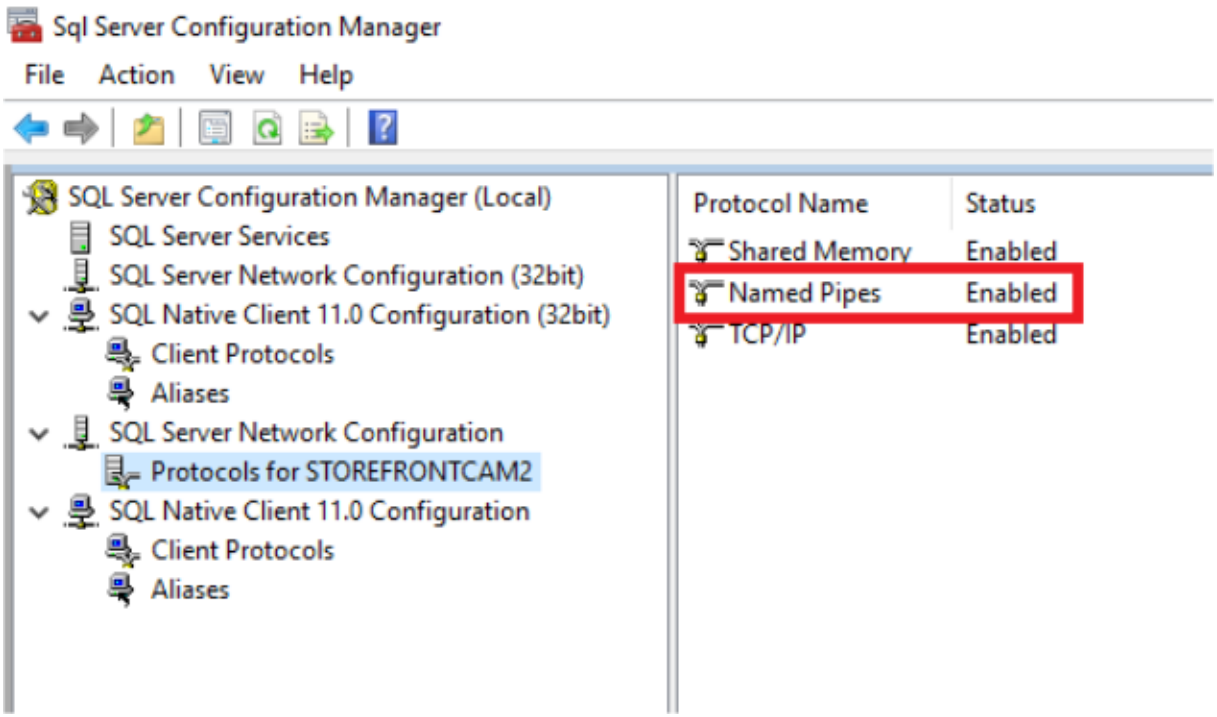
```
# Create Local Group for StoreFront servers on DB Server
$LocalGroupName = "StoreFrontServers"
$Description = "Contains StoreFront Server Machine Accounts or
    StoreFront AppPool Virtual Accounts"

# Check whether the Local Group Exists
if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))
{

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

else
{

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

# Create Local User Group
$Computer = [ADSI]"WinNT://$env:ComputerName,Computer"
$LocalGroup = $Computer.Create("group",$LocalGroupName)
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
$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)

# 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"
<!--NeedCopy-->
```

Enable named pipes within your local SQL instance using SQL server configuration manager. Named pipes are required for interprocess communication between StoreFront and SQL server.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



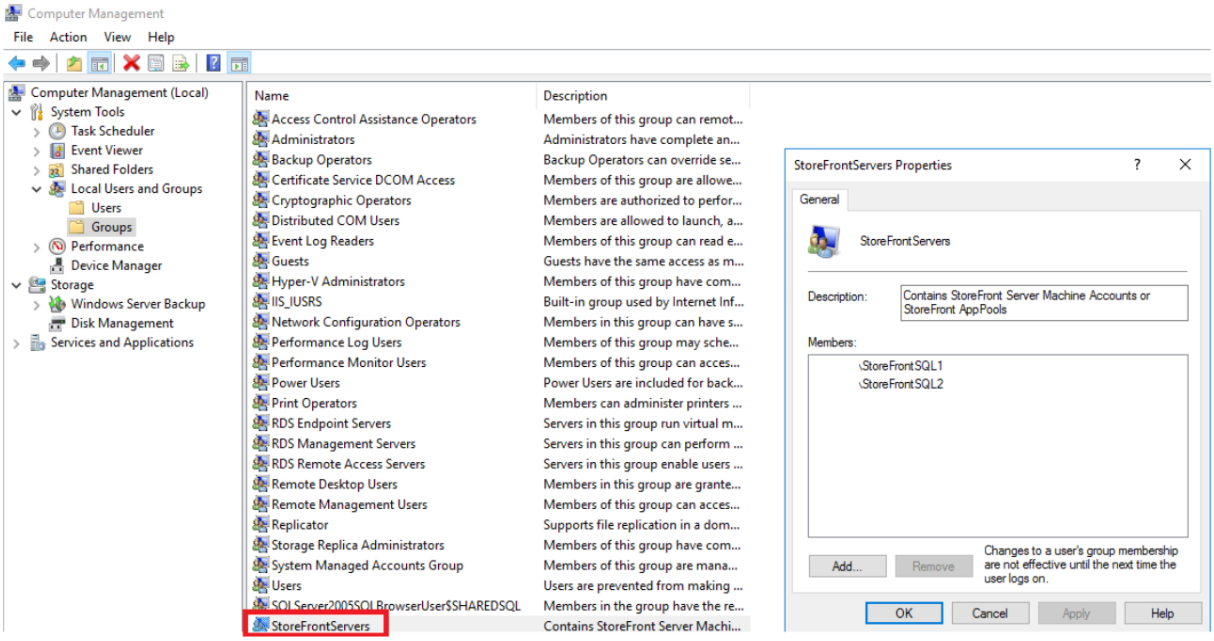
Ensure the Windows firewall rules are correctly configured to allow SQL server connections using either a specific port or dynamic ports. Refer to Microsoft documentation for how to do this in your environment.

> **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.

© 1999–2022 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"

# Check whether the Local Security Group already exists
if ([ADSI]::Exists("WinNT://$env:ComputerName/$LocalGroupName"))
{

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

```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

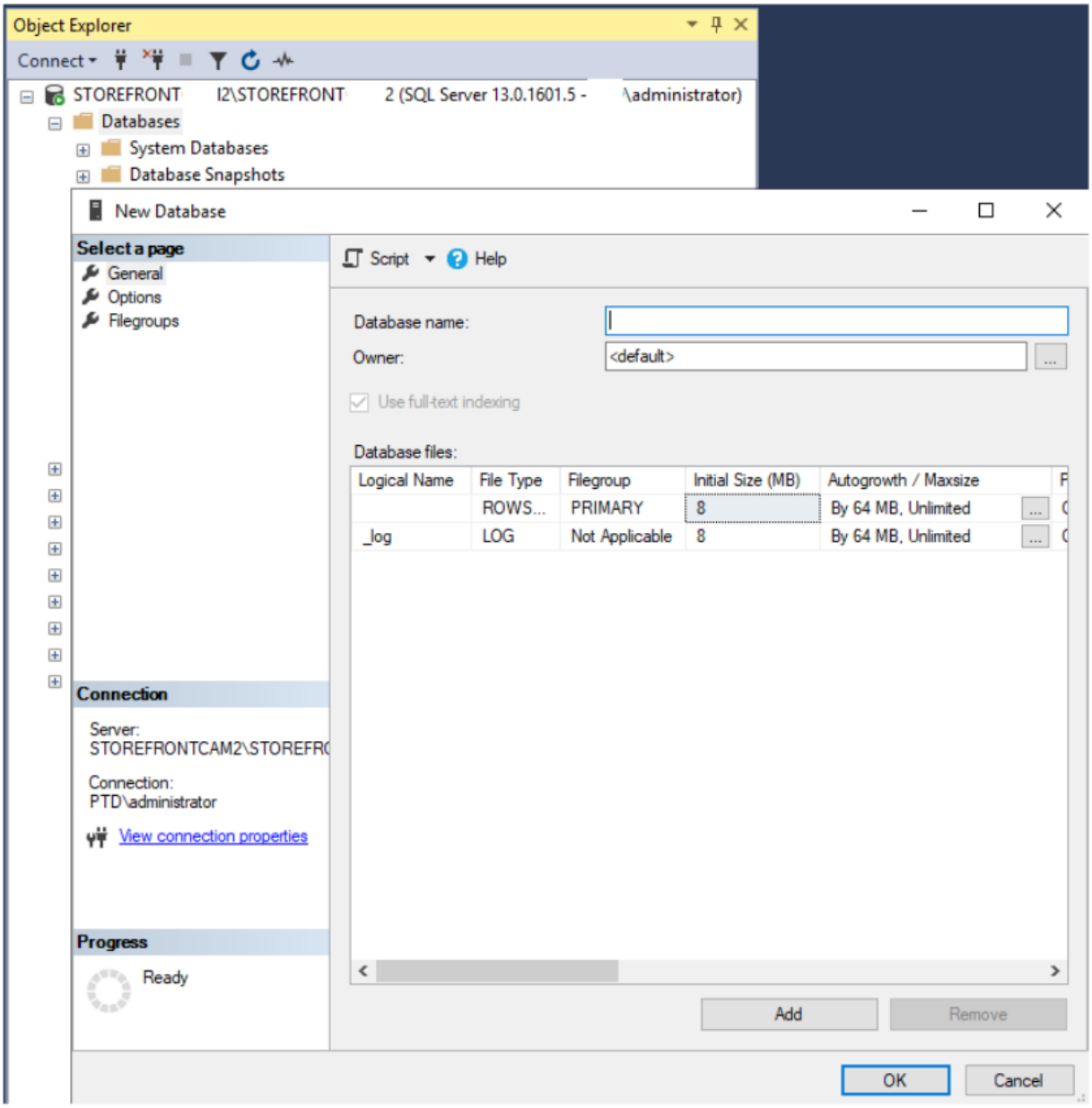
```
else
{

    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)
{

    $Group = [ADSI]"WinNT://$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")
<!--NeedCopy-->
```

Configure the subscription database schema within Microsoft SQL Server for each store

Create a named instance on your Microsoft SQL server for use by StoreFront. Set the path within the .SQL script to correspond to where your version of SQL is installed, or its database files are stored. The example script Create-StoreSubscriptionsDB-2016.sql uses SQL Server 2016 Enterprise.

Create an empty database using SQL Server Management Studio (SSMS) by right clicking **Databases** then selecting **New Database**.

© 1999–2022 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
  ```

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

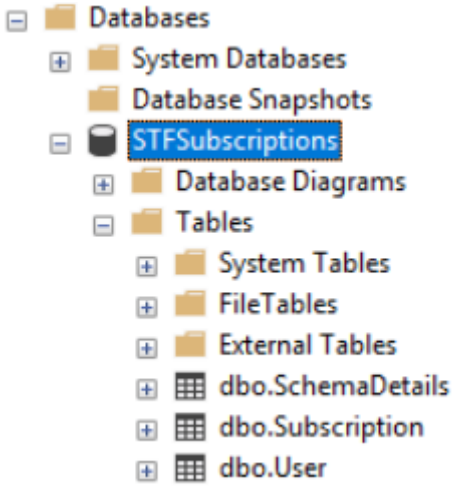
© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
STFSubscriptions.ldf
```

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

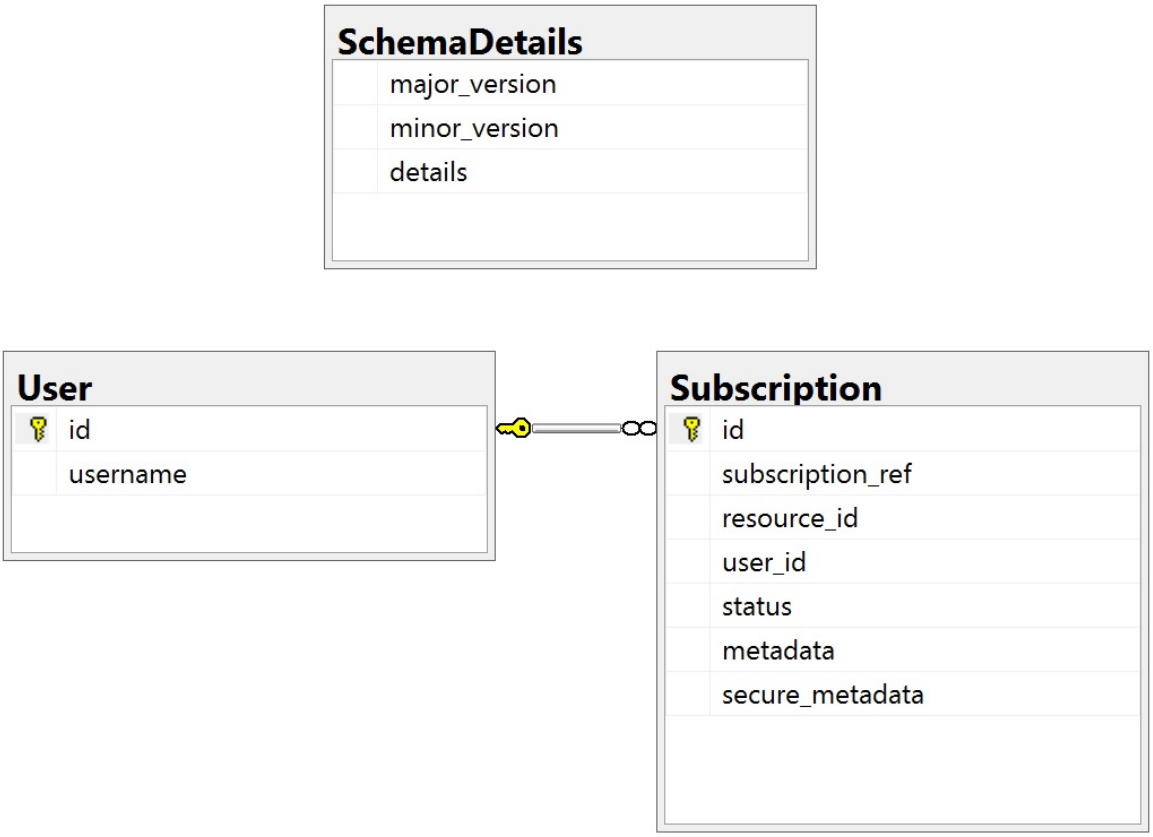
```
CREATE LOGIN [SQL2016\StoreFrontServers] FROM WINDOWS;

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:

© 1999–2022 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:

```
$SiteID = 1
$StoreVirtualPath = "/Citrix/Store1"
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```

# 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
<!--NeedCopy-->
```

Scenarios 2, 3 and 4

Open the PowerShell ISE and select **Run as Administrator**.

Specify the store you want to set a connection string for using **$StoreVirtualPath**.

```
$SiteID = 1
$VirtualPath= "/Citrix/Store1"
$DBName = "Store1"
$DBServer = "SQL2016Ent"
$DBLocalServer = "localhost"
$DBInstance = "StoreFrontInstance"
$SQLPort = "2703"
<!--NeedCopy-->
```

Configure the `$ConnectionString` variable according to the database configuration you are using:

```
# For a remote database instance use the following:
$ConnectionString = "Server=$DBServer\$DBInstance;Database=$DBName;
    Trusted_Connection=True;"
<!--NeedCopy-->
```

```
# For a remote database instance using a custom SQL TCP port number,
    use the following,
# taking care to use a comma `,` not a semi colon `;`:
$ConnectionString = "Server=$DBServer\$DBInstance,$SQLPort;Database=
    $DBName;Trusted_Connection=True;"
<!--NeedCopy-->
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
# For a locally installed database instance, use the following:
$ConnectionString = "$DBLocalServer\$SQLInstance;Database=$DBName;
    Trusted_Connection=True;"

<!--NeedCopy-->
```

Set the SQL DB connection string used by StoreFront to connect to the subscriptions database:

```
$StoreObject = Get-STFStoreService -SiteID $SiteID -VirtualPath
    $VirtualPath
Set-STFStoreSubscriptionsDatabase -StoreService $StoreObject -
    ConnectionString $ConnectionString
Get-STFStoreSubscriptionsDatabase -StoreService $StoreObject
<!--NeedCopy-->
```

Repeat the process for every store in your deployment if you want to configure them all to use an SQL connection string.

Migrate existing data from ESENT into Microsoft SQL Server

To migrate your existing ESENT data to SQL a two-step data transformation process is required. Two scripts are provided to assist you in performing this one-time operation. If the connection string in StoreFront and the SQL instance are correctly configured, then all new subscriptions are created automatically within SQL in the correct format. After migration, the historic ESENT subscription data is transformed into an SQL format and users can also see their previously subscribed resources.

Example: four SQL subscriptions for the same domain user

Results | Messages

	id	subscription_ref	resource_id	user_id	status	metadata	secure_metadata
1	1	D0D2E64B94B997D5B5DCD90F92A7005	XenDesktopSSL.Notepad++ TLS	1	1	<SubscriptionProperties xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><property key="dazzle:position"><value>1</value></property></SubscriptionProperties>	NULL
2	2	2A3C21FE0F14ECF4D9CFB83CC8118CE7	XenDesktopSSL.Windows Media Player TLS	1	1	<SubscriptionProperties xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><property key="dazzle:position"><value>2</value></property></SubscriptionProperties>	NULL
3	3	425BEA6F0810286A6C600059EED9DEA23	XenDesktopSSL.Calculator TLS	1	1	<SubscriptionProperties xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><property key="dazzle:position"><value>3</value></property><property key="position"><value>3</value></property></SubscriptionProperties>	NULL
4	4	9632ACE3170D118E1EF79C5A2692299CA	XenDesktopSSL.IE11 TLS	1	1	<SubscriptionProperties xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"><property key="dazzle:position"><value>4</value></property><property key="position"><value>4</value></property></SubscriptionProperties>	NULL

	id	username
1	1	S-1-5-21- 6059

Step 1 Use the Transform-SubscriptionDataForStore.ps1 script to convert the ESENT data into an SQL friendly format for bulk import

Log into the StoreFront server that you want to transform ESENT data from.

Any member of a server group is suitable provided they all contain the same number of subscription records.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Open the PowerShell ISE and select **Run as Administrator**.

Run the script Transform-SubscriptionDataForStore.ps1 which exports a `<StoreName>.txt` file from the ESENT database to the current user's desktop.

The PowerShell script provides verbose feedback on each subscription row that is processed to aid debugging and help you assess the success of the operation. This may take a long time to process.

The transformed data is written out to `<StoreName>SQL.txt` on the current user's desktop after the script has completed. The script summarizes the number of unique user records and the total number of subscriptions processed.

Repeat this process for every store you want to migrate to SQL server.

Step 2 Use a T-SQL stored procedure to bulk SQL import the transformed data

Each store's data must be imported one store at a time.

Copy the `<StoreName>SQL.txt` file created in Step 1 from the StoreFront server's desktop to `C:\` on the Microsoft SQL server and rename it to SubscriptionsSQL.txt.

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

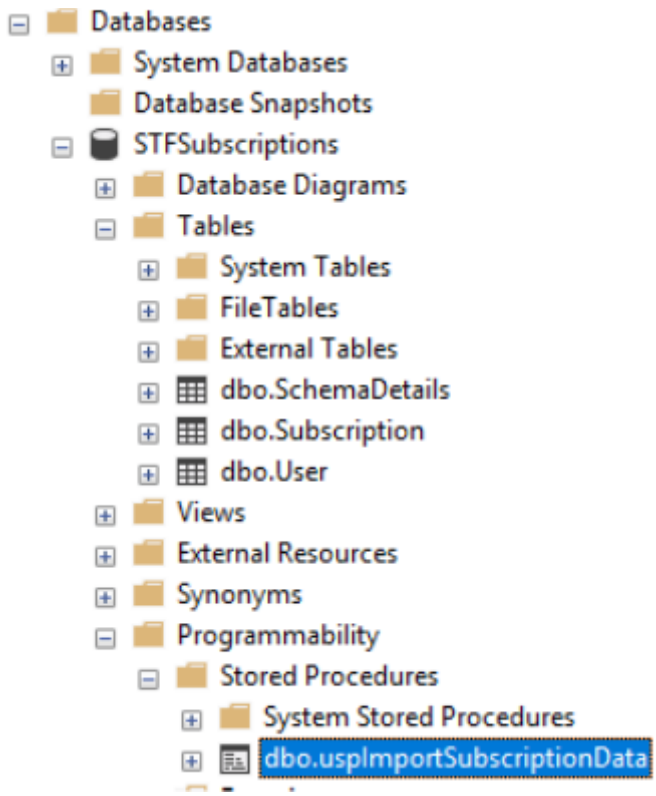
Before executing *Create-ImportSubscriptionDataSP.sql*, change `USE [STFSubscriptions]` to match the database under which you want to create the Stored Procedure.

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

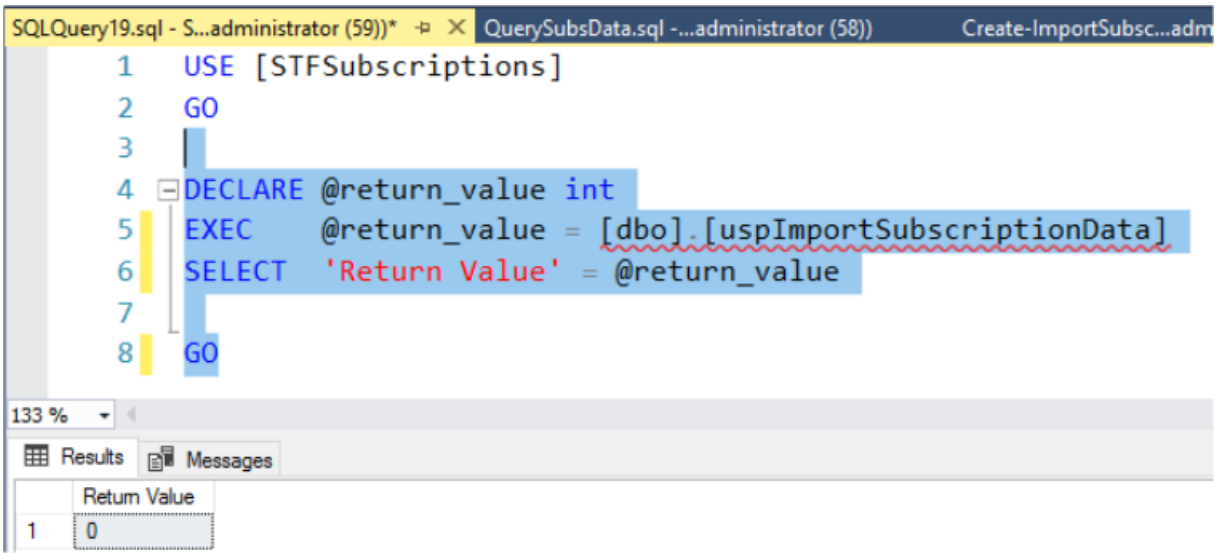
After successful creation of the Stored Procedure the following message is shown in the SQL console, and the ImportSubscriptionDataSP Stored Procedure is added to the database:

```
Commands completed successfully.
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.



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 re-

© 1999–2022 Citrix Systems, Inc. All rights reserved.

ported from SQL by

```
SELECT COUNT(*) AS TotalSubscriptions
FROM [Subscription]
<!--NeedCopy-->
```

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]
<!--NeedCopy-->
```

If the transformation script shows 100 unique users and 1000 total subscription records, then SQL should show the same two numbers after successful migration.

Log in to StoreFront to check whether existing users can see their subscription data. Existing subscription records are updated in SQL when users subscribe or unsubscribe their resources. New users and subscription records are also created in SQL.

Step 3 Run T-SQL queries on your imported data

> **Note:**
>
> All Delivery Controller names are case sensitive and must exactly match the case and name used within StoreFront.

```
-- Get all SQL subscription records
Use [STFSubscriptions]
SELECT * FROM [Subscription]
SELECT * FROM [User]
<!--NeedCopy-->
```

```
-- Get all subscription records for a particular user SID
Use [STFSubscriptions]
SELECT * FROM [Subscription]
INNER JOIN [User]
ON [Subscription].[user_id] = [User].[id]
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
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'
<!--NeedCopy-->
```

```
-- 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.%'

-- Get all subscription records for a particular application
Use [STFSubscriptions]
SELECT * FROM [Subscription]
WHERE [resource_id] = ' DeliveryController.Application'
<!--NeedCopy-->
```

Update or delete existing subscription records using T-SQL

> **DISCLAIMER:**
>
> All example SQL update and delete statements are used entirely at your own risk. Citrix is not responsible for any loss or accidental alteration of your subscription data by incorrect use of the provided examples. The following T-SQL statements are provided as a guide to enable simple updates to be performed. Back up all subscription data in SQL database full backups before attempting to update your subscriptions or remove obsolete records. Failure to perform the necessary backups may result in data loss or corruption. Before executing your own T-SQL UPDATE or DELETE statements against the production database, test them on dummy data or on a redundant copy of the production data away from the live production database.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

> **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.%'

-- OR for aggregated resources use the name of the aggregation group
Use [STFSubscriptions]
UPDATE [Subscription]
SET [resource_id] = REPLACE(resource_id,'OldDeliveryController.','
    DefaultAggregationGroup.')
WHERE [resource_id] LIKE 'OldDeliveryController.%'
<!--NeedCopy-->
```

```
-- 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'

-- 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'
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

```
-- Delete all subscription records for a particular user SID
Use [STFSubscriptions]
DELETE FROM [Subscription]
INNER JOIN [User]
ON [Subscription].[user_id] = [User].[id]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'

Use [STFSubscriptions]
DELETE FROM [User]
WHERE [User].[username] = 'S-1-5-21-xxxxxxxxxx-xxxxxxxxxx-xxxxxxxxxx-
    xxxx'
<!--NeedCopy-->
```

```
-- 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)
<!--NeedCopy-->
```

Advanced store settings

July 7, 2021

You can configure advanced store properties by using the Advanced Settings page in the Configure Store Settings.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. 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**.
3. On the **Configure Store Settings** page, select **Advanced Settings**, select the advance option you want to configure, make the required change, and click **OK**.

Address resolution type

Use the **Advanced Settings** page to specify the type of address to request from the server. The default is DnsPort. From the **Address resolution type** drop-down menu on **Advanced Settings**, select one of the following:

- Dns
- DnsPort
- IPV4
- IPV4Port
- Dot
- DotPort
- Uri
- NoChange

Allow font smoothing

You can specify if you want font smoothing for HDX sessions. The default is On.

Use the **Advanced Settings** task, 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.

Use the **Advanced Settings** task, select the **Allow session reconnect** option, and click **OK** to enable session reconnect.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Allow special folder redirection

Use the **Advanced Settings** task to enable or disable 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.

Use the **Advanced Settings** task, select or deselect the **Allow special folder redirection** option to enable or disable special folder redirection, and click **OK**.

Advanced health check

> Note:
>
> This feature is valid in StoreFront 1912 LTSR CU1 and later supported versions only. It is used for the Local Host Cache feature in a Citrix Virtual Apps and Desktops service deployment.
>
> Local Host Cache requires a customer-deployed on-premises StoreFront as part of the deployment. We recommend that you add all Cloud Connectors that have (or can have) VDAs registered with them to the StoreFront as Delivery Controllers. Cloud Connectors that are not added to the StoreFront cannot be used to launch resources. In this case, from StoreFront 1912 LTSR CU4 onwards, StoreFront attempts to launch resources of those connectors using the best online connectors of other resource locations which are configured in the StoreFront controller list. Launches will fail if those connectors are themselves in outage mode.

To ensure the availability of resources (apps and desktops) during an outage, without having to publish resources in every zone (resource location), enable the advanced health check feature in each StoreFront store in each zone.

1. In the store's `web.config` file, under `farmsets`, add `advancedHealthCheck="on"`. For example:

```
<farmsets>
  <farmset name="Default" enableFileTypeAssociation="on" pooledSockets="off"
    serverCommunicationAttempts="1" communicationTimeout="30" connectionTimeout="6"
    multiFarmAuthenticationMode="ANY" backgroundHealthCheckPollingPeriod="00:01:00"
    advancedHealthCheck="on">
    <farm name="Controller12345" xmlPort="80" transport="HTTP" sslRelayPort="443"
      bypassDuration="60" allFailedBypassDuration="0" loadBalance="on"
      ticketTimeToLive="200" farmType="XenDesktop" maxServersPerRequest="0"
      zones="">
```

2. After you update the file, manually restart IIS. Repeat the `web.config` file update and IIS restart for other stores.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Background health check polling period

StoreFront runs periodic health checks on each Citrix Virtual Desktops broker and Citrix Virtual Apps server to reduce the impact of intermittent server availability. The default is every minute (00:01:00). Use the **Advanced Settings** task, specify a time for the **Background health-check Polling period**, and click **OK** to control the frequency of the health check.

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. Use the **Advanced Settings** task, 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.

Use the **Advanced Settings** task, 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.

Use the **Advanced Settings** task, select (or deselect) the **Enable enhanced enumeration** option, and click **OK.**

Enable socket pooling

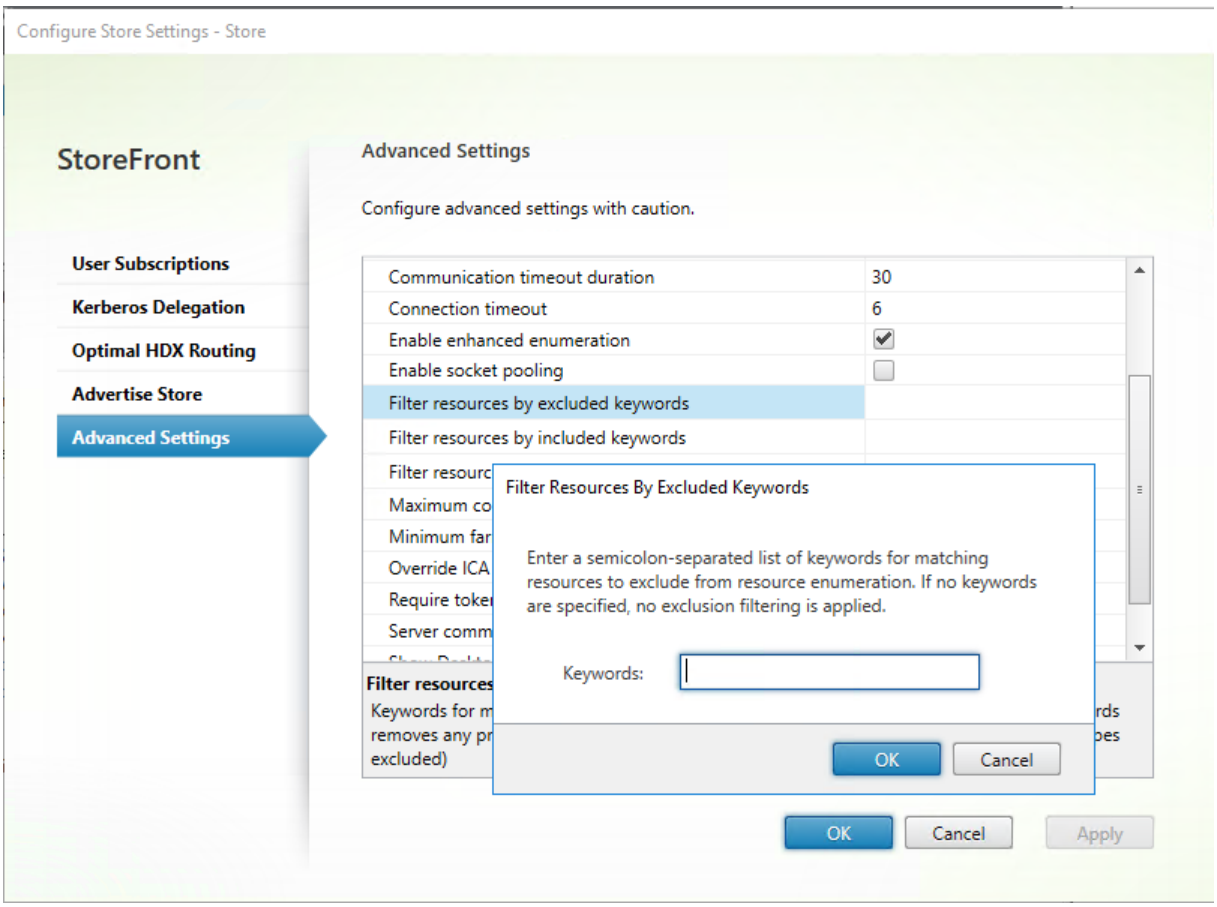
Socket pooling is disabled by default in stores. When socket pooling is enabled, StoreFront maintains a pool of sockets, rather than creating a socket each time one is needed and returning it to the operating system when the connection is closed. Enabling socket pooling enhances performance, particularly for Secure Sockets Layer (SSL) connections. To enable socket pooling, you edit the store configuration file. Use the **Advanced Settings** task, select the **Enable socket pooling** option, and click **OK** to enable socket pooling.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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).

Use the **Advanced Settings** task, select **Filter resources by excluded keywords**, click to the right of it, enter a semicolon-separated list of keywords in the enter keywords box, and click **OK**.



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).

Use the **Advanced Settings** task, select **Filter resources by included keywords**, click to the right of it, enter a semicolon-separated list of keywords in the enter keywords box, and click **OK**.

Filter resources by type

Choose the resource types to be included in resource enumeration. The default is No filtering (all resource types included).

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Use the **Advanced Settings** task, select **Filter resources by type**, click to the right of it, choose the resource types to include in the enumeration, and click **OK**.

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).

Use the **Advanced Settings** task, 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.

Use the **Advanced Settings** task, 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 an ID generated by Citrix Receiver for Web. When disabled, Citrix Workspace app specifies the client name. The default is Off.

Use the **Advanced Settings** task, 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. The default is On.

Use the **Advanced Settings** task, 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.

Use the **Advanced Settings** task, select **Server communication attempts**, enter a number, and click **OK**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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.

Use the **Advanced Settings** task, 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.

Use the **Advanced Settings** task, select the **Treat desktops as apps** option, and click **OK**.

Manage a Citrix Receiver for Web site

April 29, 2020

A *Citrix Receiver for Web* site is a website used as an app store. Users can open the site in a browser and securely access applications, data, and desktops published for them through Citrix Virtual Apps and Desktops.

Use the StoreFront management console to perform the following Citrix Receiver for Web-related tasks:

Task	Detail
Create a Citrix Receiver for Web site	Create Citrix Receiver for Web sites, which enable users to access stores through a web page.
Configure Citrix Receiver for Web sites	Modify settings for your Receiver for Web sites.
Unified user experience	StoreFront supports the unified user experience. The unified experience delivers a centrally managed HTML5 user experience.
Create and manage featured apps	Create product featured app groups for your end users that are related to or fit in a specific category.
Configure workspace control	Workspace control lets applications follow users as they move between devices.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Task	Detail
Configure Citrix Workspace app for HTML5 use of browser tabs	Specify when users start resources from shortcuts using Citrix Receiver for HTML5 or Citrix Workspace app for HTML5, whether the desktop or application replaces the Citrix Receiver for Web site in the existing browser tab rather than appearing in a new tab.
Configure communication time-out duration and retry attempts	By default, requests from a Citrix Receiver for Web site to the associated store time out after three minutes. The store is considered unavailable after one unsuccessful communication attempt. You can change the default settings.

Create a Citrix Receiver for Web site

April 29, 2020

When you create a store, a Citrix Receiver for Web site is created for it automatically. You can add additional Citrix Receiver for Web sites to existing stores.

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

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. 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 in the Actions pane, click **Manage Receiver for Web Sites**.
3. Click **Add** to create a new Citrix Receiver for Web site. Type the desired **Web Site Path** and click **Next**.
4. Select the Citrix Receiver experience and click **Next**.
5. Select authentication methods, click **Create** and when the site has been created, click **Finish**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

The URL for users to access the Citrix Receiver for Web site is displayed. For more information about modifying settings for Citrix Receiver for Web sites, see Configure Citrix Receiver for Web sites.

By default, when a user accesses a Receiver for Web site from a computer running Windows or Mac OS X, the site attempts to determine whether Citrix Workspace app is installed on the user's device. If Citrix Workspace app cannot be detected, the user is prompted to download and install it for their platform from the Citrix website. For more information about modifying this behavior, see Configure site behavior for users without Citrix Workspace app.

The default configuration for Receiver for Web sites requires that users install a compatible version of Citrix Workspace app to access their desktops and applications. However, you can enable Citrix Workspace app for HTML5 on your Receiver for Web sites so that users who cannot install Citrix Workspace app can still access resources. For more information, see Configure Citrix Receiver for Web sites.

Configure Citrix Receiver for Web sites

May 4, 2021

The tasks below enable you to modify settings for your Citrix Receiver for Web sites. Some advanced settings can only be changed by editing the site configuration files. For more information, see Configure Citrix Receiver for Web sites using the configuration files.

> **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.

Choose authentication methods

Use the Manage Authentication Methods task to assign authentication methods for users connecting to the Citrix Receiver for Web site. This action allows you to specify a subset of authentication methods for each Receiver for Web site.

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and select the relevant store that you want to modify from the Stores pane.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

3. In the Stores pane, click **Manage Receiver for Web Sites**, click **Configure**, and choose **Authentication Methods** to specify the access methods that you want to enable for your users.

   > **Note:**
   >
   > † Citrix Receiver for Web site authentication methods marked † are not defined by settings in the store's authentication methods. Configure these authentication methods independently for each Citrix Receiver for Web site. The other authentication methods described here are defined by the store's authentication methods. (That is, a selection or deselection made here for the Citrix Receiver for Web site is replaced by the setting for the store described in Create or remove a store.)

   - Select **User name and password** to enable explicit authentication. Users enter their credentials when they access their stores.
   - Select **SAML Authentication** to enable integration with a SAML Identity Provider. Users authenticate to an Identity Provider and are automatically logged on when they access their stores. From the Settings drop-down menu:
     - Select **Identity Provider** to configure the trust to the Identity Provider.
     - Select **Service Provider** to configure the trust for the Service Provider. This information is required by the Identity Provider.
   - Select **Domain pass-through†** to enable pass-through of Active Directory domain credentials from users' devices. Users authenticate to their domain-joined Windows computers and are automatically logged on when they access their stores. In order to use this option, pass-through authentication must be enabled when Citrix Receiver for Windows or Citrix Workspace app for Windows is installed on users' devices.

     > Note:
     >
     > Domain pass-through for Citrix Receiver for Web is limited to Windows operating systems using Internet Explorer, Microsoft Edge, Mozilla Firefox, and Google Chrome.

   - Select **Smart card†** to enable smart card authentication. Users authenticate using smart cards and PINs when they access their stores.
   - Select **Pass-through from Citrix Gateway** to enable pass-through authentication from Citrix Gateway. Users authenticate to Citrix Gateway and are automatically logged on when they access their stores.

4. Once the authentication method has been selected, click **OK**.

   For more information about modifying settings for authentication methods, see Configure the authentication service.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Add resource shortcuts to other websites

Use the **Add Shortcuts to Websites** task to provide users with rapid access to desktops and applications from trusted websites hosted on the internal network. You generate URLs for resources available through the Citrix Receiver for Web site and embed these links on your websites. Users click on a link and are redirected to the Receiver for Web site, where they log on if they have not already done so. The Receiver for Web site automatically starts the resource. In the case of applications, users are also subscribed to the application if they have not subscribed previously.

Before you can generate resource shortcuts, you must add the URLs of host websites to the "trusted URLs" list, using the Citrix StoreFront management console or using PowerShell. Trusted URLs are listed in the `<trustedUrls>` section of the web.config file for the Citrix Receiver for Web site. web.config is typically located in the `C:\inetpub\wwwroot\Citrix\storenameWeb\` directory, where *storename* is the name specified for the store when it was created.

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 appearing, in the Stores pane click **Manage Receiver for Web Sites**, click **Configure**, choose **Advanced Settings**, and clear the option **Prompt for untrusted shortcuts**.

Add trusted websites using the management console

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and select the site from the results pane.
3. In the **Actions** pane, click **Manage Receiver for Web Sites**, click **Configure**, and choose **Website Shortcuts**.
4. 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 hostname is the fully qualified domain name of the website host and port is the port used for communication with the host if the default port for the protocol is not available. 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.
5. Click **Get shortcuts** and then click **Save** when you are prompted to save your configuration changes.
6. Log on to the Citrix Receiver for Web site and copy the URLs you require to your website.

Add trusted websites using PowerShell

You can add 'trusted' URLs using the **Set-STFWebReceiverApplicationShortcuts** PowerShell cmdlet described in https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Citrix.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

StoreFront.SubscriptionsStore/.

Set session settings

1. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane, and in the **Actions** pane click **Manage Receiver for Web Sites**, click **Configure**, and choose **Session Settings**.

You can change the following settings:

Server Communication attempts: The number of communication attempts Receiver for Web makes to Storefront Server. This defaults to 1 attempt.

Communication timeout duration: The time after which Receiver for Web determines that the Storefront Server is unavailable. This defaults to 3 minutes.

Session timeout: The time after which user sessions on Citrix Receiver for Web sites time out. When a user session times out, users can continue to use any desktops or applications that are already running but must log on again to access Citrix Receiver for Web site functions such as subscribing to applications. The minimum value for all time intervals is 1. The maximum equates to 1 year for each time interval. By default, user sessions time out after 20 minutes of inactivity.

Sign in timeout: The time after which, if there is no activity, the Receiver for Web logon page times out. You can specify minutes for Sign in timeout. The default value is 5 minutes. NOTE: Sign in timeout should be less than session timeout.

Specify different views for applications and desktops

Use the **Application and Desktops view on Receiver for Web** task in the **Manage Receiver for Web Sites** to change the session timeout value.

1. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane and in the **Actions** pane, click Manage Receiver for Web Sites, click **Configure**, and choose **Client Interface Settings**.
3. From the **Select view** and **Default view** drop-down menus, select the views you want displayed.

To enable folder view:

1. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane and in the **Actions** pane, click **Manage Receiver for Web Sites** and click **Configure**.
3. Select **Advanced Settings** and check **Enable folder view**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Stop offering provisioning files to users

By default, Citrix Receiver for Web sites offer provisioning files that enable users to configure Citrix Receiver or Citrix Workspace app automatically for the associated store. The provisioning files contain connection details for the store that provides the resources on the site, including details of any Citrix Gateway deployments and beacons configured for the store. In this article, mentions of "Citrix Workspace app" also represent the supported versions of Citrix Receiver unless otherwise noted.

Use the **Enable Receiver configuration** task in the **Manage Receiver for Web Sites** to change the session timeout value.

1. On the Windows **Start** screen or **Apps** screen, locate and click the Citrix **StoreFront** tile.
2. Select the **Stores** node in the left pane and in the **Actions** pane, click **Manage Receiver for Web Sites**, click **Configure**, and choose **Client Interface Settings**.
3. Select **Enable Receiver/Workspace app configuration**.

Configure site behavior for users without Citrix Workspace app

Use the **Deploy Citrix Receiver/Workspace app** task to configure the behavior of a Citrix Receiver for Web site when a Windows or Mac OS X user without Citrix Workspace app installed accesses the site. By default, Citrix Receiver for Web sites automatically attempt to determine whether Citrix Workspace app is installed when accessed from computers running Windows or Mac OS X.

If Citrix Workspace app cannot be detected, the user is prompted to download and install it for their platform. The default download location is the Citrix website, but you can also copy the Citrix Workspace app installers to the StoreFront server and allow users to download copies of these directly from the StoreFront server instead.

For users who cannot install Citrix Workspace app, you can enable Citrix Workspace app for HTML5 on your Citrix Receiver for Web sites. Citrix Workspace app for HTML5 enables users to access desktops and applications directly within HTML5-compatible web browsers without needing to install Citrix Workspace app. Both internal network connections and connections through Citrix Gateway are supported. However, for connections from the internal network, Citrix Workspace app for HTML5 only enables access to resources provided by specific products. Additionally, specific versions of Citrix Gateway are required to enable connections from outside the corporate network. For more information, see Infrastructure requirements.

For local users on the internal network, access through Citrix Workspace app for HTML5 to resources provided by Citrix Virtual Apps and Desktops is disabled by default. To enable local access to desktops and applications using Citrix Workspace app for HTML5, you must 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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

1. On the Windows **Start** screen or **Apps** screen, locate and click the Citrix StoreFront tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the results pane, select a site. In the **Actions** pane, click **Manage Receiver for Web Sites** and click **Configure**.
3. Choose **Deploy Citrix Receiver/Workspace app** and specify a **Deployment option**.
   - select **Always use Receiver for HTML5** if you want the site always to access resources through an HTML5-compatible browser without prompting the user to download and install Citrix Workspace app. With this option selected, users always access desktops and applications on the site through Citrix Workspace app for HTML5, provided they use an HTML5-compatible browser. Users without an HTML5-compatible browser cannot access resources. Access through any locally installed Citrix Workspace app is disabled.
   - select **Use Receiver for HTML5 if local Receiver is unavailable** if you want the site to prompt the user to download and install Citrix Workspace app, but fall back to Citrix Workspace app for HTML5 if Citrix Workspace app cannot be installed. Users without Citrix Workspace app are prompted to download and install it every time they log on to the site.
   - select **Install locally** if you want the site always to access resources through a locally installed Citrix Workspace app. Users are prompted to download and install the appropriate Citrix Workspace app for their platform. Access through HTML5-compatible browsers is disabled.
     - If you select **Allow users to download HDX engine (plug in)**, the Citrix Receiver for Web allows the user to download and install Citrix Workspace app on the end user client if the Citrix Workspace app is not available.
     - If you select **Upgrade plug-in at logon**, the Citrix Receiver for Web offers users a choice to upgrade the Citrix Workspace app client when they log on. Users may choose to skip the upgrade and will not be prompted to upgrade again unless Citrix Receiver for Web browser cookies are cleared. To enable this feature, ensure the Citrix Workspace app files are available on the StoreFront server.
     - Select a source from the drop-down list.

Make Citrix Workspace app installation files available on the server

By default, when a user accesses a Citrix Receiver for Web site from a computer running Windows or Mac OS X, the site attempts to determine whether Citrix Workspace app is installed on the user's

© 1999–2022 Citrix Systems, Inc. All rights reserved.

device. If Citrix Workspace app cannot be detected, the user is prompted to download and install it for their platform from the Citrix website or by downloading the correct installer from the StoreFront server.

1. On the Windows **Start** screen or **Apps** screen, locate and click the Citrix **StoreFront** tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the results pane, select a site. In the **Actions** pane, click **Manage Receiver for Web Sites** and click **Configure**.
3. Choose **Deploy Citrix Receiver/Workspace app** and **Source for Receivers/Workspace app**, and then browse to the installation files.

Run the prompt to install Citrix Workspace app after logon

Before logging on to StoreFront, Citrix Receiver for Web prompts a user to install the latest Citrix Workspace app if it is not already installed on the user's computer. Depending on the configuration, the prompt may also display if the user's installation of Citrix Workspace app can be upgraded.

You can configure Citrix Receiver for Web to display the prompt after logging on to StoreFront.

1. On the **Windows Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and select the site from the results pane.
3. In the **Actions** pane, click **Manage Receiver for Web Sites**, click **Configure**.
4. Select **Advanced Settings** and check **Prompt to install Citrix Receiver/Workspace app after logon**.

Remove Citrix Receiver for Web sites

Use the **Manage Receiver for Web Sites** in the **Actions** pane to delete a Citrix Receiver for Web site. When you remove a site, users can no longer use that webpage to access the store.

Support for the unified user experience

February 23, 2022

> **Note:**
>
> "StoreFront" remains the name used to refer to the enterprise app store. It aggregates applications and desktops from Citrix Virtual Apps and Desktops sites into a single easy to use store for users. Citrix Receiver technology is now included in Citrix Workspace app. Implementing this transition in our products and documentation is an ongoing process. In-product content

© 1999–2022 Citrix Systems, Inc. All rights reserved.

> might still contain former names—for example, the unified experience refers to "Citrix Receiver". Your patience during this transition is appreciated. For more detail about our new names, see https://www.citrix.com/products/.

StoreFront supports the *unified* user experience. The unified experience delivers a centrally managed HTML5 user experience to all web and native Citrix Workspace apps. It also supports customization and featured app groups management.

Stores created using this version of StoreFront use the unified experience.

Use the StoreFront management console to do the following Citrix Receiver for Web related tasks:

- Create a Citrix Receiver for Web site.
- Change the Citrix Receiver for Web site experience.
- Select a unified Citrix Receiver for Web site to associate with the store.
- Customize the Receiver appearance.

Use JavaScript and CSS to customize Citrix Receiver for Web pages.

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.

> **Note:**
>
> If using XenApp 6.x, applications set to **Stream to client** or **Streamed if possible, otherwise accessed from a server** are not supported with the unified experience enabled.

Create a Citrix Receiver for Web website

A Citrix Receiver for Web site is created automatically, whenever you create a store. You can also create extra Receiver for Web sites using this procedure.

1. On the Windows Start screen or Apps screen, locate and click the **Citrix StoreFront tile**.
2. Select the Stores node in the left pane of the Citrix StoreFront management console and, in the Actions pane, click **Manage Receiver for Web Sites** > **Add** and follow the wizard.

Select a unified Citrix Receiver for Web site to associate with the store

When a new store is created using StoreFront, a Citrix Receiver for Web site is automatically created and associated with the store. Citrix Receiver for Web sites use the unified experience. When a store has multiple Receiver for Web sites, you need to select which Receiver for Web site is displayed when users access the store using Citrix Workspace app.

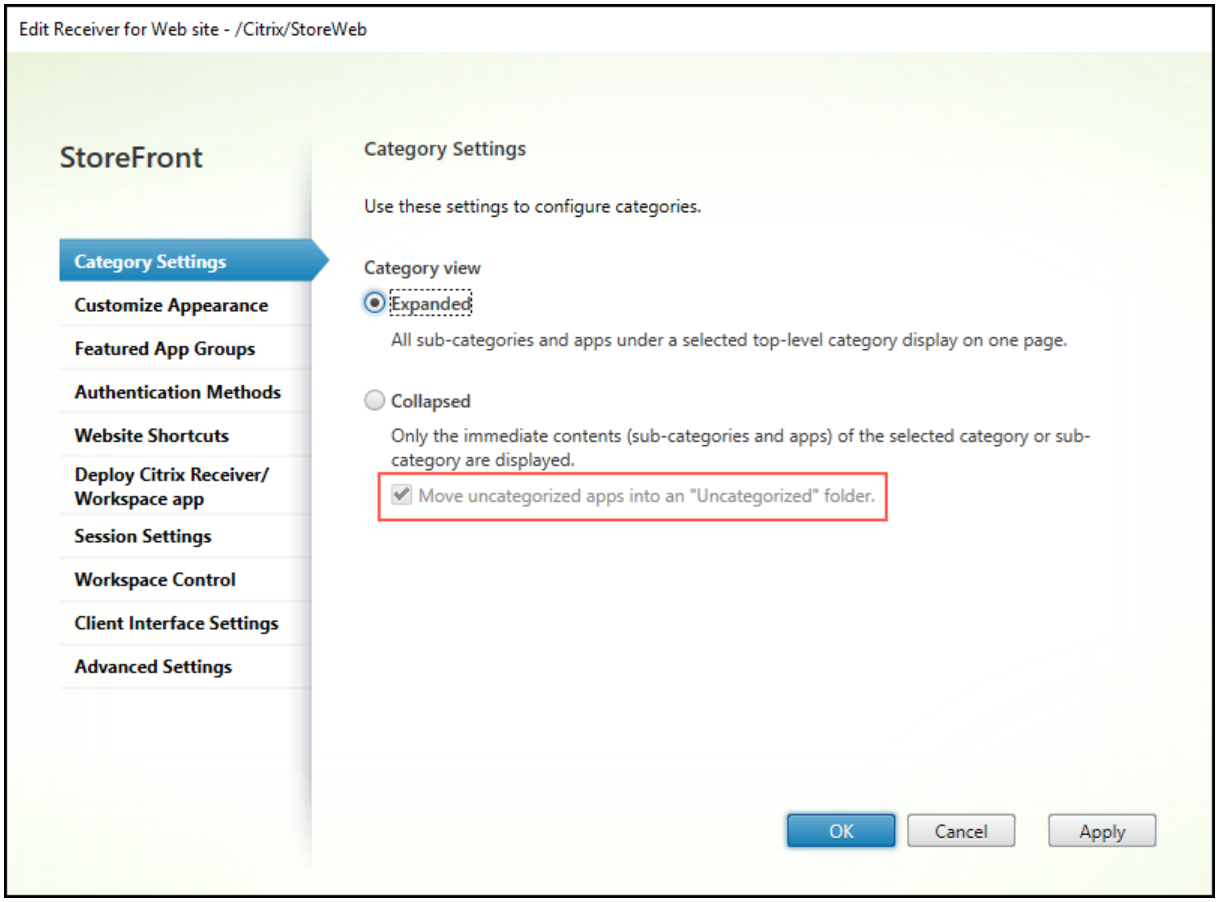
1. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and select a store in the results pane. In the Actions pane, click **Configure Unified Experience**. If you do not have a Citrix Receiver for Web website created, a message displays including a link to the Add Receiver for Web site wizard.
3. Select the default Receiver for Web site which Citrix Workspace app clients display when users access this store.
4. Click **OK**.

Configure category settings

1. On the Windows **Start** screen or Apps screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and select a store in the results pane. In the Actions pane, click **Manage Receiver for Web Sites**, select a Receiver for Web site, and click **Configure**.
3. Select **Category Settings** and make selections to customize how Categories display after logging on.



Select a category view:

Expanded – (Default) Only top-level categories can be selected. Every app under the selected top-

© 1999–2022 Citrix Systems, Inc. All rights reserved.

level category is visible, grouped by subcategory.

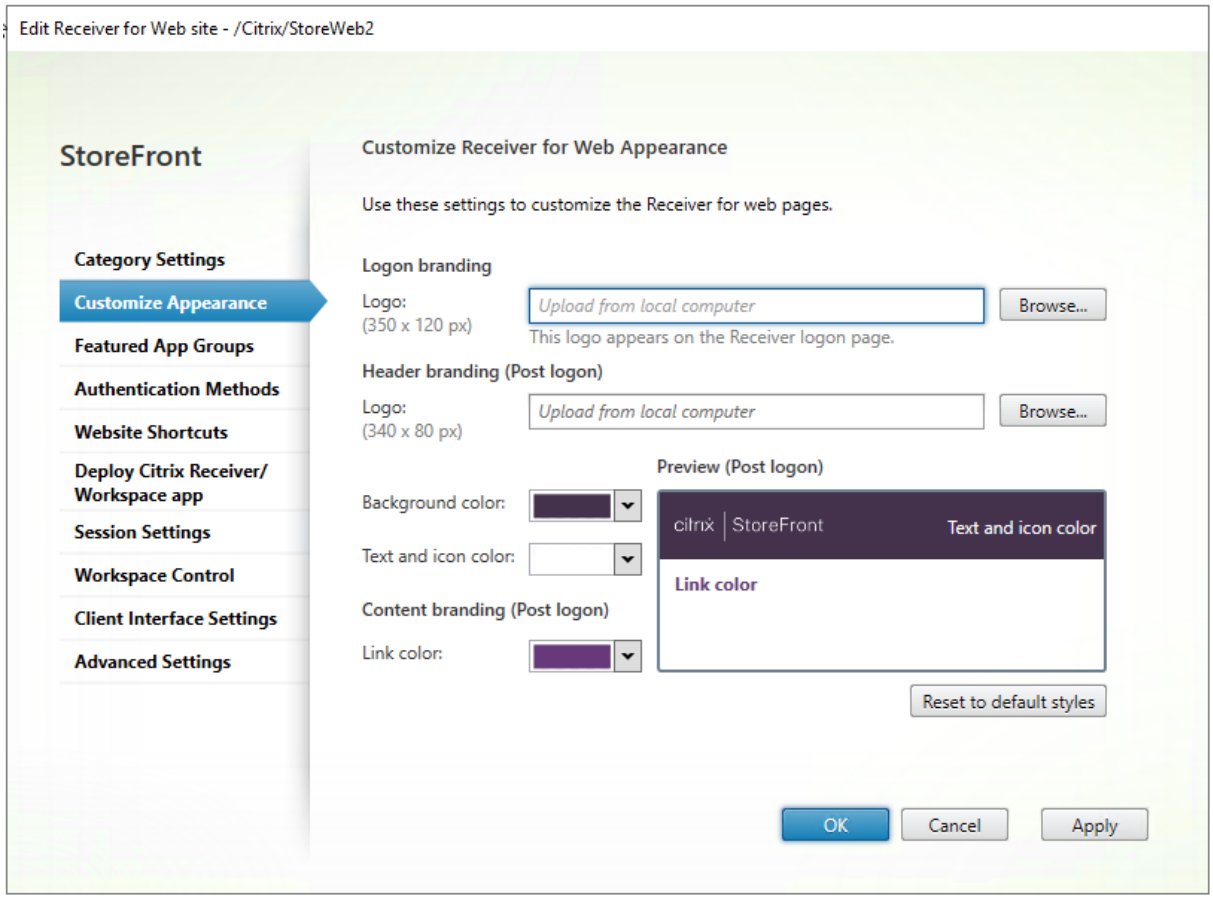
Collapsed – Top-level categories and their subcategories can be selected. Only apps in the selected category are visible. Navigation between subcategories is via a 'breadcrumb trail'.

> **Note:**
>
> Clear the **Move uncategorized apps into an Uncategorized folder** check box to view all the apps under the first layer of the category fields.

These category views are described in Unified user experience.

Customize the Citrix Receiver appearance

1. On the Windows **Start** screen or Apps screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and select a store in the results pane. In the Actions pane, click **Manage Receiver for Web Sites** and click **Configure**.
3. Select **Customize Appearance** and make selections to customize how the website displays after logging on.



© 1999–2022 Citrix Systems, Inc. All rights reserved.

Further customization using JavaScript and CSS

> **Note:**
>
> In the examples in this section, add JavaScript to the *script.js* file (for example in C:\inetpub\wwwroot\Citrix\Stor
> and add CSS to the *style.css* file in the same directory.

Add a static header to the login page in Receiver for Web

Here 'static' here means fixed text like a welcome message, or a company name. For something that changes, such as a news message or server status, see Add a dynamic header to the login page in Receiver for Web.

You can add static text in four positions using the following lines of JavaScript:

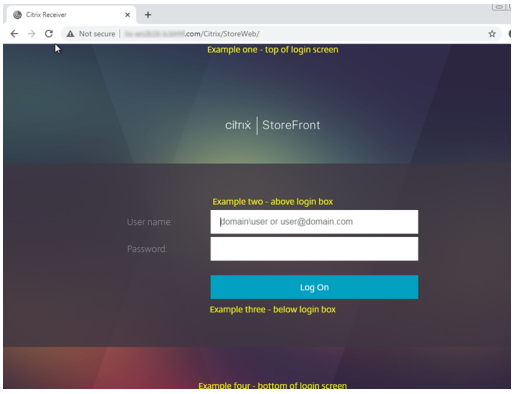
```
$('.customAuthHeader').html("Example one - top of login screen");
$('.customAuthTop').html("Example two - above login box");
$('.customAuthBottom').html("Example three - below login box");
$('.customAuthFooter').html("Example four - bottom of login screen");
<!--NeedCopy-->
```

To make the text more obvious, add the following styling to custom.css:

```
.customAuthHeader,
.customAuthFooter,
.customAuthTop,
.customAuthBottom
{

 font-size:16px;
 color:yellow;
 text-align: center;
 }

<!--NeedCopy-->
```

You get the following result:

© 1999–2022 Citrix Systems, Inc. All rights reserved.



To use HTML formatting, replace the 4 lines of javascript with the following:

```
$('.customAuthHeader').html("<b>Example one</b> - top of login screen");
$('.customAuthTop').html("<div style='background:black'>Example two - above login box</div>");
$('.customAuthBottom').html("<i>Example three - below login box</i>");
$('.customAuthFooter').html("<img src='logo.png'>Example four - bottom of login screen");
<!--NeedCopy-->
```

> **Note:**
>
> The fourth example line expects an image named *logo.png* in the custom directory.

Add a dynamic header to the login page in Receiver for Web

Here 'dynamic' means that some content is loaded and displayed every time, rather than being cached. Web browsers often cache things, but Citrix Workspace app always caches the UI, and always loads the previously cached UI. If you use the previous example for something like service status, you do not get what you intended.

Instead, you need to make an Ajax call to dynamically load the content and insert it into the page, by doing the following:

1. Define a useful utility function. One that fetches the content from a page in the *\customweb* directory on the server, and adds it to the page. It does the equivalent of the .html examples above, and the custom page can contain text, or an HTML snippet. Use the *\customweb* directory. It gets copied to all servers in a StoreFront server group (just like the \custom directory), but is not downloaded and cached.

2. Arrange for this function to be called at a suitable point. Calling the function too early causes problems in Citrix Workspace app, because the script runs before the configuration has been

© 1999–2022 Citrix Systems, Inc. All rights reserved.

fully loaded. A good time for this sort of action is **beforeDisplayHomeScreen** (but if you want to display content on the login page, then use **beforeLogin** instead). The following code handles both cases, and is suitable for web and native clients.

The full script is as follows:

```
function setDynamicContent(txtFile, element) {

   CTXS.ExtensionAPI.proxyRequest({

      url: "customweb/"+txtFile,
      success: function(txt) {
 $(element).html(txt); }
  }
 );
 }


var fetchedContent=false;
function doFetchContent(callback)
{

  if(!fetchedContent) {

    fetchedContent = true;
    setDynamicContent("ReadMe.txt", "#customScrollTop");
   }

  callback();
 }


CTXS.Extensions.beforeDisplayHomeScreen = doFetchContent;
CTXS.Extensions.beforeLogon = doFetchContent;
<!--NeedCopy-->
```

This loads content from *customweb\readme.txt* which, by default, contains some uninteresting information. Add your own file (*status.txt*) and adjust the script to call it for more useful results.

Show a click-through disclaimer before or after login

The following example is already provided in the *script.js* file as an example, but needs uncommenting. There are two versions of this code: the first is done pre-login for web browsers, and the second is

© 1999–2022 Citrix Systems, Inc. All rights reserved.

done pre-main UI for native clients. If you only want a post-login message, delete the first function. However, using a pre-login message on its own is not a good option, as the login flow is only seen on web browsers (and not on native clients). Even then, the login flow is hidden when users are accessing from Citrix Gateway.

```
var doneClickThrough = false;

// Before web login
CTXS.Extensions.beforeLogon = function (callback) {

  doneClickThrough = true;
  CTXS.ExtensionAPI.showMessage({

    messageTitle: "Welcome!",
    messageText: "Only for WWCo Employees",
    okButtonText: "Accept",
    okAction: callback
   }
 );
 }
 ;

// Before main screen (both web and native)
CTXS.Extensions.beforeDisplayHomeScreen = function (callback) {

  if (!doneClickThrough) {

    CTXS.ExtensionAPI.showMessage({

      messageTitle: "Welcome!",
      messageText: "Only for WWCo Employees",
      okButtonText: "Accept",
      okAction: callback
     }
 );
   }
  else {

    callback();
   }

 }
 ;
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

Make the click-through disclaimer box wider

The message box used for **CTXS.ExtensionAPI.showMessage()** is pre-styled. You can adjust the style to make it larger, so that it looks OK for other messages. Add the following example function to script.js to shrink the style again afterwards. Call **showLargeMessage()** instead of **CTXS.ExtensionAPI.showMessage()** when you want a larger box.

```
function mkLargeMessageExitFn(origfn)
{

  if(origfn) {

    return function() {

      origfn();
      window.setTimeout(function() {
 $('body').removeClass('largeMessage'); }
 ,500);
     }
 ;
   }

 }


function showLargeMessage(details)
{

  $('body').addClass('largeMessage');
  details.cancelAction = mkLargeMessageExitFn(details.cancelAction);
  details.okAction = mkLargeMessageExitFn(details.okAction);
  CTXS.ExtensionAPI.showMessage(details);
 }
 ;
<!--NeedCopy-->
```

A marker class is added when the large message is being shown. When the box is closed, it removes this marker class after a small delay (needed to avoid a nasty 'jump').

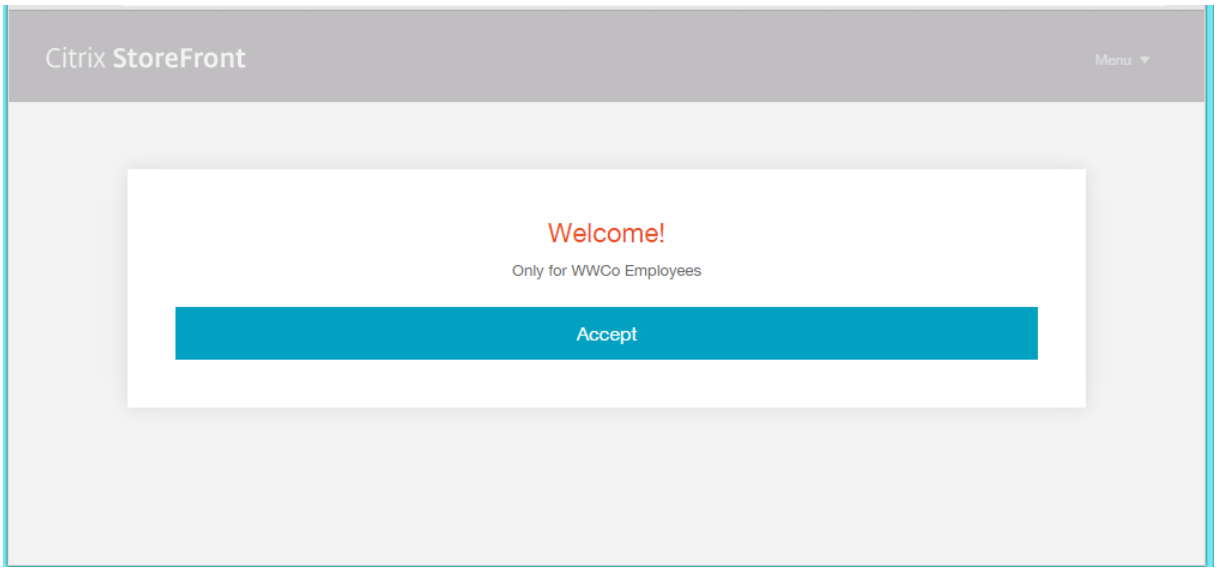
Add some CSS to adjust the size of this box based on the presence of this marker class. For example,

© 1999–2022 Citrix Systems, Inc. All rights reserved.

try the following in custom\style.css:

```
.largeTiles .largeMessage .messageBoxPopup
{

  width:800px;
 }

<!--NeedCopy-->
```

When a messageBoxPopup is shown on a large UI and the largeMessage flag is set. It is 800 pixels wide. Existing code ensures that it is centered. (On a small UI such as a mobile phone, the default message box is already full width).



To squeeze in even more text, you can reduce font size by adding the following to custom\style.css, or alternatively consider adding scrollable content.

```
.largeTiles .largeMessage .messageBoxText
{

  font-size:10px;
 }

<!--NeedCopy-->
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Make the click-through disclaimer box have scrollable content

When you call **showMessage** you can pass some HTML rather than just a string, to add style. Replace messageText, in any of the previous examples calls to showMessage, with the following:

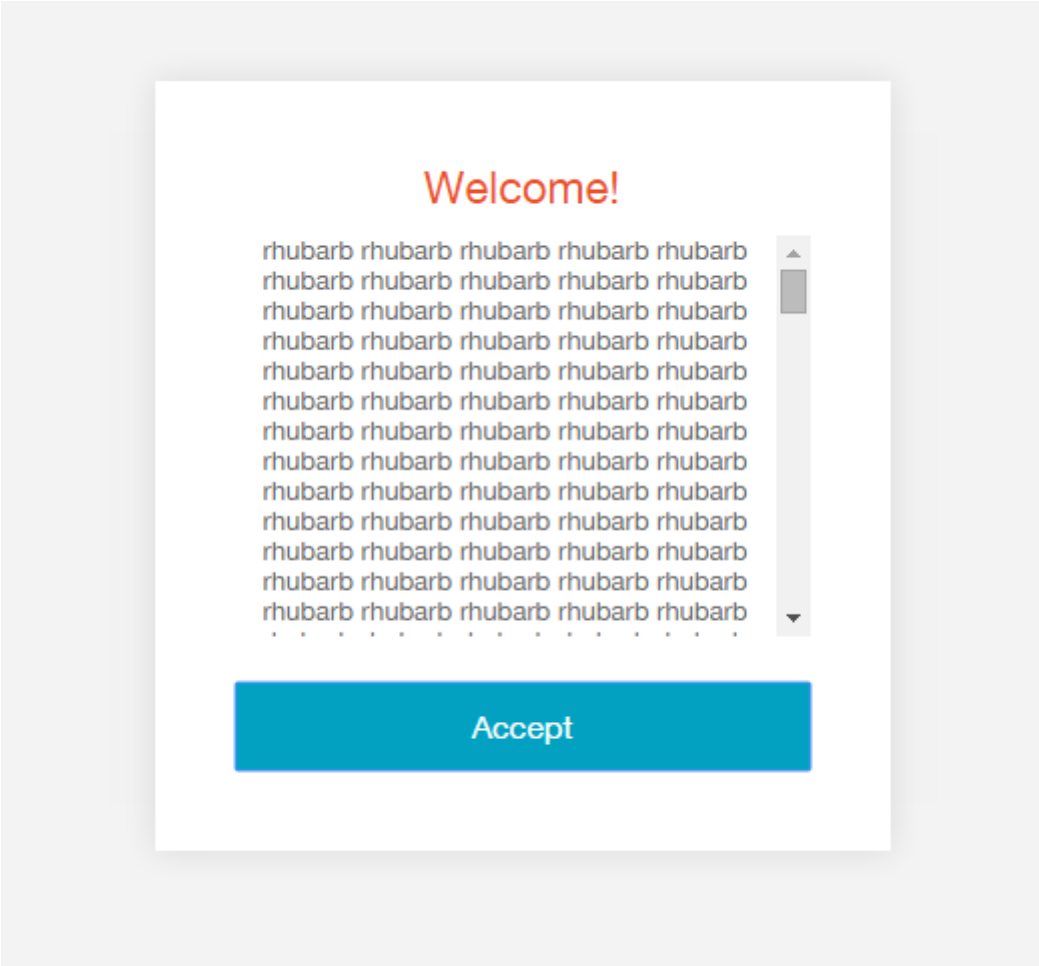
```
    CTXS.ExtensionAPI.showMessage({

          messageTitle: "Welcome!",
          messageText: "&lt;div class='disclaimer'&gt;rhubarb rhubarb
              rhubarb ... rhubarb rhubarb&lt;/div&gt;",
          okButtonText: "Accept",
          okAction: callback  }
 );
<!--NeedCopy-->
```

Then add the following to style.css:

```
.disclaimer {

    height: 200px;
    overflow-y: auto;
 }

<!--NeedCopy-->
```

You get the following result:

© 1999–2022 Citrix Systems, Inc. All rights reserved.



Add a footer to every page

There is another custom area specifically to add a footer. You can add the following line of JavaScript to set its content:

```
$('#customBottom').html("For ACME Employees Only");
<!--NeedCopy-->
```

Define the style in style.css. Set `position:static` to ensure that the scrolling area works as expected.

```
#customBottom
{

 text-align:center;
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
 font-size:30px;
 position:static;
 }

<!--NeedCopy-->
```

> **Note:**
>
> If you dynamically resize this area using a script, you must call the **CTXS.ExtensionAPI.resize()** command to let Citrix Workspace app know that something has changed.

Make the folder view the default, when users go to the Apps tab

To make the folder view the default, monitor for the 'view change' event. If the view to the 'store' (the internal name for the apps view) changes, navigate to the root folder. Watch out for:

- When the **onViewChange** event fires, to say that the store view is changing, the view has not finished drawing. Therefore, if you navigate to the folder immediately, the initialization code for the store view simply undoes your work, because it runs after your code. Avoid it by adding a 1 ms delay to ensure that your code runs after the current stack unwinds.
- The three lines containing the word 'whitespace' ensure that the initial All Apps UI is drawn off the screen by putting a large custom area above it. It stops the All Apps view flickering before the folders appear.

Add the following code to script.js as usual:

```
$('#customScrollTop').append('&lt;div class="whitespace"&gt;&lt;/div&gt;');

CTXS.Extensions.onViewChange = function(view) {

  if (view == "store") {

    $('.whitespace').height(5000);
    window.setTimeout(function() {

      CTXS.ExtensionAPI.navigateToFolder("/");
      $('.whitespace').height(0);
     }
 , 1);
   }

 }
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
 ;
<!--NeedCopy-->
```

Hide apps from All Apps that also appear in a featured category

You can use the following code to hide apps. Start by remembering every app in a bundle, and then remove them from the 'All Apps display' list.

```
var bundleApps = [];

CTXS.Extensions.sortBundleAppList = function(apps,bundle, defaultfn) {

  for (var i = 0; i &lt; apps.length; i++) {

    bundleApps.push(apps[i]);
   }

  defaultfn();
 }
 ;

CTXS.Extensions.filterAllAppsDisplay = function(allapps) {

  for (var i = 0; i &lt; allapps.length; i++) {

    if ($.inArray(allapps[i], bundleApps) != -1) {

       allapps.splice(i, 1);
       i--;
     }

   }

 }
 ;
<!--NeedCopy-->
```

If you use this customization, it is a good idea to change the text string "All Apps" to say "Other Apps", to avoid users getting confused. Edit the *strings.en.js* file in the custom directory, then add a tag for the **AllAppsTitle**. For example, with changes in yellow:

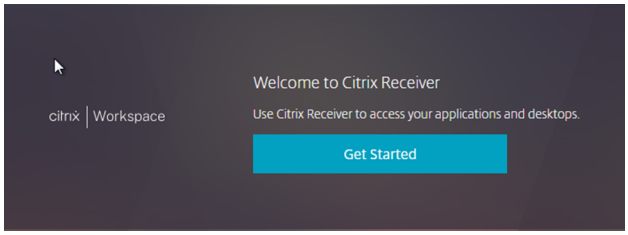
© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
(function ($) {

  $.localization.customStringBundle(”en”, {

    <span style=”background-color: yellow;”>AllAppsTitle: ”Other Apps”
        ,</span>
    Example1: ”This is an example”,
    Example2: ”This is another example”
  }
  );
  }
  )(jQuery);
<!--NeedCopy-->
```

Change the default UI text

You can change any of the texts used in the UI if you know what its label is called. For example, to change the ‘Install’ screen used in Receiver for Web on Google Chrome to ‘Get Started’, add a custom string as follows:

```
(function ($) {

  $.localization.customStringBundle(”en”, {

    <span style=”background-color: yellow;”>Install: ”Get Started”,</
        span>
    Example1: ”This is an example”,
    Example2: ”This is another example”
  }
  );
  }
  )(jQuery);
<!--NeedCopy-->
```



To discover the name of the label to change:

© 1999–2022 Citrix Systems, Inc. All rights reserved.

1. On the StoreFront server look in the directory C:\inetpub\wwwroot\citrix\StoreWeb\receiver\js\localization\
(assuming your store is called 'Store').
2. Open the file *ctxs.strings_something.js* in notepad.
3. Look for the string you want to change. **Note**: instead of editing this file directly, create override values in the custom directory as for the 'install' example.

Change the background images for featured categories

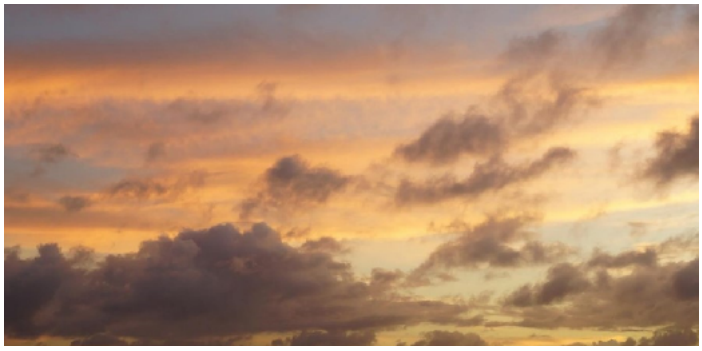
> Important:
>
> Do not try to overwrite the images on the server. It confuses any clients that have already downloaded the images, because they do not know they have changed. It also makes upgrade hard, or impossible.

You can add your own images to the *\custom* directory, and add CSS to reference them. Each featured category (called 'bundles' internally) uses two images:

- The first image is used as a tile in the carousel.
- The second image is used as a background image behind the header on the detail page. This image is stretched to fill the width of the screen, and a blur is added to its bottom edge.

You can use different images for each screen. Use the same image. Double its background height in the detail page, so that only the top half of the image is displayed. Because the image is stretched on the detail page, use an image which looks good if deformed.

The first bundle has the class 'appBundle1', the second 'appBundle2' and so on up to 'appBundle8'. The following example uses the image 'clouds.png', which you can download by right-clicking on the following image:



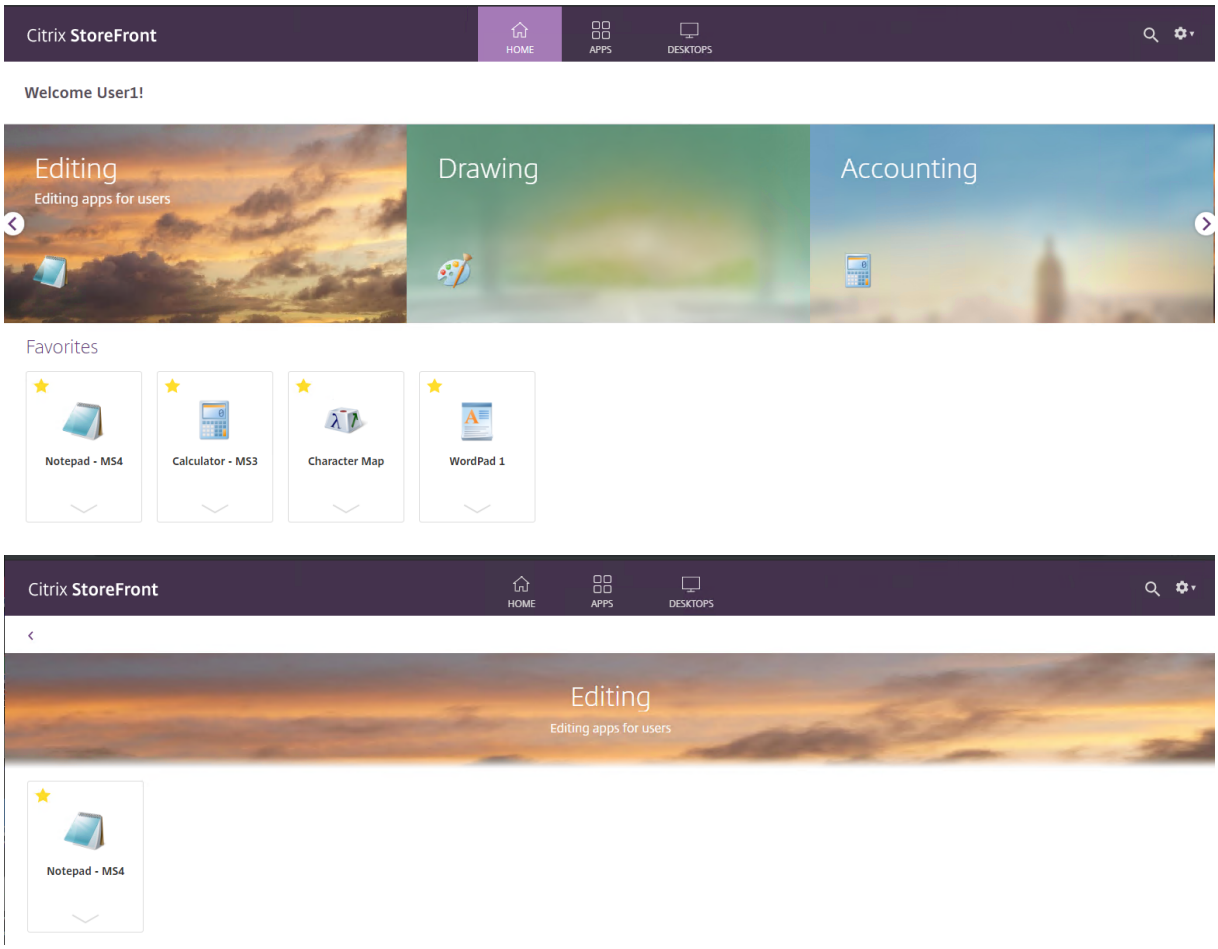
1. Save the image in the *\custom* directory. The image must be about 520 × 256 pixels to be consistent with the others (but it is scaled as needed).
2. Add the following to style.css:

```
.appBundle1 {

```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
3    background-image: url('clouds.png');
4   }
5
6
7  .bundleDetail.appBundle1 {
8
9    background-image: url('clouds.png');
10   background-size: 100% 200%;
11  }
12
13 <!--NeedCopy-->
```

You get the following result:



Prevent a company logo looking blurry

Receiver for Web needs to handle both regular ('low DPI') screens, and newer hi-res ('high DPI') screens that have a higher number of pixels per square inch, correctly. For example, **Apple Retina** screens are twice the resolution of non-retina screens. On laptops, screens are typically x1.5, x2 or even x3

© 1999–2022 Citrix Systems, Inc. All rights reserved.

the “normal” number of pixels for their size. As x2 is by far the most common, and makes the most difference, Citrix Workspace app has most of its image assets at two resolutions. An image that is 100 × 100 pixels on a normal screen, also has a x2 version at 200 × 200 pixels.

When you upload logo images from the StoreFront management console, make sure they are x2 images. In other words, they are approximately double the width and height of the ‘space’ on a regular screen. (Images uploaded at x1 are not enlarged to x2.) The ‘space’ on a regular screen is 170 × 40 pixels, so the logo image you upload must be around 340 × 80 pixels.

StoreFront creates a copy of the logo and scales it to half the size. This image is used on low DPI displays.

Occasionally, it results in a blurred image because half the image detail has been discarded. It is rare as logos tend to be bold and simple. If your logo suffers from this problem, use the following workaround:

1. Create two versions of your logo, one at the x1 size and one at the x2 size, and save them in the *\custom* directory.
2. Edit the *custom\style.css* so that it references the two different images, which can be as follows:

```
<span style=”color: green;”>/* The following section of the file is reserved for use by StoreFront. */</span>
<span style=”color: green;”>/* CITRIX DISCLAIMER: START OF MANAGED SECTION. PLEASE DO NOT EDIT ANY STYLE IN THIS SECTION */</span>
<span style=”color: green;”>/* CITRIX DISCLAIMER: END OF MANAGED SECTION. */</span>
<span style=”color: green;”>/* You may add custom styles below this line. */</span>

.logo-container {

    background-image: url('mylogo_x1.png');
    background-size: 169px 21px;
 }


.highdpi .logo-container {

    background-image: url('mylogo_x2.png');
    background-size: 169px 21px;
 }

<!--NeedCopy-->
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> - Ensure that these custom styles are not inside the 'managed section'. Otherwise they are overwritten, or they confuse the StoreFront management console.
> - Both styles specify the same background size. Because the size is specified in 'logical' units, and for the x2 image, the background size is half the width and height of the actual logo.

Set a background image

To set a background image, update *Style.css* located under `C:\inetpub\wwwroot\Citrix\<STORE>Web\custom`, where `<STORE>` is the name of the store that has the customization. The image file you specify must be in `C:\inetpub\wwwroot\Citrix\<STORE>Web\media`.

> **Note:**
>
> The unified experience is designed for a simple white background. Background images tend to be distracting. If you add a background image, try to use an image that is light and simple. If necessary, adjust any fonts so that they continue to work against this image.

Example 1: CSS reference to uploaded image

```
.large .storeViewSection,
.small .storeViewSection {

    background-image: url('../media/background.jpg');
    background-size: cover;
    background-repeat: no-repeat;
    background-position: center;
    background-attachment: fixed;
    {
 color:#4c9aff }
  }


<!--NeedCopy-->
```

Example 2: CSS reference to existing image with tweaks

```
.large .storeViewSection,
.small .storeViewSection {
```

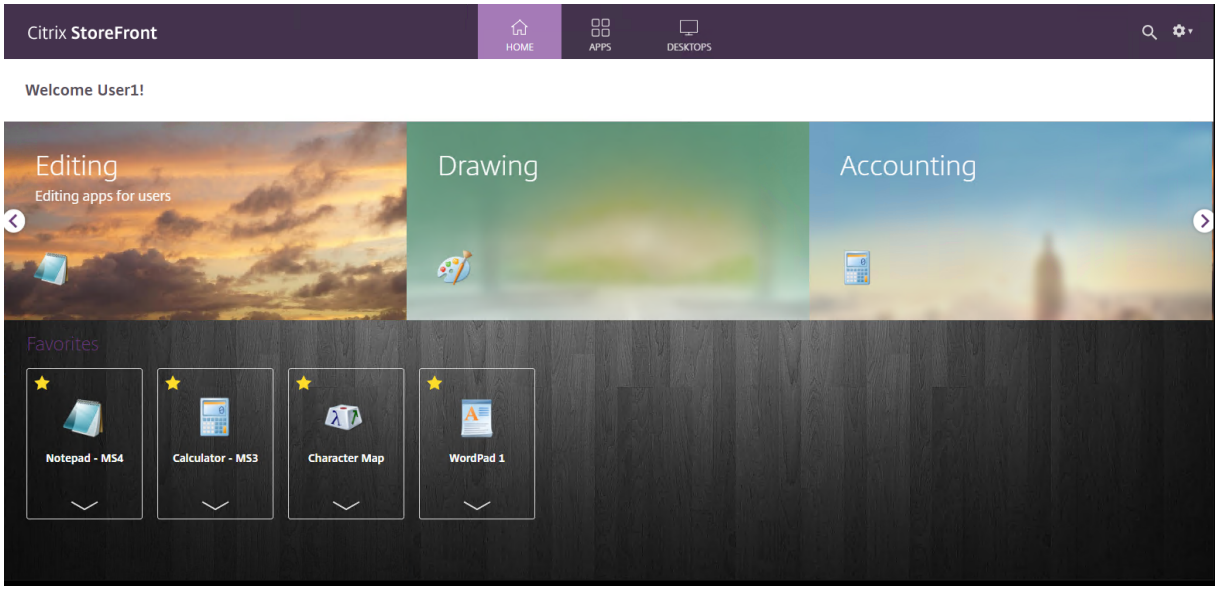
© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
3
4     background: url('../media/bg_bubbles.jpg') no-repeat center center
         fixed;
5      background-size: cover;
6      color: white;
7  }
8
9
10 // Tweak fonts
11 .smallTiles .storeapp .storeapp-name,
12 .largeTiles .storeapp .storeapp-name {
13
14     color: white;
15  }
16
17
18 // Tweak bundle area so it doesn't clash as badly
19 .largeTiles .applicationBundleContainer {
20
21     background-color: rgba(255, 255, 255, 0.4);
22     margin-top: 0;
23     padding-top: 25px;
24  }
25
26
27 .smallTiles .applicationBundleContainer {
28
29     background-color: rgba(255, 255, 255, 0.4);
30     margin-top: 0;
31     padding-top: 14px;
32  }
33
34 <!--NeedCopy-->
```

> **Note:**
>
> The `background-size:cover;` statement does not work in some older browsers.

You get the following result:

© 1999–2022 Citrix Systems, Inc. All rights reserved.



Find errors in your code

There are several ways to debug. Always try a browser first, it's far easier than debugging customizations in Citrix Workspace app. You can add the following arguments after the ? or ## in the page URL, and you can string several together. For example:

```
http://storefront.wwco.net/Citrix/StoreWeb/#-tr-nocustom
<!--NeedCopy-->
```

-errors — Normally, we try to suppress any errors that might occur in the code, but you can highlight them instead. Use this argument to display an alert box when an error occurs.

-debug — Argument disables any exception handling for customization code. It is useful with the development tools built into modern browsers (like F12 in Google Chrome or Internet Explorer), and you are debugging exceptions yourself.

-nocustom — Argument that disables your script and CSS customizations. Useful if Citrix Workspace app is not working, and you want to find out whether you introduced the error.

-tr — Argument provides tracing of the Citrix Workspace app UI code in a separate browser tab, including any tracing you add with calls to **CTXS.ExtensionAPI.trace()**.

Unified user experience

The section describes the features and appearance of the unified experience.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

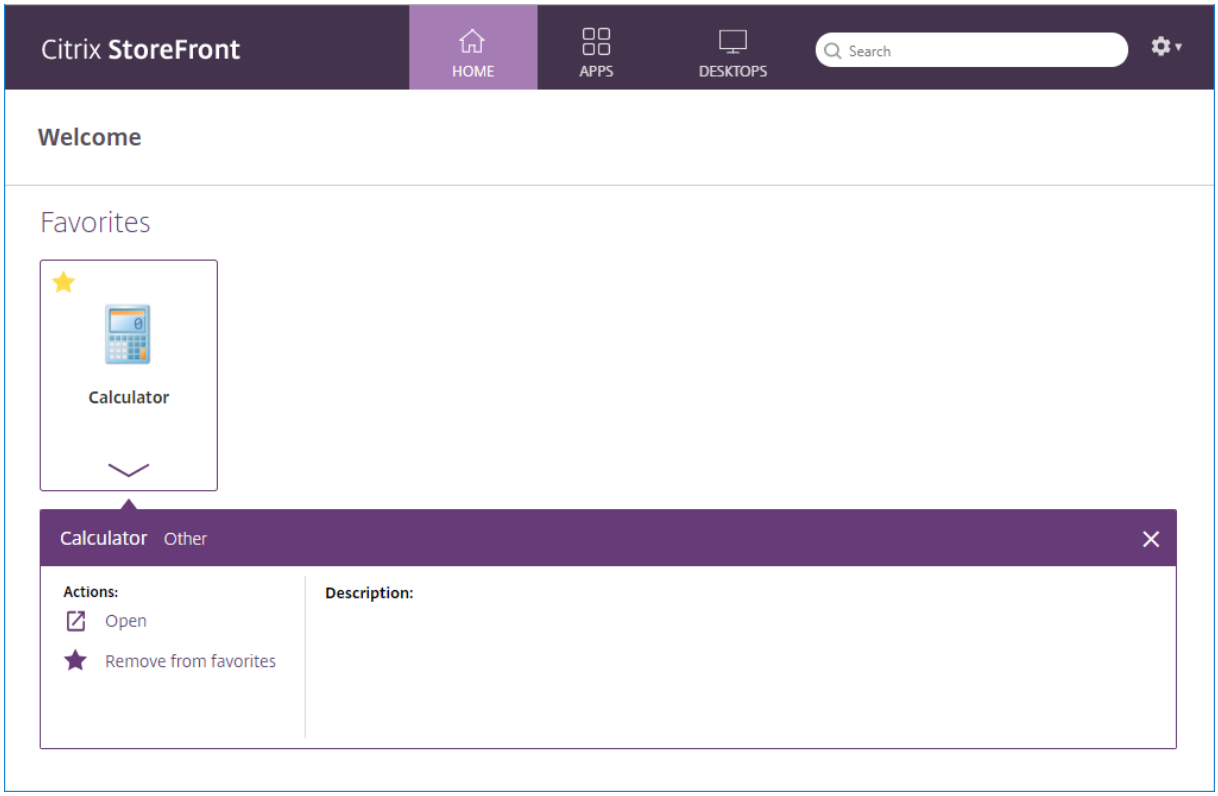
Card layout

Apps in the store are represented in a “card” layout. You can expand a panel below each card to show more details and actions.

> **Note:**
>
> The unified experience does not allow you to rearrange applications by dragging and dropping them.

Home

Home displays the favorites.



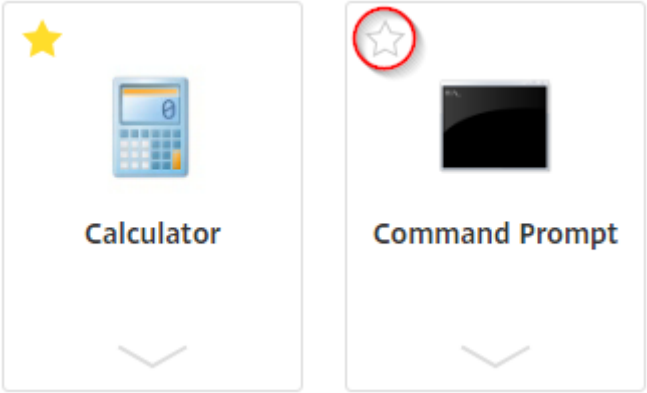
Apps

Apps display published apps. You can show the apps, Favorite Apps, or app categories.

Favorites

Click or tap the star to make an item a favorite:

© 1999–2022 Citrix Systems, Inc. All rights reserved.

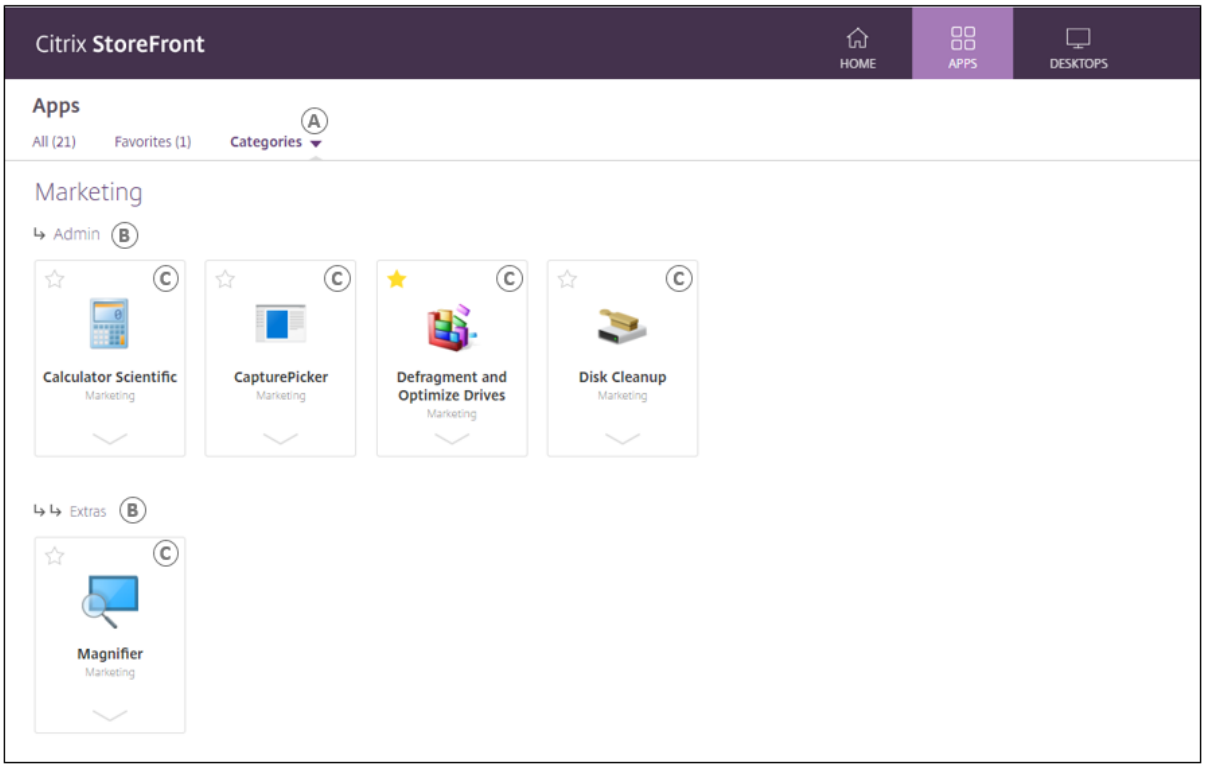


Categories

You can configure apps to display in ‘expanded’ or ‘collapsed’ categories. See Configure category settings.

Expanded categories view

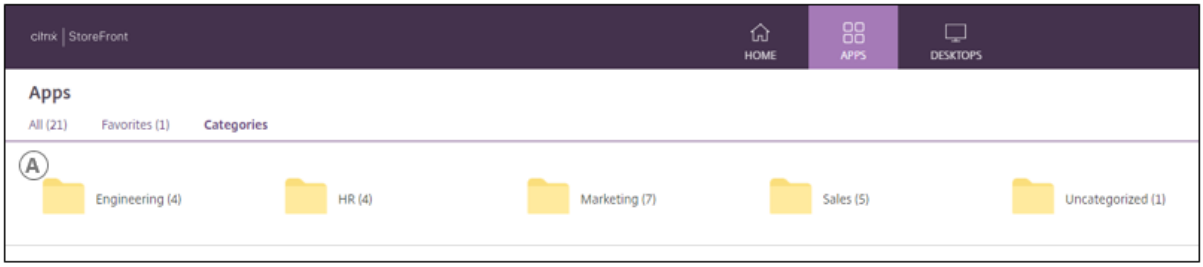
In the expanded view, click the drop-down menu control (**A**) to see all the top-level categories. When you select a subcategory (such as “Marketing”), all subcategories (**B**) and all apps (**C**) are shown on a single page.



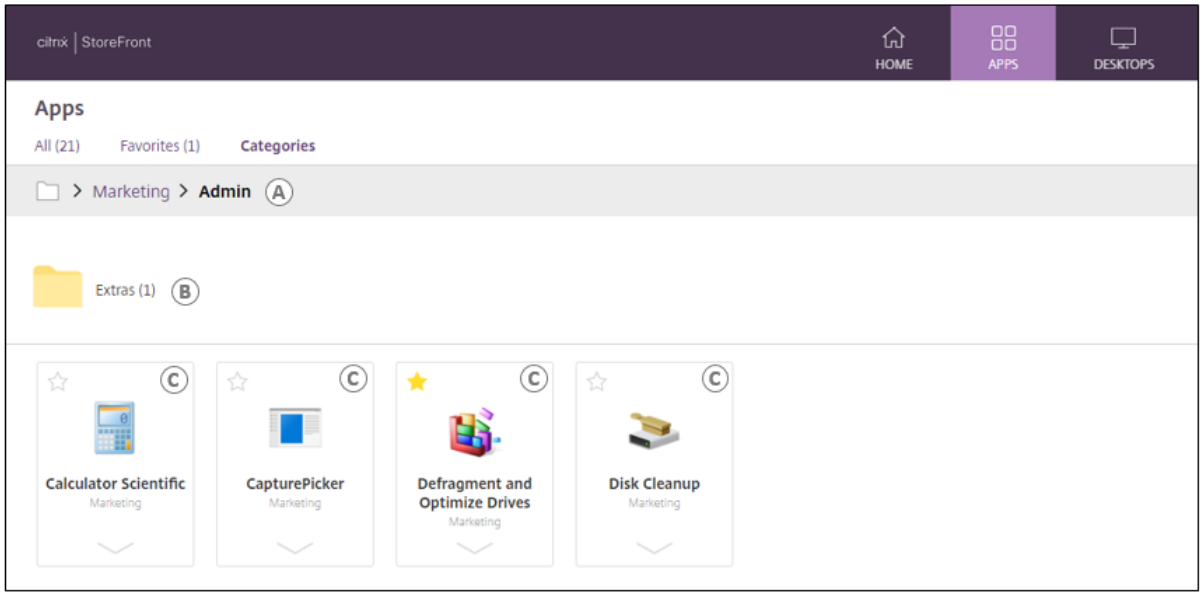
© 1999–2022 Citrix Systems, Inc. All rights reserved.

Collapsed categories view

In the collapsed view, all top-level categories are shown as folder icons (**A**).



When you select a top-level category, only the contents of that level of the category hierarchy are visible. Select a subcategory (such as “Admin”) to see the immediate subcategories (**B**) and apps (**C**) it contains. The ‘breadcrumb trail’ (**A**) indicates the current location in bold, and allows you to navigate through multi-level categories.



Search

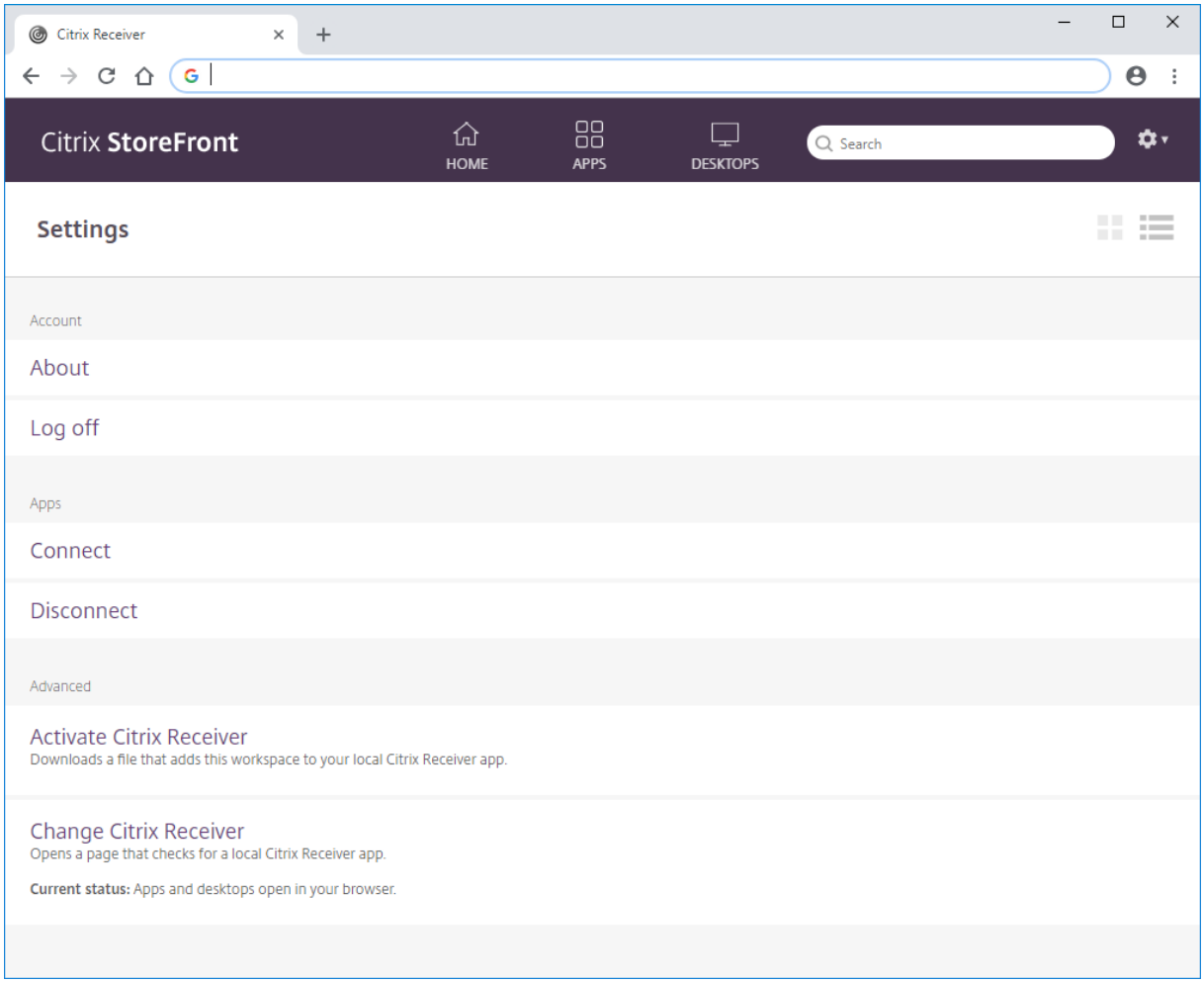
Search across all apps, desktops, and categories:

Settings

Access settings from the drop-down menu:

© 1999–2022 Citrix Systems, Inc. All rights reserved.

The menu shows the user name, taken from the Active Directory display name. If the display name is left blank, the domain and account name display. Citrix recommends that you don't leave the display name blank. Use the menu to open the Settings page, check Citrix Workspace app version, or log off.



Settings allow you to resume any disconnected sessions, and disconnect all of your current sessions and log you out respectively. Display the settings page in card or list layout:

Connect. Resumes any disconnected sessions.

Disconnect. Disconnects all of your current sessions and logs you off.

Activate Citrix Receiver. Downloads a file that adds this store to the local Citrix Workspace app.

Change Citrix Receiver. Opens a page that checks for a local Citrix Workspace app. It also allows users to switch between launching resources using the locally installed Citrix Workspace app, and launching them in an HTML5 browser.

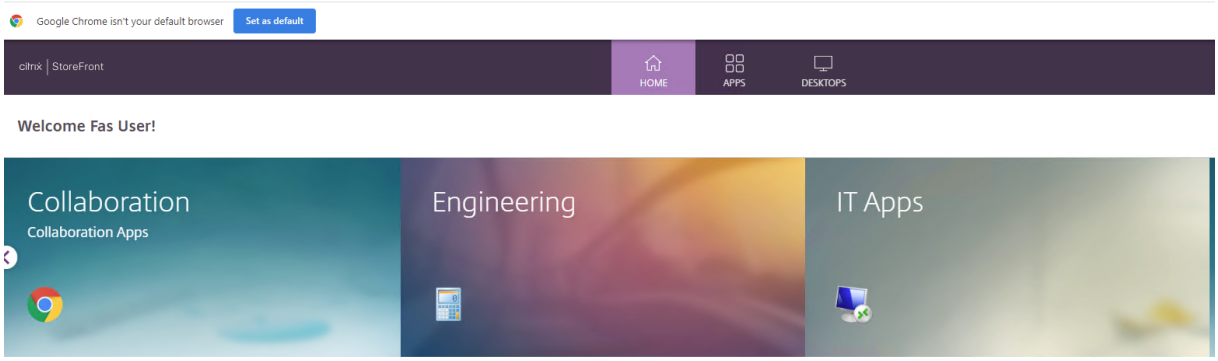
© 1999–2022 Citrix Systems, Inc. All rights reserved.

Create and manage featured apps

August 17, 2021

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.

Featured app groups are shown at the top of the **Home** tab. If User Subscriptions is disabled for the Store, you can access them on the **Apps** page in the **Collections** list.



Use the **Featured App Groups** task to add, edit, or remove featured app groups. Featured apps can be based on application names or by using keywords or application categories that have been defined in the Studio console.

> **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. On the Windows **Start** screen or Apps screen, locate and click the Citrix **StoreFront** tile.
2. Select the Stores node in the left pane of the Citrix StoreFront management console and in the Actions pane, click **Manage Receiver for Web Sites** and click **Configure**.
3. Select **Featured App Groups**.
4. In the **Featured App Groups** dialog box, click **Create** to define a new featured app group.
5. In the **Create Featured App Group** dialog box, 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, and click **OK**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

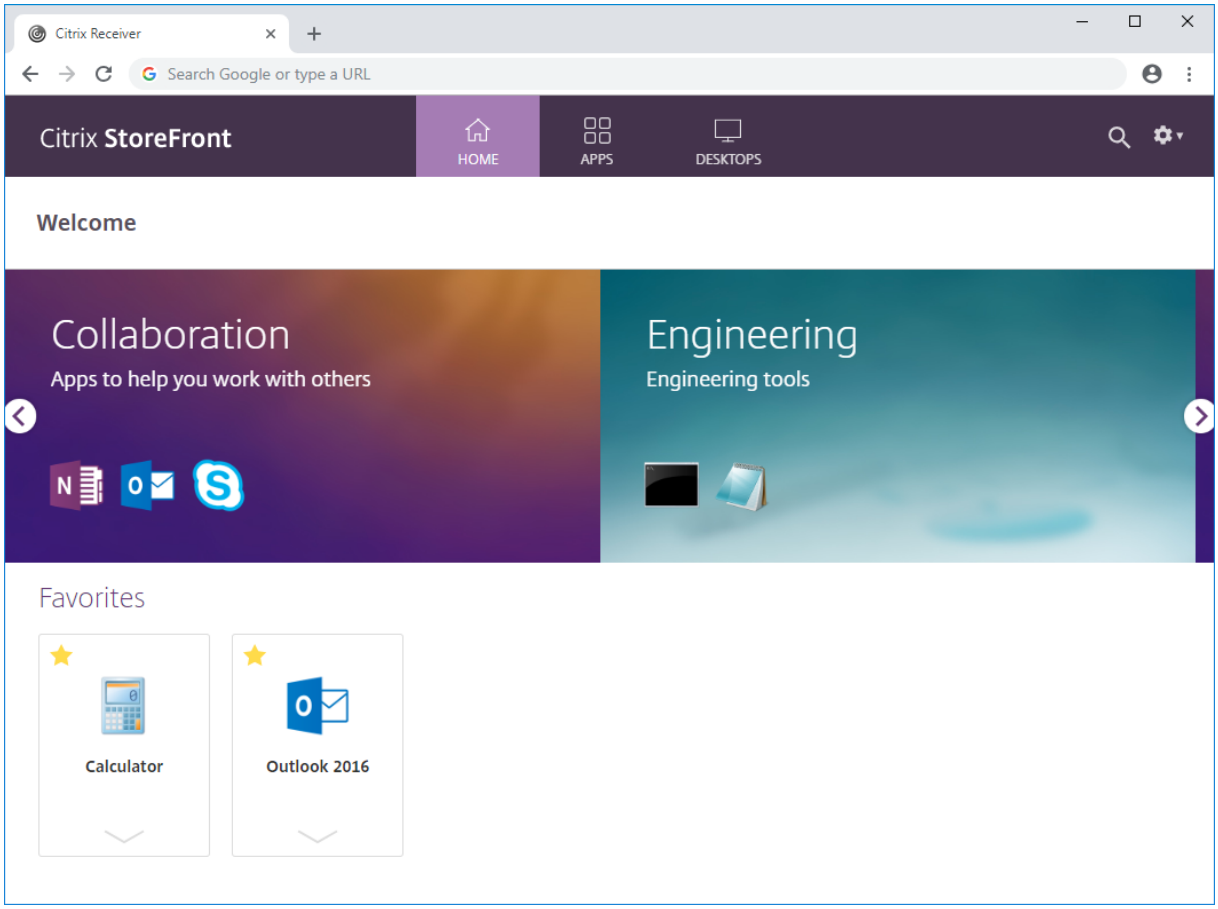
Option	Description
Keywords	Define the keywords in Studio.
Application category	Define the application category in Studio.
Application names	Use the application name to define the featured app group. All applications names matching the name included here in the Create a Featured App Group dialog screen 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.

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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



Configure workspace control

April 29, 2020

Workspace control lets applications follow users as they move between devices. This enables, for example, clinicians in hospitals to move from workstation to workstation without having to restart their applications on each device. Workspace control is enabled by default for Citrix Receiver for Web sites. To disable or configure workspace control, you edit the site configuration 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. On the Windows **Start** screen or **Apps** screen, locate and click the Citrix StoreFront tile.
2. In the left pane, select **Stores** and in the Action pane, select **Manage Receiver for Web Sites,**

© 1999–2022 Citrix Systems, Inc. All rights reserved.

and click **Configure.**

3. Select **Workspace Control**.
4. Configure default settings for workspace control, which include:
   - Enabling workspace control
   - Setting session reconnection options
   - Specifying log off action

Configure Citrix Workspace app for HTML5 use of browser tabs

February 4, 2021

By default, Citrix Workspace app for HTML5 starts desktops and applications in a new browser tab. However, when users start resources from shortcuts using Citrix Workspace app for HTML5, the desktop or application replaces the Citrix Receiver for Web site in the existing browser tab rather than appearing in a new tab.

> **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. On the Windows **Start** screen or **Apps** screen, locate and click the Citrix StoreFront tile.
2. In the left pane, select **Stores** and in the Action pane, select **Manage Receiver for Web Sites**, and click **Configure**.
3. Select **Deploy Citrix Receiver/Workspace app**.
4. In the **Deployment options** list select **Always use Receiver for HTML 5** and, depending on the tab in which you want to start applications, select or deselect **Launch applications in the same tab as Receiver for Web**.

Configure user access

October 22, 2020

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Configure support for connections through XenApp Services URLs

Use the **Configure XenApp Services Support** task to configure access to your stores through XenApp Services URLs. Users of repurposed PCs running the Citrix Desktop Lock, along with users who have older Citrix clients that cannot be upgraded, can access stores directly using the XenApp Services URL for the store. When you create a new store, the XenApp Services URL is enabled by default.

> **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. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. 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 XenApp Services Support**.
3. Select or clear **Enable XenApp Services Support** to enable or disable user access to the store through the displayed XenApp Services URL.

   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.
4. If you enable XenApp Services Support, optionally specify a default store in your StoreFront deployment for users with the Citrix Online plug-in.

   Specify a **Default store** so that your users can configure the Citrix Online plug-in with the server URL or load-balanced URL of the StoreFront deployment, rather than the XenApp Services URL for a particular store.

Disable or enable workspace control reconnect

Workspace control enables applications to follow users as they move between devices. This allows, for example, clinicians in hospitals to move from workstation to workstation without having to restart their applications on each device.

StoreFront contains a configuration to disable workspace control reconnect in the Store Service for Citrix Workspace app. Manage this feature by using the StoreFront console or PowerShell.

Use the StoreFront management console

1. On the Windows **Start** screen or Apps screen, locate and click the Citrix **StoreFront** tile.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the **Actions** pane, click **Configure Store Settings**.
3. Select **Advanced Settings** and check or uncheck **Allow session reconnect**.

Use PowerShell

Close the Administration Console then run the following code snippet to import the StoreFront PowerShell modules:

```
$dsInstallProp = Get-ItemProperty `
-Path HKLM:\SOFTWARE\Citrix\DeliveryServicesManagement -Name InstallDir
$dsInstallDir = $dsInstallProp.InstallDir
& $dsInstallDir\..\Scripts\ImportModules.ps1
```

Then the PowerShell command **Set-DSAllowSessionReconnect** turns Workspace control reconnect on or off.

Syntax

```
Set-DSAllowSessionReconnect [[-SiteId] <Int64>] [[-VirtualPath] <String> ]
[[-IsAllowed] <Boolean>]
```

For example, to turn off workspace control reconnect for a store in */Citrix/Store*, the following command configures the store:

```
Set-DSAllowSessionReconnect -SiteId 1 -VirtualPath /Citrix/Store -IsAllowed
 $false
```

Configure user subscriptions

Use the User Subscriptions task to do select one of the following options:

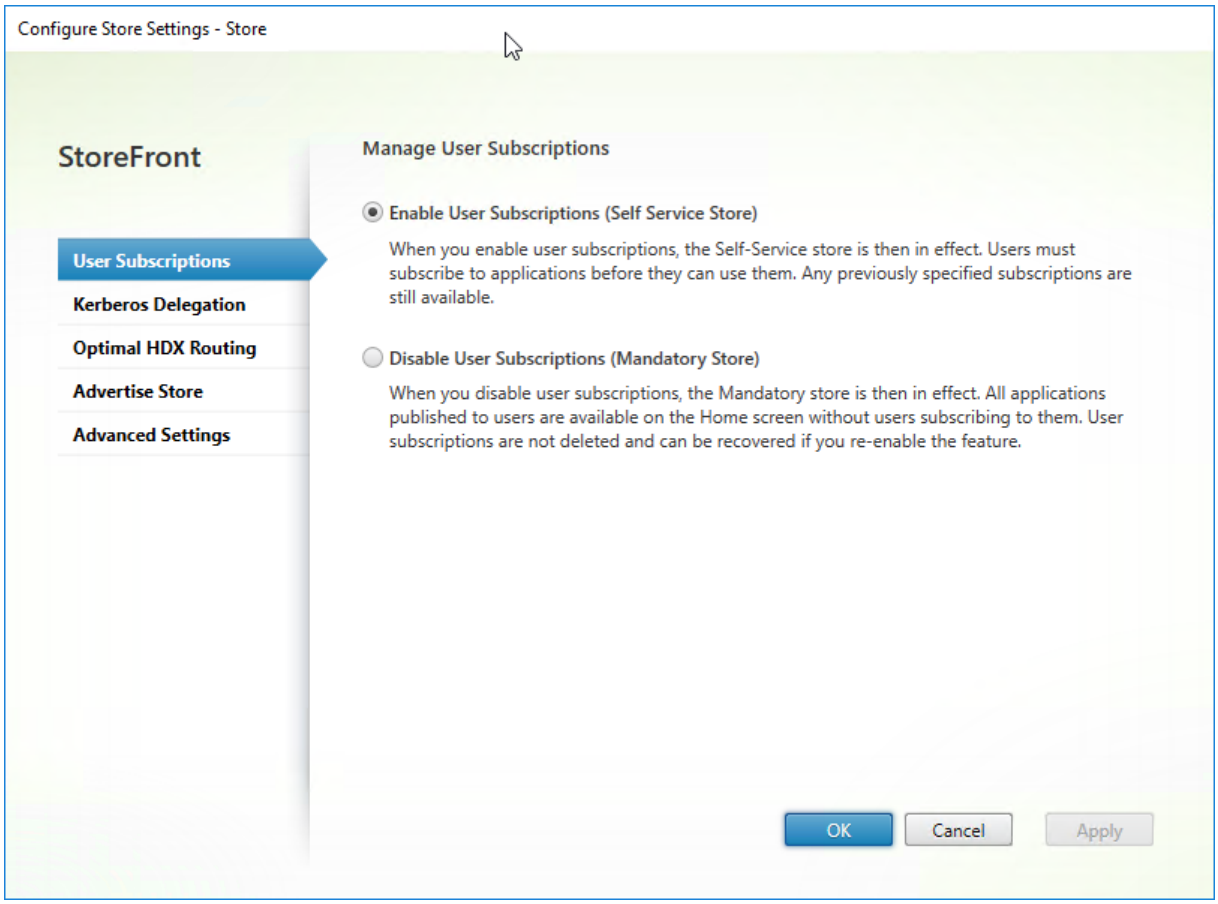
- Require users to subscribe to applications before using them (Self Service Store).
- Enable users to receive all applications when they connect to the store (Mandatory Store).

Disabling user subscriptions for a store within StoreFront also prevents the display of the Favorites tab to users in Citrix Workspace app. Disabling subscriptions does not delete the Store subscription data. Re-enabling subscriptions for the store will allow the user to see their subscribed apps in Favorites whenever they next log on.

1. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. 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** > **User Subscriptions** to toggle the user subscriptions feature off or on.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

3. Choose **Enable user subscriptions (Self Service Store)** to make users subscribe to the applications to use them. Any previously specified subscriptions are still available.
4. Choose **Disable user subscriptions (Mandatory Store)** to make all applications published to the users available on the Home screen without users subscribing to them. Their subscriptions are not deleted and they can recover them if you re-enable the feature.



In StoreFront 3.5 or later, you can use the following PowerShell script to configure user subscriptions for a store:

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

For more information on Get-STFStoreService, see https://developer-docs.citrix.com/projects/storefront-powershell-sdk/en/latest/Get-STFStoreService/

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Configure StoreFront to launch applications and desktops in Windowed Mode

September 1, 2021

Launching the applications seamlessly depends on availability of StoreFront in deployment. If you disable the seamless option for applications and desktops, consider launching your resources in Windowed Mode instead.

The following is an example of a published Notepad. Use the name of the published application exactly as shown in the application set of the Citrix Virtual Apps and Desktops console.

> **Notes:**
>
> Most of the settings in ICA files are not ***case sensitive*** except for the `DesiredHRES` and `DesiredVRES` settings. When applying the windowed app version, use the browser name to reference the app in the *default.ica* file on the StoreFront server. Verify the browser name of the application by using PowerShell on Delivery Controller:
>
> `>>asnp citrix*`
>
> `>>Get-BrokerApplication -ApplicationName`
>
> If you are using ***server groups***, after making the configuration changes on the current server, use the Propagate Changes task to update the configuration of all the other servers in your multiple-server StoreFront deployment to match the configuration of the current server.

Example

Configure StoreFront

1. Edit the default.ica file on the StoreFront server in the `\inetpub\wwwroot\Citrix\StoreName\App_Data` directory.
2. In the default.ica file, locate the lines: `[ApplicationServers] application=`.
3. Create a line after `application=`, and add the following parameters:

```
[Notepad]
TWIMode=Off
DesiredHRES=1024
DesiredVRES=768
<!--NeedCopy-->
```

4. Save the file.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Configure desktops

For published desktops from Citrix Virtual Apps and Desktops 7.x and StoreFront 3.x

1. Edit the *web.config* file on the StoreFront server in the `C:\inetpub\wwwroot\Citrix\storeWeb` directory.
2. In the web.config file, locate the following line: `showDesktopViewer=''true''`.
3. Modify the value from **True** to **False**.
4. On the Client side or from AD-GPMC, use the administrative template file (`receiver.adm` or `receiver.admx\receiver.adml`, depending on the Operating system) to configure the following policy:
   - **Computer configuration > Citrix Components > Citrix Receiver > User Experience > Client Display Settings: Enable**
   - **Seamless windows: False**
   - **Window width: <`As per requirement`>, Window height: <`As per requirement`>**

Notes

`DeisredHRES` and `DesiredVRES` can be set to any desired resolution, such as 800x600 or 1024x768.

If the application needs to run in a percent of screen size, then after setting `TWIMode=Off`, add the line `ScreenPercent=90` which configures the screen to 90 percent. You can also accomplish this with the XenApp Services site. Ensure that the corresponding file under the `conf` folder for that site (Inetpub\wwwroot\Citrix\PNAgent\conf) is edited.

If you are using the 10.x client and editing the **`default`**`.ica` or `template.ica` file, add only the `TWIMode=Off` line. It obtains the `HRES` and `VRES` settings from the published application properties. Otherwise, an error appears indicating duplicate entries in the ICA file when a user tries to launch the application.

Configure communication and session time-out

March 17, 2021

Configure communication time-out and retry attempts

By default, requests from a Citrix Receiver for Web site to the associated store time out after three minutes. The store is considered unavailable after one unsuccessful communication attempt. Use the **Session Settings** task to change the default settings.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

1. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. 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 **Manage Receiver for Web Site**, and click **Configure**.
3. Select **Session Settings**, make your changes, and click **OK/Apply** to save the changes.

Configure the session time-out

If the session time-out is not appropriately configured on StoreFront, the users may see the message "Your session has timed out due to inactivity." You can reset the session time-out value to increase the inactivity timer to suit your users' usage pattern.

Complete the following steps to configure the session time-out on StoreFront.

Change the session time-out of Citrix Receiver for Web

To configure session time-out for the users accessing StoreFront stores via Citrix Receiver for Web, perform the configuration described here. This does not have any impact on user access via Citrix Workspace app.

1. On StoreFront, navigate to `c:\inetpub\wwwroot\Citrix\<StoreWeb>`.
2. In the `web.config` file, locate the entry: `<sessionState timeout="20"/>`.
3. Change the `sessionState timeout` to the desired value in minutes.

If you configure the session time-out for Citrix Receiver for Web to **more than 1 hour**, you must also increase the token maximum lifetime appropriately in the Authentication Service.

1. On the StoreFront Server, navigate to the path of your store's Authentication Service.
   - If Storefront is installed on its own server, and you create a store `<Store>` using the Storefront management console, this path is `c:\inetpub\wwwroot\Citrix\<Store>Auth`.
   - If Storefront and the Delivery Controller are installed on the same server, when you create a Citrix Virtual Apps and Desktops site using Citrix Studio, a default store is created. In this case the path of the store's Authentication Service is `c:\inetpub\wwwroot\Citrix\Authentication`.
2. In the `web.config` file, locate the **Authentication Token Producer** service section similar to the following:

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
<tokenManager>
    <services>
    <clear />
    <service id="9c84499f-3781-42d3-b3e0-2a12efebaa8d" displayName
        ="Authentication Token Producer">
        <relyingParties signingId="462fc209-ecad-44a7-aacb-
            b75a11b6203a"
        defaultLifetime="01:00:00" maxLifetime="01:00:00">
<!--NeedCopy-->
```

3. In the entry `<defaultLifetime="01:00:00"maxLifetime="01:00:00">` *in this section only*, change `maxLifetime` to the desired value. The complete lifetime format is `.d.hh:mm:ss[.ff]`. The maximum lifetime is not limited to 24 hours.

If you configure the session time-out for Citrix Receiver for Web to **more than 8 hours**, you must also increase token life time appropriately in the StoreWeb.

1. Navigate to the StoreWeb in your file system, default `c:\inetpub\wwwroot\Citrix\<Store>Web`.
2. In the `web.config` file, locate the section similar to the following:

```
<citrix.deliveryservices>
  <webReceiver>
    <serverSettings>
      <authentication tokenLifeTime="08:00:00" locationURL="Authentication/GetAuthMethods">
```

3. Change `tokenLifeTime` to the desired value. The complete lifetime format is `.d.hh:mm:ss[.ff]`. The maximum lifetime is not limited to 24 hours.

Change the session time-out for Citrix Workspace app

To configure session time-out for the users accessing StoreFront stores via Citrix Workspace app, perform the configuration described here. This does not have any impact on user access via Receiver for Web.

1. On the StoreFront Server, navigate to the path of your store's Authentication Service.
   - If Storefront is installed on its own server, and you create a store `<Store>` using the Storefront management console, this path is `c:\inetpub\wwwroot\Citrix\<Store>Auth`.
   - If Storefront and the Delivery Controller are installed on the same server, when you create a Citrix Virtual Apps and Desktops site using Citrix Studio, a default store is created. In this case the path of the store's Authentication Service is `c:\inetpub\wwwroot\Citrix\Authentication`.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

2. In the `web.config` file, locate the **Authentication Token Producer** service section.

```
<service id="cfff7b1d-1cee-4241-93cd-b81aaca38856" displayName="Authentication Token Producer">
  <relyingParties signingId="8973bf5a-a523-4315-bad1-965246a66c63"
    defaultLifetime="01:00:00" maxLifetime="01:00:00">
    <add id="cfff7b1d-1cee-4241-93cd-b81aaca38856" encipherId="8973bf5a-a523-4315-bad1-965246a66c63"
      defaultLifetime="01:00:00" maxLifetime="20:00:00" />
    <add id="21d8b9df-8da9-4227-9687-e6abb5aba429" encipherId="8973bf5a-a523-4315-bad1-965246a66c63" />
    <add id="45e8ba75-ef9a-4ed4-bdc4-f454734d211f" encipherId="fc2dc08f-d5e9-4453-9a3a-621cbce14ca4" />
    <add id="59287a0b-2e19-40c9-85b4-2d21f1a2e9dd" encipherId="d83082ca-aa06-4e49-9003-2c9c81912553" />
  </relyingParties>
```

3. Change the indicated `maxLifetime` to the desired value in minutes. The complete lifetime format is `.d.hh:mm:ss[.ff]`. The maximum lifetime is not limited to 24 hours.

> **Note:**
>
> After they log out or the session times out, users accessing StoreFront stores via Citrix Workspace app may see Citrix Virtual Apps and Desktops in the background. However, when they click on any app or desktop after the StoreFront session times out, they need to enter their credentials again. Any already launched apps or desktops do not get logged off after storefront sessions time out.

Restart IIS

Run the `iisreset` command to apply the changes. Running this command logs off the users from Citrix Receiver for Web, and it does not impact their current ICA session.

Additional resources

- Security Token Services API

Set up highly available multi-site stores

October 22, 2020

> **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.

For stores that aggregate resources from multiple deployments, particularly geographically dispersed deployments, you can configure load balancing and failover between deployments, mapping of users to deployments, and specific disaster recovery deployments to provide highly available resources.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Where you have configured separate Citrix Gateway appliances for your deployments, you can define the optimal appliance for users to access each of the deployments.

Configure user mapping and aggregation

The StoreFront management console enables you to:

- **Map users to deployments:** Based on Active Directory group membership, you can limit which users have access to particular deployments.
- **Aggregate deployments:** You can specify which deployments have resources that you want to aggregate. Matching resources from aggregated deployments are presented to the user as a single highly-available resource.
- **Associate a zone with a deployment:** When accessed with Citrix Gateway in a global load-balancing configuration, StoreFront prioritizes deployments from zones matching the gateway zone when launching resources.

1. Ensure that you have configured the store with details of all the Citrix Virtual Apps and Desktops deployments that you want to use in your configuration. For more information about adding deployments to stores, see Manage the resources made available in stores.
2. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
3. Select the **Stores** node in the left pane of the Citrix StoreFront management console and click **Manage Delivery Controllers** in the **Actions** pane.
4. If two or more controllers are defined, click **User Mapping and Multi-Site Aggregation Configuration > Configure**.
5. Click **Map users to controllers** and make selections on the screens to specify which Delivery Controllers are available to which users.
6. Click **Aggregate resources** to aggregate resources from multiple deployments. When Delivery Controllers are aggregated, applications and desktops from Delivery Controllers with the same display name and path are presented as a single application or desktop in Citrix Workspace app.
   a) To aggregate Delivery Controllers, select multiple controllers and click **Aggregate**.
   b) Select **Aggregated Controller Settings** options:

      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 deployments.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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.

7. In the User Mapping and Multi-Site Aggregation Configuration dialog, click **OK**.
8. In the Manage Delivery Controllers dialog, click **OK**.

Advanced configurations

You can configure many common multi-site and high availability operations with the StoreFront management console. You can also configure StoreFront using PowerShell or by editing the StoreFront configuration files, 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.
- Ability to define disaster recovery deployments (deployments accessed only when all other deployments are unavailable).

> **Warning:**
>
> After configuring advanced multi-site options by manually editing the configuration file, some tasks become unavailable in the Citrix StoreFront management console to prevent misconfiguration.

1. Ensure that you have configured the store with details of all the Citrix Virtual Apps and Desktops deployments that you want to use in your configuration, including disaster recovery deployments. For more information about adding deployments to stores, see Manage the resources made available in stores.
2. Use a text editor to open the web.config file for the store, which is typically located in the directory C:\inetpub\wwwroot\Citrix\storename\, where storename is the name specified for the store when it was created.
3. Locate the following section in the file.

```
<resourcesWingConfigurations>
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
<resourcesWingConfiguration name="Default" wingName="Default" />
</resourcesWingConfigurations>
<!--NeedCopy-->
```

4. Specify your configuration as shown below.

```
<resourcesWingConfigurations>
<resourcesWingConfiguration name="Default" wingName="Default">
<userFarmMappings>
<clear />
<userFarmMapping name="user_mapping">
<groups>
<group name="domain\usergroup" sid="securityidentifier" />
<group ... />
...
</groups>
<equivalentFarmSets>
<equivalentFarmSet name="setname" loadBalanceMode="{
 LoadBalanced | Failover }
 "
aggregationGroup="aggregationgroupname">
<primaryFarmRefs>
<farm name="primaryfarmname" />
<farm ... />
...
</primaryFarmRefs>
<backupFarmRefs>
<farm name="backupfarmname" />
<farm ... />
...
</backupFarmRefs>
</equivalentFarmSet>
<equivalentFarmSet ... >
...
</equivalentFarmSet>
</equivalentFarmSets>
</userFarmMapping>
<userFarmMapping>
...
</userFarmMapping>
</userFarmMappings>
</resourcesWingConfiguration>
</resourcesWingConfigurations>
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

Use the following elements to define your configuration.

- **userFarmMapping**—Specifies groups of deployments and defines the load balancing and failover behavior between those deployments. Identifies deployments to be used for disaster recovery. Controls user access to resources by mapping Microsoft Active Directory user groups to the specified groups of deployments.
- **groups**—Specifies the names and security identifiers (SIDs) of Active Directory user groups to which the associated mapping applies. User group names must be entered in the format *domain\usergroup*. Where more than one group is listed, the mapping is only applied to users who are members of all the specified groups. To enable access for all Active Directory user accounts, set the group name & sid to **everyone**.
- **equivalentFarmSet**—Specifies a group of equivalent deployments providing resources to be aggregated for load balancing or failover, plus an optional associated group of disaster recovery deployments.

  The **loadBalanceMod**e attribute determines the allocation of users to deployments. Set the value of the **loadBalanceMode** attribute to **LoadBalanced** to randomly assign users to deployments in the equivalent deployment set, evenly distributing users across all the available deployments. When the value of the **loadBalanceMode** attribute is set to **Failover**, users are connected to the first available deployment in the order in which they are listed in the configuration, minimizing the number of deployments in use at any given time. Specify names for aggregation groups to identify equivalent deployment sets providing resources to be aggregated. Resources provided by equivalent deployment sets belonging to the same aggregation group are aggregated. To specify that the deployments defined in a particular equivalent deployment set should not be aggregated with others, set the aggregation group name to the empty string ”“.

  The **identical** attribute accepts the values **true** and **false**, and specifies whether all deployments within an equivalent deployment set provide exactly the same set of resources. When the deployments are identical, StoreFront enumerates the user’s resources from just one primary deployment in the set. When the deployments provide overlapping but not identical resources, StoreFront enumerates from each deployment to obtain the full set of resources available to a user. Load balancing (at launch time) can take place whether or not the deployments are identical. The default value for the **identical** attribute is **false**, although it is set to **true** when StoreFront is upgraded to avoid altering the pre-existing behavior following an upgrade.
- **primaryFarmRefs**—Specifies a set of equivalent Citrix Virtual Apps and Desktops sites where some or all of the resources match. Enter the names of deployments that you have already added to the store. The names of the deployments you specify must match exactly the names you entered when you added the deployments to the store.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- **optimalGatewayForFarms**—Specifies groups of deployments and defines the optimal Citrix Gateway appliances for users to access resources provided by these deployments. Typically, the optimal appliance for a deployment is colocated in the same geographical location as that deployment. You only need to define optimal Citrix Gateway appliances for deployments where the appliance through which users access StoreFront is not the optimal appliance.

Configure subscription synchronization

To configure periodic pull synchronization of users' subscriptions from stores in different StoreFront deployments, you execute Windows PowerShell commands.

> **Note:**
>
> The StoreFront and PowerShell consoles cannot be open at the same time. Always close the StoreFront admin 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 and that the Delivery Controller names are case sensitive. 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, *XenDesktop7* is different to *Xendesktop7*.

1. Use an account with local administrator permissions to start the Windows PowerShell ISE.
2. To configure synchronization to occur at a particular time every day, run the following command.

```
$RepeatMinutes = 30
Add-STFSubscriptionSynchronizationSchedule -StartTime (Get-Date -
    Format t) -RepeatMinutes $RepeatMinutes

<!--NeedCopy-->
```

Use **-StartTime** to specify when the synchronization schedule starts. Using **(Get-Date -Format t)** starts the synchronization schedule immediately, whereas specifying *10:00* starts the repeating schedule at the specified time.

-RepeatMinutes sets the frequency the schedule will run at. For example, *30* runs the schedule every half hour, and *180* runs the schedule every 3 hrs. We recommend that you stagger pull schedules to avoid two server groups attempting to pull subscription data from each other at

© 1999–2022 Citrix Systems, Inc. All rights reserved.

the same time. For example, a schedule to pull data from each server group every 60 mins would be configured as follows. Server group 1 pulls data from server group 2 at 01:00, 02:00, 03:00 and so on. Server group 2 pulls data from server group 1 at 01:30, 02:30, 03:30 and so on.

3. To specify the remote StoreFront deployment containing the store to be synchronized, type the following command. You must configure this for each data center where a StoreFront server group resides so it can pull subscription data from other remote datacenters. See the following US and UK datacenter examples:

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

```
$StoreObject = Get-STFStoreService -SiteID 1 -VirtualPath "/Citrix/Store"
Add-STFSubscriptionSynchronizationSource -FriendlyName "SyncFromUKStore" -StoreService $StoreObject -RemoteStoreFrontAddress "UKloadbalancedStoreFront.example.com"
<!--NeedCopy-->
```

   - 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"
<!--NeedCopy-->
```

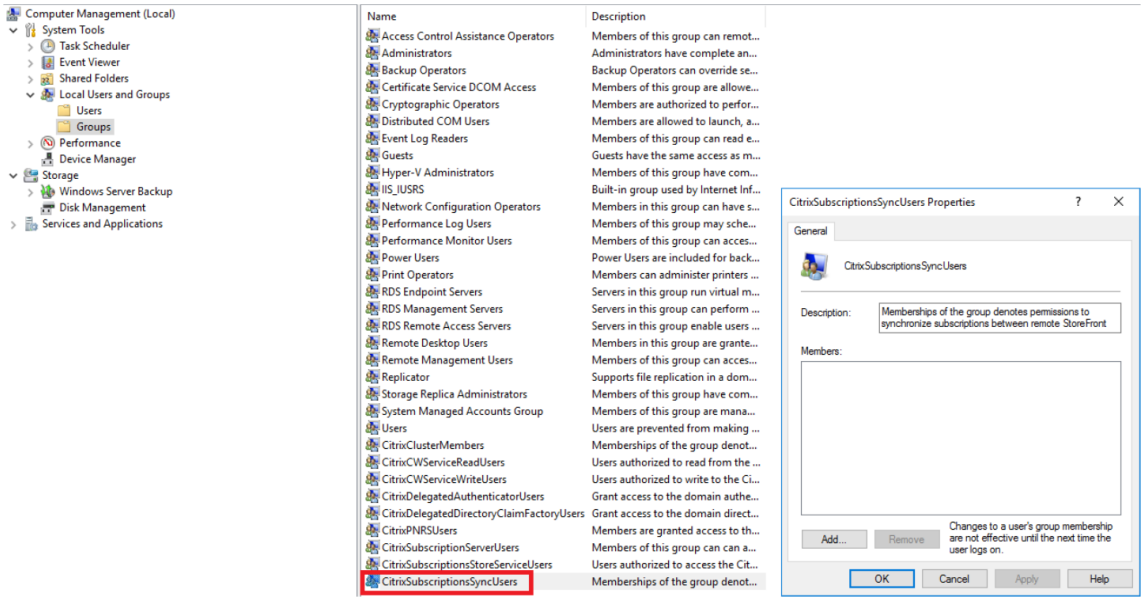
   where *FriendlyName* is a name that helps you identify the remote deployment and *RemoteStoreFrontAddress* is the FQDN of the StoreFront server or load-balanced server group for the remote deployment. To synchronize application subscriptions between two or more stores, all stores which are to be synchonised 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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc772524(v=ws.11).



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

```
Publish-STFServerGroupConfiguration
<!--NeedCopy-->
```

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

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

```
Clear-STFSubscriptionSynchronizationSchedule
<!--NeedCopy-->
```

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

```
Remove-STFSubscriptionSynchronizationSource -FriendlyName ”
    SyncFromUKStore”
<!--NeedCopy-->
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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
<!--NeedCopy-->
```

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

```
Get-STFSubscriptionSynchronizationSchedule
<!--NeedCopy-->
```

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

```
Get-STFSubscriptionSynchronizationSource
<!--NeedCopy-->
```

Configure optimal HDX routing for a store

The difference between a farm and a zone when defining optimal gateway mappings for a store

In StoreFront versions released before 3.5, you could map an optimal gateway only to a farm or farms. The concept of zones enables you to divide a Citrix Virtual Apps and Desktops deployment into zones based on the data center or geographic location where the Citrix Virtual Apps and Desktops controllers and published resources reside. Define zones in Citrix Virtual Apps and Desktops Studio. StoreFront interoperates with Citrix Virtual Apps and Desktops, and any zones defined in StoreFront must exactly match the zone names defined in Citrix Virtual Apps and Desktops.

StoreFront also allows you to create an optimal gateway mapping for all of the Delivery Controllers located in the defined zone. Mapping a zone to an optimal gateway is almost identical to creating mappings using farms, with which you might already be familiar. The only difference is that zones typically represent much larger containers with many more Delivery Controllers. You do not need to add every Delivery Controller to an optimal gateway mapping. To place the controllers into the desired zone, you need only tag each Delivery Controller with a zone name that matches a zone already defined in Citrix Virtual Apps and Desktops. You can map an optimal gateway to more than one zone, but typically you should use a single zone. A zone usually represents a data center in a geographic

© 1999–2022 Citrix Systems, Inc. All rights reserved.

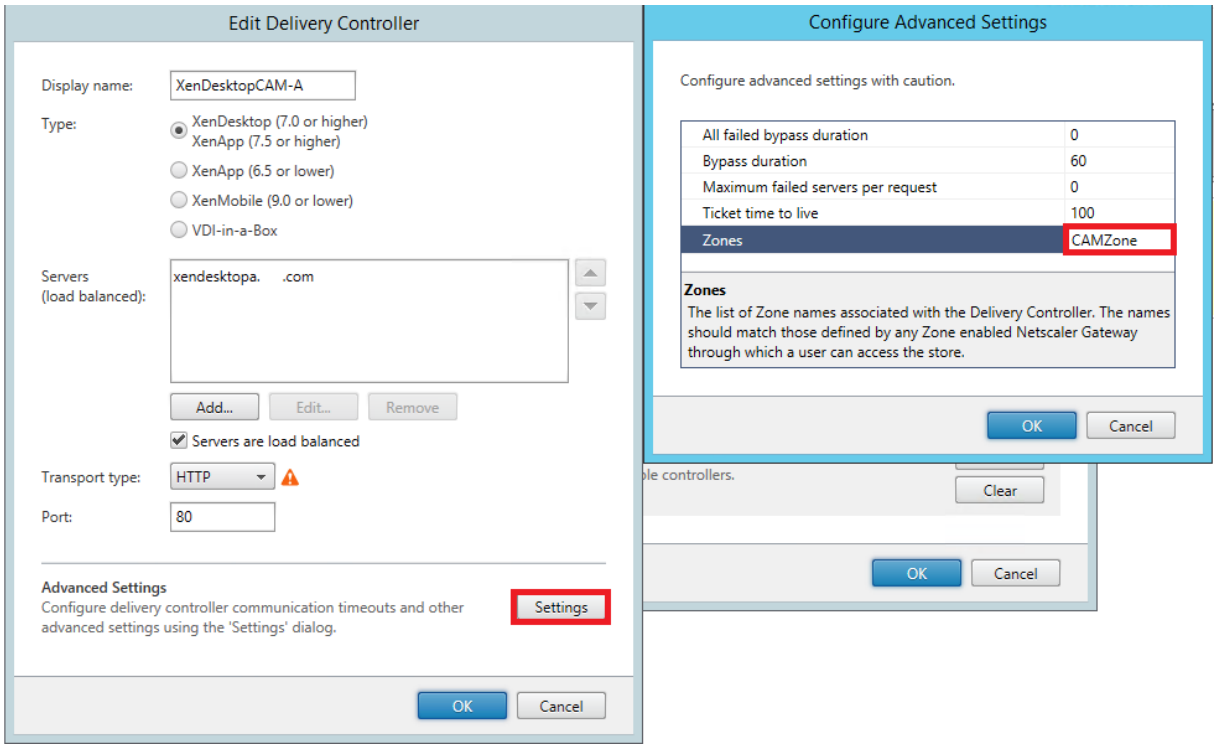
location. It is expected that each zone has at least one optimal Citrix Gateway that is used for HDX connections to resources within that zone.

For more information about zones, see Zones.

Place a Delivery Controller into a zone

Set the zone attribute on every Delivery Controller you wish to place within a Zone.

1. On the Windows **Start** screen or Apps screen, locate and click the **Citrix StoreFront** tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and click **Manage Delivery Controllers** in the **Actions** pane.
3. Select a controller, click **Edit**, and then click **Settings** on the **Edit Delivery Controller** screen.
4. On the **Zones** row, click in the second column.
5. Click **Add** on the **Delivery Controller Zone Names** screen and then add a zone name.



Configure optimal Citrix Gateway routing to optimize the handling of ICA connection routing from the HDX engine to published resources such as XenDesktop VDAs or Citrix Virtual Apps and Desktops published applications using StoreFront. Typically, the optimal gateway for a site is colocated in the same geographical location.

You need only define optimal Citrix Gateway appliances for deployments where the appliance through which users access StoreFront is not the optimal gateway. If launches should be directed back through the gateway making the launch request, StoreFront does this automatically.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Example scenario using farms

1 x UK Gateway -> 1 x UK StoreFront

- UK Apps and Desktops local
- US Apps and Desktops used only for UK failover

1 x US Gateway -> 1 x US StoreFront

- US Apps and Desktops local
- UK Apps and Desktops used only for US failover

A UK gateway provides remote access to UK hosted resources such as apps and desktops using a UK StoreFront.

The UK StoreFront has both a UK-based and US-based Citrix Gateway defined and UK and US controllers in its Delivery Controller list. UK users access remote resources through their geographically colocated gateway, StoreFront, and farms. If their UK resources become unavailable, they can connect to US resources as a temporary failover alternative.

Without optimal gateway routing all ICA launches would pass through the UK gateway that made the launch request regardless of where the resources are geographically located. By default, gateways used to make launch requests are identified dynamically by StoreFront when the request is made. Optimal gateway routing overrides this and forces US connections through the gateway closest to the US farms that provides apps and desktops.

> **Note:**
>
> You can map only one optimal gateway per site for each StoreFront store.

Example scenario using zones

1 x CAMZone -> 2 x UK StoreFronts

- Cambridge, UK: Apps and Desktops
- Fort Lauderdale, Eastern US: Apps and Desktops
- Bangalore, India: Apps and Desktops

1 x FTLZone -> 2 x US StoreFronts

- Fort Lauderdale, Eastern US: Apps and Desktops
- Cambridge, UK: Apps and Desktops
- Bangalore, India: Apps and Desktops

1 x BGLZone -> 2 x IN StoreFronts

- Bangalore, India: Apps and Desktops
- Cambridge, UK: Apps and Desktops
- Fort Lauderdale, Eastern US: Apps and Desktops

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Figure 1. Suboptimal gateway routing

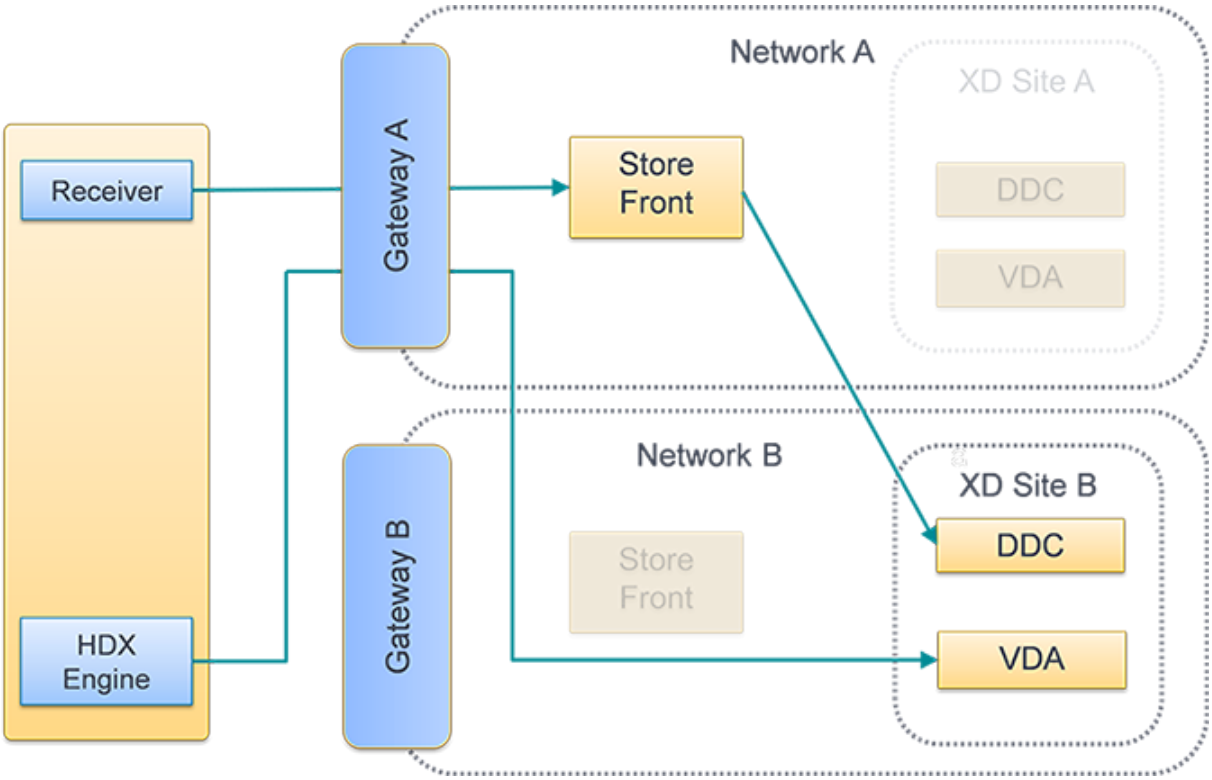
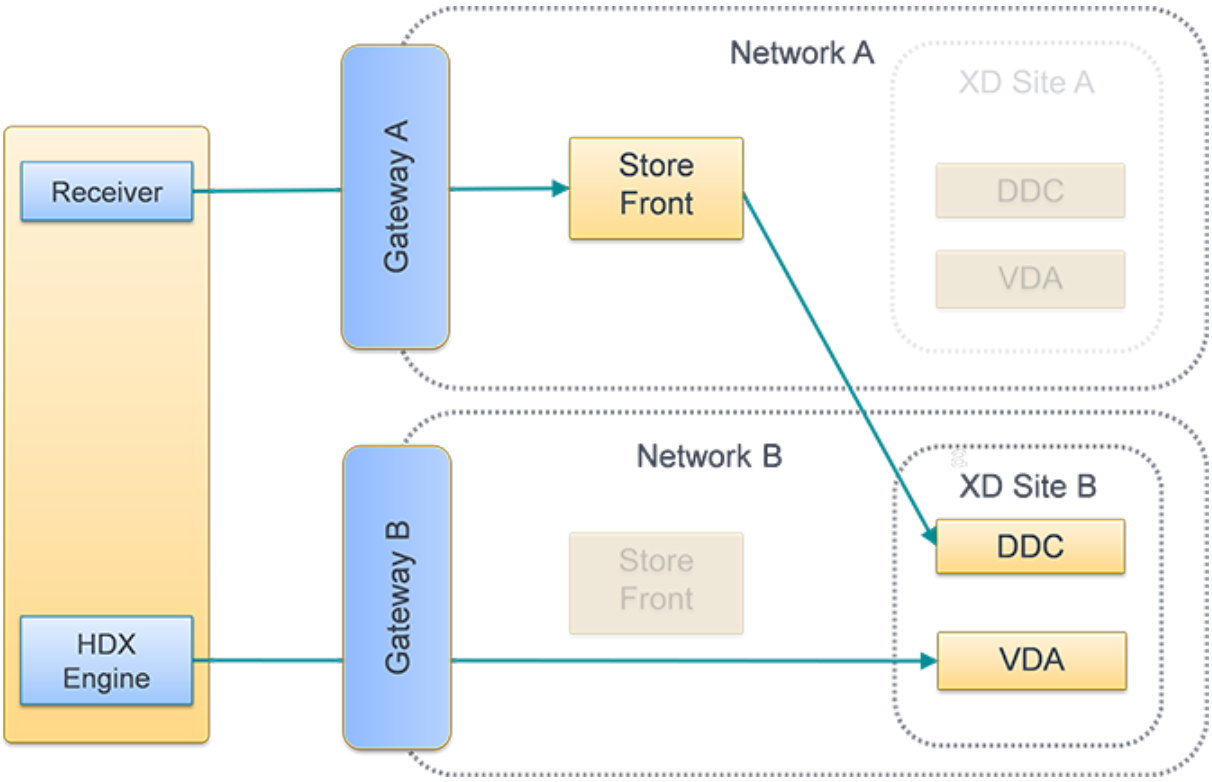


Figure 2. Optimal gateway routing

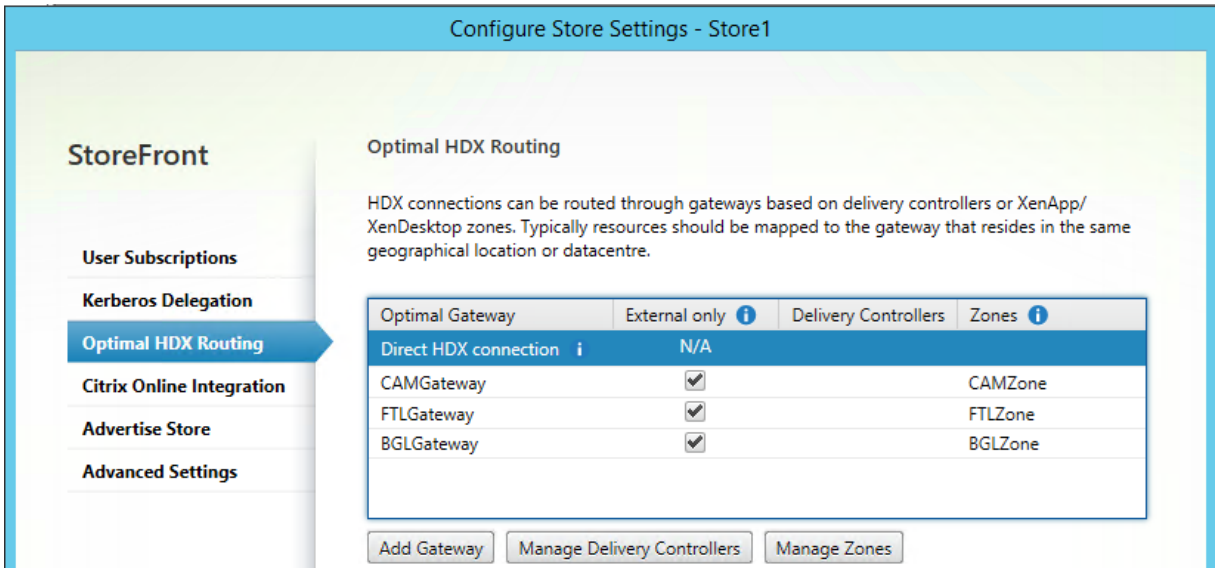


© 1999–2022 Citrix Systems, Inc. All rights reserved.

Use the Citrix StoreFront management console

After you have configured separate Citrix Gateway appliances for your deployments, you can define the optimal appliance for users to access each of the deployments.

1. On the Windows **Start** screen or **Apps** screen, locate and click the **Citrix StoreFront** tile.
2. 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**.
3. On the **Settings** > **Optimal HDX Routing** page, select a gateway.
4. If you select the **External Only** check box, it is equivalent to **-enabledOnDirectAccess = false** and Direct HDX Connection is equivalent to using **Set-DSFarmsWithNullOptimalGateway** for farms or zones.



Add a new gateway

One of the options in the previous procedure is to **Add gateway**. After you choose **Add gateway**, the Add Citrix Gateway screen displays.

1. On the **General Settings** screen, complete the Display name, Citrix Gateway URL, and Usage or Role settings to configure access to stores through Citrix Gateway for users connecting from public networks. Remote access through a Citrix Gateway cannot be applied to unauthenticated stores.
2. On the **Secure Ticket Authority (STA)** screen, complete the options displayed. STA is hosted on Citrix Virtual Apps and Desktops servers and issues session tickets in response to connection requests. These session tickets form the basis of authentication and authorization for access to Citrix Virtual Apps and Desktops resources.
3. On the **Authentication Settings** screen, enter the settings that specify how the remote user provides authentication credentials.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Use PowerShell to configure optimal Citrix Gateway routing for a store

PowerShell API parameters

-SiteId (Int)—Site ID within IIS. This is typically 1 for the site in IIS where StoreFront is installed by default.

-ResourcesVirtualPath (String)—Path to the store that is to be configured to have a farm to optimal gateway mapping.

Example: "/Citrix/Store"

-GatewayName (String)—Name given to identify the Citrix Gateway within StoreFront.

Example 1: ExternalGateway

Example 2: InternalGateway

-Hostnames (String Array)—Specifies the fully qualified domain name (FQDN) and port of the optimal Citrix Gateway appliance.

Example1 for standard vServer port 443: `gateway.example.com`

Example2 for nonstandard vServer port 500: `gateway.example.com:500`

-Farms (String Array)—Specifies a set of (typically colocated) Citrix Virtual Apps and Desktops deployments that share a common optimal Citrix Gateway appliance. A farm can contain one or more Delivery Controllers that provide published resources.

You can configure a Citrix Virtual Desktops Site in StoreFront under Delivery Controllers as "XenDesktop". This represents a single farm. This could contain multiple Delivery Controllers in its failover list.

Example: "XenDesktop"

`XenDesktop-A.example.com`

`XenDesktop-B.example.com`

`XenDesktop-C.example.com`

-Zones (String Array)—Specifies a data center or data centers containing many Delivery Controllers. This requires you tag Delivery Controller objects in StoreFront with the appropriate zone to which you want to allocate them.

-staUrls (String Array)—Specifies the URLs for Citrix Virtual Apps and Desktops servers running the Secure Ticket Authority (STA). If using multiple farms, list the STA servers on each using a comma separated list:

Example: `http://xenapp-a.example.com/scripts/ctxsta.dll,http://xendesktop-a.example.com/scripts/ctxsta.dll`

-StasUseLoadBalancing (Boolean)—Set to **true**: randomly obtains session tickets from all STAs, evenly distributing requests across all the STAs. Set to **false**: users are connected to the first available

© 1999–2022 Citrix Systems, Inc. All rights reserved.

STA in the order in which they are listed in the configuration, minimizing the number of STAs in use at any given time.

-StasBypassDuration—Set the time period, in hours, minutes, and seconds, for which an STA is considered unavailable after a failed request.

Example: 02:00:00

-EnableSessionReliability (Boolean)—Set to **true**: keeps disconnected sessions open while Receiver attempts to reconnect automatically. If you configured multiple STAs and want to ensure that session reliability is always available, set the value of the useTwoTickets attribute to **true** to obtain session tickets from two different STAs in case one STA becomes unavailable during the session.

-UseTwoTickets (Boolean)—Set to **true**: obtains session tickets from two different STAs in case one STA becomes unavailable during the session. Set to **false**: uses only a single STA server.

-EnabledOnDirectAccess (Boolean)—Set to **true**: ensures that when local users on the internal network log on to StoreFront directly, connections to their resources are still routed through the optimal appliance defined for the farm. Set to **false**: connections to resources are not routed through the optimal appliance for the farm unless users access StoreFront through a Citrix Gateway.

When PowerShell scripts span multiple lines such as shown below, each line must end with the backtick (‘) character.

> **Tip:**
>
> Citrix recommends copying any code examples into the Windows PowerShell Integrated Scripting Environment (ISE) to validate the Powershell code using the format checker before you run it.

Configure an optimal gateway for a farm

> **Note:**
>
> Configuration of Optimal HDX routing with the old PowerShell cmdlet **Set-DSOptimalGatewayForFarms**, does not work.
>
> To work around this issue:
>
> 1. Configure a global gateway with the settings you want for Optimal HDX routing using the **Add-DSGlobalV10Gateway** command and provide default values for the authentication settings.
> 2. Use the **Add-DSStoreOptimalGateway** command to add the optimal gateway configuration.
>
> Example:
>
> ```
> Add-DSGlobalV10Gateway -Id 2eba0524-af40-421e-9c5f-a1ccca80715f -Name
> ```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
LondonGateway -Address "http://example"-Logon Domain -SecureTicketAuthorityUrls
 @("http://staurl1", "http://staurl2")

Add-DSStoreOptimalGateway -SiteId 1 -VirtualPath /Citrix/Store1 -GatewayId
 2eba0524-af40-421e-9c5f-a1ccca80715f -Farms @("Controller")-EnabledOnDirectAccess
 $true
```

Example

Create or overwrite Optimal Gateway For Farms mappings for the store **Internal**.

```
& "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\ImportModules.
    ps1"

Set-DSOptimalGatewayForFarms -SiteId 1 \`

-ResourcesVirtualPath /Citrix/Internal \`
\-GatewayName "gateway1" \`
\-Hostnames "gateway1.example.com:500" \`
\-Farms "XenApp","XenDesktop" \`
\-StaUrls "https://xenapp.example.com/scripts/ctxsta.dll","https://
    xendesktop.example.com/scripts/ctxsta.dll" \`
\-StasUseLoadBalancing:$false \`
\-StasBypassDuration 02:00:00 \`
\-EnableSessionReliability:$false \`
-UseTwoTickets:$false \`
\-EnabledOnDirectAccess:$true
<!--NeedCopy-->
```

Configure an optimal gateway for a zone

Example

Create or overwrite Optimal Gateway For Farms mappings for the zone **CAMZone**.

```
**& "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\ImportModules
    .ps1" **

**Set-DSOptimalGatewayForFarms -SiteId 1 \`**

**-ResourcesVirtualPath /Citrix/Internal \`
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
\-GatewayName "gateway1" \`
\-Hostnames "gateway1.example.com:500" \`
\-Zones "CAMZone" \`
\-StaUrls "https://xenapp.example.com/scripts/ctxsta.dll","https://
    xendesktop.example.com/scripts/ctxsta.dll" \`
\-StasUseLoadBalancing:$false \`
\-StasBypassDuration 02:00:00 \`
\-EnableSessionReliability:$false \`
\-UseTwoTickets:$false \`
\-EnabledOnDirectAccess:$true   **
<!--NeedCopy-->
```

Example

This script returns all Optimal Gateway For Farms mappings for the store **Internal**.

```
Get-DSOptimalGatewayForFarms -SiteId 1 -ResourcesVirtualPath "/Citrix/
Internal"
```

Example

Remove all optimal gateway for farms mappings for store called **Internal**.

```
Remove-DSOptimalGatewayForFarms -SiteId 1 -ResourcesVirtualPath "/Citrix/
Internal"
Configure direct HDX connections for farms
```

Example

This script prevents all ICA launches from passing through a gateway for the list of specified farms for the store called **Internal**.

```
Set-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath /Citrix/
Store -Farms "Farm1","Farm2"
```

Example

This script returns all farms that are configured to prevent ICA launches from passing through a gateway for a store called **Internal**.

```
Get-DSFarmsWithNullOptimalGateway -SiteId 1 -ResourcesVirtualPath "/Citrix/
Internal"
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

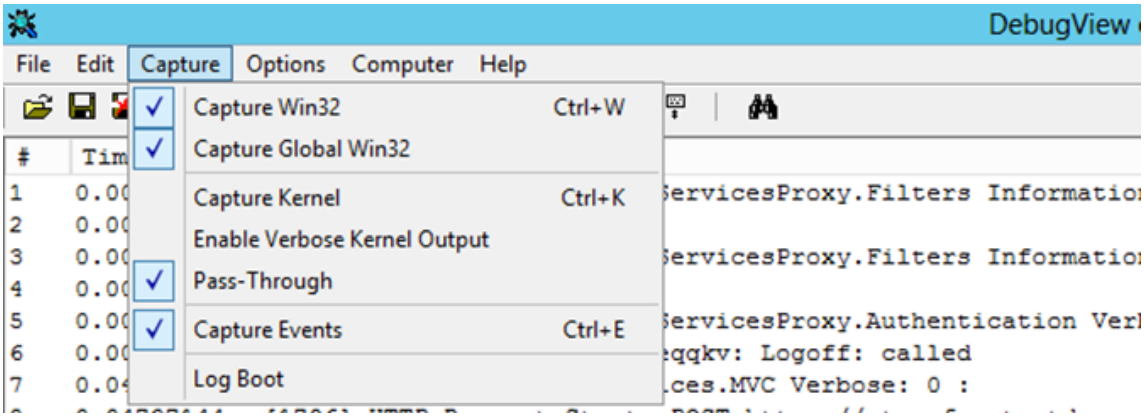
Determine if your Optimal Gateway For Farms mappings are being used by StoreFront

1. Enable StoreFront tracing on all server group nodes using PowerShell by running:

```
& "$Env:PROGRAMFILES\Citrix\Receiver StoreFront\Scripts\
    ImportModules.ps1"`

\#Traces output is to c:\Program Files\Citrix\Receiver Storefront\
    admin\trace\
Set-DSTraceLevel -All -TraceLevel Verbose
<!--NeedCopy-->
```

2. Open the Debug View tool on the desktop of a StoreFront server. If you are using a storefront server group, you might have to do this on all nodes to ensure you obtain traces from the node that receives the launch request.

3. Enable Capture Global Win32 events.



4. Save the trace output as a .log file and open the file with Notepad. Search for the log entries shown in the example scenarios below.

5. Turn tracing off afterwards, as it consumes a lot of disk space on your StoreFront servers.

```
Set-DSTraceLevel -All -TraceLevel Off
```

Tested optimal gateway scenarios

```
-  External client logs on **Gateway1**. Launch is directed through the
    designated optimal gateway **Gateway2** for the farm **Farm2**.

    `Set-DSOptimalGatewayForFarms -onDirectAccess=false`

    Farm2 is configured to use the optimal gateway Gateway2.
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```

    Farm2 has optimal gateway on direct access disabled.

    The optimal gateway Gateway2 will be used for the launch.

-  Internal client logs on using StoreFront. Launch is directed through
    the designated optimal gatewayGateway1 for the farm Farm1.

    `Set-DSOptimalGatewayForFarms -onDirectAccess=true`

    No dynamically identified gateway in request. StoreFront was
       contacted directly.

    Farm1 is configured to use the optimal gateway Gateway1.

    Farm1 has optimal gateway on direct access enabled.

    The optimal gateway Gateway1 will be used for the launch.

-  Internal client logs on using Gateway1. Launches of resources on
    Farm1 are prevented from passing through any gateway and StoreFront
    is contacted directly.

    `Set-DSFarmsWithNullOptimalGateway`

    Dynamically identified gateway in request: Gateway1

    Farm1 is configured to not use a gateway. No gateway will be used
       for launch.
```

Integrate with Citrix Gateway and Citrix ADC

April 29, 2020

Use Citrix Gateway with StoreFront to provide secure remote access for users outside the corporate network and Citrix ADC to provide load balancing.

Plan gateway and server certificate usage

Integrating StoreFront with Citrix Gateway and Citrix ADC requires a plan for gateway and server certificate usage. Consider which Citrix components are going to require server certificate(s) within your deployment:

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- Plan to obtain certificates for Internet-facing servers and gateways from external certificate authorities. Client devices may not automatically trust certificates signed by an internal certificate authority.
- Plan for both external and internal server names. Many organizations have separate namespaces for internal and external use—such as `example.com` (external) and `example.net` (internal). A single certificate can contain both of these kinds of name by using the Subject Alternative Name (SAN) extension. This is not normally recommended. A public certificate authority will only issue a certificate if the top-level domain (TLD) is registered with IANA. In this case, some commonly used internal server names (such as example.local) cannot be used, and separate certificates for external and internal names are required anyway.
- Use separate certificates for external and internal servers, where possible. A gateway may support multiple certificates, either by binding a different certificate to each interface.
- Avoid sharing certificates between Internet-facing and non-Internet-facing servers. These certificates are likely to be different—with different validity periods and different revocation policies than certificates issued by your internal certificate authorities.
- Share "wildcard" certificates only between equivalent services. Avoid sharing a certificate between different types of server (for example StoreFront servers, and other kinds of servers). Avoid sharing a certificate between servers which are under different administrative control, or which have different security policies. Typical examples of servers which provided equivalent service are:
  - A group of StoreFront servers and the server that performs load balancing between them.
  - A group of Internet-facing gateways within GSLB.
  - A group of Citrix Virtual Apps and Desktops controllers, which provide equivalent resources.
- Plan for hardware-secured private key storage. Gateways and servers, including some Citrix ADC models, can store the private key securely within a hardware security module (HSM) or Trusted Platform Module (TPM). For security reasons, these configurations are not usually intended to support sharing of certificates and their private keys, Consult the documentation for the component. If implementing GSLB with Citrix Gateway, this may require each gateway within GSLB to have an identical certificate, which contains all the FQDNs you wish to use.

For more information about securing your Citrix deployment, see the white paper End-To-End Encryption with Citrix Virtual Apps and Desktops and the Citrix Virtual Apps and Desktops Secure section.

Configure StoreFront Log On when authentication is disabled on Citrix Gateway VIP

Log on to StoreFront when authentication is disabled on Citrix Gateway VIP. This procedure works in two scenarios:

Internal networks. App launch fails from remote locations because STAs cannot be used when authentication is disabled on the Citrix Gateway if the X-Citrix-Gateway header is getting passed to Store-

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Front.

Citrix Receiver for Web. Receiver clients do not authenticate if authentication is not enabled at the Citrix Gateway VIP.

Changes on the StoreFront Server

1. Disable the **Require Token Consistency** field:
   - StoreFront 3.0
     a) Edit the `web.config` file for the store website. For example, if a StoreFront store name is `NoAuth`, the `web.config` file in the StoreFront server has the path **inetpub\wwwroot\Citrix\NoAuth**.

   a) Locate the following line in the `web.config` file and change the value from True to False.
   Before
   `<resourcesGateways requireTokenConsistency="true">`
   After
   `<resourcesGateways requireTokenConsistency="false">`

   > **Note:**
   >
   > On StoreFront 3.x, **Require Token Consistency** is a checkbox in the GUI. For more information, see Advanced store settings.

   b) Save the `web.config` file and then restart the IIS service.
2. Open the **Citrix StoreFront Management** console.
3. Click **Manage Receiver for Web Sites** for the web.
4. Select the corresponding Citrix Receiver for Web site, click **Configure** and then select **Authentication Methods**.
5. Ensure that the **Pass-through from Citrix Gateway** option is cleared.

> **Note:**
>
> Citrix Gateway and Enable Remote Access are assumed to be set up on the StoreFront server.

Changes on the Citrix Gateway

1. Open the Citrix Gateway virtual server.
2. Click the **Authentication** tab and ensure that **Enable Authentication** check-box is cleared.
3. Bind the corresponding session policy to the Citrix Gateway virtual server.
4. Test the connection.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Add a Citrix Gateway connection

April 29, 2020

Use the Add Citrix Gateway Appliance task to add Citrix Gateway deployments through which users can access your stores. You must enable the pass-through from Citrix Gateway authentication method before you can configure remote access to your stores through Citrix Gateway. For more information about configuring Citrix Gateway for StoreFront, see Using WebFront to Integrate with StoreFront.

> **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. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and in the Actions pane, click **Manage Citrix Gateways**.
3. Click **Add** and General Settings, 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 Receiver, 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.
4. Enter the URL of the virtual server or user logon point (for Access Gateway 5.0) for your deployment. Specify the product version used in your deployment.

   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.
5. If you are adding an Access Gateway 5.0 deployment, continue to Step 7. Otherwise, specify the subnet IP address of the Citrix Gateway appliance, if necessary. A subnet IP address is required for Access Gateway 9.3 appliances, but optional for more recent product versions.

   The subnet address is the IP address that Citrix Gateway uses to represent the user device when communicating with servers on the internal network. This can also be the mapped IP address of the Citrix Gateway appliance. Where specified, StoreFront uses the subnet IP address to verify that incoming requests originate from a trusted device.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

6. If you are adding an appliance running Citrix Gateway, select from the Logon type list the authentication method you configured on the appliance for Citrix Workspace app users.

   The information you provide about the configuration of your Citrix Gateway appliance is added to the provisioning file for the store. This enables Citrix Workspace app to send the appropriate connection request when contacting the appliance for the first time.

   - If users are required to enter their Microsoft Active Directory domain credentials, select Domain.
   - If users are required to enter a tokencode obtained from a security token, select Security token.
   - If users are required to enter both their domain credentials and a tokencode obtained from a security token, select Domain and security token.
   - If users are required to enter a one-time password sent by text message, select SMS authentication.
   - If users are required to present a smart card and enter a PIN, select Smart card.

   If you configure smart card authentication with a secondary authentication method to which users can fall back if they experience any issues with their smart cards, select the secondary authentication method from the Smart card fallback list. Continue to Step 8.

7. To add an Access Gateway 5.0 deployment, indicate whether the user logon point is hosted on a standalone appliance. If you are adding a cluster, click Next and continue to Step 9.

8. If you are configuring StoreFront for Citrix Gateway or a single Access Gateway 5.0 appliance, complete the Citrix Gateway authentication service URL in the Callback URL box. StoreFront automatically appends the standard portion of the URL. Click Next and continue to Step 11.

   Enter the internally accessible URL of the appliance. StoreFront contacts the Citrix Gateway authentication service to verify that requests received from Citrix Gateway originate from that appliance.

9. To configure StoreFront for an Access Gateway 5.0 cluster, list on the Appliances page the IP addresses or FQDNs of the appliances in the cluster and click Next.

10. On the Enable Silent Authentication page, list URLs for the authentication service running on the Access Controller servers. Add URLs for multiple servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence. Click Next.

    StoreFront uses the authentication service to authenticate remote users so that they do not need to re-enter their credentials when accessing stores.

11. For all deployments, if you are making resources provided by Citrix Virtual Apps and Desktops available in the store, list on the Secure Ticket Authority (STA) page URLs for servers running the STA. Add URLs for multiple STAs to enable fault tolerance, listing the servers in order of priority to set the failover sequence.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

The STA is hosted on Citrix Virtual Apps and Desktops servers and issues session tickets in response to connection requests. These session tickets form the basis of authentication and authorization for access to Citrix Virtual Apps and Desktops resources.

12. If you want Citrix Virtual Apps and Desktops to keep disconnected sessions open while Citrix Workspace app attempts to reconnect automatically, select the Enable session reliability check box. If you configured multiple STAs and want to ensure that session reliability is always available, select the Request tickets from two STAs, where available check box.

    When the Request tickets from two STAs, where available check box is selected, StoreFront obtains session tickets from two different STAs so that user sessions are not interrupted if one STA becomes unavailable during the course of the session. If, for any reason, StoreFront is unable to contact two STAs, it falls back to using a single STA.

13. Click **Create** to add details of your Citrix Gateway deployment. Once the deployment has been added, click **Finish**.

    For more information about updating the details of your deployments, see Configure Citrix Gateway connection settings.

To provide access to stores through Citrix Gateway, one internal beacon point and at least two external beacon points are required. Citrix Workspace app uses beacon points to determine whether users are connected to local or public networks and then selects the appropriate access method. By default, StoreFront uses the server URL or load-balanced URL of your deployment as the internal beacon point. The Citrix website and the virtual server or user logon point (for Access Gateway 5.0) URL of the first Citrix Gateway deployment you add are used as external beacon points by default. For more information about changing beacon points, see Configure beacon points.

To enable users to access your stores through Citrix Gateway, ensure that you configure remote user access for those stores.

Import a Citrix Gateway

October 22, 2020

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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

> **Note:**
>
> Citrix ADC appliances can only export gateway vServers created using the Citrix Virtual Apps and Desktops wizard.

- It must be possible for DNS to resolve, and for StoreFront to contact, all STA (Secure Ticket Authority) server URLs in the GatewayConfig.json file within the ZIP file generated by the Citrix ADC appliance.
- The GatewayConfig.json file within the ZIP file generated by the Citrix ADC appliance must contain the URL of an existing Citrix Receiver for Web site on the StoreFront server. Citrix ADC 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.

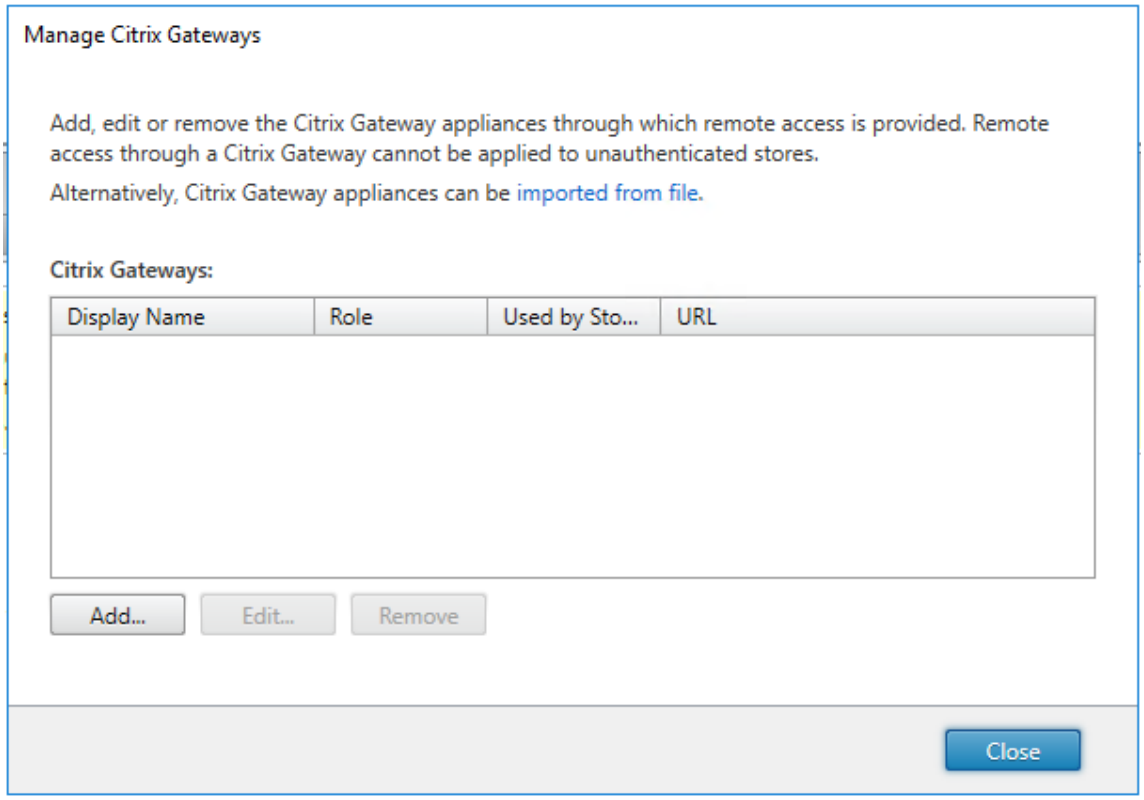
Import a Citrix Gateway using the console

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 ADC appliances, you must use multiple import files.

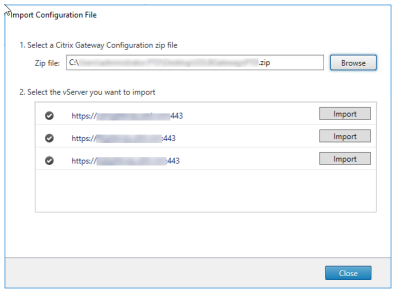
> Important:
>
> Citrix does not support manual editing of the configuration file exported from Citrix Gateway.

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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

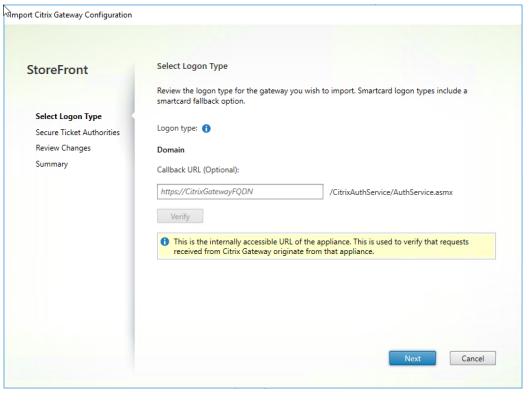


3. Browse to the Citrix Gateway virtual server configuration file.
4. A list of gateway vServers from the selected ZIP file is displayed. Select the gateway vServer you want to import and click **Import**. If you are repeating an import of a vServer, the Import button displays as Update. If you choose **Update**, you have the option later to overwrite or create a new gateway.



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 appliance 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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



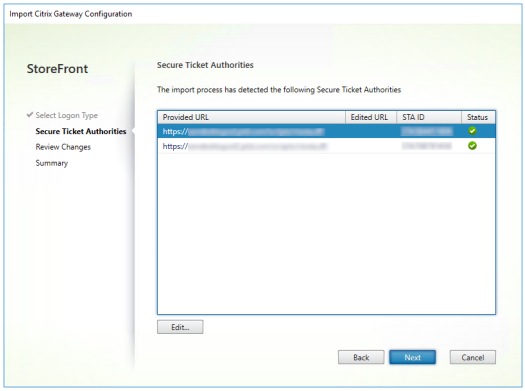
Logon type in console	LogonType in JSON file	Callback URL required
Domain	Domain	No
Domain and security token	DomainAndRSA	No
Security token	RSA	Yes
Smart card - no fallback	SmartCard	Yes
Smart card - domain	SmartCardDomain	Yes
Smart card - domain and security token	SmartCardDomainAndRSA	Yes
Smart card - security token	SmartCardRSA	Yes
Smart card - SMS authentication	SmartCardSMS	Yes
SMS authentication	SMS	Yes

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.

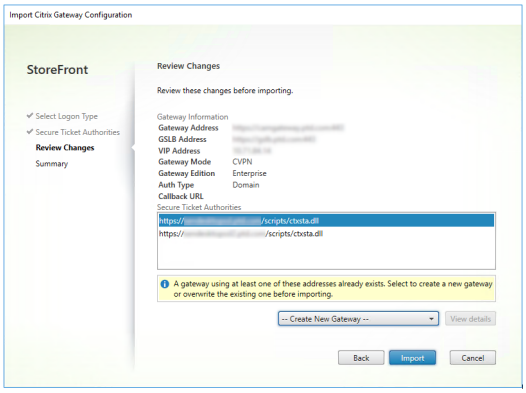
To use Smart Access, a Callback URL is required.

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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



8. Click **Next**.
9. Review the details of the import. If a gateway with the same gateway URL and port combination (GatewayURL:port) already exists, use the drop-down to select a gateway to overwrite it, or create a new gateway.



StoreFront uses the GatewayURL:port combination to determine whether a gateway you are trying to import matches an existing gateway that you may wish to update. If a gateway has a different GatewayURL:port combination then StoreFront treats it as a new gateway. This table of gateway settings shows which settings you can update.

Gateway Setting	Can be updated
Gateway URL:Port Combination	No
GSLB URL	Yes
Netscaler Trust Certificate & Thumbprint	Yes
Callback URL	Yes
Receiver for Web Site URL	Yes
Gateway Address/VIP	Yes
STA URL and STA ID	Yes

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Gateway Setting	Can be updated
All Logon Types	Yes

10. Click **Import**. If the StoreFront server is part of a server group, a message is displayed reminding you to propagate the imported gateway settings to the other servers in the group.
11. Click **Finish**.

To import another vServer configuration, repeat the steps above.

> **Note:**
>
> The default gateway for a store is the gateway that Citrix Workspace apps try to connect through unless they are configured to use a different gateway. If no gateways are configured for the store, the first gateway imported from the ZIP file will become the default gateway used by Citrix Workspace apps. Importing subsequent gateways does not change the default gateway already set for the store.

Import multiple Citrix Gateways using PowerShell

Read-STFNetScalerConfiguration

- Copy the ZIP file to the desktop of the currently logged on StoreFront administrator.
- Read the contents of the Citrix Gateway virtual server configuration file ZIP file into memory and look at the three gateways it contains using their index values.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"
<!--NeedCopy-->
```

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            :
GslbAddressUri         : https://gslb.example.com/
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
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
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
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
VipAddress              : 10.0.0.2
Stas                    : {
STA298854503, STA909374257 }

StaLoadBalance          : True
CertificateThumbprints : {
F549AFAA29EBF61E8709F2316B3981AD503AF387 }

GatewayAuthType         :SmartCard
GatewayEdition          : Enterprise
ReceiverForWebSites     : {
Citrix.StoreFront.Model.Roaming.NetScalerConfiguration.
    ReceiverForWebSite }

<!--NeedCopy-->
```

Import-STFNetScalerConfiguration without specifying a CallbackURL

Copy the ZIP file to the desktop of the currently logged in StoreFront administrator. Read in the Citrix Gateway configuration ZIP import package into memory and look at the three gateways it contains using their index values.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$env:
    USERPROFILE\desktop\GatewayConfig.zip"
<!--NeedCopy-->
```

Import three new gateways into StoreFront using the **Import-STFNetScalerConfiguration** cmdlet and specifying the gateway indexes you require. Using the **-Confirm:$False** parameter prevents the Powershell GUI from prompting you to allow every gateway to be imported. Remove this if you wish to carefully import one gateway at a time.

```
```
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 0 -Confirm:$False
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 1 -Confirm:$False
Import-STFNetScalerConfiguration -Configuration $ImportedGateways -
    GatewayIndex 2 -Confirm:$False
<!--NeedCopy--> ```
```

© 1999–2022 Citrix Systems, Inc. All rights reserved. 
```

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 $ImportedGateways -GatewayIndex 1 -CallbackUrl "https://emeagatewaycb.example.com:444 -Confirm:$False

Import-STFNetScalerConfiguration -Configuration $ImportedGateways -GatewayIndex 2 -CallbackUrl "https://emeagatewaycb.example.com:445 -Confirm:$False
<!--NeedCopy-->
```

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

Import three new gateways into StoreFront using the **Import-STFNetScalerConfiguration** cmdlet and specify a callback URL of your choice using the -callbackURL parameter.

```
$ImportedGateways = Read-STFNetScalerConfiguration -path "$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
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Configure Citrix Gateway connection settings

February 12, 2021

The tasks below enable you to update details of the Citrix Gateway deployments through which users access your stores. For more information about configuring Citrix Gateway for StoreFront, see Using WebFront to Integrate with StoreFront.

If you make any changes to your Citrix Gateway deployments, ensure that users who access stores through these deployments update Citrix Workspace app with the modified connection information. Where a Citrix Receiver for Web site is configured for a store, users can obtain an updated Citrix Workspace app provisioning file from the site. Otherwise, you can export a provisioning file for the store and make this file available to your users.

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.

Change general Citrix Gateway settings

Use the Change General Settings task to modify the Citrix Gateway deployment names shown to users and to update StoreFront with changes to the virtual server or user logon point URL, and the deployment mode of your Citrix Gateway infrastructure.

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. Select the Stores node in the left pane of the Citrix StoreFront management console and pane, click Manage Citrix Gateways.
3. Specify a 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.
4. Enter the URL of the virtual server or user logon point (for Access Gateway 5.0) for your deployment. Specify the product version used in your deployment.

   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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

5. If your deployment is running Access Gateway 5.0, continue to Step 7. Otherwise, specify the subnet IP address of the Citrix Gateway appliance, if necessary.

   The subnet address is the IP address that Citrix Gateway uses to represent the user device when communicating with servers on the internal network. This can also be the mapped IP address of the Citrix Gateway appliance. Where specified, StoreFront uses the subnet IP address to verify that incoming requests originate from a trusted device.

6. If your appliance is running Citrix Gateway, select from the Logon type list the authentication method you configured on the appliance for Citrix Workspace app users.

   The information you provide about the configuration of your Citrix Gateway appliance is added to the provisioning file for the store. This enables Citrix Workspace app to send the appropriate connection request when contacting the appliance for the first time.

   - If users are required to enter their Microsoft Active Directory domain credentials, select Domain.
   - If users are required to enter a tokencode obtained from a security token, select Security token.
   - If users are required to enter both their domain credentials and a tokencode obtained from a security token, select Domain and security token.
   - If users are required to enter a one-time password sent by text message, select SMS authentication.
   - If users are required to present a smart card and enter a PIN, select Smart card.

   If you configure smart card authentication with a secondary authentication method to which users can fall back if they experience any issues with their smart cards, select the secondary authentication method from the Smart card fallback list.

7. If your deployment consists of Citrix Gateway, or a single Access Gateway 5.0 appliance, complete the Citrix Gateway authentication service URL in the Callback URL box. StoreFront automatically appends the standard portion of the URL.

   Enter the internally accessible URL of the appliance. StoreFront contacts the Citrix Gateway authentication service to verify that requests received from Citrix Gateway originate from that appliance.

Manage Access Gateway 5.0 appliances

Use the Manage Appliances task to add, edit, or remove from StoreFront the IP addresses or FQDNs of the appliances in your Access Gateway 5.0 cluster.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Enable silent user authentication through Access Controller

Use the Enable Silent Authentication task to add, edit, or remove URLs for the authentication service running on the Access Controller servers for your Access Gateway 5.0 cluster. Enter URLs for multiple servers to enable fault tolerance, listing the servers in order of priority to set the failover sequence. StoreFront uses the authentication service to authenticate remote users so that they do not need to re-enter their credentials when accessing stores.

Manage Secure Ticket Authorities

Use the Secure Ticket Authority task to update the list of Secure Ticket Authorities (STAs) from which StoreFront obtains user session tickets and to configure session reliability. The STA is hosted on Citrix Virtual Apps and Desktops servers and issues session tickets in response to connection requests. These session tickets form the basis of authentication and authorization for access to Citrix Virtual Apps and Desktops resources.

1. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. Select the Stores node in the left pane of the Citrix StoreFront management console and, in the results pane, select a Citrix Gateway deployment. In the Actions pane, click Manage Citrix Gateways.
3. Click Add to enter the URL for a server running the STA. Specify URLs for multiple STAs to enable fault tolerance, listing the servers in order of priority to set the failover sequence. To modify a URL, select the entry in the Secure Ticket Authority URLs list and click Edit. Select a URL in the list and click Remove to stop StoreFront obtaining session tickets from that STA.

   In a Citrix Virtual Apps and Desktops *on-premises* environment, **Shared secret** lets you allow only approved StoreFront machines to communicate with Secure Ticket Authority (STA) by specifying a key. For information about key generation and configuration, see Manage security keys.

   In a Citrix Virtual Apps and Desktops *service* environment, **Shared secret** lets you allow only approved StoreFront machines to communicate with Citrix Cloud by specifying a key. For information about key generation, see Manage security keys.
4. If you want Citrix Virtual Apps and Desktops to keep disconnected sessions open while Citrix Workspace app attempts to reconnect automatically, select the Enable session reliability check box. If you configured multiple STAs and want to ensure that session reliability is always available, select the Request tickets from two STAs, where available check box.

   When the Request tickets from two STAs, where available check box is selected, StoreFront obtains session tickets from two different STAs so that user sessions are not interrupted if one STA becomes unavailable during the course of the session. If, for any reason, StoreFront is unable to contact two STAs, it falls back to using a single STA.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Remove Citrix Gateway deployments

In the **Actions** pane, use the Remove task from **Manage Citrix Gateways** to delete the details of a Citrix Gateway deployment from StoreFront. Once a Citrix Gateway deployment is removed, users are no longer be able to access stores through that deployment.

Load balancing with Citrix ADC appliance

October 22, 2020

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 Citrix ADC appliance to load balance incoming requests from Citrix Workspace app, and Citrix Receiver for Web between the StoreFront nodes in the server group. This article also shows you how to configure StoreFront Monitor for use with a Citrix ADC appliance.

The examples in this section have been tested in the following environment:

- Four Windows Server 2012 R2 StoreFront 3.x nodes in a single server group.
- One Citrix ADC appliance 12.1 load balancer configured for Least Connection and CookieInsert "sticky" load balancing.
- One Windows 10 test client with Citrix Workspace app installed.

Server certificate requirements for the load balanced deployment if you intend to use HTTPS

Review the section Plan gateway and server certificate usage.

Consider the following options before purchasing a certificate from a commercial certificate authority or issuing one from your enterprise certificate authority.

- **Option 1:** Use a **.example.com* wildcard certificate on both the Citrix ADC appliance load balancing vServer and on the StoreFront server group nodes. This simplifies the configuration and allows you to add extra StoreFront servers in the future without the need to replace the certificate.
- **Option 2**: Use a certificate including Subject Alternative Names (SANs) on both the Citrix ADC appliance load balancing vServer and on the StoreFront server group nodes. Extra SANs within the certificate that match all of StoreFront server fully qualified domain names (FQDNs) are optional, but recommended, as this allows greater flexibility in the StoreFront deployment. Include a SAN for email-based discovery discoverReceiver.example.com.

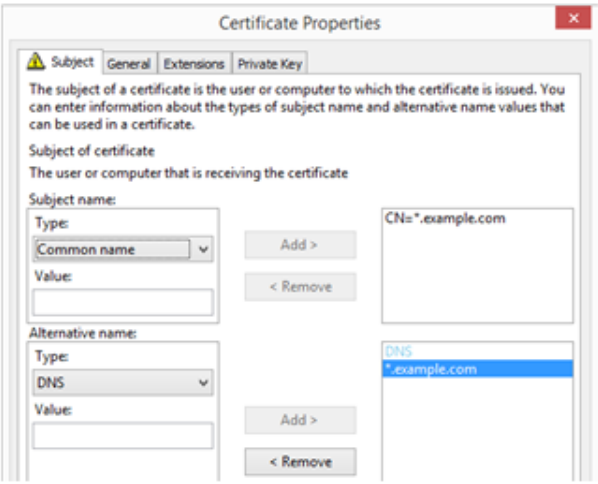
For details of email-based discovery configuration, see http://blogs.citrix.com/2013/04/01/configuring-email-based-account-discovery-for-citrix-receiver/.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

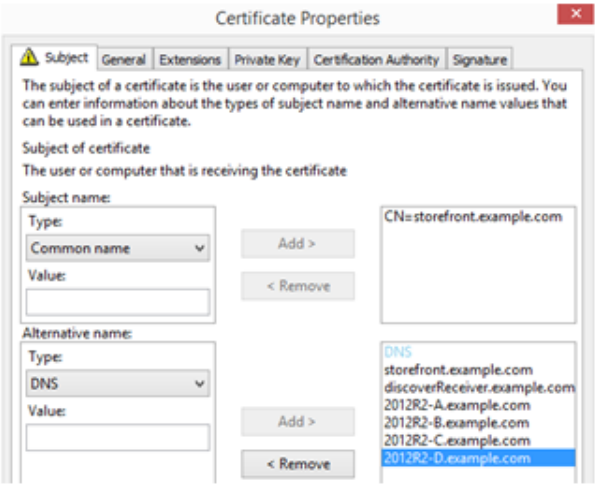
> **Note:**
>
> When exporting the private key associated with the certificate is not feasible. Use two separate certificates: one on the Citrix ADC appliance load balancing vServer and a different certificate on the StoreFront server group nodes. Both certificates must include Subject Alternative Names.

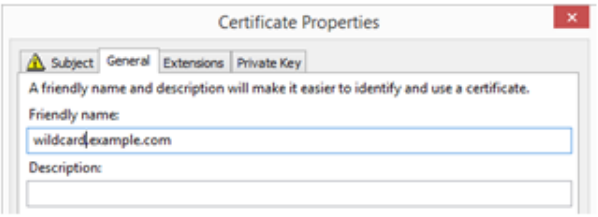
Example Web server certificates

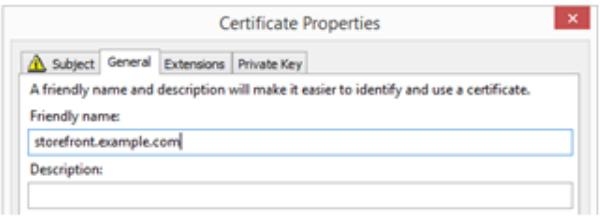
Option 1: Wildcard certificate



Option 2: SAN certificate with every StoreFront server

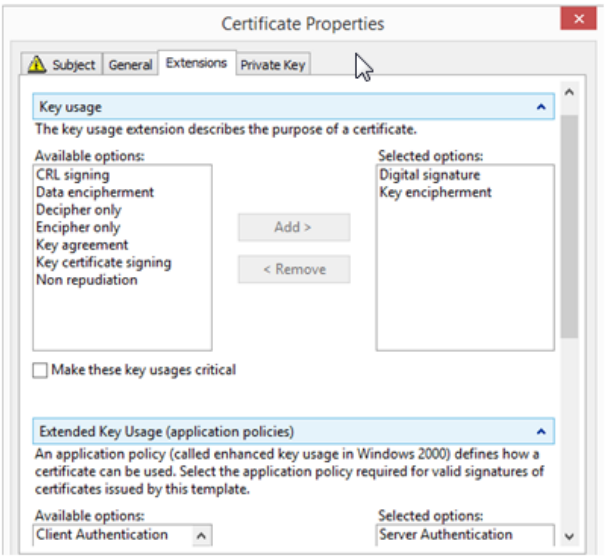


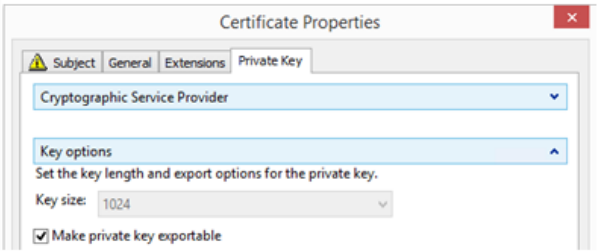




© 1999–2022 Citrix Systems, Inc. All rights reserved.

Common Properties





Create a server certificate for the Citrix ADC appliance load balancer and all StoreFront servers

Import a certificate issued from a Windows Certificate Authority onto a Citrix ADC appliance

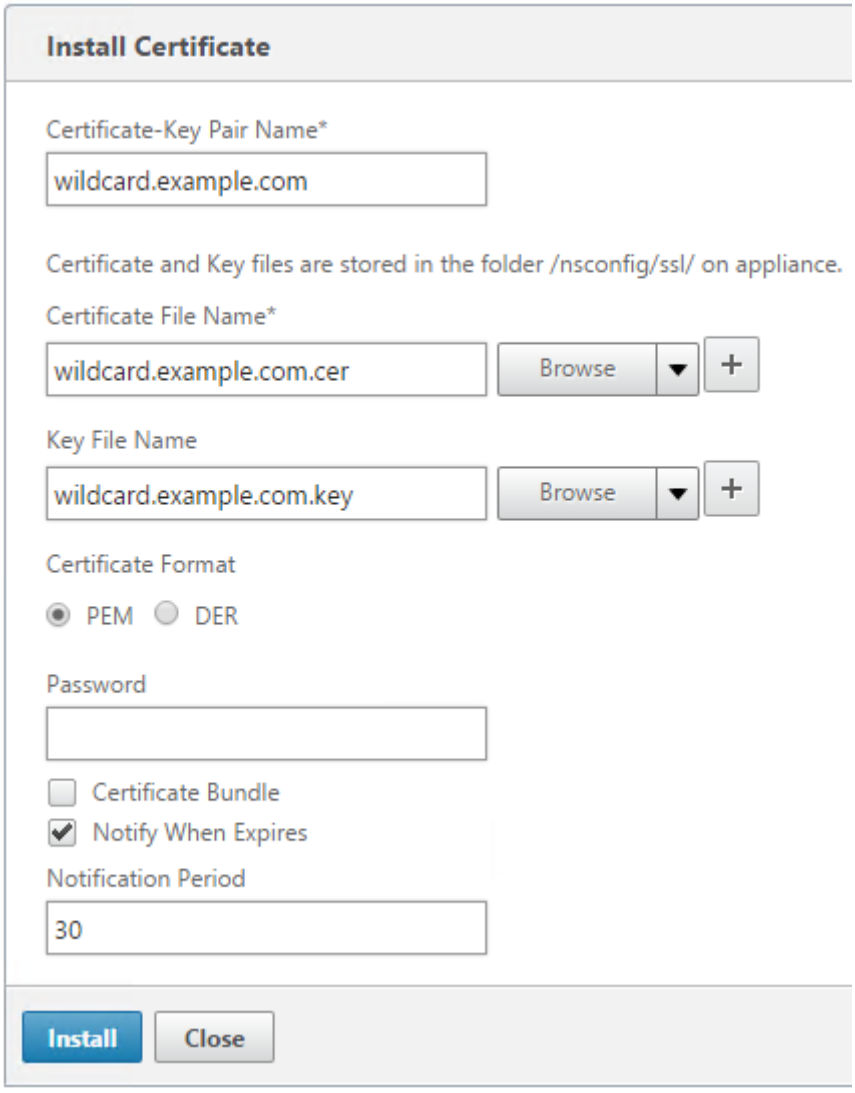
- WinSCP is a useful third party and free tool to move files from a Windows machine to a Citrix ADC appliance file system. Copy certificates for import to the */nsconfig/ssl/* folder within the Citrix ADC appliance file system.
- You can also use OpenSSL tools on the Citrix ADC appliance to extract the certificate and key from a *PKCS12/PFX* file to create a two separate .CER and .KEY X.509 files in PEM format that Citrix ADC can use.

1. Copy the PFX file into */nsconfig/ssl/* on the Citrix ADC appliance or VPX.
2. Open the Citrix ADC appliance command line interface (CLI).
3. Type **Shell** to exit the Citrix ADC appliance CLI and switch to the FreeBSD shell.
4. Change directory using `cd /nsconfig/ssl/`.
5. Run `openssl pkcs12 -in <imported cert file>.pfx -nokeys -out <certfilename>.cer` and enter the PFX password when prompted.
6. Run `openssl pkcs12 -in <imported cert file>.pfx -nocerts -out <keyfilename>.key` and enter the PFX password when prompted, and then set the private key PEM passphrase to protect the .KEY file.
7. Run `ls -al` to check the .CER and .KEY files have been successfully created inside `/nsconfig/ssl/`.
8. Type **Exit** to return to the Citrix ADC appliance CLI.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Configure the server certificate on the Citrix ADC appliance after it is imported

1. Log on to the Citrix ADC appliance management GUI.
2. Select **Traffic Management > SSL > SSL Certificates** and click **Install**.
3. On the Install Certificate window, enter the certificate and private key pair names.
   - Select the .cer certificate file on the Citrix ADC appliance file system under /nsconfig/ssl/.
   - Select the .key file containing the private key from the same location.



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 Citrix ADC appliance load balancer.

Example: `storefront.example.com` resolves to the load balancing vServer virtual IP (VIP).

© 1999–2022 Citrix Systems, Inc. All rights reserved.

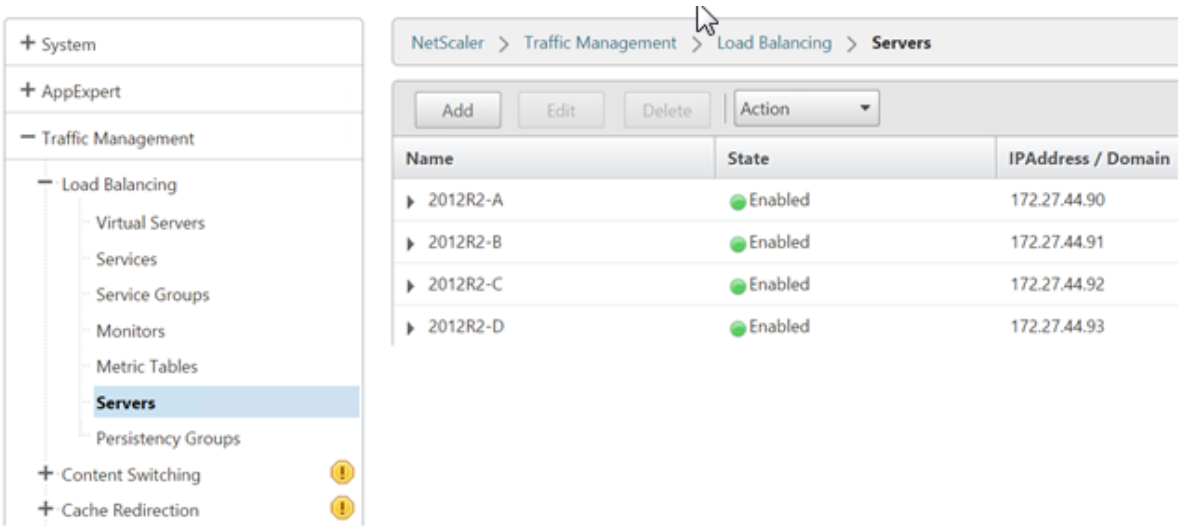
Scenario 1: End-to-end HTTPS 443 secure connection between the client and the Citrix ADC appliance load balancer, and between the load balancer and multiple StoreFront 3.x servers

This scenario uses a modified StoreFront monitor using port 443.

Add individual StoreFront server nodes to the Citrix ADC appliance load balancer

1. Log onto the Citrix ADC appliance management GUI.
2. Select **Traffic Management > Load Balancing > Servers > Add** and add each of the four StoreFront nodes to be load balanced.

   Example = 4 x 2012R2 StoreFront Nodes named 2012R2-A to -D.
3. 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

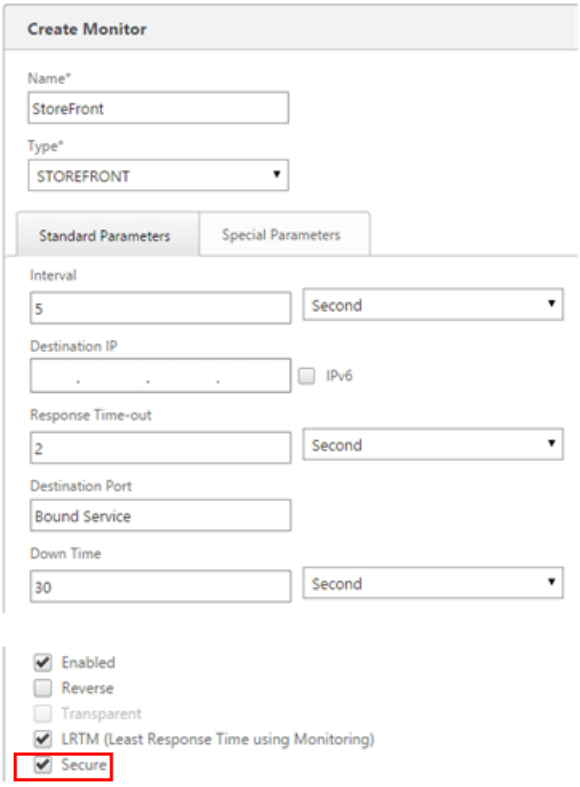
1. Log onto the Citrix ADC management GUI.
2. Select **Traffic Management > Load Balancing > Monitors > Add** and add a new monitor called *StoreFront* and accept all default settings.
3. From the **Type** drop down menu, select **StoreFront**.
4. If you are using HTTPS connections between your load balancing vServer and StoreFront, ensure that the **Secure** option is selected; otherwise leave this option unselected.
5. In the **Special Parameters** tab, type the **Store Name**.
6. In the **Special Parameters** tab, select the **Check Backend Services** option. This option enables monitoring of services running on the StoreFront server. StoreFront services are monitored by

© 1999–2022 Citrix Systems, Inc. All rights reserved.

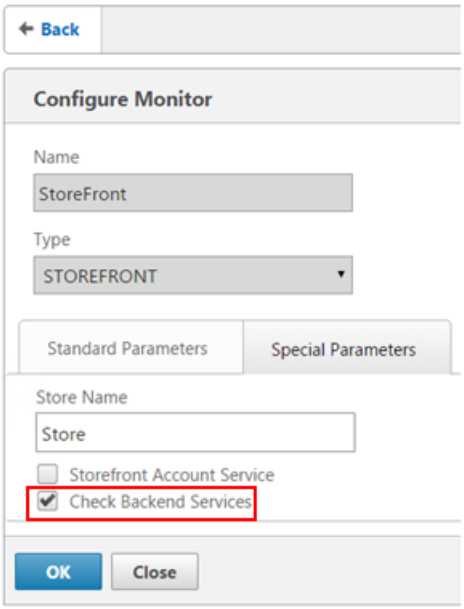
probing a Windows service that runs on the StoreFront server, which returns the status of the following services:

- W3SVC (IIS)
- WAS (Windows Process Activation Service)
- CitrixCredentialWallet
- CitrixDefaultDomainService

Standard Parameters Tab



Special Parameters Tab

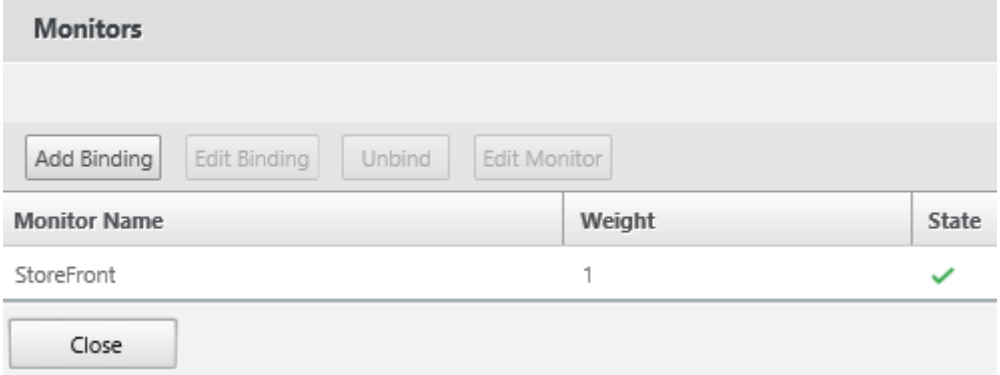


Create an HTTPS 443 service group containing all of the StoreFront servers

1. Within your Service Group, select the **Members** option on the right hand side and add all of the StoreFront server nodes you defined previously in the Servers section.
2. Set the TLS port and give each node a unique server ID as you add it.

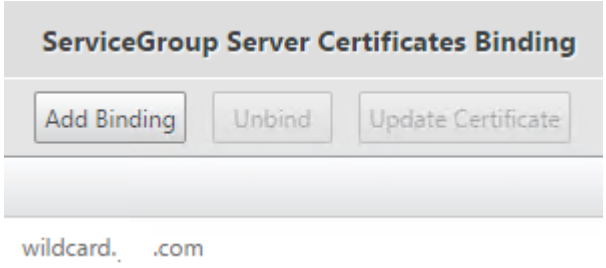
© 1999–2022 Citrix Systems, Inc. All rights reserved.

3. On the **Monitors** tab, select the StoreFront monitor you created earlier.



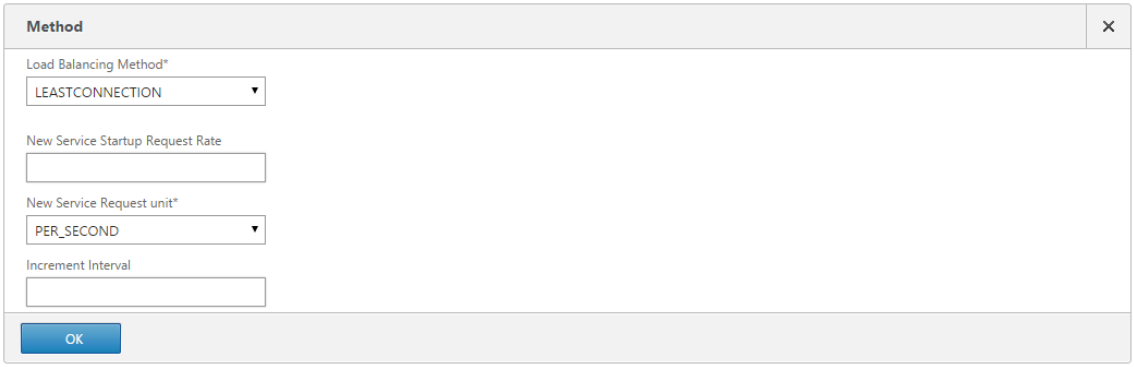
4. On the **Certificates** tab, bind the server certificate you imported earlier.
5. Bind the CA certificate used to sign the server certificate you imported earlier, and any other CAs that might be part of the PKI chain of trust.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



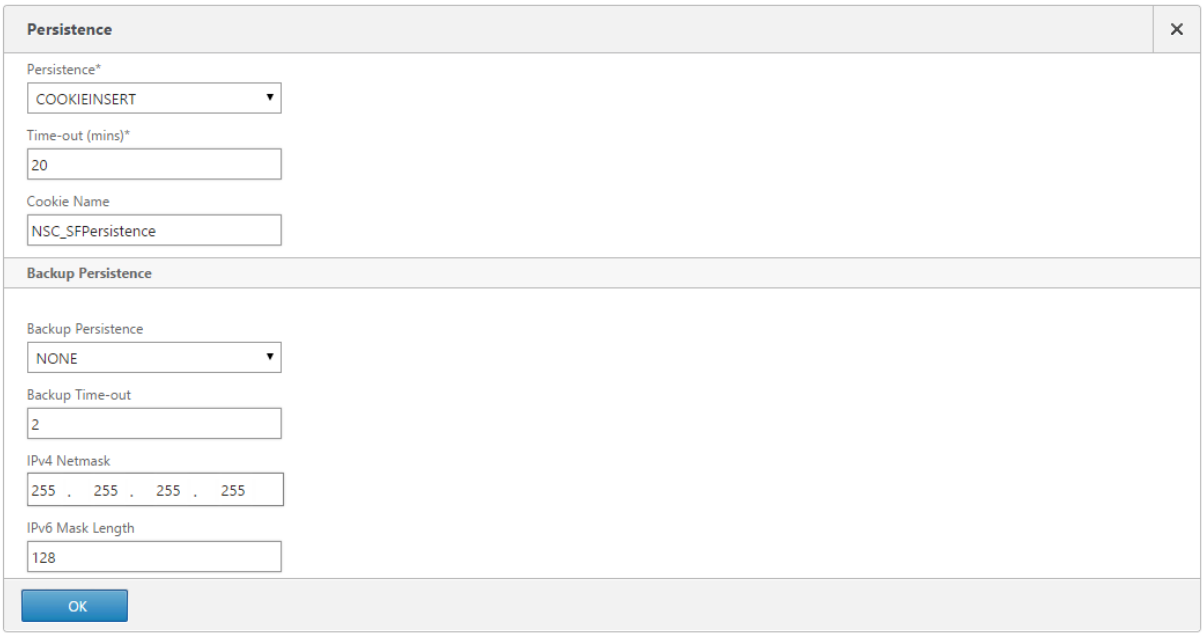
Create a load balancing vServer for user traffic

1. Log onto the Citrix ADC appliance management GUI.
2. Select **Traffic Management > Load Balancing > Virtual Servers > Add** to create a new vServer.
3. Select the load balancing method for the vServer. Common choices for StoreFront load balancing are **round robin** or **least connection**.



4. Bind the **Service Group** you created earlier to the load balancing vServer.
5. Bind the same server and CA certificate you previously bound to the service group, to the load balancing vServer.
6. From within the load balancing vServer menu, select **Persistence** on the right hand side and set the persistence method to be **COOKIEINSERT**.
7. Name the cookie. For example, **NSC_SFPersistence**, as this makes it easy to identify in Fiddler traces during debugging.
8. Set backup persistence to **NONE**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



Scenario 2: HTTPS termination—HTTPS 443 communication between the client and the Citrix ADC load balancer, and HTTP 80 connections between the load balancer and the StoreFront 3.x servers behind it

This scenario uses the default StoreFront monitor using port 8000.

Add individual StoreFront server servers to the Citrix ADC load balancer

1. Log onto the Citrix ADC management GUI.
2. Select **Traffic Management > Load Balancing > Servers > Add** and add each of the four StoreFront servers to be load balanced. Example = 4 x 2012R2 Storefront servers called 2012R2-A to -D. 3.
3. Use IP based Server configuration and enter the server IP address for each Storefront server.

Define an HTTP 8000 StoreFront monitor to check the status of all StoreFront servers in the server group

1. Log onto the Citrix ADC management GUI.
2. Select **Traffic Management > Monitors > Add** and add a new monitor called StoreFront.
3. Add a name for the new monitor and accept all default settings.
4. In the **Type** list select **StoreFront**.
5. In the **Special Parameters** tab, type the **Store Name**.
6. Type 8000 into **Destination Port**. This matches the default monitor instance that is created on each StoreFront server.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

7. In the **Special Parameters** tab, select the **Check Backend Services** option. This option enables monitoring of services running on the StoreFront server. StoreFront services are monitored by probing to a Windows service that runs on the StoreFront server, which returns the status of all running StoreFront services.

Create an HTTP 80 service group containing all of the StoreFront servers

1. Within your Service Group, select the **Members** option on the right hand side and add all of the StoreFront server nodes you defined previously in the Servers section.
2. Set the HTTP port to 80 and give each server a unique server ID as you add it.
3. On the **Monitors** tab, select the StoreFront monitor you created earlier.

Create an HTTPS terminating load balancing vServer for user traffic

1. Select **Traffic Management > Load Balancing > Virtual Servers > Add** to create a new vServer.
2. Select the load balancing method vServer will use. Common choices for StoreFront load balancing
   are round robin or least connection.
3. Bind the Service Group you created earlier to the load balancing vServer.
4. Bind the same server and CA certificate you previously bound to the service group, to the load balancing vServer.

   > **Note:**
   >
   > If the client is not allowed to store the HTTP cookie, the subsequent requests do not have the HTTP cookie and Persistence is not used.

5. From within the load balancing vServer menu, select **Persistence** on the right hand side and set the persistence method to be **COOKIEINSERT**.
6. Name the cookie. For example, **NSC_SFPersistence**, as this makes it easy to identify in Fiddler traces during debugging.
7. Set backup persistence to **NONE**.

Create a load balancing vServer for subscription synchronization between server groups

Considerations before creating a load balancing vServer include the following:

- **Option 1:** Create a single vServer: to load balance only user traffic. This is all that is needed if performing only ICA launches of published apps and desktops. (Mandatory and usually all that is required.)

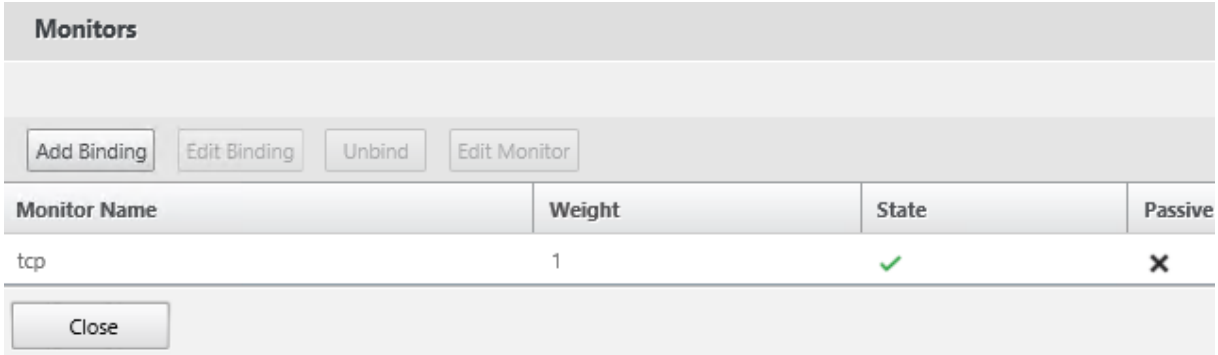
© 1999–2022 Citrix Systems, Inc. All rights reserved.

- **Option 2:** Create a pair of vServers: one to load balance user traffic for performing ICA launches of published apps and desktops and another for load balancing subscription data synchronization operations. (Necessary only when propagating subscription data between two or more load balanced StoreFront server groups in a large multi-site deployment.)

If a multisite deployment consists of two or more StoreFront server groups located in separate geographic locations, 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 vServer on HTTP port 80 or HTTPS 443 fails. To provide high availability for this service, create a second vServer on each Citrix ADC appliance in your deployment to load balance TCP port 808 for each of the StoreFront server groups. When configuring the replication schedule, specify a server group address that matches the subscription synching vServer virtual IP address. Ensure the server group address is the FQDN of the load balancer for the server group at that location.

Configure a service group for subscription synchronization

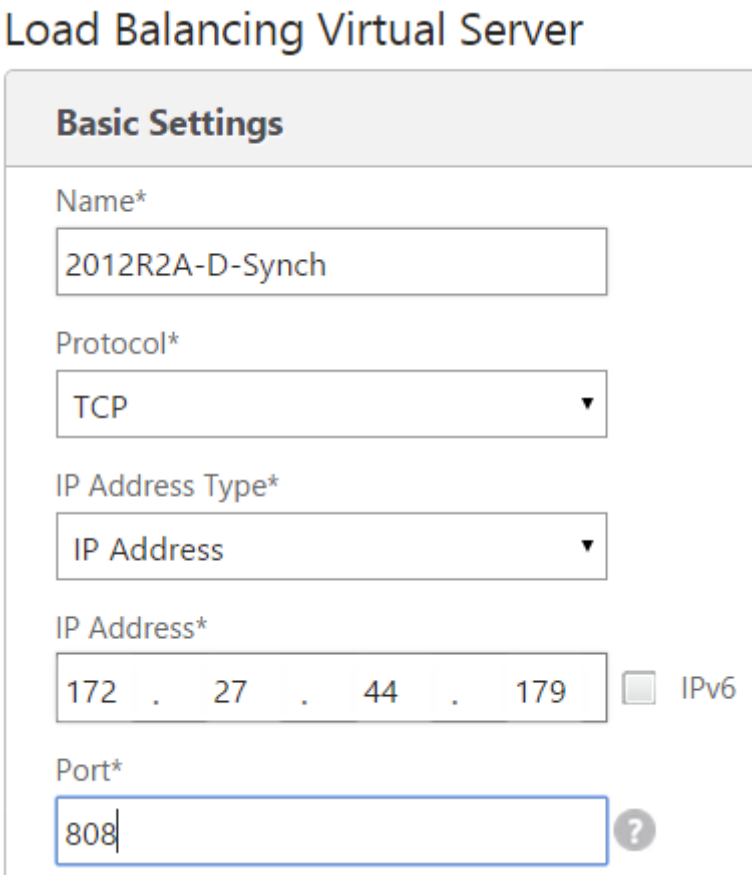
1. Log onto the Citrix ADC appliance management GUI.
2. Select **Traffic Management > Service Groups > Add** and add a new service group.
3. Change the protocol to **TCP**.
4. Within your Service Group, select the **Members** option on the right hand side and add all of the StoreFront server nodes you defined previously in the Servers section.
5. On the **Monitors** tab, select the TCP monitor.



Create a load balancing vServer for subscription synchronization between server groups

1. Log onto the Citrix ADC appliance management GUI.
2. Select **Traffic Management > Service Groups > Add** and add a new service group.
3. Set the load balancing method to **round robin**.
4. Change the protocol to **TCP**.
5. Enter **808** and NOT **443** as the port number.

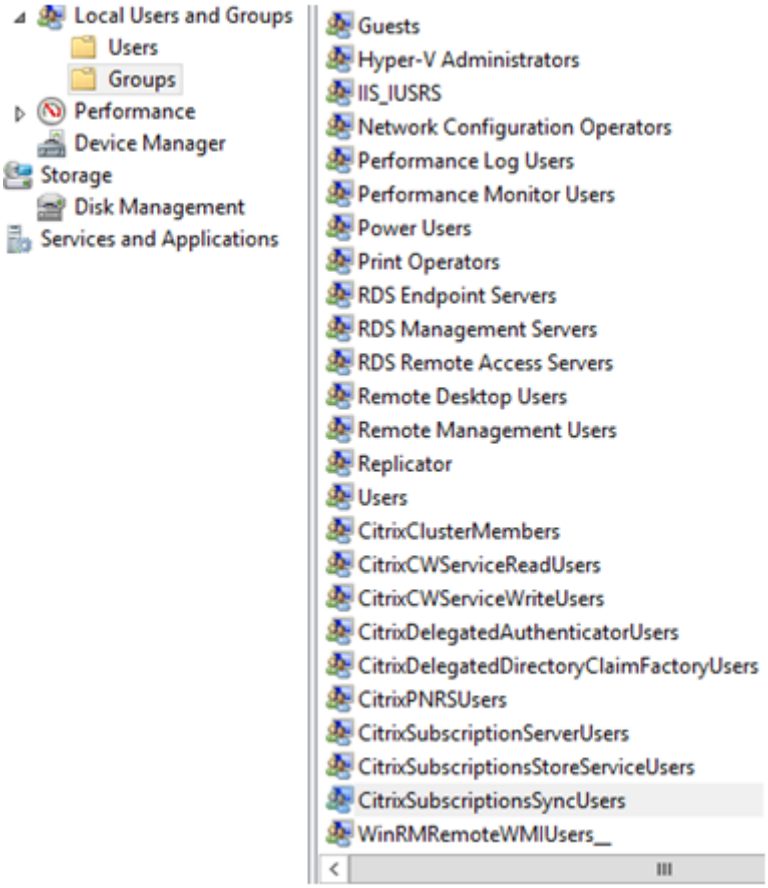
© 1999–2022 Citrix Systems, Inc. All rights reserved.



Membership within CitrixSubscriptionsSyncUsers

For **StoreFront server A** at **Location A** to request and pull subscription data from **server B** at a different location, server A must be a member of the **CitrixSubscriptionsSyncUsers** local security group on server B. The **CitrixSubscriptionsSyncUsers** local group contains an access control list of all remote StoreFront servers authorized to pull subscription data from a particular server. For bidirectional subscription synchronization, server B must also be a member of the **CitrixSubscriptionsSyncUsers** security group on server A to pull subscription data from it.

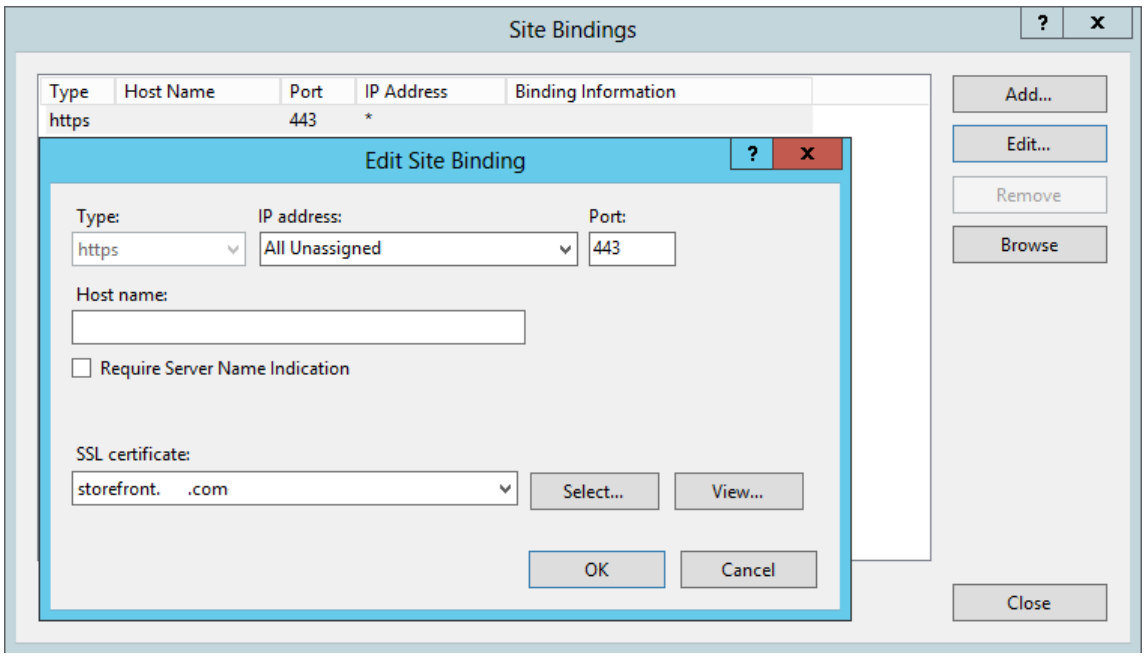
© 1999–2022 Citrix Systems, Inc. All rights reserved.



Scenario 1: Configure the StoreFront server group using HTTPS between Citrix ADC and StoreFront

1. Import the same certificate and private key that was deployed on the Citrix ADC appliance load balancing vServer to every StoreFront node in the server group.
2. Create an HTTPS binding in IIS on every StoreFront node, and then bind the certificate you imported earlier to it.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



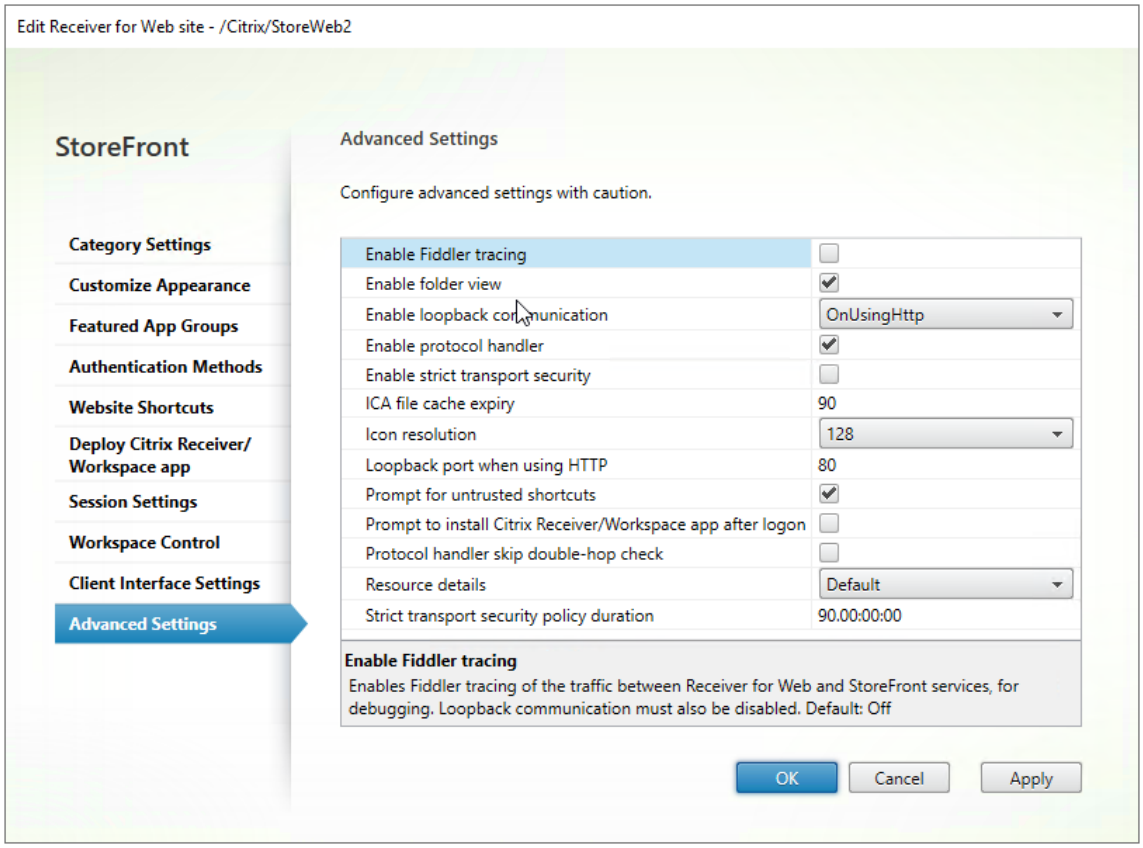
3. If you are using HTTPS between the Citrix ADC load balancer and StoreFront, you must use a certificate containing the load balanced FQDN as a Common Name (CN) or as a Subject Alternative Name (SAN).

   See Create a server certificate for the Citrix ADC appliance load balancer and StoreFront servers.

Scenario 2: Configure the StoreFront server group using HTTP between Citrix ADC and StoreFront

1. Remove the HTTPS binding in IIS from every StoreFront node if this already exists.
2. Ensure that the HTTP binding is present in IIS, and that it is set to use port 80.
3. Configure the loopback settings within Receiver for Web as **OnUsingHTTP** and port **80**. This step is essential to ensure that client detection between native Citrix Workspace App and Receiver for Web succeeds.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

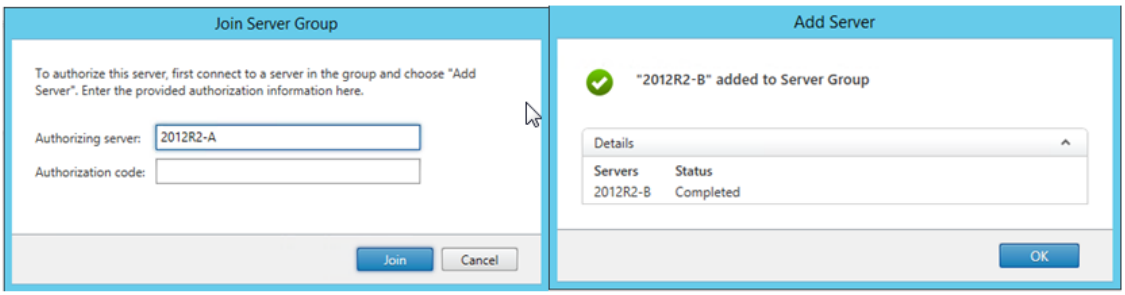


Steps common to both Scenarios 1 and 2

1. Install StoreFront on every node in the server group.
2. During installation of StoreFront, set the host base URL on the primary node to be the shared FQDN used by all members of the server group. This should always be `https://storefrontlb.domain.com` for both scenario 1 and 2 and must match the FQDN of the Citrix ADC load balancing vServer.

   See the Create a server certificate for the Citrix ADC appliance load balancer and StoreFront servers.
3. After you have completed the initial StoreFront configuration, join each of the nodes, one after the other, to the server group using the primary node.
4. Select **Server Group > Add Server > Copy the Authorization Code** to the joining Server.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



5. Propagate the configuration from the primary node to all other server group nodes in the group.
6. Test the load balanced server group using a client that can contact and resolve the shared FQDN of the load balancer.

Citrix Service Monitor

To enable external monitoring of the run-state of the Windows services on which StoreFront relies for correct operation, use the **Citrix Service Monitor** Windows service. This service has no other service dependencies and can monitor and report the failure of other critical StoreFront services. The monitor enables the relative health of a StoreFront server deployment to be determined externally by other Citrix components, such as a Citrix ADC appliance. Third party software can consume the StoreFront monitor XML response to monitor the health of essential StoreFront services.

After StoreFront is deployed, a default monitor that uses HTTP and port 8000 is created.

> **Note:**
>
> Only one instance of a monitor can exist within a Storefront deployment.

To make any changes to the existing default monitor, such as changing the protocol and port to HTTPS 443, use PowerShell cmdlets to view or reconfigure the StoreFront monitor service URL.

Remove the default Service Monitor and replace it with one that uses HTTPS and 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.

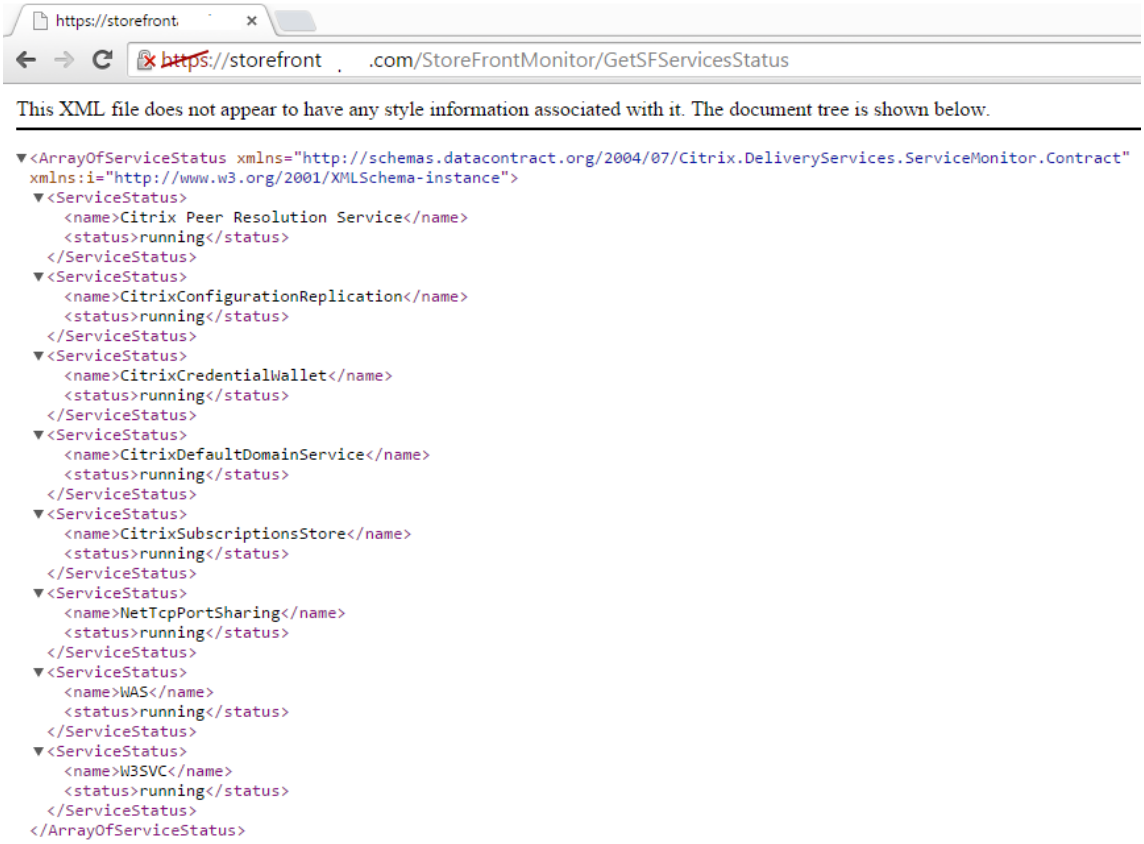
```
$ServiceUrl = ”https://localhost:443/StorefrontMonitor”
Set-STFServiceMonitor -ServiceUrl $ServiceUrl
Get-STFServiceMonitor
<!--NeedCopy-->
```

2. Once completed, propagate the changes to all other servers in the StoreFront server group.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

3. To perform a quick test on the new 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 should return an XML summary of the status of every Storefront service.

```
https://<loadbalancingFQDN>:443/StoreFrontMonitor/GetSFServicesStatus
```



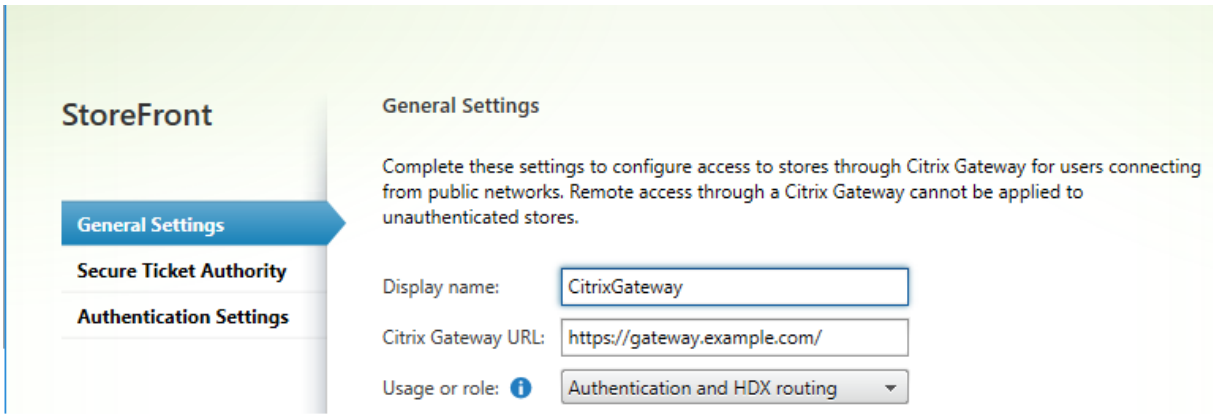
Citrix Gateway and load balancing vServers on the same Citrix ADC appliance

If you have configured the Citrix Gateway virtual server and load balancing vServer on the same Citrix ADC appliance, internal domain users might experience issues when trying to access the StoreFront load balanced host base URL directly rather than passing through the Citrix Gateway virtual server.

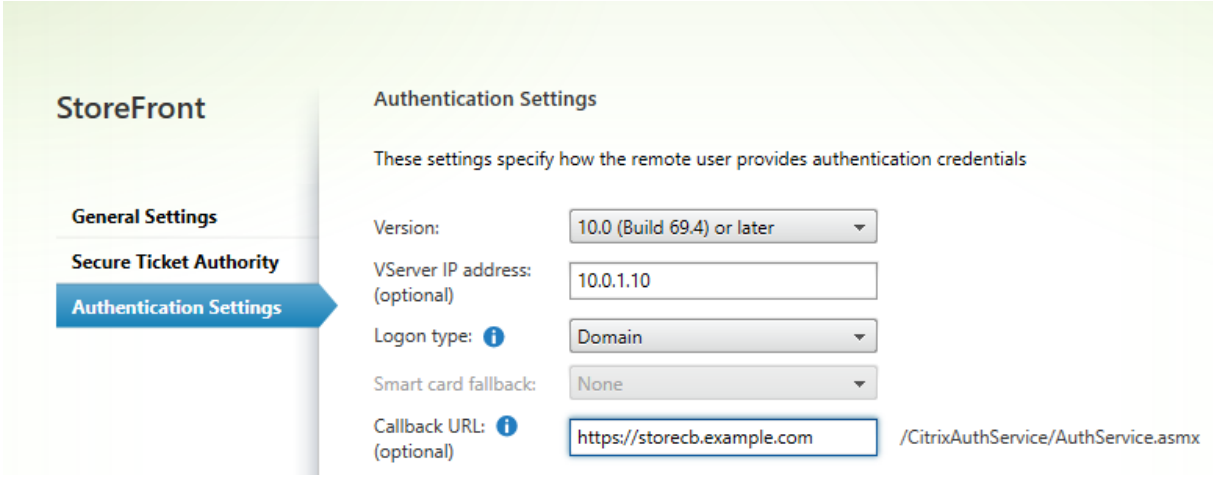
In this scenario StoreFront assumes that the end user has already authenticated at the Citrix Gateway because StoreFront correlates the source IP address of the incoming user with the Citrix Gateway Subnet IP Address (SNIP). This triggers StoreFront to attempt to use the AGBasic protocol to perform Citrix Gateway silent authentication, rather than actually prompting the user to log on with their domain credentials. To avoid this issue, omit a SNIP address as shown below or enter a VIP so that username and password authentication is used instead of the AGBasic logon protocol.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Configure a Citrix Gateway on the Storefront Server Group



Enter the Citrix Gateway VIP and into the VServer IP address field. Do NOT use the SNIP for the Citrix Gateway if the load balancing vServer resides on the same Citrix ADC appliance.



Loopback options when load balancing a StoreFront server group using a Citrix ADC appliance

You can set loopback options using PowerShell.

Example Receiver for Web web.config file

```
<communication attempts="2" timeout="00:01:00" loopback="On"
    loopbackPortUsingHttp="80">
<!--NeedCopy-->
```

Example PowerShell command

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
& "c:\program files\Citrix\receiver storefront\scripts\ImportModules.
    ps1"
Set-DSLoopback -SiteId 1 -VirtualPath "/Citrix/StoreWeb" -Loopback "
    OnUsingHttp" -LoopbackPortUsingHttp 81
<!--NeedCopy-->
```

The **-Loopback** parameter can take three possible values:

Value	Context
On — Changes the host of the URL to 127.0.0.1. The schema and port (if specified) are not changed.	Cannot be used if TLS-terminating load balancer is used.
OnUsingHttp — Changes the host to 127.0.0.1 and schema to HTTP and modifies the port the value configured for **loopbackPortUsingHttp** attribute.	Use only when the load balancer is TLS terminating. Communication between the load balancer and StoreFront servers is with HTTP. You can explicitly configure the HTTP port using the -loopbackPortUsingHttp attribute.
Off — The URL in the request is not modified in any way.	Use for trouble shooting. Tools like Fiddler cannot capture the traffic between Receiver for Web and StoreFront Services if loopback is set to **On**.

Configure two URLs for the same Citrix Gateway

October 22, 2020

In StoreFront, you can add a single Citrix Gateway URL from the StoreFront management console in **Manage Citrix Gateways > Add** or **Edit**. It is also possible to add both a public Citrix Gateway URL and a GSLB (Global Server Load Balancing) URL in **Manage Citrix Gateways > imported from file**.

This article shows you how to use PowerShell cmdlets and the StoreFront PowerShell SDK to use an optional parameter, -gslburl, to set the GslbLocation attribute of a gateway. This feature simplifies the Citrix Gateway administration in StoreFront in the following use cases:

1. **GSLB and multiple Citrix Gateways**. Use GSLB and multiple Citrix Gateways to load balance remote connections to published resources in two or more locations within a large global Citrix deployment.
2. **Single Citrix Gateway using a public or private URL**. Use the same Citrix Gateway for external

© 1999–2022 Citrix Systems, Inc. All rights reserved.

access using a public URL, and for internal access using a private URL.

This is an advanced feature and topic. If you are new to StoreFront gateway and Global Server Load Balancing (GSLB) concepts, see the Related information links at the end of this article.

This feature offers the following benefits:

- Support two simultaneous URLs for a single gateway object.
- Users can switch between two different URLs to access the Citrix Gateway without the administrator reconfiguring the StoreFront gateway object to match the gateway URL the user wants to use.
- Shorter setup and test times to validate the StoreFront gateway configuration when using multiple GSLB gateways.
- Use the same Citrix Gateway object in StoreFront inside the DMZ for both external and internal access.
- Support both URLs for optimal gateway routing. For more information on optimal gateway routing, see Set up highly available multi-site stores.

Deployment considerations when using two Gateway URLs

- The gatewayURL FQDN is displayed for each gateway within the StoreFront admin console. The GSLBURL property of each gateway is only visible via the use of PowerShell cmdlets.
- The gatewayURL is used by native Citrix Receivers and Citrix Workspace apps for authentication.
- The gatewayURL is included in the location tag within the provisioning file (receiver.cr) used to configure Citrix Receivers and Citrix Workspace apps with store and gateway information.
- Use the provided Powershell to modify Store and Roaming web.config files. Do not do this manually.

> **Important:**
>
> Before configuring a second gateway URL using the -gslburl parameter, 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. For more information about server certificates, see Plan gateway and server certificate usage.

DNS

- **Split DNS**. It is common for large enterprises to use split DNS. Split DNS involves using different namespaces and different DNS servers for public and private DNS resolution. Check if you have the existing DNS infrastructure to support this.
- **Single URL for external and internal access to published resources**. Decide if you want to use the same URL to access published resources from both outside and inside your corporate

© 1999–2022 Citrix Systems, Inc. All rights reserved.

network, or consider if two different URLs are acceptable such as `example.com` and `example.net`.

Server certificate examples

This section contains example server certificate deployments when using two Gateway URLs.

Example server certificate for a load balanced StoreFront deployment

A privately signed wildcard server certificate should contain the FQDN *.storefront.example.net.

Or

A privately signed SAN server certificate should contain all the FQDNs needed to load balance three StoreFront servers.

```
loadbalancer.storefront.example.net
server1.storefront.example.net
server2.storefront.example.net
server3.storefront.example.net
<!--NeedCopy-->
```

Set the host base URL of the StoreFront server group to be the shared FQDN, which resolves to the load balancer IP address:

```
loadbalancer.storefront.example.net
<!--NeedCopy-->
```

Example server certificate for a Citrix Gateway which is accessed both externally and internally using split DNS

A publically signed SAN server certificate for both external and internal access should contain both the external and internal FQDNs.

```
gateway.example.com
gateway.example.net
<!--NeedCopy-->
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Example server certificate for all GSLB Gateways which are accessed externally

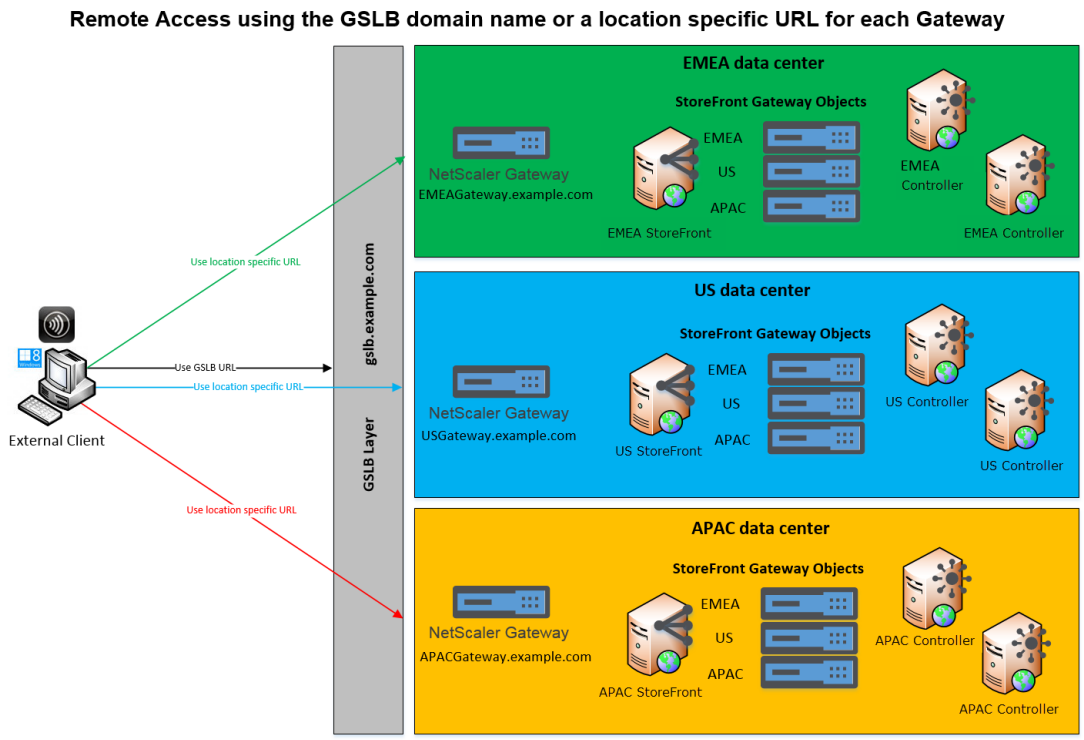
A publically signed SAN server certificate for external access through GSLB should contain the FQDNs.

```
gslbdomain.example.com
emeagateway.example.com
usgateway.example.com
apacgateway.example.com
<!--NeedCopy-->
```

This allows the user to access the closest gateway using GSLB or to pick a gateway in the location of their choice using its unique FQDN.

Use Case #1: Receiver for Web: GSLB and multiple Citrix Gateways

The administrator uses GSLB and multiple Citrix Gateways to load balance remote connections to published resources in two or more locations within a large global Citrix deployment.



In this example:

- Each location or data center contains at least one gateway, one or more StoreFront servers, and one or more XenApp and XenDesktop Controllers to provide published resources for that location. Each GSLB service configured on the GSLB Citrix ADC Appliances within the global

© 1999–2022 Citrix Systems, Inc. All rights reserved.

deployment represents a gateway VPN vServer. All of the StoreFront servers in the deployment must be configured to contain all of the Citrix Gateway virtual servers that make up the GSLB layer. The GSLB Citrix Gateways are used in active/active mode but can also provide failover if the network connection, DNS, gateway, StoreFront server or Citrix Virtual Apps and Desktops Controllers at one location fail. Users are automatically directed to another gateway if a GSLB service is unavailable.

- External clients are directed to the closest gateway based on the configured GSLB load balancing algorithm such as round trip time (RTT) or Static Proximity when making remote connections.
- The unique URL for each gateway allows users to manually select which data center they want to launch resources from by choosing the location-specific URL for the gateway they want to use.
- GSLB can be bypassed when GSLB or a DNS delegation is not working as expected. Users can continue to access remote resources at any data center using its location-specific URL until any GSLB related issues are resolved.

Use Case #1: Receiver for Web, and Citrix Receivers or Citrix Workspace apps: GSLB and multiple Citrix Gateways

Gateway attributes

To use GSLB with native Citrix Receivers or Citrix Workspace apps, use **Add-STFRoamingGateway** (create) or **Set-STFRoamingGateway** (modify) to specify the following attributes:

-GatewayUrl — set as the shared FQDN for all GSLB gateways

-GSLBurl — set as the unique gateway FQDN for each gateway

> Note:
>
> This may seem counterintuitive but it has no impact on this web use case. It ensures that native Citrix Receivers or Citrix Workspace apps receive the shared FQDN used by GSLB within the discovery document found by accessing the endpoint `https://storefront.domain.com/citrix/<storename>/discovery`. It also ensures that the provisioning file (receiver.cr) exported by StoreFront's **Export Provisioning File** command contains the shared GSLB FQDN.

Example provisioning files

Example file 1 using `–GatewayUrl https://gslb.domain.com`. This allows native Citrix Receivers or Citrix Workspace apps to use GSLB to connect to gateways.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```xml
<?xml version="1.0" encoding="utf-8"?>
<Services version="1.0"
    xmlns="http://www.citrix.com/ServiceRecord">
    <Service type="store">
        <SRID>167659780</SRID>
        <Name>Store</Name>
        <Address>https://storefront.domain.com/Citrix/Store/discovery</Address>
        <Gateways>
            <Gateway Name="EMEAGateway" Default="true" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
            <Gateway Name="USGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
            <Gateway Name="APACGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://gslb.domain.com/</Location>
            </Gateway>
        </Gateways>
        <Beacons>
            <Internal>
                <Beacon>https://storefront.domain.com/</Beacon>
            </Internal>
            <External>
                <Beacon>https://emeagateway.domain.com</Beacon>
                <Beacon>https://usgateway.domain.com</Beacon>
                <Beacon>https://apacgateway.domain.com</Beacon>
                <Beacon>http://gslb.domain.com</Beacon>
            </External>
        </Beacons>
    </Service>
</Services>
```

Example file 2 using `-GatewayUrl https://emeagateway.domain.com, https://usgateway.domain.com and https://apacgateway.domain.com`. This allows native Citrix Receivers or Citrix Workspace apps to use the unique URLs to connect to gateways.

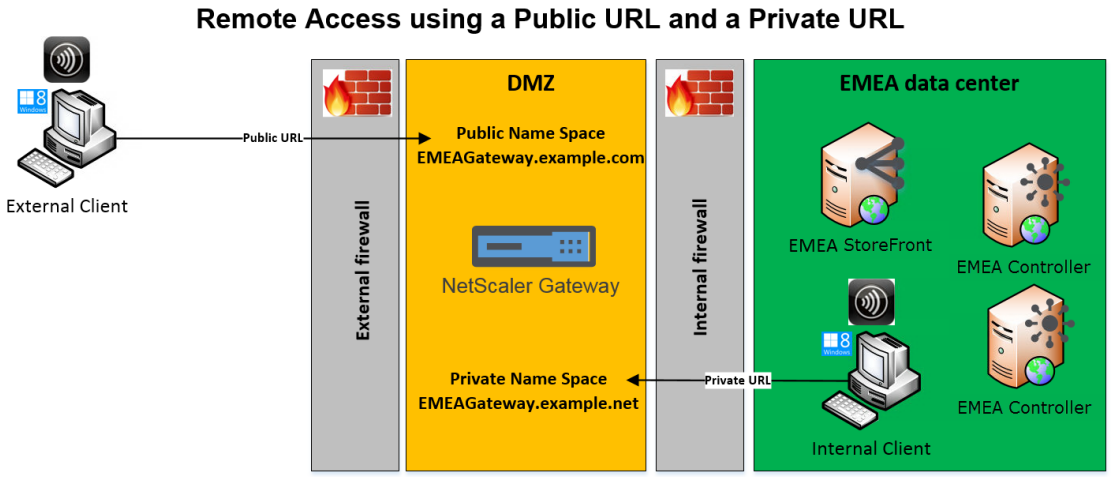
```xml
<?xml version="1.0" encoding="utf-8"?>
<Services version="1.0"
    xmlns="http://www.citrix.com/ServiceRecord">
    <Service type="store">
        <SRID>167659780</SRID>
        <Name>Store</Name>
        <Address>https://storefront.domain.com/Citrix/Store/discovery</Address>
        <Gateways>
            <Gateway Name="EMEAGateway" Default="true" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://emeagateway.domain.com/</Location>
            </Gateway>
            <Gateway Name="USGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://ftlgateway.domain.com/</Location>
            </Gateway>
            <Gateway Name="APACGateway" Edition="Enterprise" Auth="Domain" RewriteMode="NONE">
                <Location>https://bglgateway.domain.com/</Location>
            </Gateway>
        </Gateways>
        <Beacons>
            <Internal>
                <Beacon>https://storefront.domain.com/</Beacon>
            </Internal>
            <External>
                <Beacon>https://emeagateway.domain.com</Beacon>
                <Beacon>https://usgateway.domain.com</Beacon>
                <Beacon>https://apacgateway.domain.com</Beacon>
                <Beacon>http://gslb.domain.com</Beacon>
            </External>
        </Beacons>
    </Service>
</Services>
```

The shared FQDN is used for authentication by native Citrix Receivers and Citrix Workspace apps.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Use Case #2: Single Citrix Gateway using a public or private URL

The administrator uses the same Citrix Gateway for both external access using a public URL, and also internally using a private URL.



In this example:

- The administrator wants all access to published resources and HDX launch traffic to pass through a Citrix Gateway even if the client is internal.
- The Citrix Gateway is located in a DMZ.
- There are two different network routes to the Citrix Gateway through the two firewalls on either side of the DMZ.
- The public-facing, external namespace is different from the internal namespace.

PowerShell cmdlet examples

Use the PowerShell cmdlets **Add-STFRoamingGateway** and **Set-STFRoamingGateway** with the parameter, -gslburl, to set the **GslbLocation** attribute on the StoreFront gateway object. For example:

```
1 Add-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://
    emeagateway.example.com" -GSLBurl "https://gslb.example.com" -
    SubnetIPAddress "10.0.0.1" -CallbackUrl "https://emeagateway.example
    .com" -LogonType "DomainAndRSA" -SmartCardFallbackLogonType "None" -
    Version "Version10_0_69_4" -SecureTicketAuthorityUrls "https://emea-
    controller.example.com/scripts/ctxsta.dll,https://us-controller.
    example.com/scripts/ctxsta.dll,https://apac-controller.example.com/
    scripts/ctxsta.dll"
2 Set-STFRoamingGateway -Name "EMEAGateway" -GatewayUrl "https://
    emeagateway.example.com" -GSLBurl "https://gslb.example.com"
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
Get-STFRoamingGateway -Name "EMEAGateway" (returns just the EMEA gateway object)
Or
Get-STFRoamingGateway (returns all gateway object configured in StoreFront)
<!--NeedCopy-->
```

For use case #1, you can remove the GSLBurl from the "EMEAGateway" by setting its **GslbLocation** to NULL. The following PowerShell modifies the gateway object $EMEAGateway stored in memory. **Set-STFRoamingGateway** can then be passed $EMEAGateway to update the StoreFront config and remove the GSLBurl.

```
$EMEAGateway = Get-STFRoamingGateway
$EMEAGateway.GslbLocation = $Null
Set-STFRoamingGateway -Gateway $EMEAGateway
<!--NeedCopy-->
```

For use case #1, the following gateways are returned using **Get-STFRoamingGateway**:

```
Name: EMEAGateway
Location: https://emeagateway.example.com/ (Unique URL for the EMEA Gateway)
GslbLocation: https://gslb.example.com/ (GSLB URL for all three gateways)

Name: USGateway
Location: https://USgateway.example.com/ (Unique URL for the US Gateway )
GslbLocation: https://gslb.example.com/ (GSLB URL for all three gateways)

Name: APACGateway
Location: https://APACgateway.example.com/ (Unique URL for the APAC Gateway)
GslbLocation:  https://gslb.example.com/ (GSLB URL for all three gateways)
<!--NeedCopy-->
```

For use case #2: the following gateways are returned using **Get-STFRoamingGateway**:

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
Name: EMEAGateway
Location: https://emeagateway.example.com/ (Public URL for the Gateway)
GslbLocation: https://emeagateway.example.net/ (Private URL for the
    Gateway)
<!--NeedCopy-->
```

For use case #1, Optimal Gateway Routing is returned using **Get-STFStoreRegisteredOptimalLaunchGateway**:

```
$StoreObject = Get-STFStoreService -SiteId 1 -VirtualPath "/Citrix/<
    YourStore>"

Get-STFStoreRegisteredOptimalLaunchGateway -StoreService $StoreObject

Hostnames:       {
 emeagateway.example.com, gslb.example.com }

Hostnames:       {
 usgateway.example.com, gslb.example.com }

Hostnames:       {
 apacgateway.example.com, gslb.example.com }

<!--NeedCopy-->
```

GSLB URL or Internal URL for each Gateway is stored in the Roaming service web.config file

StoreFront does not display the GSLB URL or internal URL for each Gateway within the StoreFront management console, however it is possible to view the configured GSLBLocation path for all GSLB gateways by opening the roaming service Web.Config file location in C:\inetpub\wwwroot\Citrix\Roaming\web.config on the StoreFront server.

Use Case #1 Gateways in Roaming web.config file

```
<gateway id="cca13269-18c1-10fd-a0df-7931b3897aa8" name="EMEAGateway"
    default="false" edition="Enterprise" version="Version10_0_69_1" auth
    ="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.1" rwmode
    ="NONE" deployment="Appliance" callbackurl=https://emeagateway.
    example.com/CitrixAuthService/AuthService.asmx sessionreliability="
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
    true" requesttickettwosta="false" stasUseLoadBalancing="false"
    stasBypassDuration="01:00:00">
2 <location path="https://emeagateway.example.com/" /><gslbLocation path=
    "https://gslb.example.com/" /><clusternodes>
3 <clear />
4 </clusternodes>
5 <silentauthenticationurls>
6 <clear />
7 </silentauthenticationurls>
8 <secureticketauthorityurls>
9 <clear />
10 <location path="https://emea-controller.example.com/scripts/ctxsta.dll"
     />
11 <location path="https://us-controller.example.com/scripts/ctxsta.dll"
    />
12 <location path="https://apac-controller.example.com/scripts/ctxsta.dll"
     />
13 </secureticketauthorityurls>
14 </gateway>
15
16 <gateway id="b8ec720c-d85e-1889-8188-1cf08a2cf762" name="USGateway"
    default="false" edition="Enterprise" version="Version10_0_69_1" auth
    ="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.2" rwmode
    ="NONE" deployment="Appliance" callbackurl="https://usgateway.
    example.com/CitrixAuthService/AuthService.asmx" sessionreliability="
    true" requesttickettwosta="false" stasUseLoadBalancing="false"
    stasBypassDuration="01:00:00"><location path="https://usgateway.
    example.com/" /><gslbLocation path="https://gslb.example.com/" /><
    clusternodes>
17 <clear />
18 </clusternodes>
19 <silentauthenticationurls>
20 <clear />
21 </silentauthenticationurls>
22 <secureticketauthorityurls>
23 <clear />
24 <location path="https://emea-controller.example.com/scripts/ctxsta.dll"
     />
25 <location path="https://us-controller.example.com/scripts/ctxsta.dll"
    />
26 <location path="https://apac-controller.example.com/scripts/ctxsta.dll"
     />
27 </secureticketauthorityurls>
28 </gateway>
29
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
<gateway id="c57117b5-e111-1eed-9117-a1ffa1c8100e" name="APACGateway" default="false" edition="Enterprise" version="Version10_0_69_1" auth="DomainAndRSA" smartcardfallback="None" ipaddress="10.0.0.3" rwmode="NONE" deployment="Appliance" callbackurl="https://apacgateway.example.com/CitrixAuthService/AuthService.asmx" sessionreliability="true" requesttickettwosta="false" stasUseLoadBalancing="false" stasBypassDuration="01:00:00"><location path="https://apacGateway.example.com/" /><gslbLocation path="https://gslb.example.com/" /><clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.com/scripts/ctxsta.dll" />
<location path="https://us-controller.example.com/scripts/ctxsta.dll" />
<location path="https://apac-controller.example.com/scripts/ctxsta.dll" />
</secureticketauthorityurls>
</gateway>
<!--NeedCopy-->
```

Use Case #2: Gateways in Roaming web.config file

```
<gateway id="cca13269-18c1-10fd-a0df-7931b3897aa8" name="EMEAGateway" default="false" edition="Enterprise" version="Version10_0_69_1" auth="Domain" smartcardfallback="None" ipaddress="10.0.0.1" rwmode="NONE" deployment="Appliance" callbackurl="https://emeagateway.example.com/CitrixAuthService/AuthService.asmx" sessionreliability="true" requesttickettwosta="false" stasUseLoadBalancing="false" stasBypassDuration="01:00:00">
<location path="https://emeagateway.example.com/" />
<gslbLocation path=" https://emeagateway.example.net/" />
<clusternodes>
<clear />
</clusternodes>
<silentauthenticationurls>
<clear />
</silentauthenticationurls>
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
<secureticketauthorityurls>
<clear />
<location path="https://emea-controller.example.net/scripts/ctxsta.dll"
    />
</secureticketauthorityurls>
</gateway>
<!--NeedCopy-->
```

Related information

In Developer Documentation see Citrix StoreFront SDK PowerShell Modules.

Configure Citrix ADC and StoreFront for Delegated Forms Authentication (DFA)

April 29, 2020

Extensible authentication provides a single customization point for extension of the Citrix ADC appliance'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 ADC appliance 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 ADC appliance 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 ADC appliance 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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- 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> & .\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, 860
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
                                        e9401-39c8-4f2c-928d-34251102
                                        b840] }

ParameterData                   : {
 [FeatureClassId, e1eb3668-9c1c-4ad8-bbae-c08b2682c1bc], [
    ParentInstanceId, 8dd182c7-f
                                  970-466c-ad4c-27a5980f716c], [
                                        TenantId, 860e9401-39c8-4f2c
                                        -928d-34251102b840] }

AdditionalInstanceDependencies : {
 b1e48ef0-b9e5-4697-af9b-0910062aa2a3 }

IsDeployed                      : True
FeatureClass                    : Citrix.DeliveryServices.Framework
    .Feature.FeatureClass
<!--NeedCopy-->
```

2. Add Citrix Trusted Client. Configure the shared secret key (passphrase) between StoreFront and the Citrix ADC appliance. Your passphrase and client ID must be identical to what you configured on the Citrix ADC appliance.

```
PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Add-
    DSCitrixPSKTrustedClient -clientId netscaler.fqdn.com -
    passphrase secret
<!--NeedCopy-->
```

3. Set the Delegated Forms Authentication conversation factory to route all the traffic to the custom form. To find the conversation factory, look for ConversationFactory in C:\inetpub\wwwroot\Citrix\Authentication\web.config.This is an example of what you might see.

```
<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" />
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
7                <add param="action" value="AuthenticateStart" />
8                <add param="postbackAction" value="Authenticate" />
9                <add param="cancelAction" value="CancelAuthenticate"
                     />
10               <add param="conversationFactory" value="
                    ExampleBridgeAuthentication" />
11               <add param="changePasswordAction" value="
                    StartChangePassword" />
12               <add param="changePasswordController" value="
                    ChangePassword" />
13               <add param="protocol" value="CustomForms" />
14             </defaults>
15           </route>
16 <!--NeedCopy-->
```

4. In PowerShell, set the Delegated Forms Authentication conversation factory. In this example, to ExampleBridgeAuthentication.

```
1 PS C:\Program Files\Citrix\Receiver StoreFront\Scripts> Set-
     DSDFAProperty -ConversationFactory ExampleBridgeAuthentication
2 <!--NeedCopy-->
```

PowerShell arguments are not case-sensitive: **-ConversationFactory** is identical to **-conversationfactory**.

Uninstall StoreFront

Before you uninstall StoreFront, uninstall any third party authentication plugin, as it will impact the functionality of StoreFront.

Authenticate using different domains

October 22, 2020

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.

© 1999–2022 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.

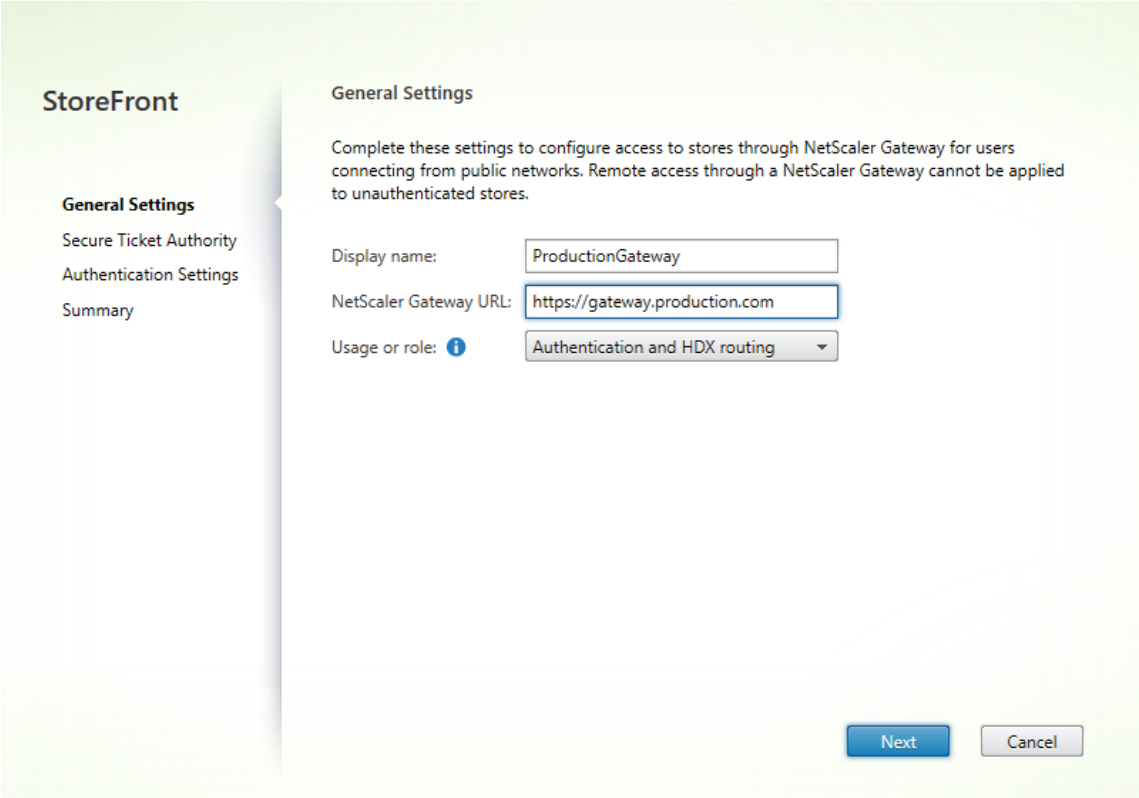
Configure a Citrix Gateway for the store

To configure a Citrix Gateway for the store:

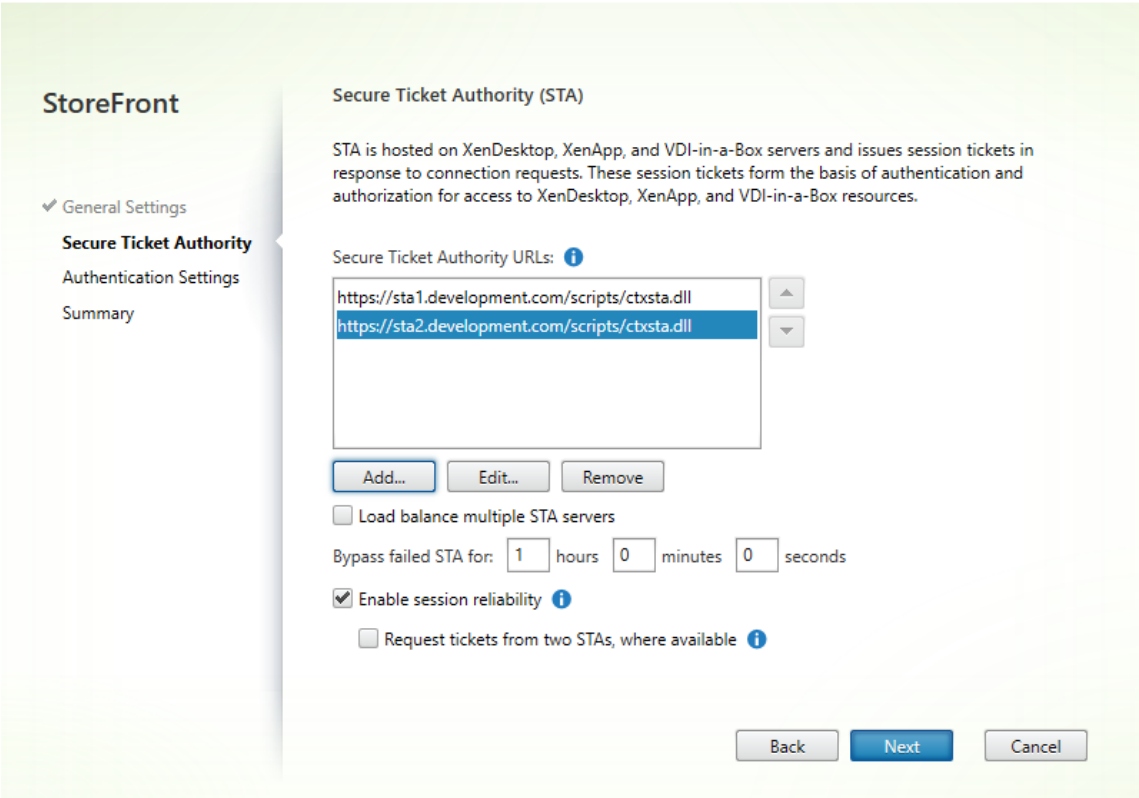
1. Select **Stores** in the left pane of the Citrix StoreFront management console, and in the **Actions** pane, click **Manage Citrix Gateways**.
2. On the Manage Citrix Gateways screen, click **Add**.
3. Complete the General Settings, Secure Ticket Authority, and Authentication steps.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

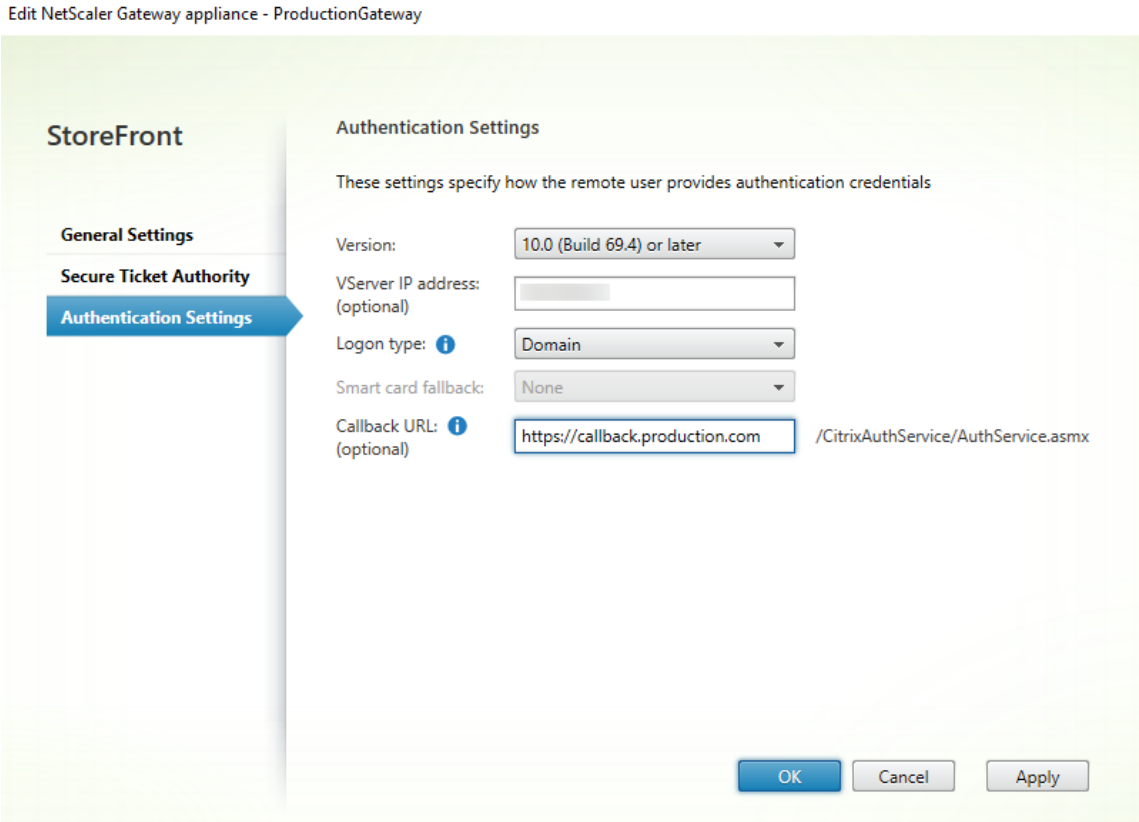
Add NetScaler Gateway Appliance



Add NetScaler Gateway Appliance



© 1999–2022 Citrix Systems, Inc. All rights reserved.

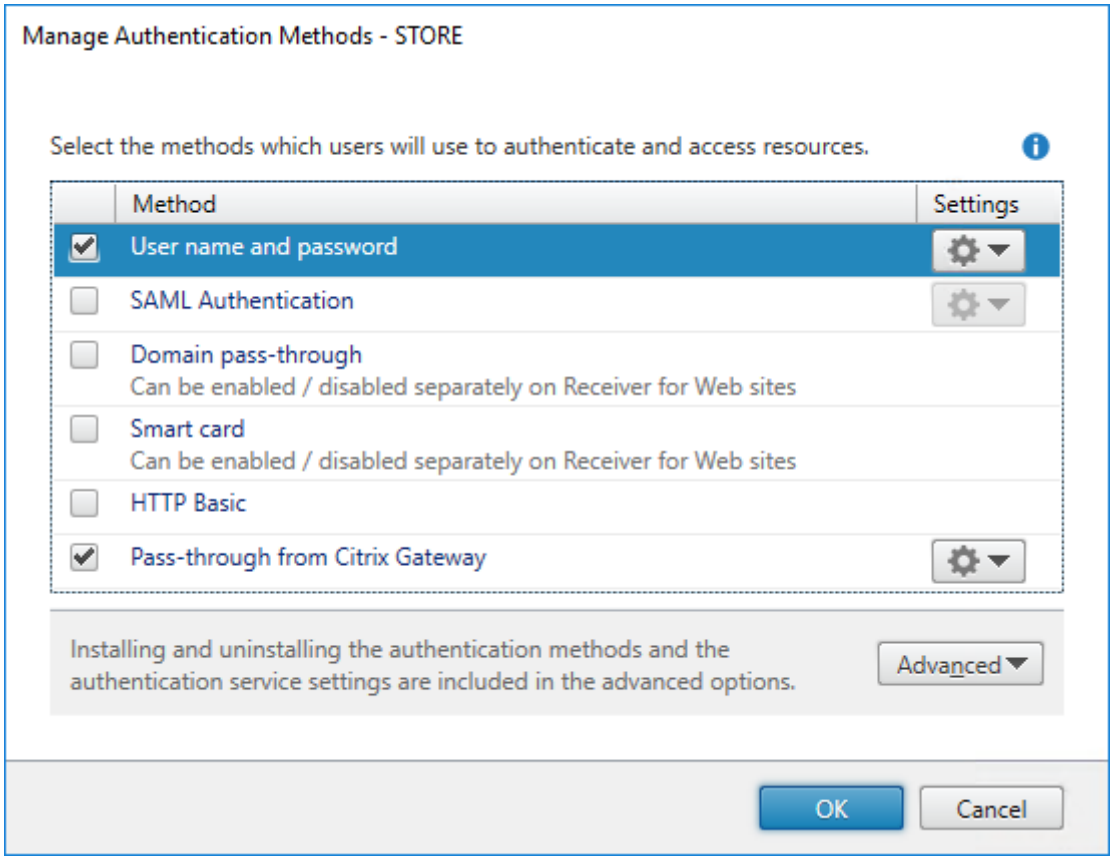


> **Note:**
>
> DNS conditional forwarders may need to be added so that the DNS servers in use on both domains can resolve FQDNs on the other domain. The Citrix ADC appliance must be able to resolve the STA server FQDNs on the `development.com` domain using its `production.com` DNS server. StoreFront 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**.

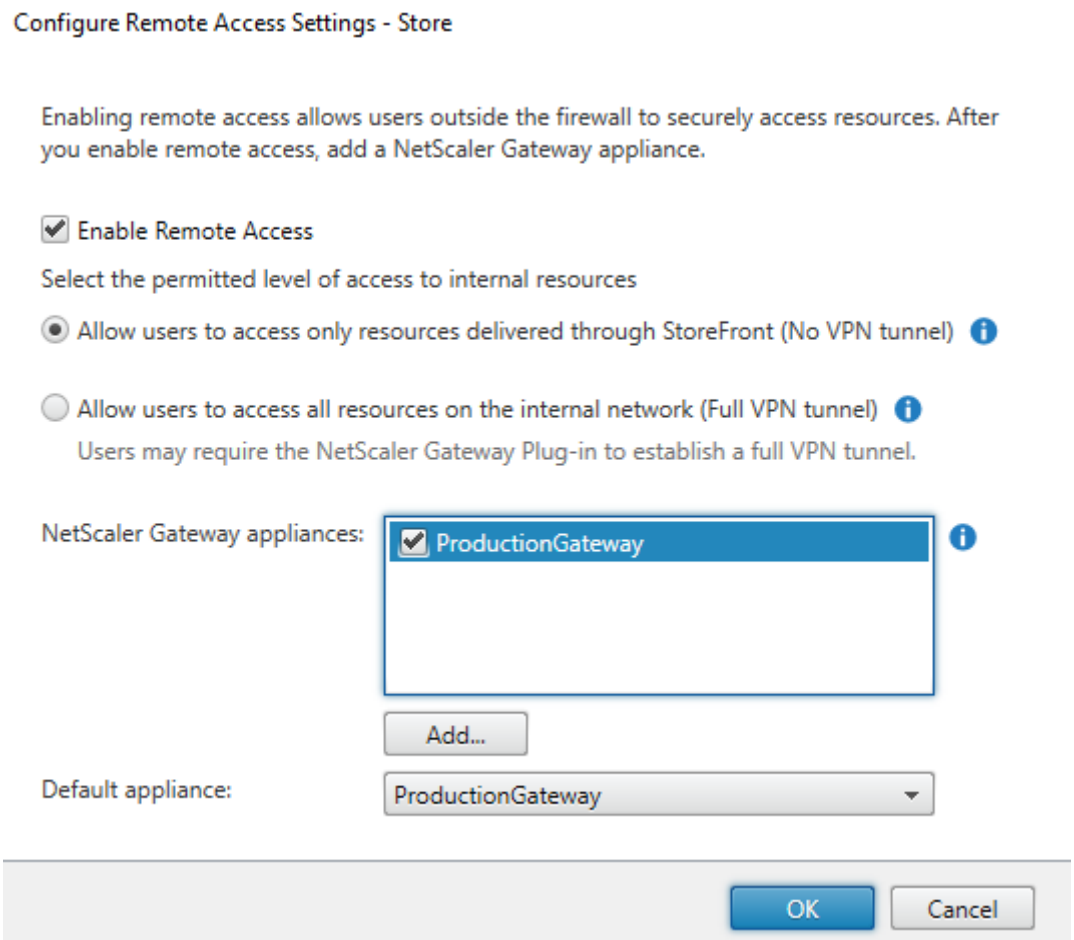
© 1999–2022 Citrix Systems, Inc. All rights reserved.



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.

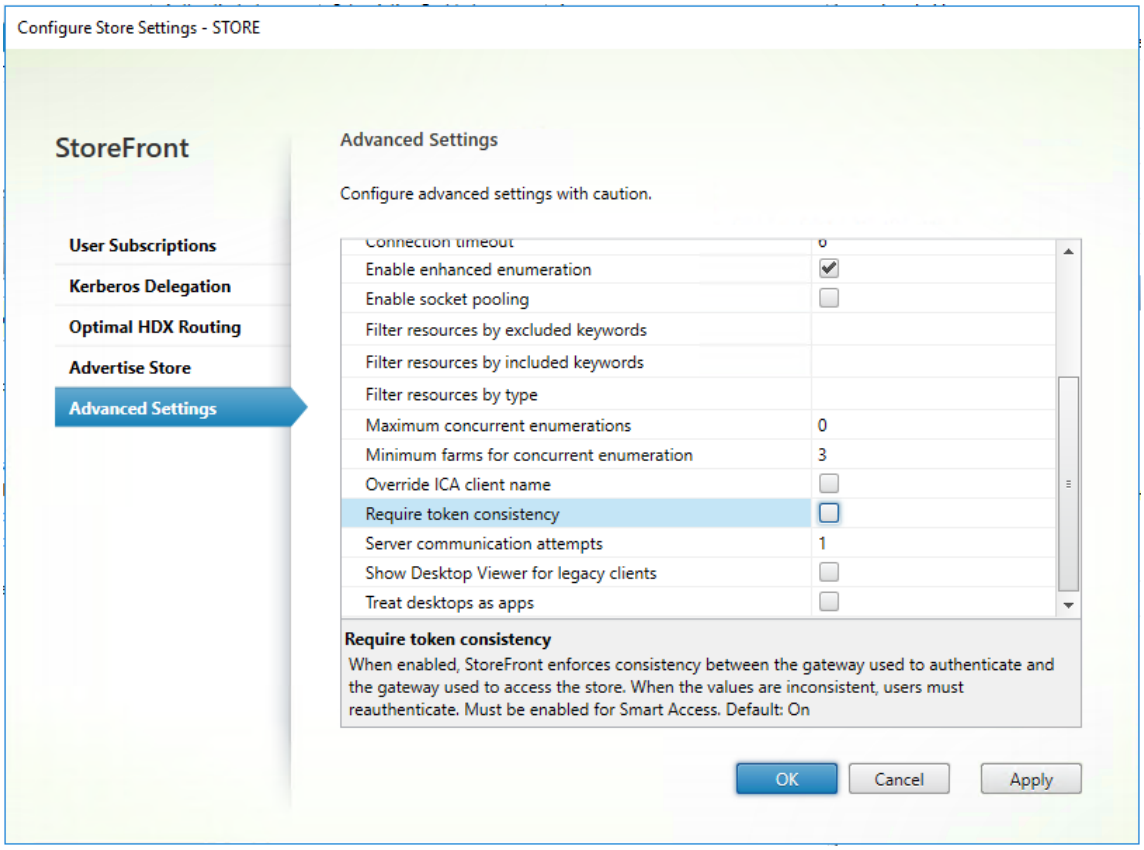
© 1999–2022 Citrix Systems, Inc. All rights reserved.



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.
4. Click **OK**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



> Note:
>
> The Require token consistency setting is selected (on) by default. If you disable this setting, SmartAccess features used for Citrix ADC End Point Analysis (EPA) stop working. For more information on SmartAccess, see CTX138110.

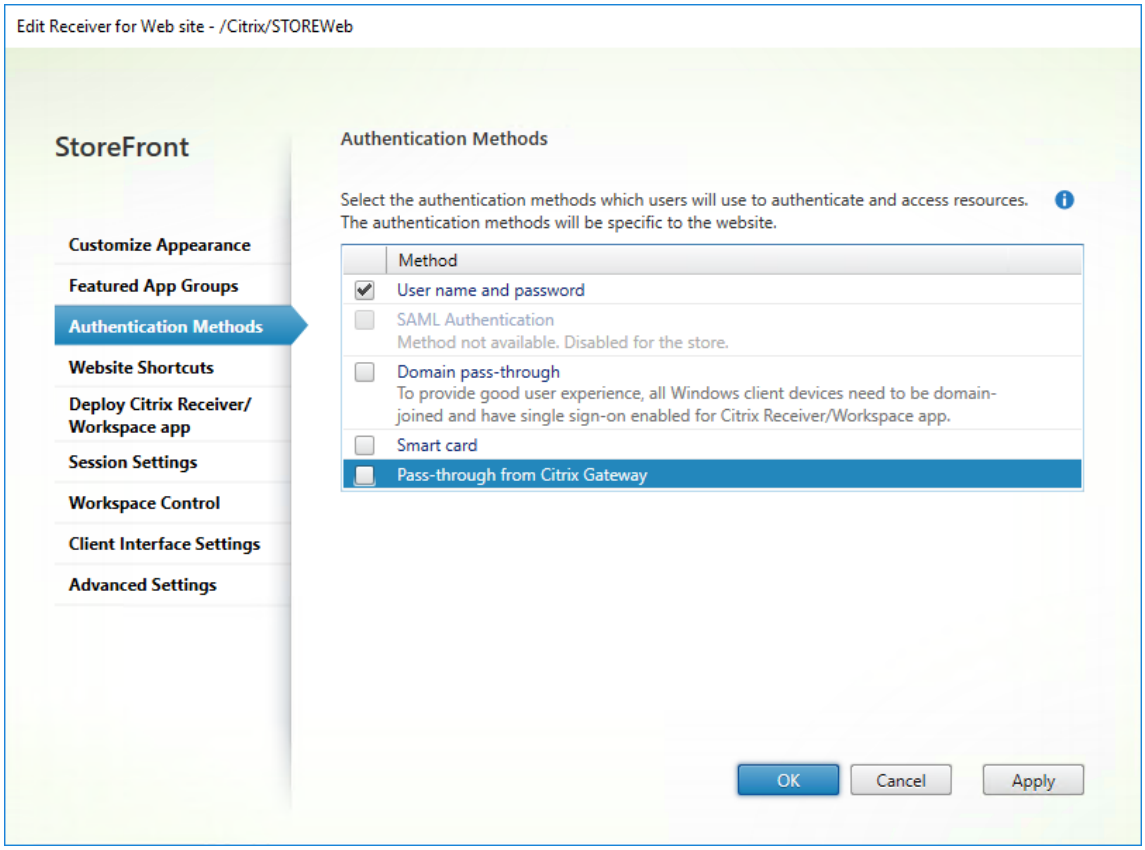
Disable pass-through from Citrix Gateway for the Receiver for Web site

> **Important:**
>
> Disabling pass-through from Citrix Gateway prevents Receiver for Web from trying to use the incorrect credentials from the `production.com` domain passed from the Citrix ADC appliance. Disabling pass-through from Citrix Gateway causes Receiver for Web to prompt the user to enter credentials. These credentials are different from the credentials used to log on through the Citrix Gateway.

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

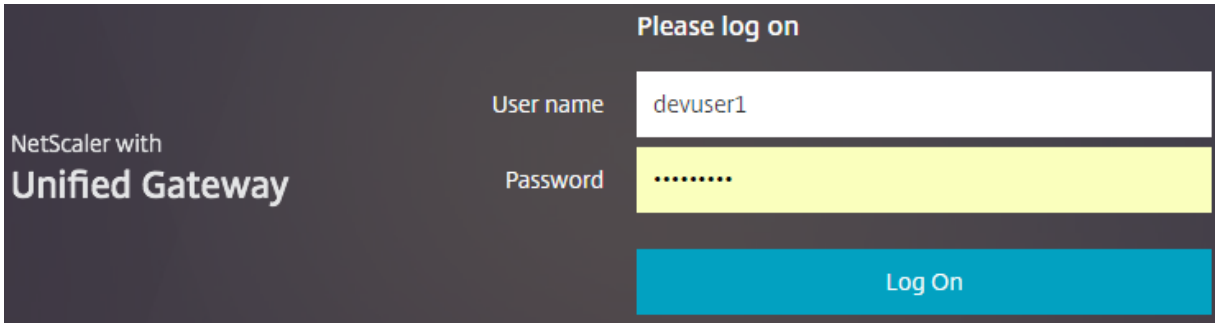
© 1999–2022 Citrix Systems, Inc. All rights reserved.

5. Click **OK**.



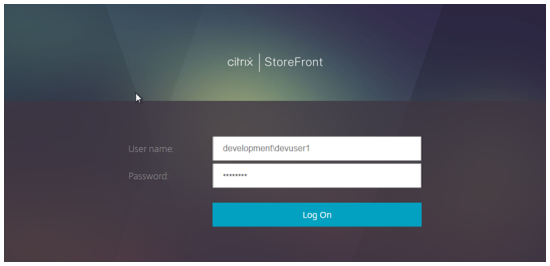
Log on to Gateway using a `production.com` user and credentials

To test, log on to Gateway using a `production.com` user and credentials.



After logon, the user is prompted to enter `development.com` credentials.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

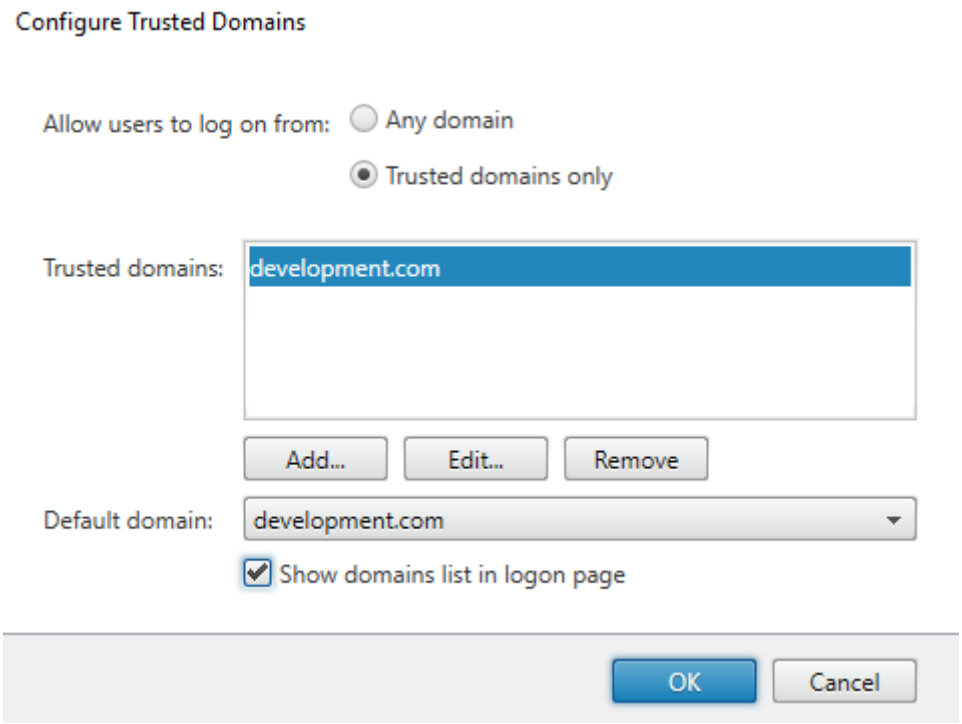


Add a trusted domain drop-down list in StoreFront (optional)

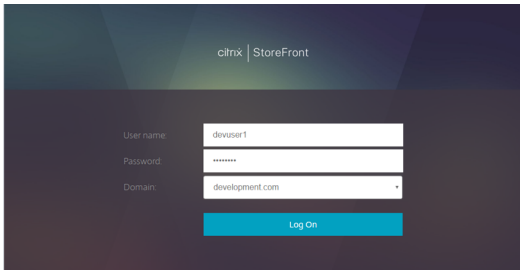
This setting is optional, but it may help prevent the user from accidentally entering the wrong domain to authenticate through the Citrix Gateway.

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**.



© 1999–2022 Citrix Systems, Inc. All rights reserved.

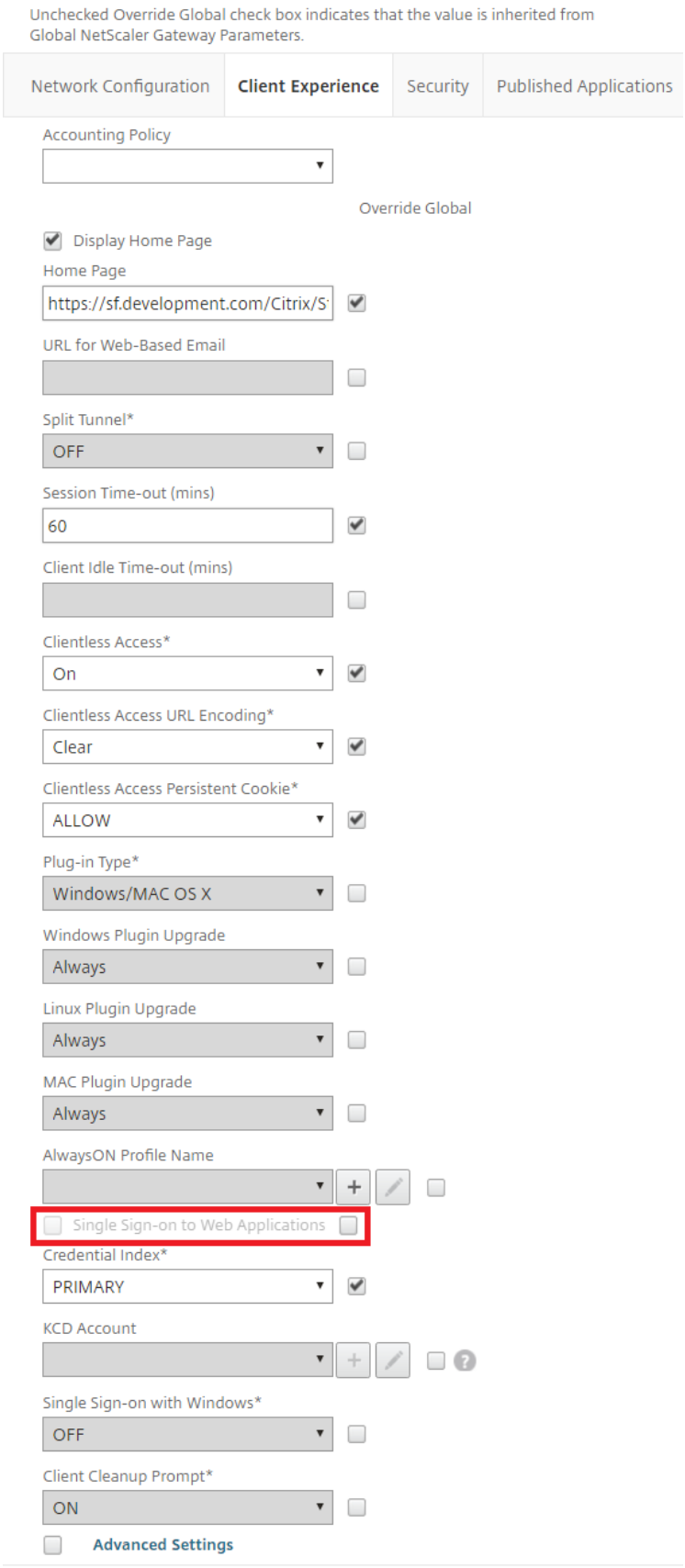


> **Note:**
>
> Browser password caching is not recommended in this authentication scenario. If users have different passwords for the two different domain accounts, password caching can lead to a poor experience.

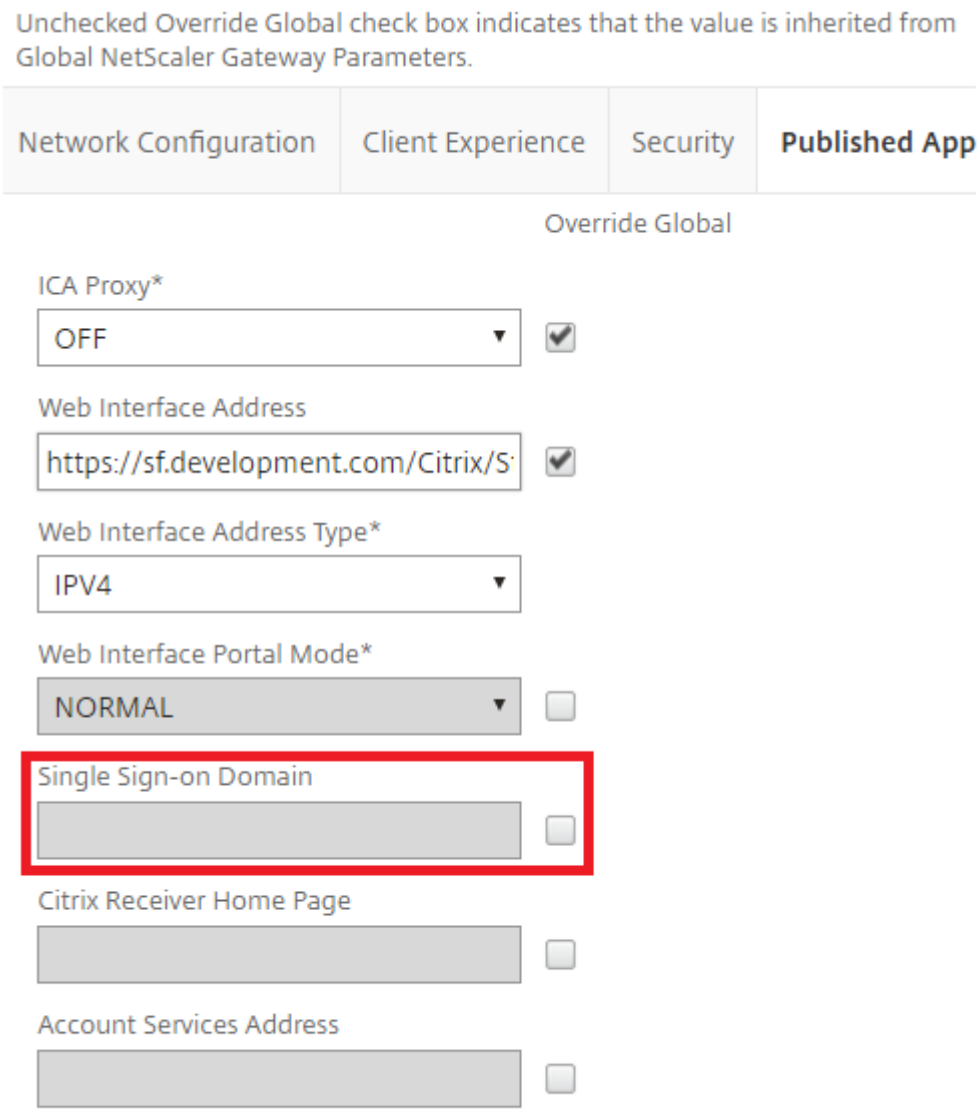
Citrix Gateway clientless VPN (CVPN) session action policy

- If Single Sign-on to web applications is enabled within your Citrix Gateway session policy, incorrect credentials sent by Citrix ADC appliance to Receiver for Web are ignored because you disabled the **Pass-through from Citrix Gateway** authentication method on the Receiver for Web site. Receiver for Web 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 ADC appliance does not change the behavior described in this article.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



© 1999–2022 Citrix Systems, Inc. All rights reserved.



Configure beacon points

April 29, 2020

Use the Manage Beacons task to specify URLs inside and outside your internal network to be used as beacon points. Citrix Workspace app attempts to contact beacon points and uses the responses to determine whether users are connected to local or public networks. When a user accesses a desktop or application, the location information is passed to the server providing the resource so that appropriate connection details can be returned to Citrix Workspace app. This ensures that users are not prompted to log on again when they access a desktop or application.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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 uses the server URL or load-balanced URL of your deployment as the internal beacon point. The Citrix website and the virtual server or user logon point (for Access Gateway 5.0) URL of the first Citrix Gateway deployment you add are used as external beacon points by default.

If you change any beacon points, ensure that users update Citrix Workspace app with the modified beacon information. Where a Receiver for Web site is configured for a store, users can obtain an updated Citrix Workspace app provisioning file from the site. Otherwise, you can export a provisioning file for the store and make this file available to your users.

> 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. On the Windows Start screen or Apps screen, locate and click the Citrix StoreFront tile.
2. Select the **Stores** node in the left pane of the Citrix StoreFront management console and, in the Actions pane, click **Manage Beacons**.
3. 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.
4. Click **Add** to enter the URL of an external beacon point. To modify a beacon point, select the URL in the External beacons list and click **Edit**. Select a URL in the list and click **Remove** to stop using that address as a beacon point.

   You must specify at least two highly available external beacon points that can be resolved from public networks. The beacon URLs should be fully qualified domain names (`http://example.com`) and not the abbreviated NetBIOS name (`http://example`). This enables Citrix Workspace app to determine whether users are located behind an Internet paywall, such

© 1999–2022 Citrix Systems, Inc. All rights reserved.

as in a hotel or Internet café. In such cases, all the external beacon points connect to the same proxy.

Create a single Fully Qualified Domain Name (FQDN) to access a store internally and externally

February 24, 2022

You can provide access to resources from within your corporate network and from the Internet through a Citrix Gateway and simplify the user experience by creating a single FQDN for both internal and roaming external clients.

Creating a single FQDN is helpful to users who configure any of the native Receivers. They need remember only a single URL whether they are currently connected to an internal or public network.

> **Note:**
>
> Direct access to private network endpoints from public websites is deprecated as part of the Private Network Access (PNA) specification. As a result, you might get errors when switching from an external network to an internal network while using a single FQDN. These errors occur on the latest version of Chrome and Microsoft Edge version 98 and later.
>
> As a temporary workaround, we recommend adding the following HTTP Response headers in IIS on the StoreFront server:
>
> - Access-Control-Allow-Headers: *
> - Access-Control-Allow-Origin: FQDN site URL
> - Access-Control-Allow-Private-Network: true
>
> **Caution**: Review the headers with your administrator before setting them up on the StoreFront server.

StoreFront beacons for Citrix Workspace app

Citrix Workspace app attempts to contact beacon points and uses the responses to determine whether users are connected to local or public networks. When a user accesses a desktop or application, the location information is passed to the server providing the resource so that appropriate connection details can be returned to Citrix Workspace app. This ensures that users are not prompted to log on again when they access a desktop or application. For information about configuring beacon points, see Configure beacon points.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

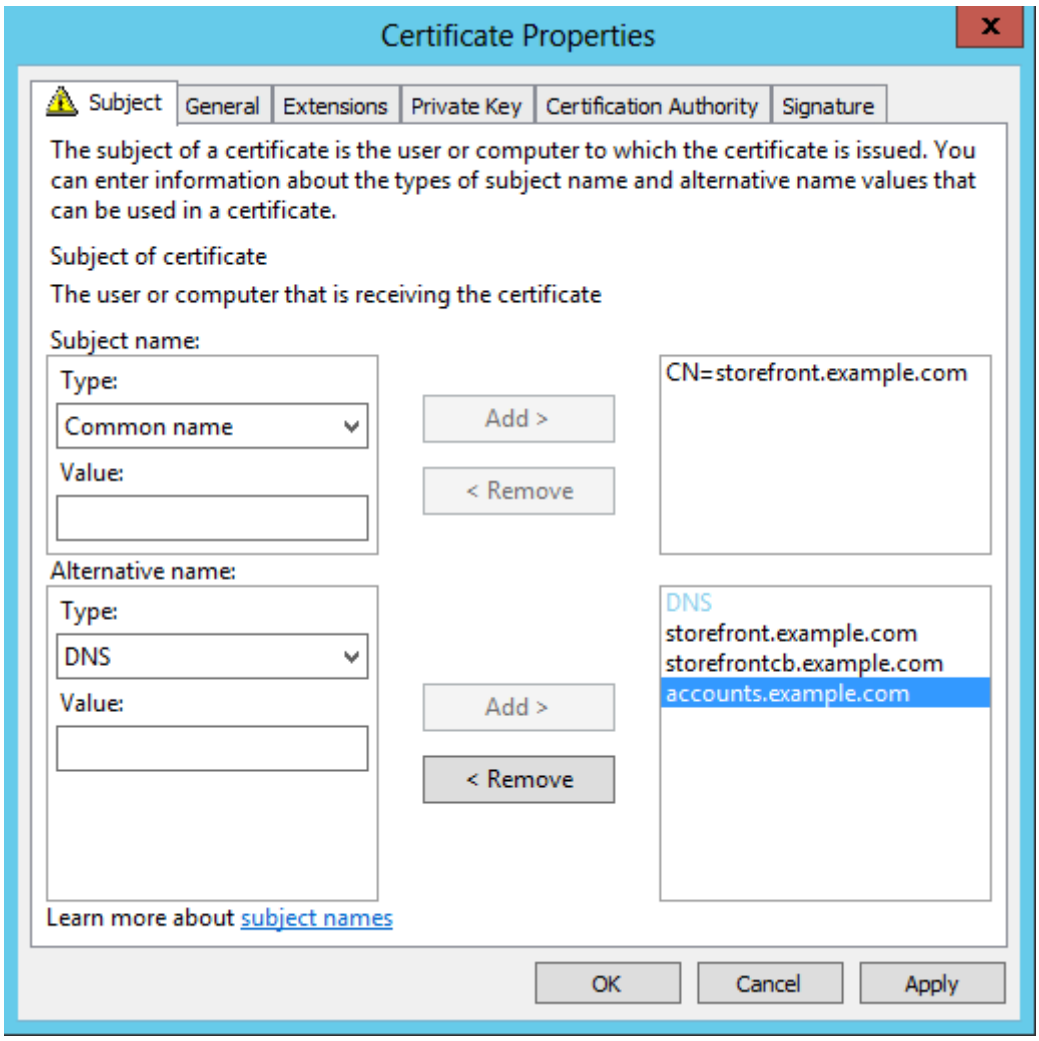
> **Notes**:
>
> - In this article, mentions of “Citrix Workspace app” also apply to the supported versions of Citrix Receiver unless otherwise noted.
> - Citrix Workspace app for Linux does not support single FQDN scenarios because it is not able to detect an internal beacon point to a separate client location. For more information see CTX223989.

Configure the Citrix Gateway virtual server and SSL Certificate

The shared FQDN resolves either to an external firewall router interface IP or Citrix Gateway virtual server IP in the DMZ when external clients try to access resources from outside of the corporate network. Ensure the Common Name and Subject Alternative Name fields of the SSL certificate contain the shared FQDN to be used to access the store externally. By using a third party root CA such as Verisign instead of an enterprise Certification Authority (CA) to sign the gateway certificate, any external client automatically trusts the certificate bound to the gateway vServer. If you use a third party root CA such as Verisign, no additional root CA certificates need to be imported on to external clients.

To deploy a single certificate with the Common Name of the shared FQDN to both the Citrix Gateway and the StoreFront server, consider whether you want to support remote discovery. If so, make sure the certificate follows the specification for the Subject Alternative Names.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



Citrix Gateway virtual server example certificate: `storefront.example.com`

1. Ensure that the shared FQDN, the callback URL, and the accounts alias URL are included in the DNS field as Subject Alternative Name (SANs).
2. Ensure that the private key is exportable so the certificate and key can be imported into the Citrix Gateway.
3. Ensure that Default Authorization is set to Allow.
4. Sign the certificate using a third party CA such as Verisign or an enterprise root CA for your organization.

Two-node server group example SANs

`storefront.example.com` (mandatory)

`storefrontcb.example.com` (mandatory)

© 1999–2022 Citrix Systems, Inc. All rights reserved.

`accounts.example.com` (mandatory)

`storefrontserver1.example.com` (optional)

`storefrontserver2.example.com` (optional)

Sign the Citrix Gateway virtual server SSL certificate using a Certification Authority (CA)

Based on your requirements, you have two options for choosing the type of CA signed certificate.

- Option 1 - Third Party CA signed certificate: If the certificate bound to the Citrix Gateway virtual server is signed by a trusted third party, external clients will likely NOT need any root CA certificates copied to the their trusted root CA certificate stores. Windows clients ship with the root CA certificates of the most common signing agencies. Examples of commercial third party CAs that could be used include DigiCert, Thawte, and Verisign. Note that mobile devices such as iPads, iPhones, and Android tablets and phones might still require the root CA to be copied onto the device to trust the Citrix Gateway virtual server.
- Option 2 - Enterprise Root CA signed certificate: If you choose this option, every external client requires the enterprise root CA certificate copied to their trusted root CA stores. If using portable devices with native Receiver installed, such as iPhones and iPads, create a security profile on these devices.

Import the root certificate into portable devices

- iOS devices can import .CER x.509 certificate files using email attachments, because accessing the local storage of iOS devices is usually not possible.
- Android devices require the same .CER x.509 format. The certificate can be imported from the device local storage or email attachments.

External DNS: storefront.example.com

Ensure that the DNS resolution provided by your organization's Internet service provider resolves to the externally facing IP of the firewall router on the outside edge of DMZ or to the Citrix Gateway virtual server VIP.

Split view DNS

- When split-view DNS is correctly configured, the source address of the DNS request should send the client to the correct DNS A record.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- When clients roam between public and corporate networks, their IP should change. Depending on the network to which they are currently connected, they should receive the correct A record when they query storefront.example.com.

Import certificates issued from a Windows CA to Citrix Gateway

WinSCP is a useful and free third party tool to move files from a Windows machine to a Citrix Gateway file system. Copy certificates for import to the /nsconfig/ssl/ folder within the Citrix Gateway file system. You can use the OpenSSL tools on the Citrix Gateway to extract the certificate and key from a PKCS12/PFX file to create two separate .CER and .KEY X.509 files in PEM format that can be used by the Citrix Gateway

1. Copy the PFX file into /nsconfig/ssl on the Citrix Gateway appliance or VPX.
2. Open the Citrix Gateway command line interface.
3. To switch to the FreeBSD shell, type **Shell** to exit the Citrix Gateway command line interface.
4. To change directory, use `cd /nsconfig/ssl`.
5. Run `openssl pkcs12 -in <imported cert file>.pfx -nokeys -out <certfilename>.cer` and enter the PFX password when prompted.
6. Run `openssl pkcs12 -in <imported cert file>.pfx -nocerts -out <keyfilename>.key`
7. Enter the PFX password when prompted and then set a private key PEM passphrase to protect the .KEY file.
8. To ensure that the .CER and .KEY files were successfully created inside /nsconfig/ssl/, run `ls -al`.
9. To return to the Citrix Gateway command line interface, type Exit.

Citrix Receivers for Windows, or Citrix Receivers for Mac, Citrix Gateway session policy

REQ.HTTP.HEADER User-Agent CONTAINS CitrixReceiver && REQ.HTTP.HEADER X-Citrix-Gateway EXISTS

Receiver for Web Gateway session policy

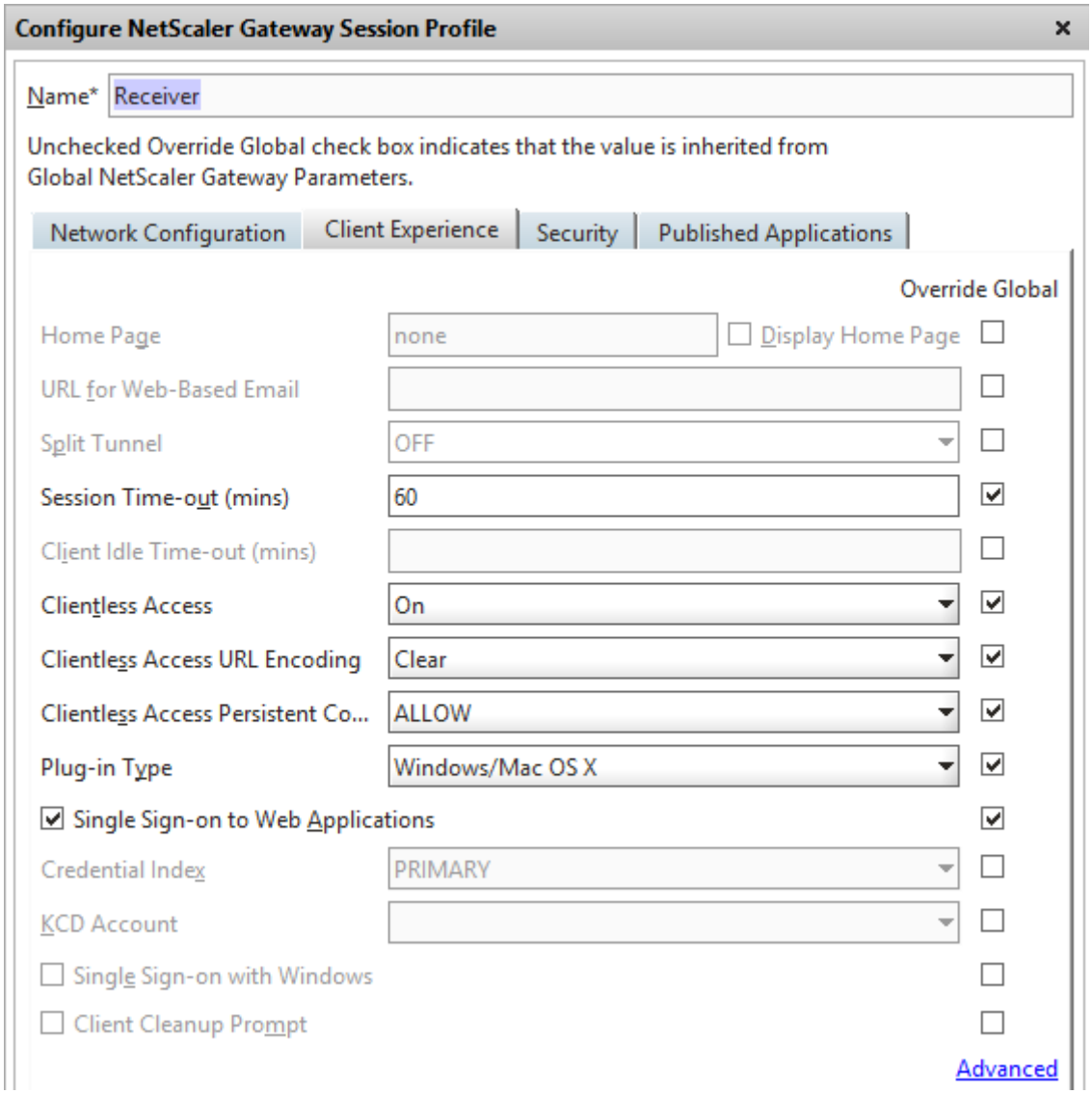
REQ.HTTP.HEADER User-Agent NOTCONTAINS CitrixReceiver && REQ.HTTP.HEADER Referer EXISTS

cVPN and Smart Access Settings

If you use SmartAccess, enable smart access mode on the Citrix Gateway virtual server properties page. Universal Licenses are required for every concurrent user who accesses remote resources.

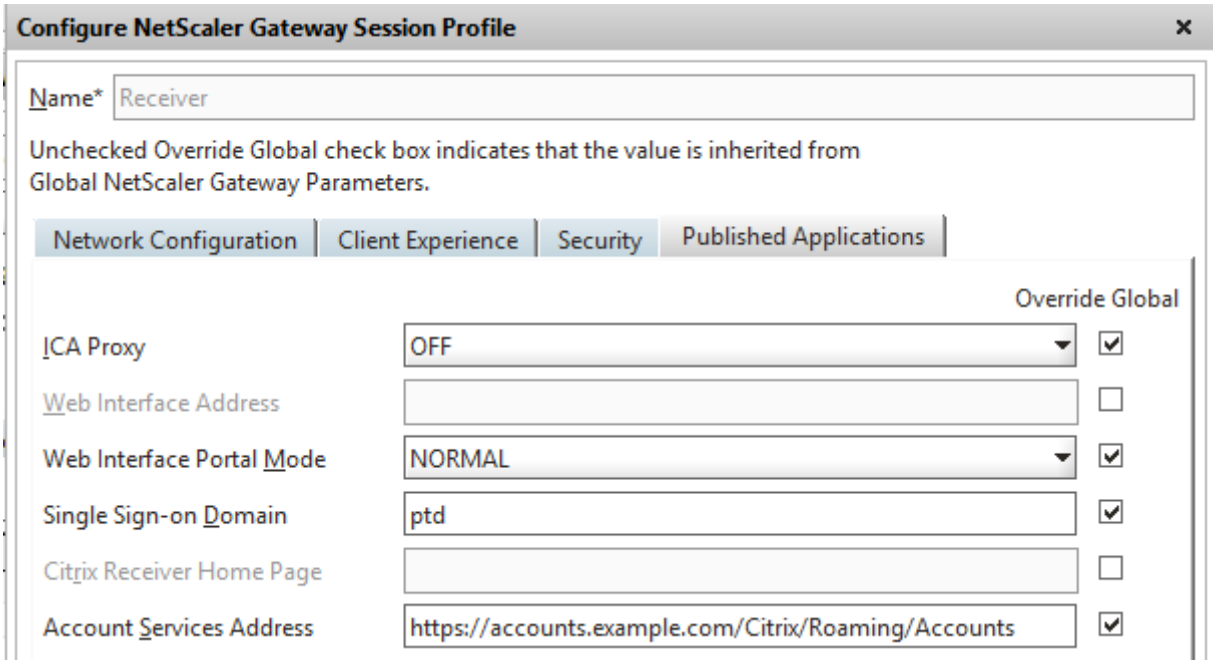
© 1999–2022 Citrix Systems, Inc. All rights reserved.

Receiver profile



Configure the session profile accounts service URL to be `https://accounts.example.com/Citrix/Roaming/Accounts` NOT `https://storefront.example.com/Citrix/Roaming/Accounts`.

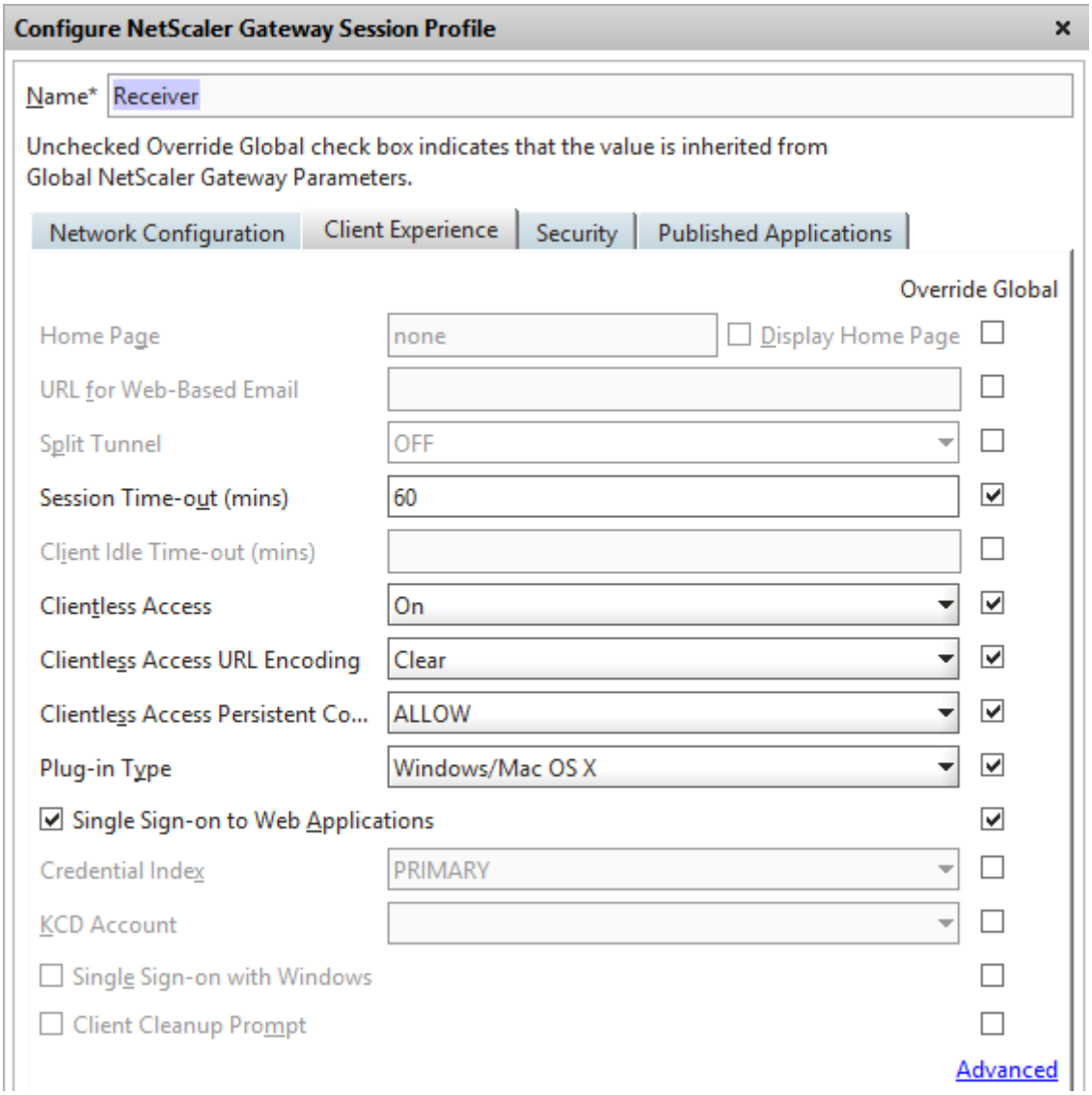
© 1999–2022 Citrix Systems, Inc. All rights reserved.



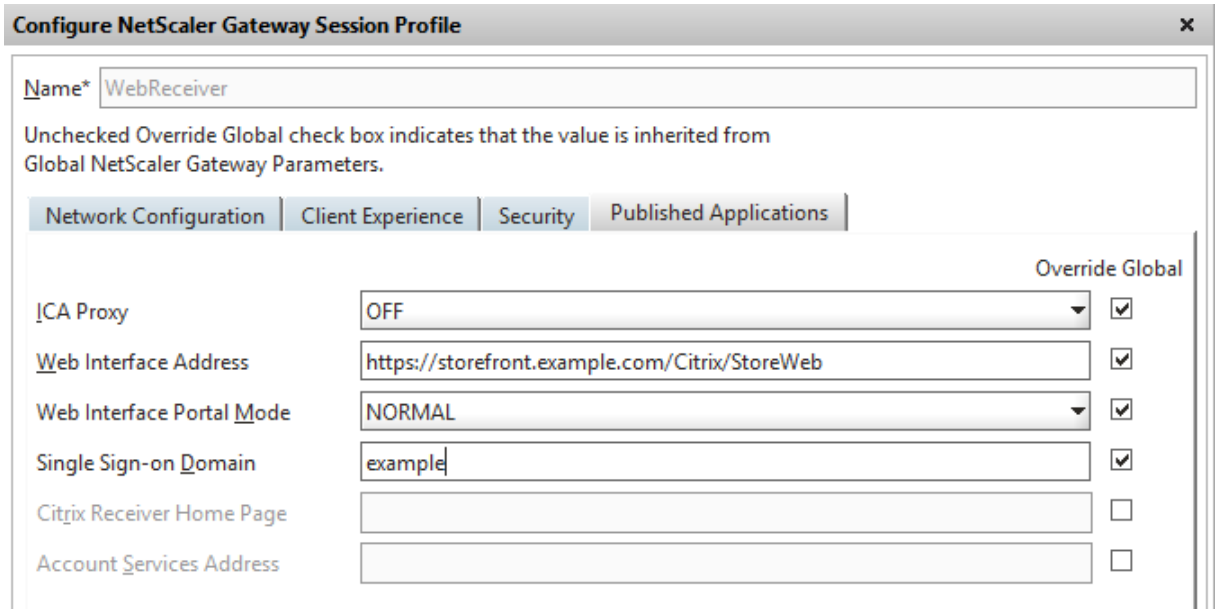
Also add this URL as an additional <allowedAudiences> in the authentication and roaming web.config files on the StoreFront server. For more information, see the “Configure the StoreFront server host base URL, gateway, and SSL certificate” section below.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Receiver for Web profile



© 1999–2022 Citrix Systems, Inc. All rights reserved.

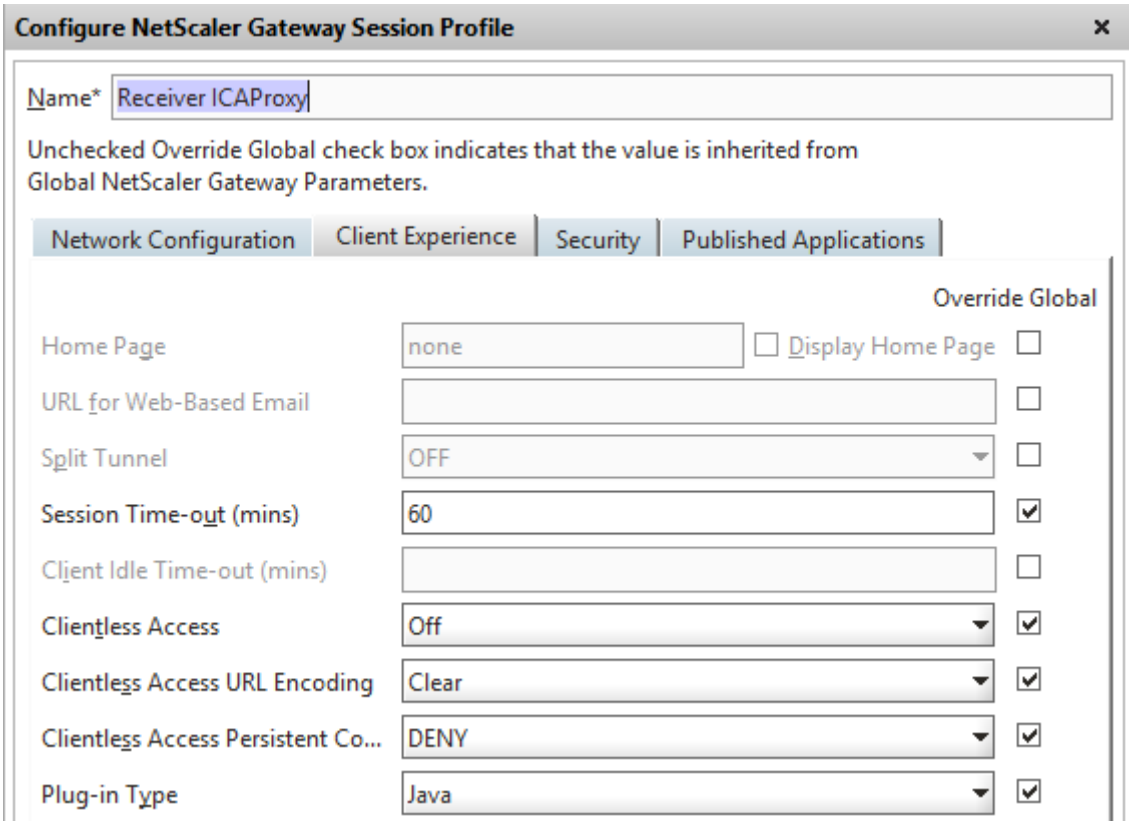


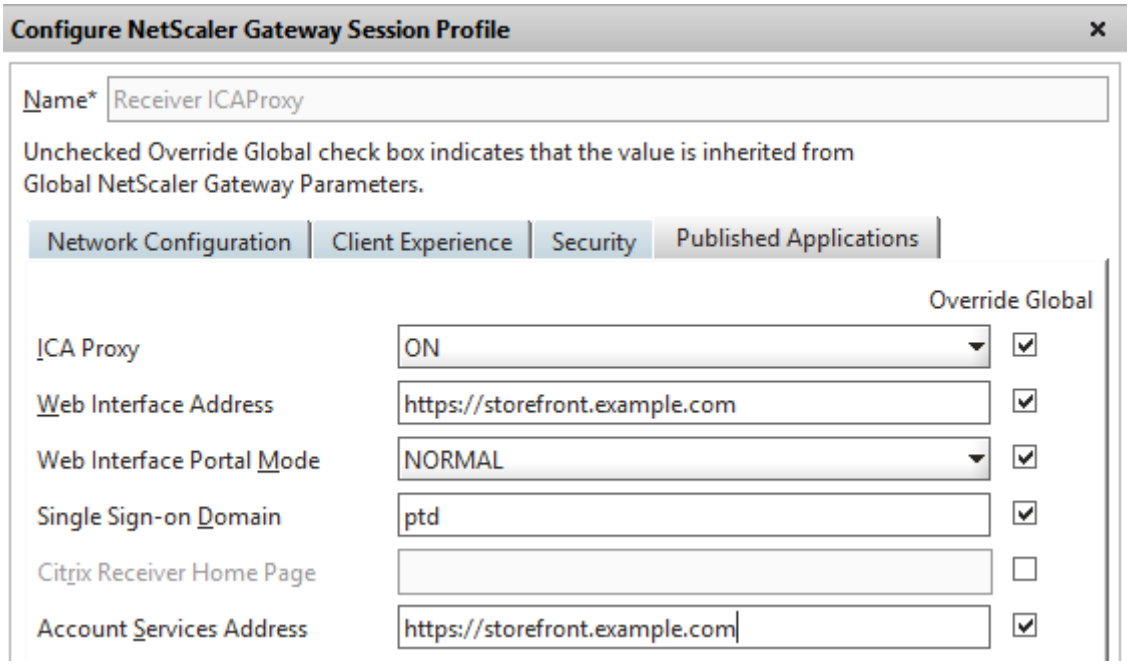
ICA Proxy & Basic Mode settings

If you use ICA proxy, enable basic mode on the Citrix Gateway virtual server properties page. Only a Citrix ADC platform license is required.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

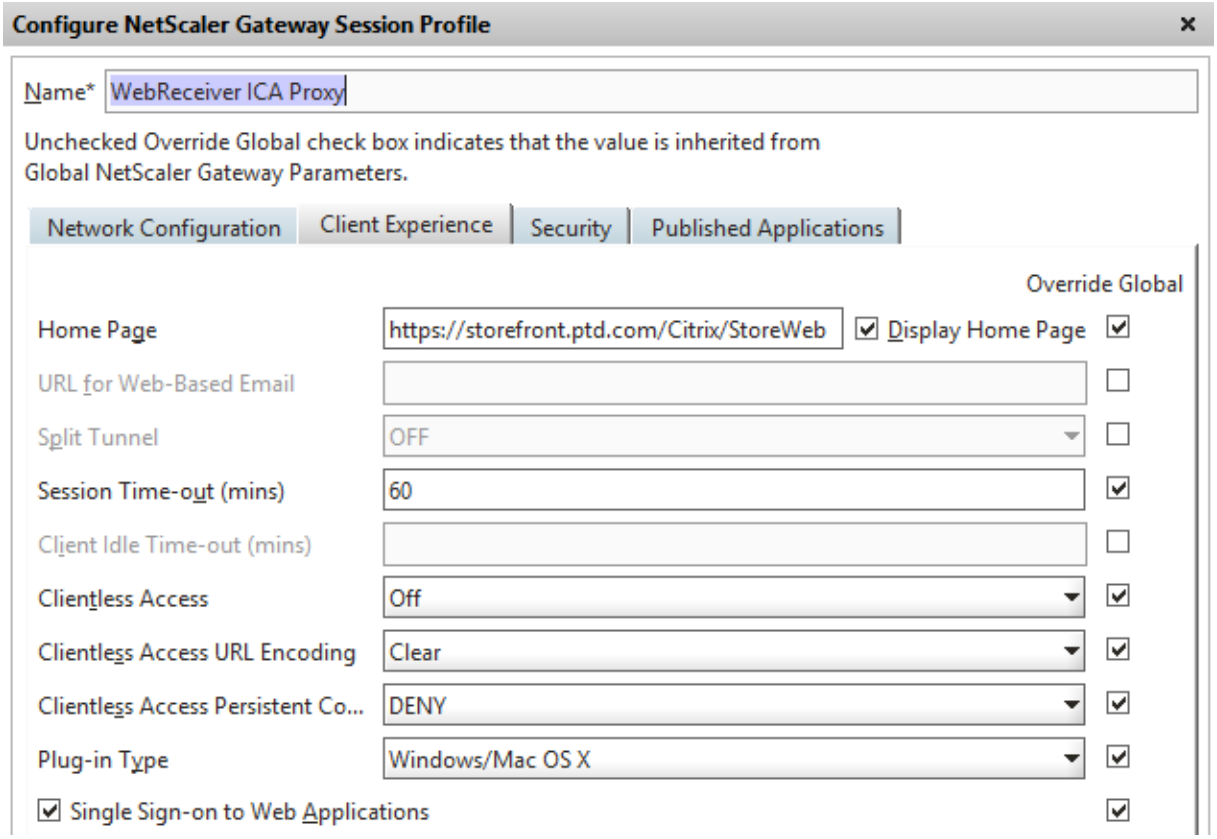
Receiver profile

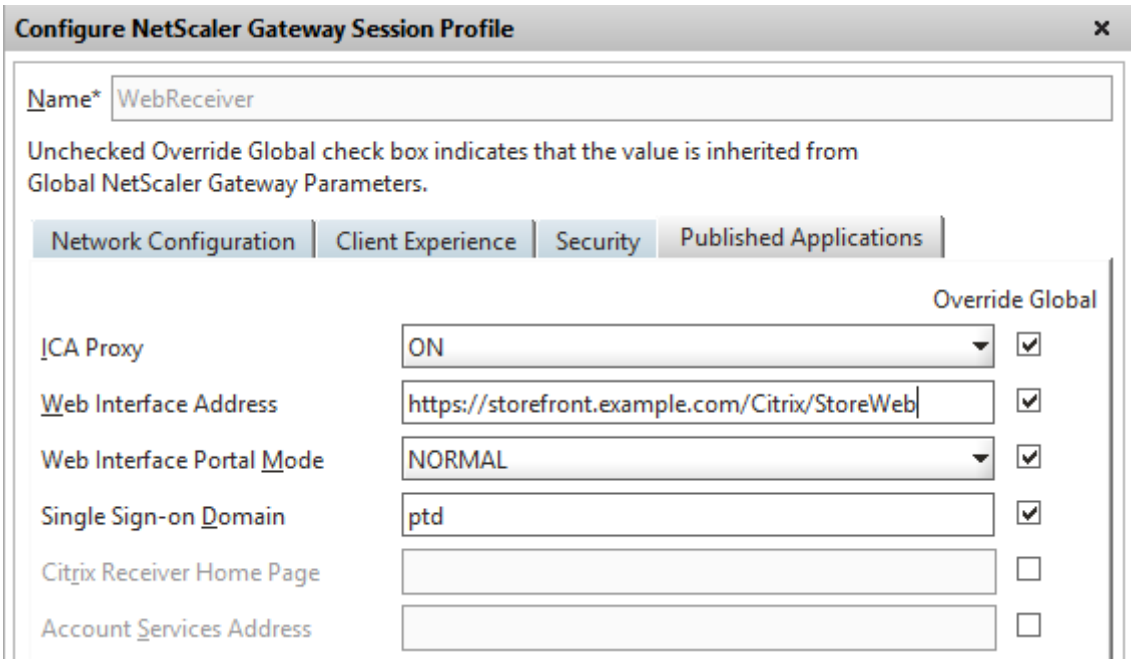




© 1999–2022 Citrix Systems, Inc. All rights reserved.

Receiver for Web profile





© 1999–2022 Citrix Systems, Inc. All rights reserved.

Configure the StoreFront server host base URL, gateway, and SSL certificate

The same shared FQDN that resolves to the Citrix Gateway virtual server should also resolve directly to the StoreFront load balancer, if a StoreFront cluster was created or a single StoreFront IP that hosts the store.

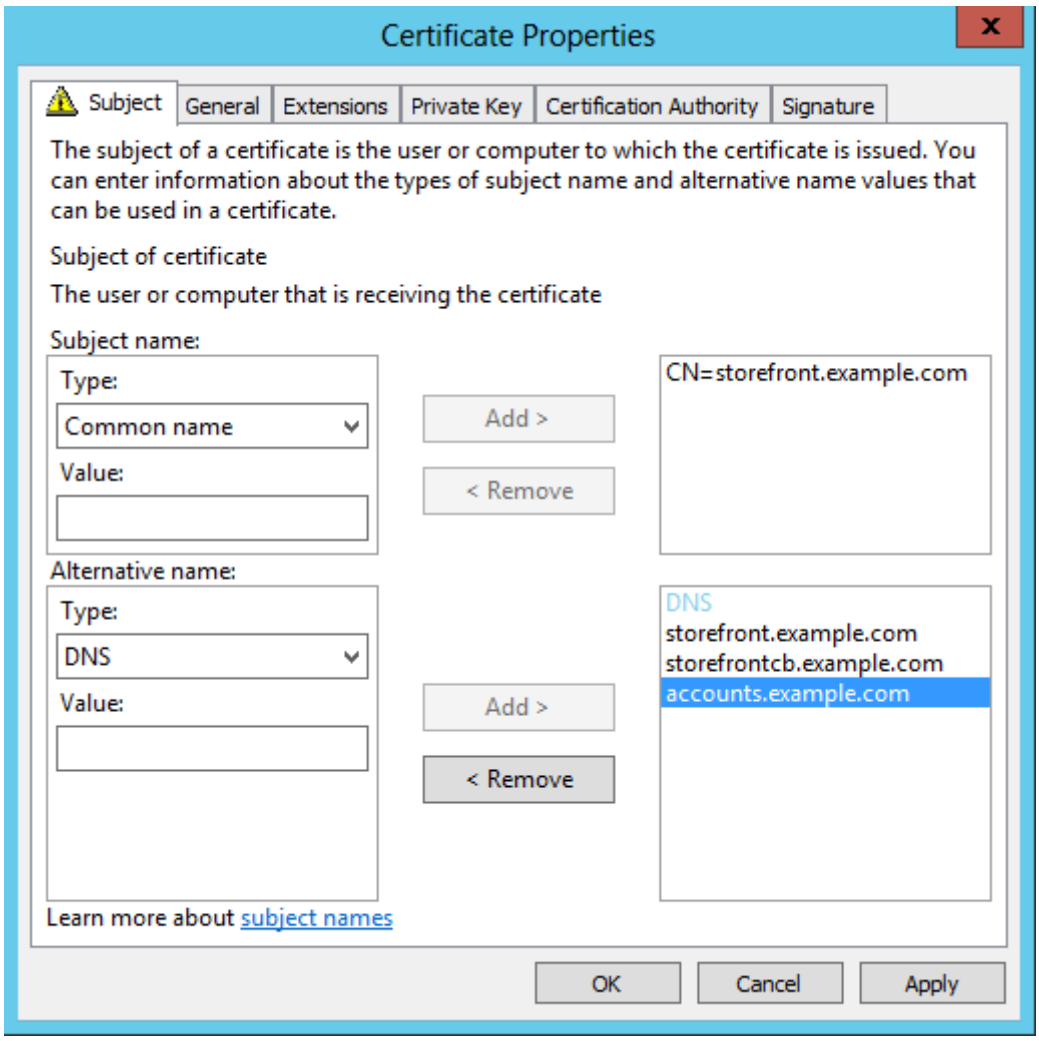
Internal DNS: Create three DNS A records

- storefront.example.com should resolve to the storefront load balancer or single StoreFront server IP.
- storefrontcb.example.com should resolve to the gateway vServer VIP so if a firewall exists between the DMZ and the enterprise local network, allow for this.
- accounts.example.com — create as a DNS alias for storefront.example.com. It also resolves to the load balancer IP for the StoreFront cluster or a single StoreFront server IP.

StoreFront server example certificate: storefront.example.com

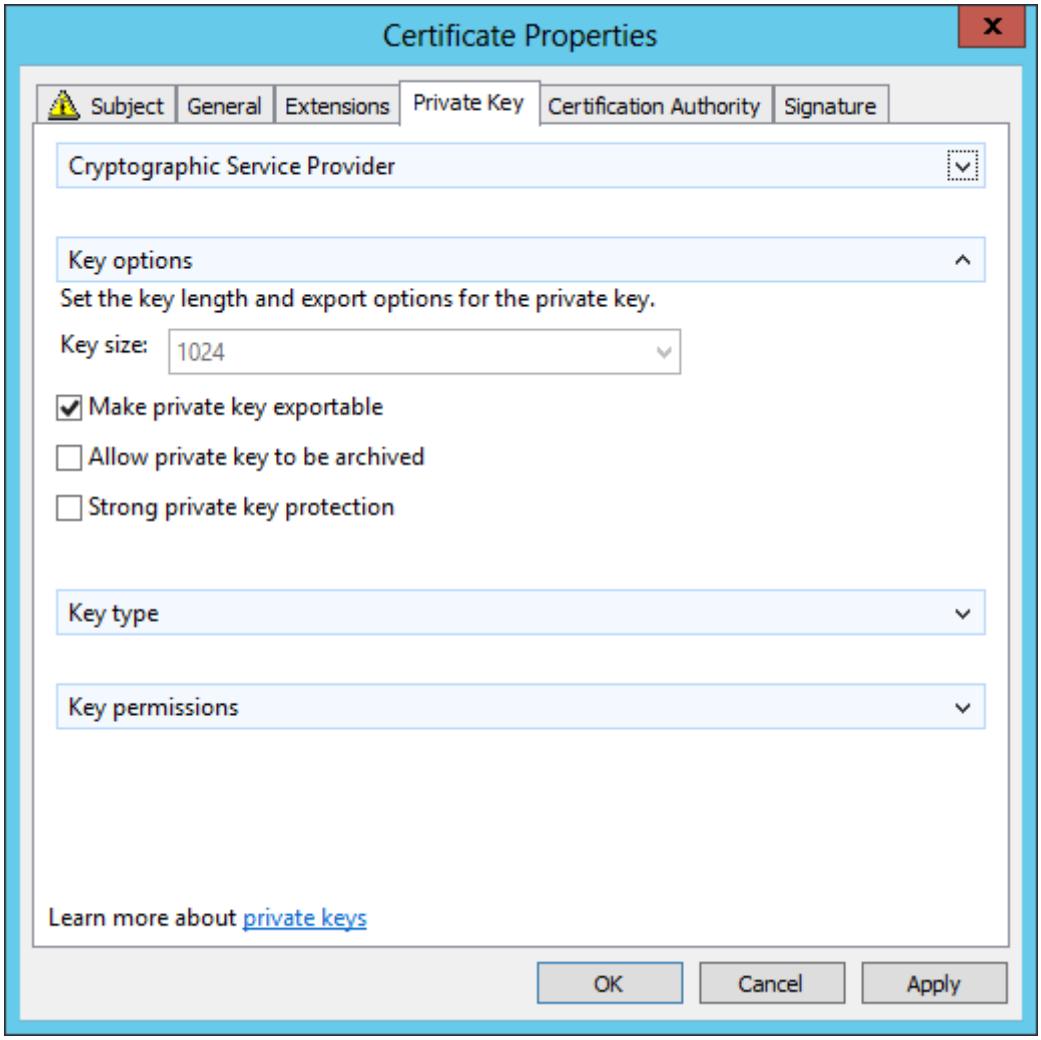
1. Create a suitable certificate for the StoreFront server or server group before installing StoreFront.
2. Add the shared FQDN to the Common name and DNS fields. Ensure this matches the FQDN used in the SSL certificate bound to the Citrix Gateway virtual server that you created earlier or use the same certificate bound to the Citrix Gateway virtual server.
3. Add the account's alias (`accounts.example.com`) as another SAN to the certificate. Note that the accounts alias used in the SAN is the one used in the Citrix Gateway Session Profile in the earlier procedure - **Native Receiver Gateway session policy and profile**.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



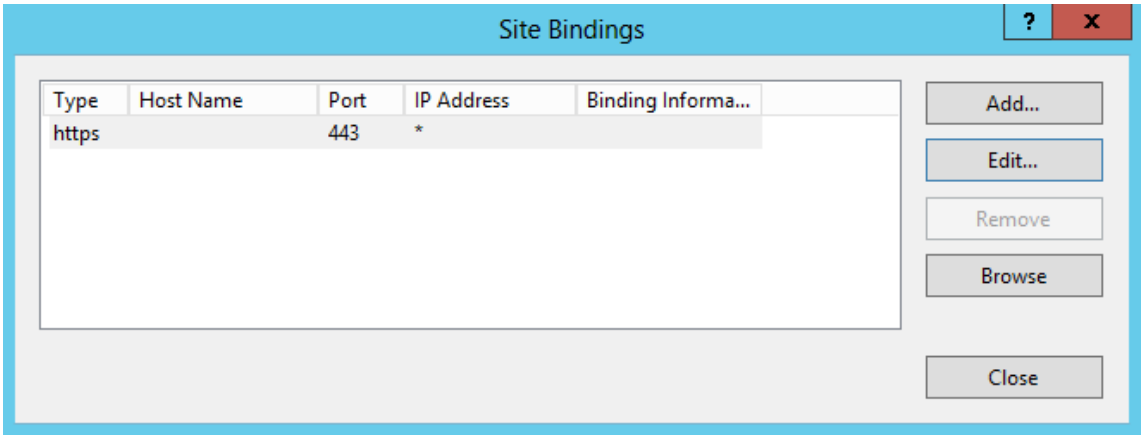
4. Ensure that the private key is exportable so the certificate can be transferred to another server or to multiple StoreFront server group nodes.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



5. Sign the certificate using a third party CA such as VeriSign, your enterprise root CA, or intermediate CA.
6. Export the certificate in PFX format including the private key.
7. Import the certificate and private key into the StoreFront server. If deploying a Windows NLB StoreFront cluster, import the certificate into every node. If using an alternative load balancer, such as a Citrix ADC load balancing virtual server, import the certificate there instead.
8. Create an HTTPS binding in IIS on the StoreFront server and bind the imported SSL certificate to it.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



9. Configure the host base URL on the StoreFront server to match the already chosen shared FQDN.

> Note:
>
> StoreFront always auto selects the last Subject Alternative Name in the list of SANs within the certificate. This is merely a suggested host base URL to assist StoreFront administrators and is usually correct. You can manually set it to any valid `HTTPS://<FQDN>` provided it exists within the certificate as a SAN. Example: `https://storefront.example.com`.

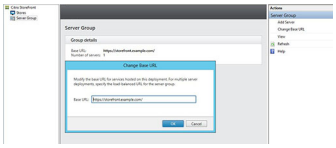
Change the server base URL from HTTP to HTTPS

The host base URL option is available when configuring Single Server deployment or Server Group deployment on Citrix StoreFront. This applies to customers who have installed and configured Citrix StoreFront without a server certificate. After installing the certificate, ensure StoreFront and its services use a secure connection moving forward.

> Note:
>
> The IT Administrator must generate and install a server certificate on Citrix StoreFront server before running this procedure. In addition, an IIS binding needs to be created over HTTPS (443) to secure any new connection.

Complete the following steps to change the base URL on StoreFront 3.x:

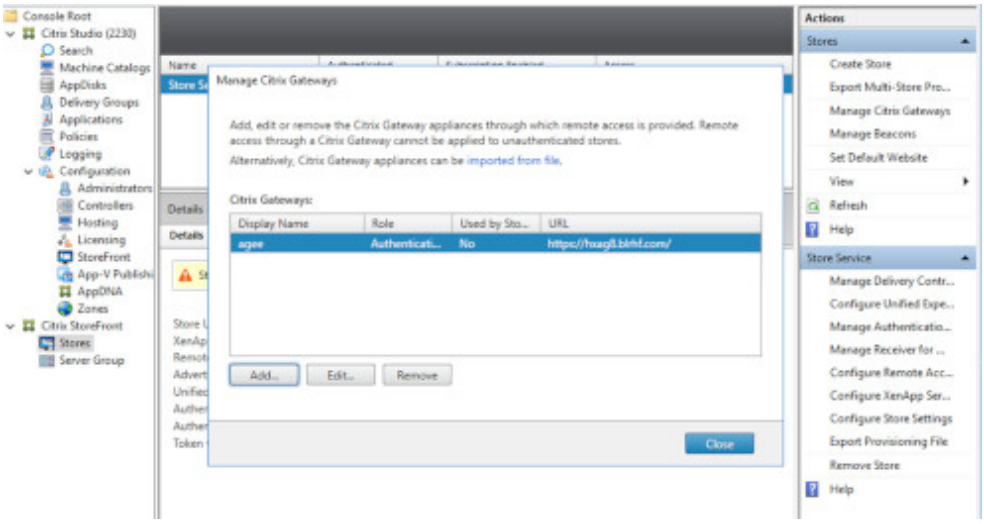
1. In the StoreFront, click **Server Group** on the left panel.
2. Click **Change Base URL** on the right panel.
3. Type the base URL and click **OK**.



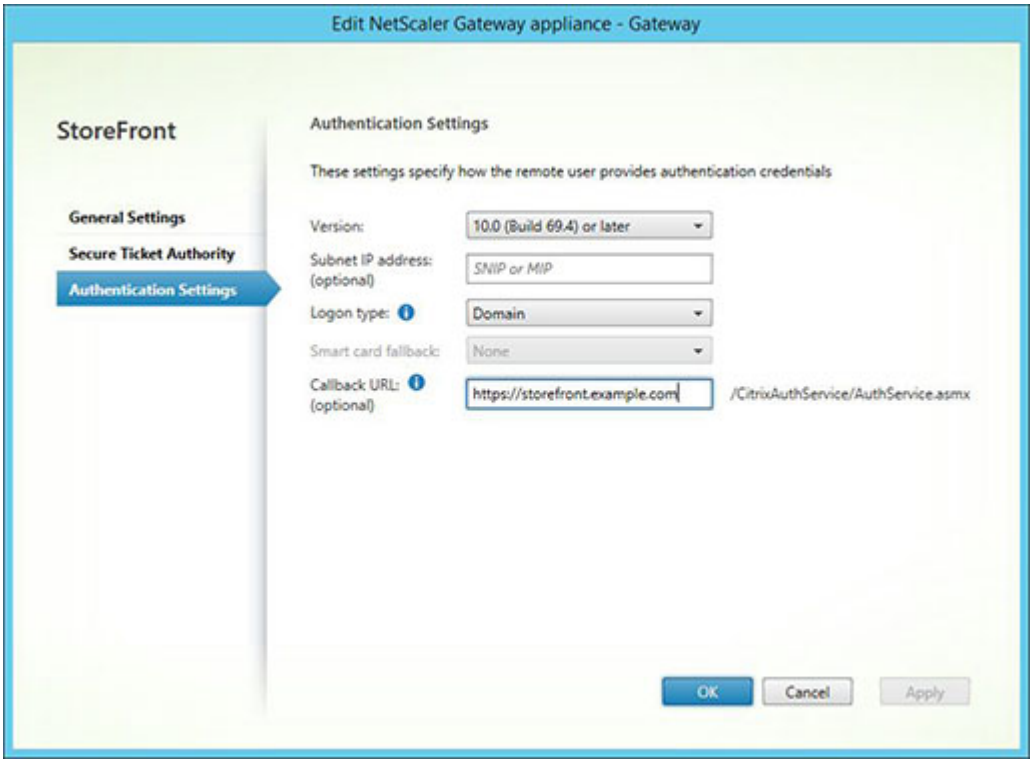
© 1999–2022 Citrix Systems, Inc. All rights reserved.

Configure the Gateway on the StoreFront server: storefront.example.com

1. From the **Stores** node, click on **Manage Citrix Gateways** in the **Actions** pane.
2. Select the **Gateway** from the list and click **Edit**.



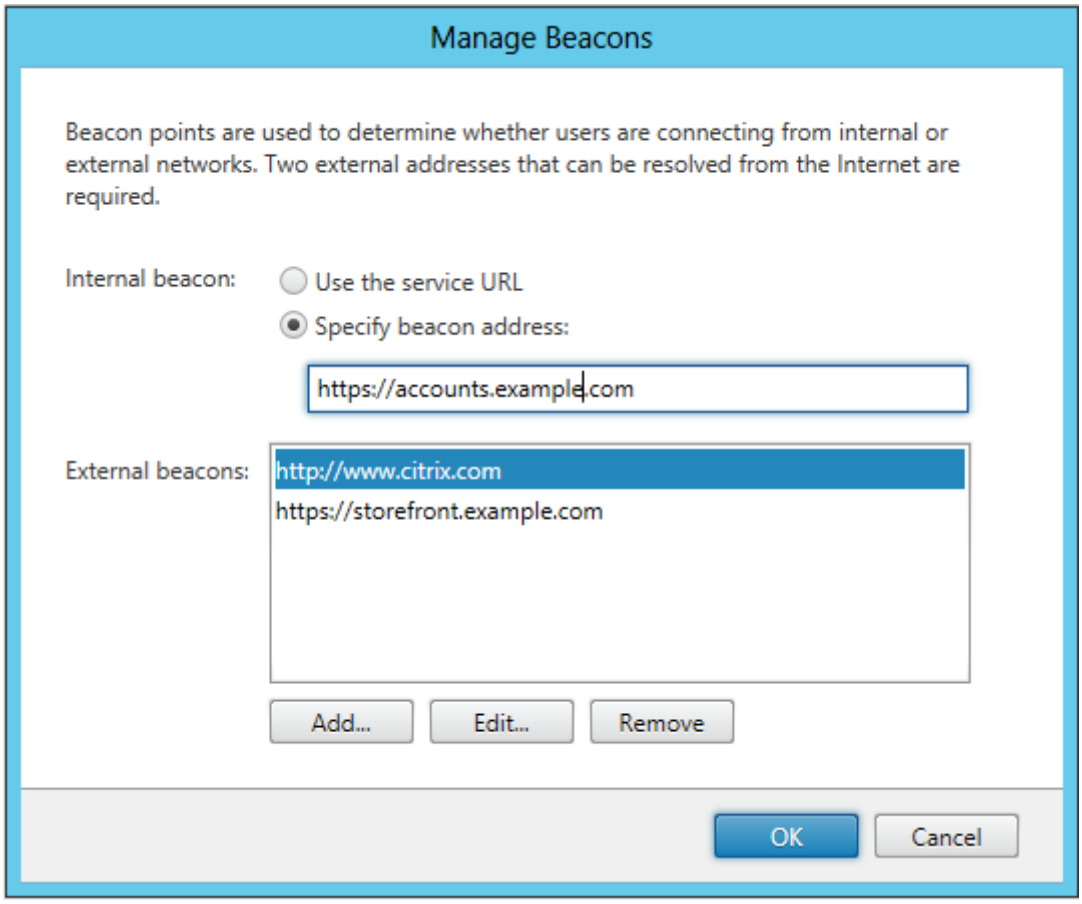
3. On the **General Settings** page, type the shared FQDN in the **Citrix Gateway URL** field.
4. Select the **Authentication Settings** tab and type the callback FQDN into the **Callback URL** field.



5. Select the **Secure Ticket Authority** tab and ensure that the Secure Ticket Authority (STA) servers match the list of Delivery Controllers already configured within the **Store** node.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

6. Enable remote access for the store.
7. Manually set the internal beacon to the accounts alias (accounts.example.com) and it must not be resolvable from outside the gateway. This FQDN must be distinct from the external beacon that is shared by the StoreFront hostbase URL and Citrix Gateway virtual server (storefront.example.com). DO NOT use the shared FQDN, as this creates a situation where both the internal and external beacons are identical.



Support discovery using multiple different FQDNs

To allow Citrix Workspace app to discover a Store using multiple FQDNS, use the following steps. If the provisioning file configuration is enough or if you are using only Receiver for Web, you can skip the following steps.

Add an additional `<allowedAudiences>` entry in *C:\inetpub\wwwroot\Citrix\Authentication\web.config*. There are two `<allowedAudiences>` entries in this file. Only the first entry in the file for the Authentication Token Producer requires you to add an additional `<allowedAudience>` entry.

1. In the section <service id>, find the <allowedAudiences> string. Add a line for `audience="https://accounts.example.com/"` as shown here. Save, and close the web.config file.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

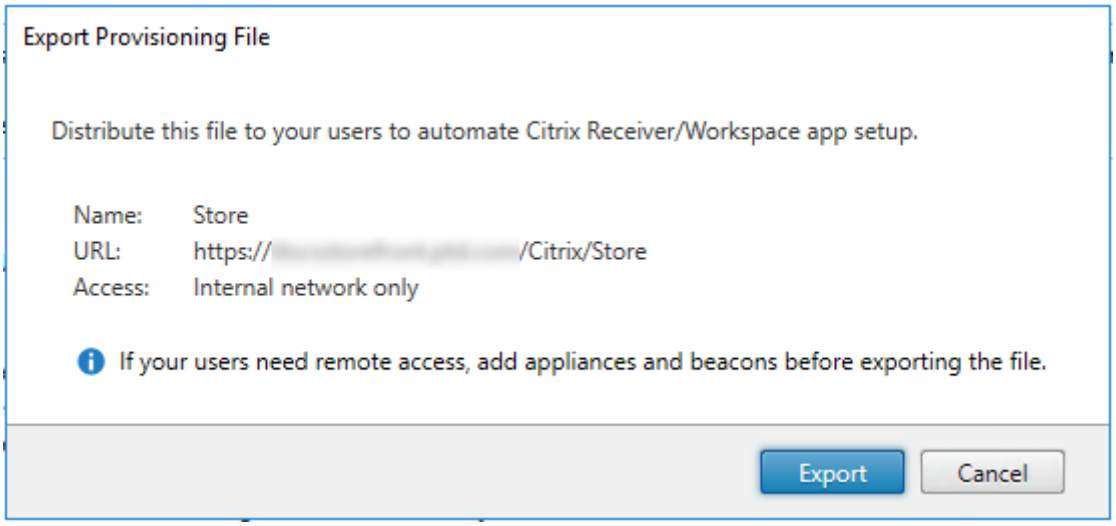
```
\<service id="abd6f54b-7d1c-4a1b-a8d7-14804e6c8c64" displayName="
    Authentication Token Producer">
...
\<allowedAudiences>
\<add name="https-storefront.example.com" audience="https://
    storefront.example.com/" />
\<add name="https-accounts.example.com" audience="https://accounts
    .example.com/" />
\</allowedAudiences>
<!--NeedCopy-->
```

2. In *C:\inetpub\wwwroot\Citrix\Roaming\web.config*, locate the <tokenManager> section and add a line for `audience="https://accounts.example.com/"` as shown here. Save, and close the web.config file.

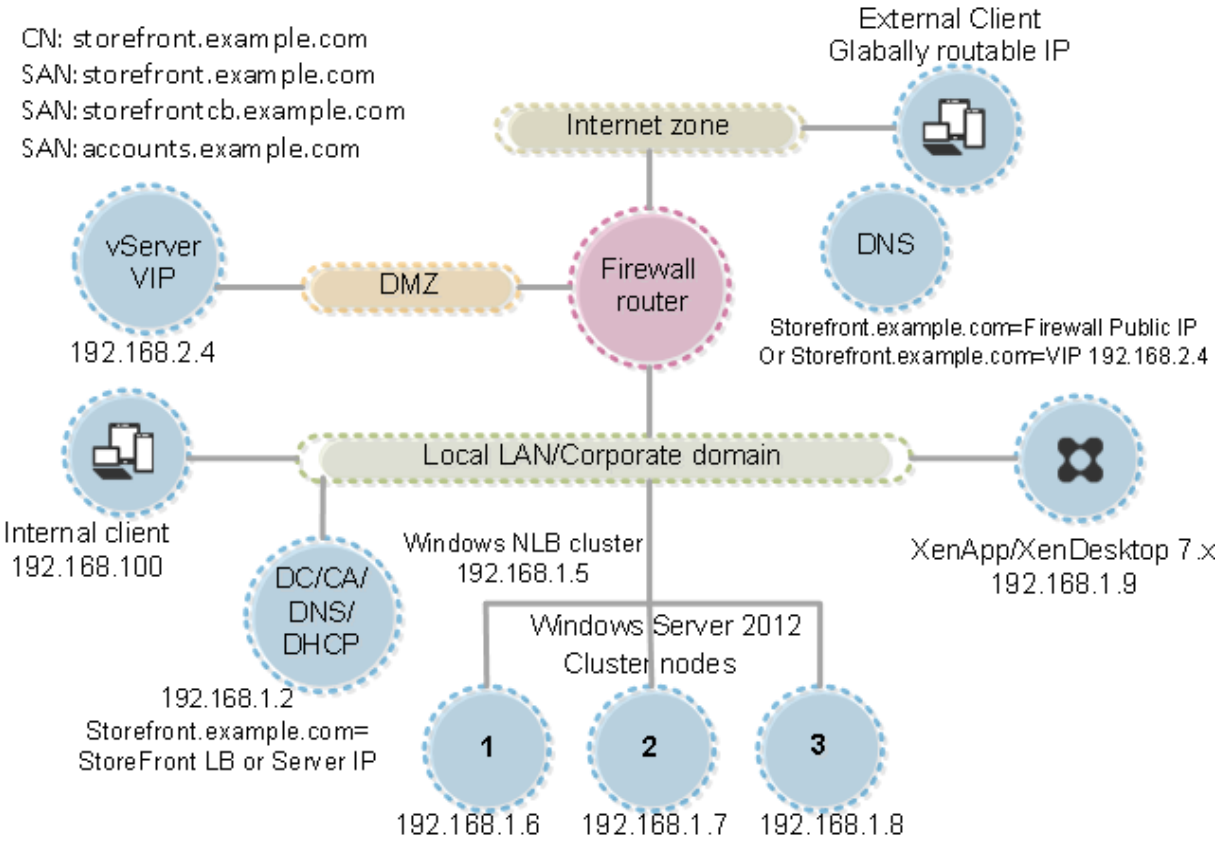
```
\<tokenManager>
\<services>
\<clear />
...
\</trustedIssuers>
\<allowedAudiences>
\<add name="https-storefront.example.com" audience="https://
    storefront.example.com/" />
\<add name="https-accounts.example.com" audience="https://accounts
    .example.com/" />
\</allowedAudiences>
\</service>
\</services>
\</tokenManager>
<!--NeedCopy-->
```

Alternatively, you can export the native receiver .CR provisioning file for the store. This eliminates the need for First Time Use configuration of Citrix Workspace app. Distribute this file to all Windows and MAC Citrix Workspace app clients.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



If Citrix Workspace app is installed on the client, the .CR file type is recognized and double clicking on the provisioning file starts the import.



© 1999–2022 Citrix Systems, Inc. All rights reserved.

Advanced configurations

April 29, 2020

You can configure the following advanced option using the StoreFront console, PowerShell, certificate properties, or configuration files.

Task	Detail
Configure Resource Filtering	Filter enumeration resources based on resource type and keywords.

Configure Resource Filtering

April 29, 2020

This topic explains how to filter enumeration resources based on resource type and keywords. You can use this type of filtering with the more advanced customization offered by the Store Customization SDK. Using this SDK, you can control which apps and desktops are displayed to users, modify access conditions, and adjust launch parameters. For more information, see the Citrix StoreFront SDK PowerShell Modules.

> Note:
>
> The StoreFront and PowerShell consoles cannot be open at the same time. Always close the StoreFront admin console before using the PowerShell console to administer your StoreFront configuration. Likewise, close all instances of PowerShell before opening the StoreFront console.

Configure filtering

Configure the filter using PowerShell cmdlets defined within the StoresModule. Use the following PowerShell snippet to load the required modules:

```
$dsInstallProp = Get-ItemProperty `
 -Path HKLM:\SOFTWARE\Citrix\DeliveryServicesManagement -Name
    InstallDir
$dsInstallDir = $dsInstallProp.InstallDir
& $dsInstallDir\..\Scripts\ImportModules.ps1
<!--NeedCopy-->
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Filter by type

Use this to filter the resource enumeration by resource type. This is an inclusive filter, meaning it removes any resources that are not of the specified types from the resource enumeration result. Use the following cmdlets:

Set-DSResourceFilterType: Sets up enumeration filtering based on resource types.

Get-DSResourceFilterType: Gets the list of resource types that Storefront is allowed to return in enumeration.

Note: Resource types are applied before keywords.

Filter by keywords

Use this to filter resources based on keywords, such as resources derived from Citrix Virtual Apps and Desktops. Keywords are generated from mark-up in the description field of the corresponding resource.

The filter can operate either in inclusive or exclusive mode, but not both. The inclusive filter allows enumeration of resources matching the configured keywords and removes non matching resources from the enumeration. The exclusive filter removes resources matching the configured keywords from the enumeration. Use the following cmdlets:

Set-DSResourceFilterKeyword: Sets up enumeration filtering based on resource keywords.

Get-DSResourceFilterKeyword: Gets the list of filter keywords.

The following keywords are reserved and must not be used for filtering:

- Auto
- Mandatory

For more information on keywords, see Optimize the user experience and Configuring application delivery.

Examples

This command sets filtering to exclude workflow resources from enumeration:

```
Set-DSResourceFilterKeyword -SiteId 1 -VirtualPath "/Citrix/Store" -
    ExcludeKeywords @("WFS")
<!--NeedCopy-->
```

This example sets allowed resource types to applications only:

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
Set-DSResourceFilterType -SiteId 1 -VirtualPath "/Citrix/Store" -
    IncludeTypes @("Applications")
<!--NeedCopy-->
```

Configure using configuration files

April 29, 2020

You can use configuration files to configure additional settings for Citrix StoreFront and Citrix Receiver for Web that cannot be set with the Citrix StoreFront management console.

The Citrix StoreFront settings you can configure include:

- Enable ICA file signing
- Disable file type association
- Customize the Citrix Workspace app logon dialog box
- Prevent Citrix Workspace app for Windows from caching passwords and usernames

The Citrix Receiver for Web settings you can configure include:

- How resources are displayed for users
- Disable the My Apps Folder View

Configure StoreFront using the configuration files

October 13, 2020

This article describes additional configuration tasks that cannot be carried out using the Citrix StoreFront management console.

> **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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Enable 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 Receiver, the configuration of which determines whether the unsigned file is accepted.

To be used for ICA file signing with StoreFront, certificates must include the private key and be within the allowed validity period. If the certificate contains a key usage extension, this must allow the key to be used for digital signatures. Where an extended key usage extension is included, it must be set to code signing or server authentication.

For ICA file signing, Citrix recommends using a code signing or SSL signing certificate obtained from a public certification authority or from your organization's private certification authority. If you are unable to obtain a suitable certificate from a certification authority, you can either use an existing SSL certificate, such as a server certificate, or create a new root certification authority certificate and distribute it to users' devices.

ICA file signing is disabled by default in stores. To enable ICA file signing, you edit the store configuration file and execute Windows PowerShell commands. For more information about enabling ICA file signing in Citrix Workspace app, see ICA File Signing to protect against application or desktop launches from untrusted servers.

> Note:
>
> The StoreFront and PowerShell consoles cannot be open at the same time. Always close the StoreFront admin console before using the PowerShell console to administer your StoreFront configuration. Likewise, close all instances of PowerShell before opening the StoreFront console.

1. Ensure that the certificate you want to use to sign ICA files is available in the Citrix Delivery Services certificate store on the StoreFront server and not in the current user's certificate store.

   Do this by launching MMC.exe console, adding Certificate Snap-in \Local Machine, expand the Cert Store node, find "Citrix Delivery Services", and import the certificate.

2. Use a text editor to open the web.config file for the store, which is typically located in the C:\inetpub\wwwroot\Citrix\storename\ directory, where storename is the name specified for the store when it was created.

3. Locate the following section in the file.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
<certificateManager>
    <certificates>
        <clear />
        <add ... />
        ...
    </certificates>
</certificateManager>
<!--NeedCopy-->
```

4. Include details of the certificate to use for signing.

```
<certificateManager>
    <certificates>
        <clear />
        <add id="certificateid" thumb="certificatethumbprint" />
        <add ... />
    ...
    </certificates>
</certificateManager>
<!--NeedCopy-->
```

Where **certificateid** is a value that helps you to identify the certificate in the store configuration file and **certificatethumbprint** is the digest (or thumbprint) of the certificate data produced by the hash algorithm. **certificateID** can be any number you choose, as long as it is not used for any other certificates.

5. Locate the following element in the file.

```
<icaFileSigning enabled="False" certificateId="" hashAlgorithm="
    sha1" />
<!--NeedCopy-->
```

6. Change the value of the enabled attribute to True to enable ICA file signing for the store. Set the value of the **certificateId** attribute to the ID you used to identify the certificate, that is, **certificateid** in Step 4.
7. If you want to use a hash algorithm other than SHA-1, set the value of the hashAgorithm attribute to sha256, sha384, or sha512, as required.
8. Using an account with local administrator permissions, start Windows PowerShell and, at a command prompt, type the following commands to enable the store to access the private key.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
Add-PSSnapin Citrix.DeliveryServices.Framework.Commands
$certificate = Get-DSCertificate "Certificate_thumbprint_ID"
Add-DSCertificateKeyReadAccess -certificate $certificate[0] -
    accountName "IIS APPPOOL\Citrix Delivery Services Resources"

<!--NeedCopy-->
```

where `Certificate_thumbprint_ID` is the digest (or thumbprint) of the certificate data produced by the hash algorithm.

> **Note:**
>
> If the `$certificate` value is null, use the following commands instead:
>
> ‘‘‘
>
> Add-PSSnapin Citrix.DeliveryServices.Framework.Commands
> $certificate = Get-Item ‘Cert:\LocalMachine\Citrix Delivery Services\Certificate_thumbprint_ID’
> Add-DSCertificateKeyReadAccess -certificate $certificate[0] -accountName “IIS APPPOOL\Citrix Delivery Services Resources”

Disable 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 disable file type association, you edit the store configuration file.

1. Use a text editor to open the web.config file for the store, which is typically located in the C:\inetpub\wwwroot\Citrix\storename\ directory, where storename is the name specified for the store when it was created.
2. Locate the following element in the file.

```
<farmset ... enableFileTypeAssociation="on" ... >
```

3. Change the value of the enableFileTypeAssociation attribute to off to disable file type association for the store.

Configure how resources are displayed for users

When both desktops and applications are available in a store, separate desktop and application views are displayed by default. Users see the desktop view first when they access the store. If only a single

© 1999–2022 Citrix Systems, Inc. All rights reserved.

desktop is available for a user, regardless of whether applications are also available in the store, that desktop starts automatically when the user accesses the store. To change these settings, edit the StoreWeb's configuration file.

1. Use a text editor to open the `web.config` file for the Citrix Receiver for Web site, which is typically located in the `C:\inetpub\wwwroot\Citrix\<storename>Web\` directory, where storename is the name specified for the store when it was created.
2. Locate the following element in the file.

```
<uiViews showDesktopsView="true" showAppsView="true" defaultView="
    desktops" />
```

3. Change the value of the **showDesktopsView** and **showAppsView** attributes to false to prevent desktops and applications, respectively, being displayed to users, even if they are available in the store. When both the desktop and application views are enabled, set the value of the defaultView attribute to apps to display the application view first when users access the store.
4. Locate the following element in the file.

```
<userInterface ... autoLaunchDesktop="true">
```

5. Change the value of the **autoLaunchDesktop** attribute to **false** to prevent StoreFront automatically starting a desktop when a user accesses the store and only a single desktop is available for that user.

   When the **autoLaunchDesktop** attribute is set to **true** and a user for whom only one desktop is available accesses the store, that user's applications are not reconnected, regardless of the workspace control configuration.

Customize the Citrix Workspace app logon dialog box

When users log on to a store, no title text is displayed on the logon dialog box, by default. You can display the default text "Please log on" or compose your own custom message. To display and customize the title text on the logon dialog box, you edit the files for the authentication service.

1. Use a text editor to open the UsernamePassword.tfrm file for the authentication service, which is typically located in the C:\inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\ directory.
2. Locate the following lines in the file.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

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

```
@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\Authentication\App_Data\r 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 Receiver for Windows or Citrix Workspace app for Windows, but not Citrix Receiver for Windows Enterprise, from caching users' passwords, you edit the files for the authentication service.

1. Use a text editor to open the file inetpub\wwwroot\Citrix\Authentication\App_Data\Templates\UsernamePa
2. Locate the following line in the file.

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

3. Comment the statement as shown below.

```
<!-- @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. This setting does not apply to Citrix Receiver for Windows Enterprise.

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

By default, Citrix Receiver for Windows automatically populated the last username entered. To supress population of the username field, edit the registry on the user device:

1. Create a REG_SZ value HKLM\SOFTWARE\Citrix\AuthManager\RememberUsername.
2. Set its value "false".
   "'

Configure Citrix Receiver for Web sites using the configuration files

April 29, 2020

This article describes additional configuration tasks for Citrix Receiver for Web sites that cannot be carried out using the Citrix StoreFront management console.

> **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.

Configure how resources are displayed for users

When both desktops and applications are available from a Citrix Receiver for Web site, separate desktop and application views are displayed by default. Users see the desktop view first when they log

© 1999–2022 Citrix Systems, Inc. All rights reserved.

on to the site. If only a single desktop is available for a user, regardless of whether applications are also available from a site, that desktop starts automatically when the user logs on. To change these settings, you edit the site configuration file.

1. Use a text editor to open the web.config file for the Citrix Receiver for Web site, which is typically located in the C:\inetpub\wwwroot\Citrix\storenameWeb\ directory, where storename is the name specified for the store when it was created.
2. Locate the following element in the file.

```
<uiViews showDesktopsView="true" showAppsView="true" defaultView="
    desktops" />
<!--NeedCopy-->
```

3. Change the value of the **showDesktopsView** and **showAppsView** attributes to false to prevent desktops and applications, respectively, being displayed to users, even if they are available from the site. When both the desktop and application views are enabled, set the value of the defaultView attribute to apps to display the application view first when users log on to the site.
4. Locate the following element in the file.

```
<userInterface ... autoLaunchDesktop="true">
<!--NeedCopy-->
```

5. Change the value of the **autoLaunchDesktop** attribute to **false** to prevent Citrix Receiver for Web sites from automatically starting a desktop when a user logs on to the site and only a single desktop is available for that user.

   When the **autoLaunchDesktop** attribute is set to **true** and a user for whom only one desktop is available logs on, that user's applications are not reconnected, regardless of the workspace control configuration.

> **Note:**
>
> To enable Citrix Receiver for Web sites to start their desktops automatically, users accessing the site through Internet Explorer must add the site to the Local intranet or Trusted sites zones.

Disable the My Apps Folder View

1. Use a text editor to open the web.config file for the Citrix Receiver for Web site, which is typically located in the C:\inetpub\wwwroot\Citrix\storenameWeb\ directory, where storename is the name specified for the store when it was created.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

2. Locate the following element in the file.

```
<userInterface enableAppsFolderView="true">
<!--NeedCopy-->
```

3. Change the value of the **enableAppsFolderView** attribute to **false** to disable Citrix Receiver for Web My Apps Folder View.

Secure your StoreFront deployment

January 11, 2022

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

Application Pool recycling limits

You can set the following Application Pool recycling limits:

- Virtual Memory Limit: 4,294,967,295
- Private Memory Limit: the size of the physical memory of the StoreFront server
- Request Limit: 4,000,000,000

Configure Microsoft Internet Information Services (IIS)

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

Filename extensions

You can disallow unlisted file name extensions.

StoreFront requires the following file name extensions in Request Filtering:

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

If download or upgrade of Citrix Workspace app is enabled for Citrix Receiver for Web, 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

MIME Types

You can remove MIME Types corresponding to the following file types:

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

Request Filtering

StoreFront requires the following HTTP verbs in Request Filtering. You can disallow unlisted verbs.

- GET
- POST
- HEAD

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Other Microsoft IIS settings

StoreFront does not require:

- ISAPI filters
- ISAPI extensions
- CGI programs
- FastCGI programs

> **Important:**
>
> - Do not configure IIS Authorization Rules. StoreFront supports authentication directly, and does not use or support IIS authentication.
> - Do not select **Client certificates: Require**, in the SSL Settings for the StoreFront site. StoreFront installation configures the appropriate pages of the StoreFront site with this setting.
> - StoreFront requires cookies. The Use Cookies setting must be selected. Do not select the cookieless/Use URI setting.
> - StoreFront requires Full Trust. Do not set the global .NET trust level to High or lower.
> - StoreFront does not support a separate application pool for each site. Do not modify these site settings.

Configure user rights

> Note:
>
> 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, its application pools are granted the logon right **Log on as a service** and the privileges **Adjust memory quotas for a process, Generate security audits**, and **Replace a process level token**. This is normal installation behavior when application pools are created. The application pools are Citrix Configuration Api, Citrix Delivery Services Resources, Citrix Delivery Services Authentication, and Citrix Receiver for Web.

You do not need to change these user rights. These privileges are not used by StoreFront and are automatically disabled.

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)

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- Citrix Subscriptions Store (NT SERVICE\CitrixSubscriptionsStore)
- Citrix Default Domain Services (NT SERVICE\CitrixDefaultDomainService)

If you configure StoreFront Kerberos constrained delegation for XenApp 6.5, this creates the Citrix StoreFront Protocol Transition service (NT SERVICE\SYSTEM). This service requires a privilege not normally granted to Windows services.

Configure service settings

The StoreFront Windows services listed above in the "Configure user rights" section are configured to log on as the NETWORK SERVICE identity; do not change this configuration. The Citrix StoreFront Protocol Transition service logs on as SYSTEM; do not change this configuration.

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.

Do not replace these virtual accounts with domain accounts with less permission. These group memberships are required for StoreFront to operate correctly, to:

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

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

StoreFront installation also creates the following local security groups:

- CitrixClusterMembers
- CitrixCWServiceReadUsers
- CitrixCWServiceWriteUsers
- CitrixDelegatedAuthenticatorUsers
- CitrixDelegatedDirectoryClaimFactoryUsers
- CitrixPNRSUsers

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- CitrixStoreFrontPTServiceUsers
- CitrixSubscriptionServerUsers
- CitrixSubscriptionsStoreServiceUsers
- CitrixSubscriptionsSyncUsers
- CitrixStoreFrontAdministrators (from StoreFront 1912 LTSR CU1 onwards)

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.

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.

To enable email-based account discovery for users installing Citrix Workspace app on a device for the first time, you must install a valid server certificate on the StoreFront server. The full chain to the root certificate must also be valid. For the best user experience, install a certificate with a Subject or Subject Alternative Name entry of **discoverReceiver.domain**, where domain is the Microsoft Active Directory domain containing your users' email accounts. Although you can use a wildcard certificate for the domain containing your users' email accounts, you must first ensure that the deployment of such certificates is permitted by your corporate security policy. Other certificates for the domain containing your users' email accounts can also be used, but users will see a certificate warning dialog box when Citrix Workspace app first connects to the StoreFront server. Email-based account discovery cannot be used with any other certificate identities. For more information, see Configure email-based account discovery.

If your users configure their accounts by entering store URLs directly into Citrix Workspace app and do not use email-based account discovery, the certificate on the StoreFront server need only be valid for that server and have a valid chain to the root certificate.

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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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 installs various PowerShell scripts (.ps1) in the folder in `<InstallDirectory>\Scripts`. The default StoreFront installation does not use these scripts, but you can use them to simplify specific and infrequent configuration tasks. These scripts are signed, allowing StoreFront to support PowerShell execution policy. We recommend the **AllSigned** policy. (The **Restricted** policy is not supported, as it prevents PowerShell scripts from running.) StoreFront does not alter the PowerShell execution policy.

Add a code signing certificate to the Trusted Publishers store, because StoreFront does not add it automatically. Without a certificate added the StoreFront management console Snap-in does not load when you enable the **Turn on Script Execution** policy setting and set **Allow only signed script**.

If you run the scripts in a PowerShell session, Windows automatically adds the code signing certificate in the Trusted Publishers store when the PowerShell script is run with the **Always run** option in the **AllSigned** execution policy. (If you select the **Never run** option, the certificate is added to the Untrusted Certificates store, and StoreFront PowerShell scripts do not run.)

Once the code signing certificate is 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 communications

In a production environment, Citrix recommends using the Internet Protocol security (IPsec) or HTTPS protocols to secure data passing between StoreFront and your servers. IPsec is a set of standard extensions to the Internet Protocol that provides authenticated and encrypted communications with data integrity and replay protection. Because IPsec is a network-layer protocol set, higher level protocols can use it without modification. HTTPS uses the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) protocols to provide strong data encryption.

The SSL Relay can be used to secure data traffic between StoreFront and Citrix Virtual Apps servers. The SSL Relay is a default component of Citrix Virtual Apps that performs host authentication and data encryption.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Citrix recommends that you disable TLS 1.0 and 1.1 support in the Web Server hosting StoreFront. You should enforce this via group policy objects, which create the necessary registry settings on the StoreFront server to disable older protocols like TLS 1.0 and TLS 1.1. See also the Microsoft TLS/SSL Settings reference topic.

Citrix recommends securing communications between StoreFront and users' devices using Citrix Gateway and HTTPS. To use HTTPS, StoreFront requires that the Microsoft Internet Information Services (IIS) instance hosting the authentication service and associated stores is configured for HTTPS. In the absence of the appropriate IIS configuration, StoreFront uses HTTP for communications. Citrix strongly recommends that you do not enable unsecured user connections to StoreFront in a production environment.

Storefront does not support ECDSA (Elliptic Curve DSA) certificates.

StoreFront security separation

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

ICA file signing

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

User change password

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Change StoreFront server base URL from HTTP to HTTPS

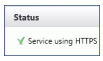
To use HTTPS to secure communications between StoreFront and users' devices, you must configure Microsoft Internet Information Services (IIS) for HTTPS. If you install and configure Citrix StoreFront without first installing and configuring an SSL certificate, StoreFront uses HTTP for communications.

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.

Example:

Before changing base URL to HTTPS:

After changing base URL to HTTPS:



1. Configure Microsoft Internet Information Services (IIS) for HTTPS on the StoreFront server:
   a) Use the Internet Information Services (IIS) Manager console to import an SSL server certificate signed by your Microsoft Active Directory domain certification authority.
   b) Add an IIS binding over HTTPS (443) to the default web site.

   For detailed instructions, see CTX200292.
2. In the Citrix StoreFront management console, in the left pane select **Server Group**.
3. In the Actions pane, select **Change Base URL**.
4. Type the base URL and click **OK**.

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 Citrix Receiver for Web site 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.

Additional security information

> **Note:**
>
> This information may change at any time, without notice.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Security scans

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.

When interpreting security scan reports, note the following:

- HTML pages in StoreFront may not include clickjacking protection (by Content Security Policy or X-Frame-Options response headers). However, these HTML pages consist only of static content, and therefore clickjacking attacks are not relevant.
- The version of Microsoft IIS and the use of ASP.NET are visible in HTTP headers. However, this information is already apparent from the presence of StoreFront itself, because it relies on these technologies.
- When launching applications and desktops, StoreFront uses a token to protect against cross-site request forgery (CSRF). This token is sent as a cookie in a response without being marked as Secure or HttpOnly. When later sent in a request, the token is included in the query string of a URL. However, StoreFront does not rely on this mechanism to authenticate HTTP requests.
- StoreFront uses the open source component jQuery. One version used is jQuery 1.3.2. According to the jQuery open source project, a change was made in jQuery 1.12.0 to mitigate potential vulnerabilities in a specific form of cross-domain request. This change was not a mitigation to a vulnerability in jQuery itself; it was a mitigation to potential misuse by application logic. The relevant Citrix application logic, in the Receiver for Web feature shared by NetScaler and StoreFront, does not use this specific form of cross-domain request, is not affected by this vulnerability, and did not benefit from this mitigation.

  This mitigation was later removed in jQuery 1.12.3 for compatibility reasons. Since the Citrix application logic did not benefit from this mitigation, this removal has no material impact in the versions of NetScaler and StoreFront using jQuery 1.12.4.

CSRF token usage

Certain GET requests made by clients to a StoreFront server include CSRF tokens that are placed in the URL query parameters. Customer reports regarding this issue were reviewed for security impact. Although this behavior is not a directly exploitable security issue, it is not considered to be best practice. This is because it allows tokens to be retained in (for example) browser history, or in logs of intermediate devices such as proxy servers.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

As a defense-in-depth measure, from StoreFront 1912 LTSR CU4 onwards you can disable CSRF token usage for specific, identified GET request endpoints using the following PowerShell script on a StoreFront server:

```
Add-STFFeatureState -Name " Citrix.DeliveryServices.WebUI.
    CsrfValidation.IgnoreOnSpecificRequests" -IsEnabled $True
<!--NeedCopy-->
```

If you do this, you must also remove CSRF tokens from URLs in any WebAPI-based customizations you use.

Export and import the StoreFront configuration

June 29, 2021

> Note:
>
> You can only import StoreFront configurations which are the same StoreFront version as the target StoreFront installation. This includes CU versions. For example, you can export and import the configuration between StoreFront version 1912 LTSR and 1912 LTSR, or between version 1912 LTSR CU1 and 1912 LTSR CU1, but not between version 1912 LTSR CU1 and 1912 LTSR CU2.

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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

- Moving StoreFront during OS migrations such as upgrading the hosting OS from 2008R2 to 2019.
- Building extra server groups in multigeo deployments such as in large enterprises with multiple datacenters.

Things to consider when exporting and importing a StoreFront configuration

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

PowerShell cmdlets

The following cmdlets are provided in the Citrix StoreFront SDK which is installed automatically when you install and configure various StoreFront components. For more information see the StoreFront SDK article.

Export-STFConfiguration

Parameter	Description
-TargetFolder (String)	The export path to the backup archive. Example: “$env:userprofile\desktop\”

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Parameter	Description
-Credential (PSCredential Object)	Specify a credential object to create an encrypted .ctxzip backup archive during export. The PowerShell credential object should contain the password to use for encryption and decryption. Do not use **-Credential** at the same time as the **-NoEncryption** parameter. Example: $CredObject
-NoEncryption (Switch)	Specify that the backup archive should be an unencrypted .zip. Do not use **-NoEncryption** at the same time as the **-Credential** parameter.
-ZipFileName (String)	The name for the StoreFront configuration backup archive. Do not add a file extension, such as .zip or .ctxzip. The file extension is added automatically depending on whether the **-Credential** or **-NoEncryption** parameter is specified during export. Example: “backup”
-Force (Boolean)	This parameter automatically overwrites backup archives with the same file name as existing backup files already present in the specified export location.

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

Import-STFConfiguration

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Parameter	Description
-ConfigurationZip (String)	The full path to the backup archive you want to import. This should also include the file extension. Use .zip for unencrypted and .ctxzip for encrypted backup archives. Example: `$env:userprofile\desktop\backup.ctxzip`
-Credential (PSCredential Object)	Specify a credential object to decrypt an encrypted backup during import. Example: `$CredObject`
-HostBaseURL (String)	If this parameter is included, the Host base URL you specify is used instead of the Host base URL from the exporting server. Example: `https://<importingserver>.example.com`

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\`

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Parameter	Description
-Force (Boolean)	This parameter automatically overwrites backup archives with the same file name as existing backup files already present in the specified export location.

Configuration export and import examples

Import the StoreFront cmdlets into the current PowerShell session

Open the PowerShell Integrated Scripting Environment (ISE) on the StoreFront server and run:

```
$env:PSModulePath = [Environment]::GetEnvironmentVariable('PSModulePath
    ','Machine')
$SDKModules = 'C:\Program Files\Citrix\Receiver StoreFront\
    PowerShellSDK\Modules\Citrix.StoreFront'
Import-Module "$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.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

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

Export the configuration of the server you wish to back up.

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

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

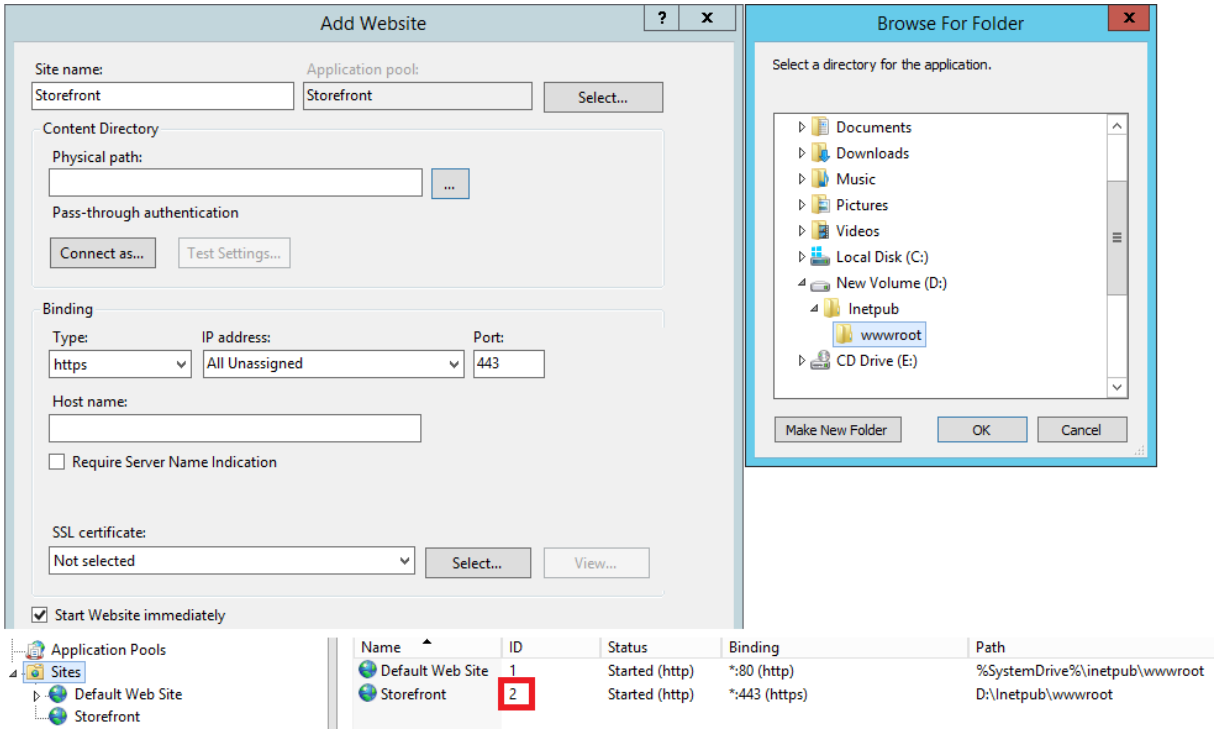
```
Import-STFConfiguration -configurationZip "$env:userprofile\desktop\backup.zip" -HostBaseURL "https://serverB.example.com"
```

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`
.

© 1999–2022 Citrix Systems, Inc. All rights reserved.



1. Export a copy of the Server A configuration.
2. On Server B, configure IIS with a new website called **StoreFront**, which also uses **SiteID 2**.
3. Import the Server A configuration onto Server B. The site ID contained in the backup is used and must match the target website where you want to import the StoreFront configuration.

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

Server group scenarios

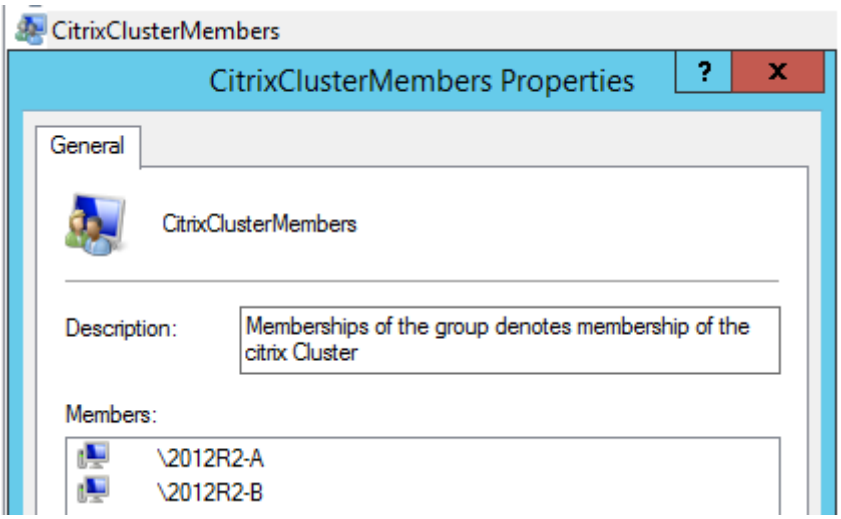
Scenario 1: Backup an existing server group configuration and restore it later onto the same server group deployment

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

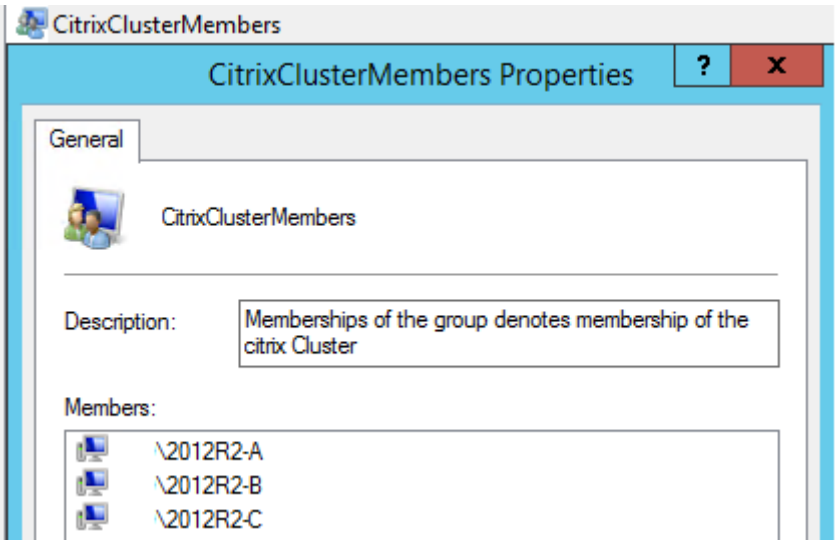
© 1999–2022 Citrix Systems, Inc. All rights reserved.

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.



1. Later you add an additional server, 2012R2-C to the existing server group.



1. 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.
2. Import the Server Group 1 configuration back onto node 2012R2-A.

```
Import-STFConfiguration -configurationZip ”$env:userprofile\desktop\
backup.ctxzip”-HostBaseURL ”https://servergroup1.example.com”
```

3. Propagate the newly imported configuration to the entire server group, so all servers have a consistent configuration after import.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Scenario 2: Backup an existing configuration from Server Group 1 and use it to create a new Server Group on a different factory default installation. You can then add other new server group members to the new primary server

Server Group 2 is created containing two new servers, 2012R2-C and 2012R2-D. The Server Group 2 configuration will be based on the configuration of an existing deployment, Server Group 1, which also contains two servers 2012R2-A and 2012R2-B. The CitrixClusterMembership contained within the backup archive is not used when creating a new server group. The current CitrixClusterMembership is always backed up and then restored after the import is successful. When creating a new deployment using an imported configuration, the CitrixClusterMembership security group contains only the importing server until additional servers are joined to the new group. Server Group 2 is a new deployment and intended to coexist alongside Server Group 1. Specify the -HostBaseURL parameter. Server Group 2 will be created using a new factory default StoreFront installation.

1. Export the Server Group 1 configuration from 2012R2-A, which is the primary server used to manage the entire server group.
2. Import the Server Group 1 configuration onto node 2012R2-C, which will be the primary server used to manage the newly created Server Group 2.

   ```
   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
   ```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

”

Create an encrypted backup of your server configuration

A PowerShell credential object comprises both a Windows account username and a password. PowerShell credential objects ensure that your password stays protected in memory.

> **Note:**
>
> To encrypt a configuration backup archive, you need only the password to perform encryption and decryption. The username stored within the credential object is not used. You must create a credential object containing the same password within the PowerShell session that is used on both the exporting and importing servers. Within the credential object you can specify any user.

PowerShell requires that you specify a user when creating a new credential object. This example code obtains the currently logged on Windows user for convenience.

Create a PowerShell Credential Object within your Powershell session on the exporting server.

```
$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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
$User = [System.Security.Principal.WindowsIdentity]::GetCurrent().Name
$Password = "Pa55w0rd"
$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
```

StoreFront SDK

April 29, 2020

Citrix StoreFront provides an SDK based on a number of Microsoft Windows PowerShell version 3.0 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.

For the SDK Reference, see StoreFront SDK.

Key differences between the StoreFront 3.0 and current StoreFront SDK

- **High-level SDK Examples** - This version provides high-level SDK scripts that enable you to script and automate StoreFront deployments quickly and easily. You can tailor the high-level examples to your particular requirements enabling you to create a new deployment simply by running one script.
- **New low-level SDK** - Citrix provides a documented low-level StoreFront SDK enabling the configuration of deployments including stores, authentication methods, Citrix Receiver for Web and Unified Citrix Receiver sites, as well as remote access with Citrix Gateway.
- **Backwards Compatibility** - StoreFront 3.6 still contains the StoreFront 3.0 and earlier APIs so existing scripts can be gradually transitioned to the new SDK.

> **Important:**
>
> Backwards compatibility with StoreFront 3.0 has been maintained where possible and practicable. However, Citrix recommends when writing new scripts, use the new **Citrix.StoreFront.*** modules, as the StoreFront 3.0 SDK is deprecated and will eventually be removed.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Use the SDK

The SDK comprises of a number of PowerShell snap-ins installed automatically by the installation wizard when you install and configure various StoreFront components.

To access and run the cmdlets:

1. Start a shell in PowerShell 3.0.

   You must run the shell or script using a member of the local administrators group on the StoreFront server.

2. To use SDK cmdlets within scripts, set the execution policy in PowerShell.

   For more information about PowerShell execution policy, see your Microsoft documentation.

3. Add the modules you require into the PowerShell environment using the **Add -Module** command in the Windows PowerShell console. For example, type:

   ```
   Import-Module Citrix.StoreFront
   ```

   To import all the cmdlets, type:

   ```
   Get-Module -ListAvailable | Where-Object { $_.Name.StartsWith("Citrix.
   StoreFront")} | Import-Module
   ```

After importing, you have access to the cmdlets and their associated help.

Get started with the SDK

To create a script, perform the following steps:

1. Take one of the provided SDK examples installed by StoreFront into the **%ProgramFiles%\Citrix\Receiver StoreFront\PowerShellSDK\Examples** folder.
2. To help you customize your own script. review the example script to understand what each part is doing. For more information, see the example use case, which explains in detail the script's actions.
3. Convert and adapt the example scripts to turn them into a script that is more consumable. To do this:
   - Use the PowerShell ISE or a similar tool to edit the script.
   - Use variables to assign values that are to be reused or modified.
   - Remove any commands that are not required.
   - Note that StoreFront cmdlets can be identified by the prefix STF.
   - Use the **Get-Help** cmdlet supplying the cmdlet name and **-Full** parameter for more information on a specific command.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Examples

> **Note:**
>
> When creating a script, to ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described above rather than copying and pasting the example scripts.

Examples	Description
Create a Simple Deployment	Script: creates a simple deployment with a StoreFront controller configured with a single XenDesktop server.
Create a Remote Access Deployment	Script: builds on the previous script to add remote access to the deployment.
Create a Remote Access Deployment with Optimal Launch Gateway	Script: builds on the previous script to add preferred optimal launch gateways for a better user experience.

Example: Create a simple deployment

The following example shows how to create a simple deployment configured with one XenDesktop controller.

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

> **Note:**
>
> To ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described in this document, rather than copying and pasting the example script.

Understand the script

This section explains what each part of the script produced by StoreFront is doing. This will help you with the customization of your own script.

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

```
Param(
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
    [Parameter(Mandatory=$true)]
    [Uri]$HostbaseUrl,
    [long]$SiteId = 1,
    [ValidateSet("XenDesktop","XenApp","AppController","VDIinaBox
        ")]
    [string]$Farmtype = "XenDesktop",
    [Parameter(Mandatory=$true)]
    [string[]]$FarmServers,
    [string]$StoreVirtualPath = "/Citrix/Store",
    [bool]$LoadbalanceServers = $false,
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet("HTTP","HTTPS","SSL")]
    [string]$TransportType = "HTTP"
    )
    \# Import StoreFront modules. Required for versions of
        PowerShell earlier than 3.0 that do not support
        autoloading
    Import-Module Citrix.StoreFront
    Import-Module Citrix.StoreFront.Stores
    Import-Module Citrix.StoreFront.Authentication
    Import-Module Citrix.StoreFront.WebReceiver
<!--NeedCopy-->
```

- Automates the virtual path of the authentication and Citrix Receiver for Web services based on the **$StoreVirtualPath** supplied. **$StoreVirtualPath** is equivalent to **$StoreIISpath** because Virtual paths are always the path in IIS. Therefore in Powershell they have a value such as "/Citrix/Store", "/Citrix/StoreWeb", or "/Citrix/StoreAuth".

```
\# Determine the Authentication and Receiver virtual path to use
    based of the Store
$authenticationVirtualPath = "$($StoreIISPath.TrimEnd('/'))Auth"
$receiverVirtualPath = "$($StoreVirtualPath.TrimEnd('/'))Web"
<!--NeedCopy-->
```

- 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
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
if(-not $existingDeployment)
{

    \# Install the required StoreFront components
    Add-STFDeployment -HostBaseUrl $HostbaseUrl -SiteId $SiteId -Confirm:$false
 }

elseif($existingDeployment.HostbaseUrl -eq $HostbaseUrl)
{

    \# The deployment exists but it is configured to the desired hostbase url
    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."
 }

<!--NeedCopy-->
```

- Creates a new authentication service if one does not exist at the specified virtual path. The default authentication method of username and password is enabled.

```
\# Determine if the authentication service at the specified virtual path exists
$authentication = Get-STFAuthenticationService -VirtualPath $authenticationVirtualPath
if(-not $authentication)
{

    \# Add an Authentication service using the IIS path of the Store appended with Auth
    $authentication = Add-STFAuthenticationService $authenticationVirtualPath
 }

else
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
{

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

<!--NeedCopy-->
```

- Creates the new store service configured with one XenDesktop controller with the servers defined in the array **$XenDesktopServers** at the specified virtual path if one does not already exist.

```
\# Determine if the store service at the specified virtual path exists
$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
if(-not $store)
{

\# Add a Store that uses the new Authentication service configured to publish resources from the supplied servers
$store = Add-STFStoreService -VirtualPath $StoreVirtualPath -AuthenticationService $authentication -FarmName $Farmtype -FarmType $Farmtype -Servers $FarmServers -LoadBalance $LoadbalanceServers \`
        -Port $Port -SSLRelayPort $SSLRelayPort -TransportType $TransportType
 }

else
{

    Write-Output "A Store service already exists at the specified virtual path and will be used. Farm and servers will be appended to this store."
    \# Get the number of farms configured in the store
    $farmCount = (Get-STFStoreFarmConfiguration $store).Farms.Count
    \# Append the farm to the store with a unique name
    Add-STFStoreFarm -StoreService $store -FarmName "Controller$($farmCount + 1)" -FarmType $Farmtype -Servers $FarmServers -LoadBalance $LoadbalanceServers -Port $Port \`
        -SSLRelayPort $SSLRelayPort -TransportType $TransportType
 }
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

- 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
{

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

<!--NeedCopy-->
```

- 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
 }

```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
10  <!--NeedCopy-->
```

Example: Create a remote access deployment

The following example builds on the previous script to add a deployment with remote access.

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

> **Note:**
>
> To ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described in this document, rather than copying and pasting the example script.

Understand the script

This section explains what each part of the script produced by StoreFront is doing. This will help you with the customization of your own script.

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

```
1   Param(
2       [Parameter(Mandatory=$true)]
3       [Uri]$HostbaseUrl,
4       [Parameter(Mandatory=$true)]
5       [long]$SiteId = 1,
6       [string]$Farmtype = ”XenDesktop”,
7       [Parameter(Mandatory=$true)]
8       [string[]]$FarmServers,
9       [string]$StoreVirtualPath = ”/Citrix/Store”,
10      [bool]$LoadbalanceServers = $false,
11      [int]$Port = 80,
12      [int]$SSLRelayPort = 443,
13      [ValidateSet(”HTTP”,”HTTPS”,”SSL”)]
14      [string]$TransportType = ”HTTP”,
15      [Parameter(Mandatory=$true)]
16      [Uri]$GatewayUrl,
17      [Parameter(Mandatory=$true)]
18      [Uri]$GatewayCallbackUrl,
19      [Parameter(Mandatory=$true)]
20      [string[]]$GatewaySTAUrls,
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
21      [string]$GatewaySubnetIP,
22      [Parameter(Mandatory=$true)]
23      [string]$GatewayName
24  )
25  Set-StrictMode -Version 2.0
26
27  \# Any failure is a terminating failure.
28  $ErrorActionPreference = 'Stop'
29  $ReportErrorShowStackTrace = $true
30  $ReportErrorShowInnerException = $true
31  \# Import StoreFront modules. Required for versions of PowerShell
        earlier than 3.0 that do not support autoloading
32  Import-Module Citrix.StoreFront
33  Import-Module Citrix.StoreFront.Stores
34  Import-Module Citrix.StoreFront.Roaming
35  <!--NeedCopy-->
```

- Create an internal access StoreFront deployment by calling the previous examples script. The base deployment will be extended to support remote access.

```
1  \# Create a simple deployment by invoking the SimpleDeployment
       example
2  $scriptDirectory = Split-Path -Path $MyInvocation.MyCommand.
       Definition -Parent
3  $scriptPath = Join-Path $scriptDirectory "SimpleDeployment.ps1"
4  & $scriptPath -HostbaseUrl $HostbaseUrl -SiteId $SiteId -
       FarmServers $FarmServers -StoreVirtualPath $StoreVirtualPath -
       Farmtype $Farmtype \`
5      -LoadbalanceServers $LoadbalanceServers -Port $Port  -
           SSLRelayPort $SSLRelayPort -TransportType $TransportType
6  <!--NeedCopy-->
```

- Gets services created in the simple deployment as they need to be updated to support the remote access scenario.

```
1  \# Determine the Authentication and Receiver sites based on the
       Store
2  $store = Get-STFStoreService -VirtualPath $StoreVirtualPath
3  $authentication = Get-STFAuthenticationService -StoreService
       $store
4  $receiverForWeb = Get-STFWebReceiverService -StoreService $store
5  <!--NeedCopy-->
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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

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

```
\# Get the CitrixAGBasic authentication method from the protocols installed.
\# Included for demonstration purposes as the protocol name can be used directly if known
$citrixAGBasic = Get-STFAuthenticationProtocolsAvailable | Where-Object {
 $_ -match "CitrixAGBasic"  }

\# Enable CitrixAGBasic in the Authentication service (required for remote access)
Enable-STFAuthenticationServiceProtocol -AuthenticationService $authentication -Name $citrixAGBasic
<!--NeedCopy-->
```

- 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 '
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
\-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
 }

\# Register the Gateway with the new Store
Register-STFStoreGateway -Gateway $gateway -StoreService $store -DefaultGateway
<!--NeedCopy-->
```

Example: Create a remote access deployment with optimal launch Gateway

The following example builds on the previous script to add a deployment with optimal launch Gateway remote access.

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

> **Note:**
>
> To ensure you always get the latest enhancements and fixes, Citrix recommends you follow the procedure described in this document, rather than copying and pasting the example script.

Understand the script

This section explains what each part of the script produced by StoreFront is doing. This will help you with the customization of your own script.

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

```
Param(
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
    [Parameter(Mandatory=$true)]
    [Uri]$HostbaseUrl,
    [long]$SiteId = 1,
    [string]$Farmtype = ”XenDesktop”,
    [Parameter(Mandatory=$true)]
    [string[]]$FarmServers,
    [string]$StoreVirtualPath = ”/Citrix/Store”,
    [bool]$LoadbalanceServers = $false,
    [int]$Port = 80,
    [int]$SSLRelayPort = 443,
    [ValidateSet(”HTTP”,”HTTPS”,”SSL”)]
    [string]$TransportType = ”HTTP”,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayUrl,
    [Parameter(Mandatory=$true)]
    [Uri]$GatewayCallbackUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$GatewaySTAUrls,
    [string]$GatewaySubnetIP,
    [Parameter(Mandatory=$true)]
    [string]$GatewayName,
    [Parameter(Mandatory=$true)]
    [Uri]$OptimalGatewayUrl,
    [Parameter(Mandatory=$true)]
    [string[]]$OptimalGatewaySTAUrls,
    [Parameter(Mandatory=$true)]
    [string]$OptimalGatewayName
)
Set-StrictMode -Version 2.0
\# Any failure is a terminating failure.
$ErrorActionPreference = 'Stop'
$ReportErrorShowStackTrace = $true
$ReportErrorShowInnerException = $true
\# Import StoreFront modules. Required for versions of PowerShell
    earlier than 3.0 that do not support autoloading
Import-Module Citrix.StoreFront
Import-Module Citrix.StoreFront.Stores
Import-Module Citrix.StoreFront.Roaming
<!--NeedCopy-->
```

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
\# 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
<!--NeedCopy-->
```

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

```
\# Add a new Gateway used for remote HDX access to desktops and apps
$gateway = Add-STFRoamingGateway -Name $OptimalGatewayName -LogonType UsedForHDXOnly -GatewayUrl $OptimalGatewayUrl -SecureTicketAuthorityUrls $OptimalGatewaySTAUrls -PassThru
<!--NeedCopy-->
```

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Example: Exchange metadata between the Identity Provider and the Service Provider (StoreFront) for SAML authentication

SAML authentication can be configured in the StoreFront management console (see Configure the authentication service or using the following PowerShell cmdlets:

- Export-STFSamlEncryptionCertificate
- Export-STFSamlSigningCertificate
- Import-STFSamlEncryptionCertificate
- Import-STFSamlSigningCertificate
- New-STFSamlEncryptionCertificate
- New-STFSamlIdPCertificate
- New-STFSamlSigningCertificate

You can use the cmdlet, **Update-STFSamlIdPFromMetadata**, to exchange metadata (identifiers, certificates, endpoints and other configuration) between the Identity Provider and the Service Provider, which is StoreFront in this case.

For a StoreFront Store, named “Store”, with its dedicated authentication service, the metadata endpoint will be:

```
https://<storefront host>/Citrix/StoreAuth/SamlForms/ServiceProvider/
Metadata
```

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

For StoreFront to consume the metadata from an Identity Provider, the following PowerShell can be used:

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

# Remember to change this with the virtual path of your Store.
$StoreVirtualPath = ”/Citrix/Store”

$store = Get-STFStoreService -VirtualPath $StoreVirtualPath
$auth = Get-STFAuthenticationService -StoreService $store

# To read the metadata directly from the Identity Provider, use the
    following:
# Note again this is only allowed for https endpoints
Update-STFSamlIdPFromMetadata -AuthenticationService $auth -Url https:
    //example.com/FederationMetadata/2007-06/FederationMetadata.xml

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
# Note: Ensure that the file is encoded as UTF-8
Update-STFSamlIdPFromMetadata -AuthenticationService $auth -FilePath "C:\Users\exampleusername\Downloads\FederationMetadata.xml"
<!--NeedCopy-->
```

Example: List the metadata and ACS endpoints for a specified store for SAML authentication

You can use the following script to list out the metadata and ACS (Assertion Consumer Service) 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:
Service Provider ID: $spId
Assertion Consumer Service: $acs
Metadata: $md
Test Page: $samlTest"
<!--NeedCopy-->
```

Example of the output:

```
SAML Service Provider information:
Service Provider 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
<!--NeedCopy-->
```

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Troubleshoot StoreFront

October 22, 2020

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.

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.

The Citrix StoreFront management console automatically records tracing information. By default, tracing for other operations is disabled and must be enabled manually. Logs created by Windows PowerShell commands are stored in the \Admin\logs\ directory of the StoreFront installation, typically located at C:\Program Files\Citrix\Receiver StoreFront. The log file names contain command actions and subjects, along with time stamps that can be used to differentiate command sequences.

> 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.

Troubleshoot authentication failures

StoreFront logs password-based authentication failures using the LogonUser API (https://docs.microsoft.com/en-us/windows/desktop/api/winbase/nf-winbase-logonusera), which returns Error 1326 when the logon fails because either username or password is incorrect. From more information, please refer https://docs.microsoft.com/en-us/windows/desktop/debug/system-error-codes--1300-1699-.

You can monitor the Security Audit log for Event ID 4625, which is describe in https://www.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4625. The sub-status indicates what was wrong with the authentication attempt.

To configure log throttling

1. Use a text editor to open the *web.config* file for the authentication service, store, or Receiver for Web site, which are typically located in the C:\inetpub\wwwroot\Citrix\Authentication\, C:\inetpub\wwwroot\Citrix\storename\, and C:\inetpub\wwwroot\Citrix\storenameWeb\ directories, respectively, where storename is the name specified for the store when it was created.
2. Locate the following element in the file.

   ```
   <logger duplicateInterval="00:01:00"duplicateLimit="10">
   ```

   By default, StoreFront is configured to limit the number of duplicate log entries to 10 per minute.
3. Change the value of the duplicateInterval attribute to the set the time period in hours, minutes, and seconds over which duplicate log entries are monitored. Use the duplicateLimit attribute to set the number of duplicate entries that must be logged within the specified time interval to trigger log throttling.

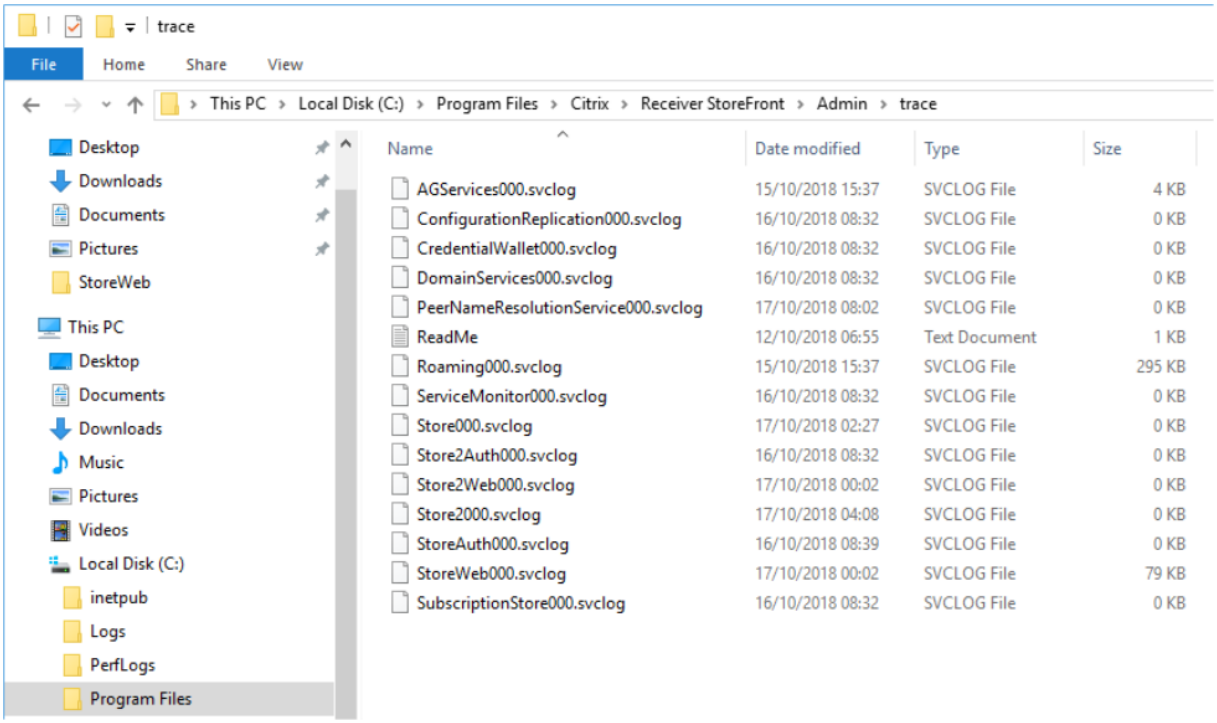
When log throttling is triggered, a warning message is logged to indicate that further identical log entries will be suppressed. Once the time limit elapses, normal logging resumes and an informational message is logged indicating that duplicate log entries are no longer being suppressed.

To enable tracing for debugging

> **Important:**
>
> The StoreFront and PowerShell consoles cannot be open at the same time. Always close the StoreFront admin console before using the PowerShell console to administer your StoreFront configuration. Likewise, close all instances of the PowerShell console before opening the StoreFront console.

Trace output is sent to c:\Program Files\Citrix\Receiver StoreFront\admin\trace

© 1999–2022 Citrix Systems, Inc. All rights reserved.



> **Note:**
>
> Run `Get-Help Set-STFDiagnostics -detailed` to obtain Powershell help and instructions on how to use the Set-STFDiagnostics cmdlet.

Use an account with local administrator permissions to start Windows PowerShell and, at a command prompt, specify the following mandatory parameters to enable or disable tracing.

- **-All**. A flag indicating that tracing should be updated for all instances and services.
- **-TraceLevel**. In increasing levels of tracing detail, allowed values for -TraceLevel are: Off, Error, Warning, Info, or Verbose. Due to the large amount of data that can be generated, tracing may significantly impact the performance of StoreFront. The Info or Verbose levels are not recommended unless specifically required for troubleshooting.

Optional parameters:

- **-FileSizeKb**. The trace file size in KB.
- **-FileCount**. The number of trace files to maintain on disk at a time.
- **-confirm:$False**. Suppresses Windows prompts to allow the StoreFront cmdlet to run each time.

Examples

To enable Verbose level tracing for all service for debugging purposes:

© 1999–2022 Citrix Systems, Inc. All rights reserved.

```
Set-STFDiagnostics -All -TraceLevel "Verbose" -confirm:$False
<!--NeedCopy-->
```

To disable Verbose level tracing, and set the tracing level back to the default value for all services:

```
Set-STFDiagnostics -All -TraceLevel "Error" -confirm:$False
<!--NeedCopy-->
```

For more information on the Set-STFDiagnostics cmdlet, see the StoreFront PowerShell SDK documentation.

To enable logging of the launch.ica file

Save the information in the launch.ica file to the client computer to troubleshoot multiple issues. The launch.ica file is generated by Citrix Web Interface or Citrix StoreFront Servers.

To enable logging of the launch.ica file, complete the following steps:

1. Navigate to the following registry key by using the registry editor:

   32-bit Systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

   64-bit Systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Citrix\ICA Client\Engine\Configuration\Advanced\Modules\Logging`

2. Set the following two string key values:

   - LogFile="path to the log file"
   - LogICAFile=true

   For example:

   ```
   LogFile=C:\ica\ica.log
   LogICAFile=true
   <!--NeedCopy-->
   ```

Additional resources

> Note:

© 1999–2022 Citrix Systems, Inc. All rights reserved.

> The use of an ICA file in your environment for anything other than troubleshooting purposes is further outlined in CTX200126.

Troubleshoot StoreFront upgrade issues

Use the following steps to troubleshoot StoreFront upgrade issues.

Before attempting an upgrade

1. Confirm that you have a backup of all StoreFront servers.
2. Verify that you are not attempting to upgrade from an End of Life StoreFront version. For more information see CTX200356.
3. Verify that you are upgrading from a supported version of StoreFront to the current version only.
4. If the StoreFront server is part of a StoreFront server group, all servers in the group must be upgraded sequentially. Simultaneously upgrading a StoreFront server group is not supported.
5. Delete any *thumbs.db* files inside *C:\inetpub\wwwroot\citrix* or its subdirectories. Show hidden files to complete this step: **Folder Options > View**, choose option **Show hidden files, folders and drives** and clear the option **Hide protected operating system files (Recommended)**.
6. Disable antivirus software before starting the upgrade procedure.
7. Confirm that servers being upgraded are removed from any load balancer, and that they have no active user sessions connected.
8. Reboot the StoreFront server before performing the upgrade.
9. Manually stop the following Services:
   - CitrixConfigurationReplication
   - CitrixCredentialWallet
   - CitrixDefaultDomainService
   - CitrixPeerResolutionService
   - CitrixSubscriptionsStore
10. Ensure that the StoreFront management console is closed.

If the upgrade fails

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

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

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

© 1999–2022 Citrix Systems, Inc. All rights reserved.

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.
4. Check the installation log files for the following error:

   Failed to set process execution policy: caused by the certificate signing the PowerShell modules not being trusted. To see whether any certificates are not trusted, extract CitrixStoreFront-x64.exe then, on one of the PowerShell files, use the context command **Properties > Digital Signature > Details > View Certificate > Certification path**.

To manually remove StoreFront

> Warning:
>
> Manually removing StoreFront clears all existing information.

To manually remove StoreFront:

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

You can now reinstall StoreFront.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

© 1999–2022 Citrix Systems, Inc. All rights reserved.

Locations
Corporate Headquarters | 851 Cypress Creek Road Fort Lauderdale, FL 33309, United States
Silicon Valley | 4988 Great America Parkway Santa Clara, CA 95054, United States

© 2022 Citrix Systems, Inc. All rights reserved. Citrix, the Citrix logo, and other marks appearing herein are property of Citrix Systems, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).